ФИЗИЧЕСКИЕ ОСНОВЫ КВАНТОВОЙ ИНФОРМАЦИИ

КУЛИК
СЕРГЕЙ ПАВЛОВИЧ

—

ФИЗФАК МГУ

ФИЗИЧЕСКИЙ
ФАКУЛЬТЕТ
МГУ ИМЕНИ
М.В. ЛОМОНОСОВА

Лекция 1. Введение.

1. Что такое квантовая информация?
2. Закон Мура, роль квантовых эффектов. Биты и их реализация. Регистры. Понятие машины Тьюринга. Классические вычисления. Логические операции. Сложение по модулю 2.
3. Требования, предъявляемые к квантовому компьютеру. Основные проблемы на пути к его созданию.

1. ***Квантовая информация*** - это новая область науки и технологии, сочетающая в себе разделы физики, математики, кибернетики и инженерии. Ее целью является выяснение роли фундаментальных законов физики, открытых в XX-ом веке в процессах получения, передачи и обработки информации. Сейчас ясно, что теория классической информации не может адекватно ответить на вопрос, как информация может быть использована в реальном (физическом) мире - т.е. в квантовом мире. Некоторые выводы теории квантовой информации могут быть представлены как обобщение классической теории в тех случаях, когда информация передается и хранится с помощью квантовых состояний, а не в терминах классических битов.

Вычисление - это процесс, в ходе которого происходит определенное для каждой логической операции (ЛО) нелинейное взаимодействие потоков информации друг с другом и их преобразование. В зависимости от типа ЛО определенным образом изменяется состояние логического элемента (ЛЭ), а поступающая на его входы информация либо передается далее, либо как-то преобразуется. Управление или преобразование происходит под воздействием внешних сигналов. Это, например, переключение или инверсия (0?1, 1?0), запись, сброс. Носитель информации на физическом уровне называется сигналом.

2. ***Закон Мура***. С 1959 года, когда был создан первый транзистор - это эмпирический закон, согласно которому число транзисторов в кристалле одной интегральной схемы в течение первых 15 лет удваивалось каждый год, а затем и до сих пор такое удвоение происходит за 1.5 года. Если первые кремниевые микросхемы имели размеры элементов в плоскости кристалла порядка десятков микрон, то современные образцы характеризуются размерами порядка 100нм, а контроль осуществляется с точностью порядка 10нм. Согласно закону Мура

менее чем через 20 лет размеры интегральной схемы станут порядка атомных, а следовательно, законы их функционирования будут определяться законами микромира, т.е. квантовой механикой. Общеизвестно, что объекты микромира ведут себя совершенно необычно с точки зрения классического мира. Так, наблюдение за атомом возмущает его движение, в то же время в отсутствие наблюдения, атом как бы размыт по пространству и скоростям (отсутствие траектории - соотношение неопределенности Гайзенберга), как будто бы он находился бы в нескольких различных местах в одинаковые моменты времени.

Таким образом до сих пор квантовые эффекты, связанные с малостью размеров различных устройств воспринимались как преграда на пути к миниатюризации электронных устройств. Квантовая информатика должна выяснить как использовать фундаментальные квантовые свойства.

К настоящему времени, пожалуй, единственным приложением квантовой информатики является криптография. Здесь уже разработаны и реализованы алгоритмы, использующие свойства квантовых объектов (неклонируемость и невозможность измерения без возмущения). Основной выигрыш в квантовых криптографических протоколах - даже не абсолютная их секретность (в классической криптографии существуют безусловно секретные ключи), а то, что сам факт подслушивания становится известным для пользователей!

Итак, **Проблема 1** -уменьшение размеров интегральных схем, т.е. отдельных элементов. Нанотехнологии. Естественный предел здесь - характерный масштаб атома, когда вступают в силу законы микромира, т.е. квантовой механики.

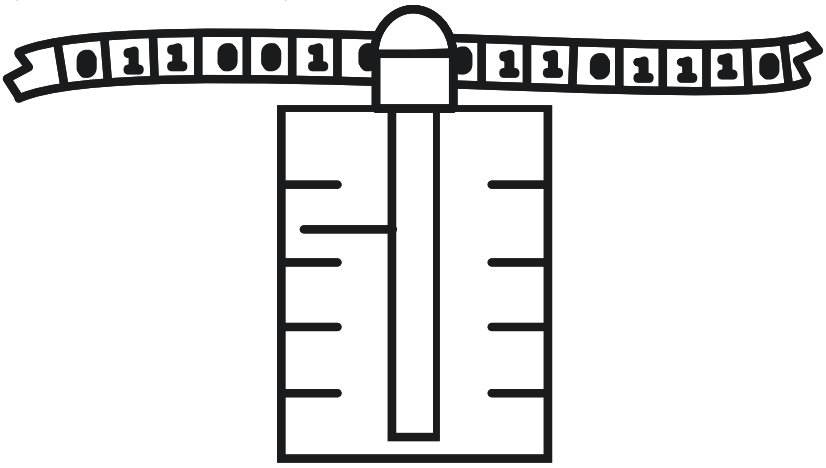
Проблема 2- уменьшение доли рассеиваемой энергии. Логически обратимые операции - те, которые не сопровождаются рассеянием энергии (Ландауэр, 1961г.). Универсальный цифровой компьютер типа вычислительной машины Тьюринга может быть построен на логически и термодинамически обратимых ЛЭ так, что энергия будет рассеиваться только за счет необратимых периферийных процессов (типа ввода информации в машину либо ее вывода – Беннет, 1982г). Типичные классические обратимые универсальные ЛЭ - это ЛЭ Тоффоли и Фредкина.

Для выполнения классических вычислений необходима физическая система, имеющая два устойчивых состояния. Триггеры - в радиоэлектронике. Представление в виде двоичной системы: 0;1 - биты.

Бит (binary digits = двоичные разряды)- это система, имеющая два устойчивых состояния. Между этими состояниями должен быть достаточно большой энергетический барьер, чтобы система не могла спонтанно переходить из одного состояния в другое. Например, в TTL (транзисторно-транзисторной)-логике уровню “0” (низкий уровень) соответствуют сигналы, принадлежащие диапазону $-0.5 < U_0 < 0.4$В, а уровню “1” - $2.4 < U_1 < 5.5$В. В булевой алгебре им соответствуют понятия “ЛОЖЬ” (“FALSE”) и “ИСТИНА” (“TRUE”). Термин “помехоустойчивость” используется для обозначения максимального уровня помехи, которая будучи прибавлена к логическому сигналу при самых неблагоприятных условиях, не будет приводить к ошибочной работе схемы. Для ТТЛ устройств помехоустойчивость составляет 0.4В

Классический регистр - это совокупность некоторого числа L битов. Он имеет 2^L различных состояний, В данный момент времени может существовать лишь одно из этих состояний.

Машина Тьюринга - это математическая модель идеализированного вычислительного устройства. Можно показать, что она в состоянии эффективно симулировать все классические вычислительные методы.
Машина имеет конечный набор внутренних состояний и фиксированное устройство. Она считывает один бинарный символ за время, в течение которого она работает с лентой. Действие машины по считыванию данного символа s зависит только от этого символа и от внутреннего состояния K. Это действие состоит в переписывании нового символа s' на текущее положение ленты, изменения внутреннего состояния в K' и передвижения ленты на одну позицию в направлении d (вправо или влево). Внутреннее устройство машины, таким образом, можно описать конечным и фиксированным набором правил в форме $\left(s, K \to s', K', d\right)$.



Существует одно специфическое внутреннее состояние: «стоп». Оказавшись в нем, машина прекращает дальнейшую работу. Входная «программа», записанная на ленте преобразуется машиной в выходной результат, записываемый на ленте.
Более подробно:
Машина содержит
1) ленту, разбитую на конечное число ячеек, в каждой ячейке ленты в определенный момент времени записан один из символов a0,a1,a2,...,aN. Совокупность этих символов называется входным алфавитом;
2) конечное управление, которое может находиться в каждый момент времени в каком-то одном состоянии q0, q1, q2,...,qM;
3) управляющую головку, которая может перемещаться вдоль ленты, считывать или записывать символы.

Машина действует в дискретные моменты времени. В зависимости от внутреннего состояния и от символа, считанного головкой, в следующий момент времени машина может перейти в другое состояние и записать в ячейке символ. Эти переходы из одной конфигурации в другую она выполняет согласно командам. Попав в представляющее состояние машина останавливается. Формальное определение базовой модели машины Тьюринга:
T= (K,S, Γ, d, q_0, F);
K - конечное множество внутренних состояний;
S - входной алфавит;
Γ - ленточный алфавит: S: Γ-{$}, $-пробел;
d - команды, частичное отображение

d: KxГ->Kx (Г-{$})x{L,R}, где L,R -движение влево и вправо головки;
q_0- начальное состояние, с него машина начинает обработку, q0cK;
F - множество конечных состояний, из которых машина переходит в представляющее состояние.
Любая машина Тьюринга описывается таблицей, состоящей из строк вида (q_j c_k v_{jk} q_{jk}) , имеющих следующее значение: из состояния q_j, если под считывающей головкой находится символ c_k , принадлежащий Г, перейти в состояние q_{jk} и выполнить действие, предписываемое символом v_{jk} , принадлежащим CU{$, R, L, s}, где Г - рабочий алфавит машины Тьюринга; $ - пустая буква; R, L - сдвиг считывающей головки соответственно вправо или влево; s - символ останова

Классические вычисления.

Вычисление - это алгоритм, по которому некоторому значению на входе в систему (X) ставится в соответствие значение на ее выходе (Y).
X ? Y=F(X).
В общем случае классическое вычисление не является обратимым, т.е. не существует алгоритма, по которому
Y ? $X=F^{-1}(Y)$.

Основные ЛО это: И (AND), ИЛИ (OR), НЕ(NOT) и их комбинации, например, И-НЕ, ИЛИ-НЕ
ПРИМЕР 1: двухбитовая операция “Сложение по модулю 2” (операция исключающего НЕ, или CNOT или XOR).

a	b	a?b
0	0	0
1	0	1
0	1	1
1	1	0

Ее квантовый аналог

Сохраняем значение (ку)бита a, в то время как (ку)бит b меняется по закону XOR:

a	b	a?	b?
0	0	0	0
1	0	1	1
0	1	0	1
1	1	1	0

- бит **b** (мишень = target) меняет свое состояние тогда и только тогда, когда состояние контрольного (control) бита **a** соответствует 1; при этом, состояние контрольного бита не меняется.

ПРИМЕР 2: однобитовая операция “НЕ” (NOT).

a	**F(a)**
0	**1**
1	**0**

Эта операция обратимая, т.е. **F(F(a))=a.** В общем случае это не так.

Однако, классический компьютер (классическое вычисление) может быть сделан обратимым, если сохранять в памяти входной сигнал.

ПРИМЕР: Сложение по модулю 2, с сохранением **a**.

(a,b) ⊕ (a,a⊕ b)

(a, a⊕ b) ⊕ (a, a⊕ b⊕ a)

F=F^{-1}, в том смысле, что подействовав на входные данные два раза по одному и тому же алгоритму мы опять получаем входные данные:

F(F(X))=X, или F(Y)=X

a	**b**	**a⊕ b**	**a⊕ b⊕ a⊕ b**
0	**0**	**0**	**0**
1	**0**	**1**	**0**
0	**1**	**1**	**1**
1	**1**	**0**	**1**

Логическая операция XOR (CNOT) иллюстрирует почему классические данные могут быть клонированы, а квантовые - нет. Заметим, что в общем случае под квантовыми данными мы будем понимать суперпозиции вида

$$\left|\Psi\right\rangle = \alpha\left|0\right\rangle + \beta\left|1\right\rangle, \qquad (1)$$

где α и β - комплексные числа или амплитуды состояний, причем, $\left|\alpha\right|^2 + \left|\beta\right|^2 = 1$.

Согласно таблице истинности, если XOR применить к булевым данным, в которых второй бит находится в состоянии “0” (b), а первый - в состоянии “X” (a), то первый бит не изменяется, а второй становится его копией:

$U_{XOR}(X, 0) = (X, X)$, где X = “0” или “1”.

В квантовом случае, в качестве данных, обозначенных символом “X”, нужно рассматривать суперпозицию (1):

$$U_{XOR}\left|X,0\right\rangle = \left|X,X\right\rangle.$$

Физически, данные можно закодировать, например, в поляризационном базисе |V> = 1, |H> = 0 (H,V)= (0,1):

$U_{XOR}\left|0,0\right\rangle = \left|0,0\right\rangle$, и $U_{XOR}\left|1,0\right\rangle = \left|1,1\right\rangle$.

В первом случае действительно имеет место копирование состояния. Теорема о запрете клонирования утверждает, что невозможно копирование *произвольного* квантового состояния. В рассмотренном примере копирование произошло, поскольку операция производилась в собственном базисе (|0>, |1>), т.е. в частном случае квантового состояния.

Казалось бы, что операцию XOR можно использовать и для копирования суперпозиций двух булевых состояний, таких как $|45^0>$? |V> + |H>:

$$U_{XOR}\left|45^o, H\right\rangle = \left|45^o, 45^o\right\rangle.$$

Но это не так! Унитарность квантовой эволюции требует, чтобы суперпозиция входных состояний преобразовывалась в соответствующую суперпозицию выходных состояний:

$U_{XOR}\left|45^o, H\right\rangle = \left(\left|45^o\right\rangle = 1/\sqrt{2}\left[\left|H\right\rangle + \left|V\right\rangle\right]\right) = 1/\sqrt{2}\left[\left|H,H\right\rangle + \left|V,V\right\rangle\right]$ или

$U_{XOR}\left|s,0\right\rangle = \left(\left|\mathrm{s}\right\rangle = 1/\sqrt{2}\left[\left|0\right\rangle + \left|1\right\rangle\right]\right) = 1/\sqrt{2}\left[\left|0,0\right\rangle + \left|1,1\right\rangle\right].$

Это т.н. перепутанное состояние (Φ^+), в котором каждый из двух выходных кубитов не имеет определенного значения (в данном случае - поляризации). Этот пример показывает, что логические операции, выполняемые над квантовыми объектами происходят по другим правилам, нежели в классических вычислительных процессах.

<u>3. Квантовый компьютер</u> - физическое устройство, выполняющее логические операции над квантовыми состояниями путем унитарных преобразований (т.е. сохраняющих энергию), не нарушающих квантовые суперпозиции в процессе вычислений. Схематично, работа квантового компьютера может быть представлена как последовательность трех операций:

1. “ЗАПИСЬ” (приготовление) начального состояния,
2. “ВЫЧИСЛЕНИЕ” (унитарные преобразования начальных состояний)
3. “ВЫВОД” результата (измерение, проецирование конечного состояния).

Также сюда следует отнести вспомогательную операцию “СБРОС”, приводящую регистр к основному состоянию.

ОБЩИЕ ТРЕБОВАНИЯ, ПРЕДЪЯВЛЯЕМЫЕ К КВАНТОВЫМ КОМПЬЮТЕРАМ.

1. Должна быть реализована система квантовых битов или кубитов:
   $\left|\Psi\right\rangle = \alpha\left|0\right\rangle + \beta\left|1\right\rangle$, где α и β - комплексные числа или амплитуды состояний, причем, $\left|\alpha\right|^2 + \left|\beta\right|^2 = 1$. Кубит - это когерентная суперпозиция двух различимых квантовых состояний. Например, поляризации фотона (H, V), два состояния спина электрона, внутренние электронные состояния индивидуального атома.
2. Должен существовать механизм, осуществляющий “перепутывание” кубитов:
   $\left|0\right\rangle\left|0\right\rangle \rightarrow \frac{1}{\sqrt{2}}\left\{\left|0\right\rangle\left|0\right\rangle + \left|1\right\rangle\left|1\right\rangle\right\}$, см. пример выше.

Перепутывание - (“запутывание”, “сцепленность”, “переплетение” - от немецкого verschrankung) - это квантовая разновидность корреляции, не имеющей классического аналога. Грубо говоря, *две подсистемы являются перепутанными, когда их совместное состояние более определено и менее стохастично, чем состояние любой из подсистем*.

3. Необходимо осуществлять контролируемым образом логические операции над кубитами (“условная динамика”).
   например, $\left|a\right\rangle_A\left|b\right\rangle_B \rightarrow \left|a\right\rangle_A\left|a \oplus b\right\rangle_B$. Устройства, служащие для этого называются логическим элементами (ЛЭ, gates).
4. Система должна быть масштабируемой, т.е. логические операции должны распространяться на N кубитов, а затрачиваемое время расти по полиномиальному закону.

5. Физическая система, представляющая собой данные, должна быть квантово-механически стабильна.
6. Необходим механизм, осуществляющий запись, чтение и сброс данных.

Зачем нужен квантовый компьютер? Например, рассмотрим математическую проблему факторизации больших чисел - т.е. разложения произвольного числа на простые множители (Любое число можно разложить на простые множители. Док-во: Каждое целое число является либо простым, либо - нет. Если оно простое - то оно представимо в виде произведения единицы на само себя. Если нет - то оно выражается в виде произведения двух чисел. Рассмотрим каждое из них. Оно либо является простым, либо нет. И т.д.).
Эта задача непосредственно связана с криптографией, где секретные ключи формируются именно посредством такого алгоритма.
Математики твердо верят, хотя они и не доказали это, что для факторизации числа с N десятичными разрядами любому классическому компьютеру требуется число шагов, которое растет экспоненциально с N. Иначе говоря, добавление одного десятичного разряда к числу общем случае умножает время, необходимое для его факторизации, на постоянный множитель. Конкретно, время растет с ростом длины N факторизуемого числа как $\exp(N^{1/3})$. Так, задача вычисления произведения двух простых чисел 521 и 809 не вызывает проблем. Однако, обратная задача - нахождение простых сомножителей числа 421489 потребует определенного времени – задача класса NP.
Таким образом, при увеличении числа разрядов задача быстро становится неразрешимой. Наибольшее число, которое было разложено на простые множители в качестве математического соревнования, т.е. число, чьи простые множители были втайне выбраны математиками, чтобы составить задачу для других математиков, состояло из 129 разрядов. Если же число разрядов окажется порядка 1000, то никто не знает, как решить эту задачу. Квантовый алгоритм факторизации (П.Шора) позволит реализовать эту операцию за долю секунды. Невыполнимость факторизации лежит в основе наиболее надежных на сегодняшний день методов шифрования (в частности системы RSA - Rivest, Shamir, Adleman), которая используется для защиты электронных банковских счетов. Когда будет построена машина для квантовой факторизации все такие криптографические системы станут абсолютно бесполезны.

*Дополнительно - (если есть время). Как действует классический компьютер при факторизации числа на простые множители?
Алгоритм решения этой задачи сводится к нахождению периода вспомогательной функции. Такой функцией является остаток от деления степенной функции вида a^x на целое число N
$f_N(x) = a^x \ mod\ N$,
(где x = 0, 1, 2...), a - любое число, не имеющее общих делителей с рассматриваемым числом N.
Например, $N = 10$. Выберем $a = 7$.

x	0	1	2	3	4	5	6
a^x	7^0	7^1	7^2	7^3	7^4	7^5	7^6
a^x	1	7	49	343	2401	16807	117649
$a^x \ mod\ 10$	1	7	9	3	1	7	9

Видно, что период функции f равен 4: $r = 4$. Далее необходимо найти наибольшие общие делители чисел N (исходное число, которое нужно разложить) и $a^{r/2} \sim 1$. Для этого используют алгоритм Евклида:
Требуется найти наибольший общий делитель чисел P и Q.
$P = Q\,T + R_1$,
$Q = R_1T_2 + R_2$,
$R_1 = R_2T_3 + R_3$,
.....,
$R_{m-2} = R_{m-1}T_m + R_m$,
$R_{m-1} = R_mT_{m+1}$. Предшествующий остаток R_m и является наибольшим общим делителем.
В нашем примере:
$a^{r/2}$ (+-) 1 = 48, 50.
50 = 10 x 5, т.е. первый делитель - число 5,
48 = 10 x 4 + 8,
10 = 8 x 1 + 2,
8 = 2 x 4. Другой делитель - число 2
Итого, 10 = 5 x 2.

Если же одно из получившихся чисел не является простым, то для него указанный алгоритм повторяется.

Еще пример: N = 12

x	0	1	2	3	4
a^x	7^0	7^1	7^2	7^3	7^4
a^x	1	7	49=12x 4+1	343=12x28 +7	2401=12x200 +1
a^x *mod* 12	1	7	1	7	1

$a^{r/2}$ (+-) 1 = 6, 8.
12 = 6 x 2, т.е. первый делитель - число 6, а 6 = 3x2
12 = 8 x 1 + 4,
8 = 4 x 2 , Другой делитель - число 2
Итого, 12 = 3 x 2 x 2.

Другой пример - Классическому компьютеру требуется время, пропорциональное N для поиска определенного элемента в базе данных, состоящей из N элементов. Это делается, например, методом перебора. Это пример т.н. проблема ***NP***-класса сложности, в смысле их выполнимости (*Nondeterministic polynomial-time complete*). Другими словами, это задачи, для которых трудно найти решение, но его легко проверить. Квантовый компьютер, работающей по алгоритму Гровера может выполнить эту операцию за время пропорциональное $\sqrt{N}$.
Заметим, что огромное увеличение производительности квантовых компьютеров по сравнению с классическими позволят рассчитать такие фундаментальные физические задачи как эволюция квантовой системы многих тел.

<u>ПРОБЛЕМЫ:</u>

1. Декогерентность (ее наличие ведет к необходимости использовать алгоритмы “коррекции ошибок”)
2. Как осуществить перепутывание контролируемым образом?

3. Как передать информацию от одной части вычислительного устройства к другой? Что является квантово-механическим аналогом проводов и шин данных в классических компьютерах
4. Проблема квантовых измерений. Как выполнять измерения без разрушения квантовых состояний? Необходимы алгоритмы “коррекции детектирования” и чтения данных.

Вычисление на (квантовом) компьютере называется эффективным, если число элементарных операций Q растет не быстрее, чем по полиномиальному закону по числу входных (ку)битов L Если убрать то, что стоит в скобках, получится классическое определение эффективности.

Пусть $1/R$ - некоторое характерное время, требуемое для выполнения элементарной операции. Пусть T_{dec} - время декогерентности системы (T_2). Тогда должно выполняться соотношение:

$Q/R<T_{dec}$.

Обозначим, $T_{dec} = L\gamma$, где γ - некоторое характерное время декогерентности кубита. Тогда число элементарных операций ограничено фактором:

$Q<R(L\gamma)$.

Роль неравенств Белла в квантовой информации.

Дж. Белл (1964) анализировал системы, для которых формулировался парадокс ЭПР (1935). Это коррелированные системы, которые взаимодействовали в прошлом, но затем рассматриваются изолированно, т.е. больше не влияют друг на друга. В основе выводов Бела лежат очень простые предположения:

- системы не влияют друг на друга (локальность), в смысле, измерения, выполненные над одной системой не влияют на результат измерения, выполненного над другой системой;
- существуют совместные распределения вероятностей неких наблюдаемых величин двух систем;
- Эти вероятности неотрицательны.

Суть неравенств Белла состоит в том, что уровень корреляций в таких (двух) квантовых системах, не превышает некий уровень, предсказанных на основе любых законов физики, описывающих частицы (системы) в терминах классических переменных.

Классический компьютер может симулировать поведение квантовой системы. Однако существует принципиальное ограничение - нет классических процессов, которые позволили бы приготовить коррелированные удаленные системы, в которых нарушаются неравенства Белла! Но на таких корреляциях строятся все известные алгоритмы квантовых вычислений (но не все криптографические протоколы)!

Дэвид Дойч (1985). Предложил одну из первых реалистичных моделей квантового компьютера. Она включает линейку двухуровневых систем, выполняющих фиксированное число простых операций (gates). Он доказал, что с помощью такой модели можно симулировать унитарную эволюцию любой физической (квантовой) системы. Его модель близка по архитектуре к машине Тьюринга, в смысле, что обе модели являются универсальными классическими машинами).

Универсальный компьютер - такой, который может воспроизвести (симулировать) действие любого другого компьютера с не меньшей скоростью. “Не меньшая скорость” определяется в терминах числа требуемых вычислительных процедур или шагов: это число не должно возрастать экспоненциально с размером входных данных.

Компьютер Дойча не является универсальным в полном смысле, однако он позволяет эффективно симулировать широкий класс квантовых систем. Также он впервые использовал понятие квантовых сетей и логических элементов.

Кубиты.

Возникает вопрос, как количественно охарактеризовать квантовую информацию, подобно тому, как это сделал Шеннон для классической информации (с помощью битов)?

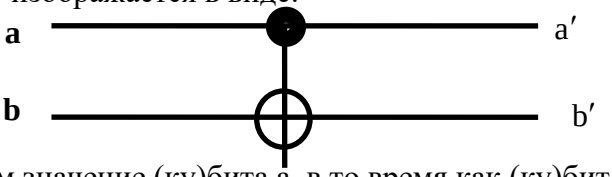
Здесь имелась определенная трудность, которую удобно пояснить с помощью следующего примера. Простейшая квантовая система - двухуровневая система, скажем, частица со спином 1/2 в магнитном поле. Квантовое состояние спина представляет собой непрерывную величину, определяемую двумя действительными числами, поэтому, в принципе, она заключает бесконечное количество классической информации! Однако, измерение спина дают только один двухкомпонентный ответ (спин направлен вверх или спин вниз) - и, таким образом, нет способа извлечь эту бесконечную информацию, заложенную в системе. Поэтому является некорректным рассматривать информационное содержание квантовой системы в этих терминах. Проблема восходит к перенормировке в квантовой электродинамике. И все же, сколько информации можно запасти в квантовой двухуровневой системе? Ответ был дан в работах Джозсы и Шумахера (1994, 1995). Оказывается, что его можно выразить в терминах одной двухуровневой системы! Они показали, что двухуровневая система играет в квантовой теории информации такую же роль как бит в классической. Таким образом, информационное содержание любой квантовой системы можно выразить в минимальном числе двухуровневых систем или кубитов, которое необходимо, чтобы запасти или передать состояние этой (любой) системы с высокой точностью.

Лекция 2.

1. Сведения из термодинамики и статистической физики. Функция распределения. Теорема Лиувилля. Микроканоническое распределение. Первое начало термодинамики. Адиабатические процессы. Энтропия. Статистический вес. Формула Больцмана. Второе начало термодинамики. Обратимые и необратимые процессы.
2. Информационная энтропия Шеннона. Биты, наты, триты и проч. Связь энтропии и информации.

Эта часть относится к лекции 1. Ее лучше рассматривать в разделе V (“Концепция “перепутывания” (entanglement) квантовых состояний”).

ЛЭ CNOT изображается в виде:



Сохраняем значение (ку)бита a, в то время как (ку)бит b меняется по закону XOR:

a	**b**	a′	$b' = a \oplus b$
0	**0**	**0**	**0**
1	**0**	**1**	**1**
0	**1**	**0**	**1**
1	**1**	**1**	**0**

бит **b** (мишень = target) меняет свое состояние тогда и только тогда, когда состояние контрольного (control) бита **a** соответствует 1; при этом, состояние контрольного бита не меняется.

Логическая операция XOR (CNOT) иллюстрирует почему классические данные могут быть клонированы, а квантовые - нет. Заметим, что в общем случае под квантовыми данными мы будем понимать суперпозиции вида

$$\left|\Psi\right\rangle = \alpha\left|0\right\rangle + \beta\left|1\right\rangle, \qquad (1)$$

где α и β - комплексные числа или амплитуды состояний, причем, $\left|\alpha\right|^2 + \left|\beta\right|^2 = 1$.

Согласно таблице истинности, если XOR применить к булевым данным, в которых второй бит находится в состоянии “0” (b), а первый -в состоянии “X” (a), то первый бит не изменяется, а второй становится его копией:

U_{XOR}(X, 0) = (X, X), где X = “0” или “1”.

В квантовом случае, в качестве данных, обозначенных символом “X”, нужно рассматривать суперпозицию (1):

$U_{XOR}\left|X,0\right\rangle = \left|X,X\right\rangle$.

Физически, данные можно закодировать, например, в поляризационном базисе |V> = 1, |H> = 0 (H,V)= (0,1):

$U_{XOR}\left|0,0\right\rangle = \left|0,0\right\rangle$, и $U_{XOR}\left|1,0\right\rangle = \left|1,1\right\rangle$.

Видно, что действительно имеет место копирование состояния. Теорема о запрете клонирования утверждает, что невозможно копирование *произвольного* квантового состояния. В рассмотренном примере копирование произошло, поскольку операция производилась в собственном базисе (|0>, |1>), т.е. в частном случае квантового состояния.

Казалось бы, что операцию XOR можно использовать и для копирования суперпозиций двух булевых состояний, таких как $|45^0\rangle$? |V> + |H>:

$U_{XOR}\left|45^o, H\right\rangle = \left|45^o, 45^o\right\rangle$.

Но это не так! Унитарность квантовой эволюции требует, чтобы суперпозиция входных состояний преобразовывалась в соответствующую суперпозицию выходных состояний:

$U_{XOR}\left|45^o, H\right\rangle = \left(\left|45^o\right\rangle = 1/\sqrt{2}\left[\left|H\right\rangle + \left|V\right\rangle\right]\right) = 1/\sqrt{2}\left[\left|H,H\right\rangle + \left|V,V\right\rangle\right]$ или

$U_{XOR}\left|s,0\right\rangle = \left(\left|s\right\rangle = 1/\sqrt{2}\left[\left|0\right\rangle + \left|1\right\rangle\right]\right) = 1/\sqrt{2}\left[\left|0,0\right\rangle + \left|1,1\right\rangle\right]$.

$\Phi^+ = 1/\sqrt{2}\left[\left|0,0\right\rangle + \left|1,1\right\rangle\right]$ (2)

Это т.н. перепутанное состояние (Φ^+), в котором каждый из двух выходных кубитов не имеет определенного значения (в данном случае - поляризации). Этот пример показывает, что логические операции, выполняемые над квантовыми объектами происходят по другим правилам, нежели в классических вычислительных процессах.

Возникает следующий вопрос: Вроде бы состояние в выходной моде **a** опять-таки можно представить в виде суперпозиции $\left|s\right\rangle = 1/\sqrt{2}\left[\left|0\right\rangle + \left|1\right\rangle\right]$, как и состояние в моде **b**. Как показать, что это не так, т.е., что вообще нет смысла говорить о состояниях моды (бита) **a** и моды (бита) **b**?

Воспользуемся поляризационной аналогией, когда

$\left|s\right\rangle \equiv \left|45^o\right\rangle = 1/\sqrt{2}\left[\left|H\right\rangle + \left|V\right\rangle\right]$ (3).

Есть два пути. Путь 1 - длинный, но более последовательный. Надо посчитать средние значения параметров Стокса для обеих выходных мод. Средние берутся по волновой функции (2). Если все $\langle S_i\rangle$, кроме $\langle S_0\rangle$ окажутся равными нулю - то это состояние неполяризованное, т.е. смешанное и суперпозиция (3) смысла не имеет. Работаем в представлении Гейзенберга, когда преобразуются операторы, а волновая функция - нет. Итак, находим $\langle S_i\rangle$ в моде **a**.

$S_0 \equiv a_x^\dagger a_x + a_y^\dagger a_y$, - общая интенсивность пучка a,

$S_1 \equiv a_x^\dagger a_x - a_y^\dagger a_y$, - доля вертикальной поляризации,

$S_2 \equiv a_x^\dagger a_y + a_x a_y^\dagger$ - доля $+45^0$-ой поляризации,

$S_3 \equiv \frac{1}{i}\left\{a_x^\dagger a_y - a_x a_y^\dagger\right\}$ - доля право-циркулярной поляризации.

Волновая функция, по которой производится усреднение, берется в виде (2):

$\Phi^+ = 1/\sqrt{2}\left[\left|H,H\right\rangle + \left|V,V\right\rangle\right] = 1/\sqrt{2}\left[a_x^\dagger b_x^\dagger + a_y^\dagger b_y^\dagger\right]\left|vac\right\rangle$,

где операторы рождения и уничтожения в модах **a** и **b** действуют по правилам:

$a\left|N\right\rangle = N^{1/2}\left|N-1\right\rangle$,

$a^\dagger\left|N\right\rangle = (N+1)^{1/2}\left|N+1\right\rangle$.

{Вычисления $\langle S_i\rangle$ сделать в разделе V (см.тетрадь). Там же рассчитать и вероятность регистрации совпадений или коррелятор вида $R_{ab} = \left\langle \Phi^+ \left| a^\dagger b^\dagger a b \right| \Phi^+ \right\rangle$ }

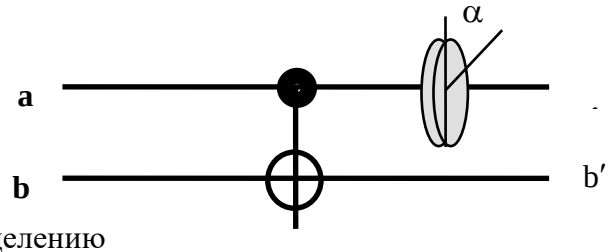
Путь II - более наглядный, но менее “честный”!

Найдем зависимость интенсивности света в моде **a** от угла поворота поляроида, помещенного в эту моду. Это стандартный квантово-оптический способ проверки

состояния (2) - интенсивность не должна зависеть от поворота. В то же время, аналогичная зависимость числа совпадений имеет вид

$R_{совп} \sim \cos^2(\alpha \pm \beta)$. Впервые такие зависимости были получены Э.Фраем (1976) и А.Аспеком (1985) и часто интерпретируется как доказательство нелокальности квантовой механики.

Итак, экспериментальная ситуация изображена на рисунке:



По определению

$R_a \sim \left\langle \Phi^+ \middle| a'^{\dagger} a' \middle| \Phi^+ \right\rangle$,

где $a^{\dagger}$ - оператор уничтожения в моде a. Известно, что преобразование операторов двух ортогонально поляризованных мод x и y при прохождении света через поляроид, ориентированный под углом α имеет вид:

$a' = a_x \sin\alpha + a_y \cos\alpha$.

Тогда

$$R \equiv \frac{1}{2}\left[\left\langle vac\middle|\left(a_x b_x + a_y b_y\right)\left(a_x^{\dagger}\sin\alpha + a_y^{\dagger}\cos\alpha\right)\left(a_x \sin\alpha + a_y \cos\alpha\right)\left(a_x^{\dagger}b_x^{\dagger} + a_y^{\dagger}b_y^{\dagger}\right)\middle|vac\right\rangle\right] =$$

$$= \frac{1}{2}\left[\left\langle vac\middle|\left(a_x b_x + a_y b_y\right)\left(a_x^{\dagger}a_x \sin^2\alpha + a_x^{\dagger}a_y \sin\alpha\cos\alpha + a_y^{\dagger}a_y \sin\alpha\cos\alpha + a_x^{\dagger}a_y \cos^2\alpha\right)\left(a_x^{\dagger}b_x^{\dagger} + a_y^{\dagger}b_y^{\dagger}\right)\middle|vac\right\rangle\right] =$$

$$= \frac{1}{2}[\left\langle vac\middle|\left(a_x b_x + a_y b_y\right)(a_x^{\dagger}a_x a_x^{\dagger}b_x^{\dagger}\sin^2\alpha + a_x^{\dagger}a_x a_y^{\dagger}b_y^{\dagger}\sin^2\alpha +$$

$$+ a_x^{\dagger}a_y a_x^{\dagger}b_x^{\dagger}\sin\alpha\cos\alpha + a_x^{\dagger}a_y a_y^{\dagger}b_y^{\dagger}\sin\alpha\cos\alpha +$$

$$+ a_y^{\dagger}a_x a_x^{\dagger}b_x^{\dagger}\sin\alpha\cos\alpha + a_y^{\dagger}a_x a_y^{\dagger}b_y^{\dagger}\sin\alpha\cos\alpha +$$

$$+ a_y^{\dagger}a_y a_x^{\dagger}b_x^{\dagger}\cos^2\alpha + a_y^{\dagger}a_y a_y^{\dagger}b_y^{\dagger}\cos^2\alpha)\left|vac\right\rangle] = (\text{только первое, четвертое, пятое и восьмое слагаемые отличны от нуля}) =$$

$$= \frac{1}{2}[\left\langle vac\middle|a_x b_x a_x^{\dagger}a_x a_x^{\dagger}b_x^{\dagger}\sin^2\alpha + a_x b_x a_x^{\dagger}a_y a_y^{\dagger}b_y^{\dagger}\sin\alpha\cos\alpha +$$

$$+ a_x b_x a_y^{\dagger}a_x a_x^{\dagger}b_x^{\dagger}\sin\alpha\cos\alpha + a_x b_x a_y^{\dagger}a_y a_y^{\dagger}b_y^{\dagger}\cos^2\alpha +$$

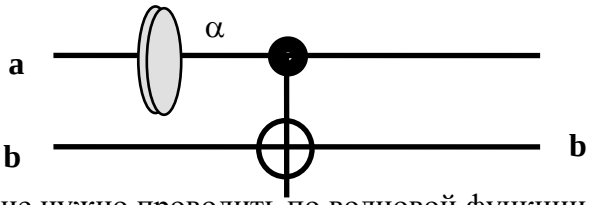
$$+ a_y b_y a_x^{\dagger}a_x a_x^{\dagger}b_x^{\dagger}\sin^2\alpha + a_y b_y a_x^{\dagger}a_y a_y^{\dagger}b_y^{\dagger}\sin\alpha\cos\alpha +$$

$$+ a_y b_y a_y^{\dagger}a_x a_x^{\dagger}b_x^{\dagger}\sin\alpha\cos\alpha + a_y b_y a_y^{\dagger}a_y a_y^{\dagger}b_y^{\dagger}\cos^2\alpha\left|vac\right\rangle] = (\text{только первое и восьмое слагаемые отличны от нуля}) = \frac{1}{2}\left[\left\langle vac\middle|\sin^2\alpha + \cos^2\alpha\middle|vac\right\rangle\right] = \frac{1}{2}\left[\left(\sin^2\alpha + \cos^2\alpha\right)\left\langle vac||vac\right\rangle\right] = \frac{1}{2}$$ - не зависит от угла ?!

Физически это происходит потому, что волновая функция (2) не факторизуется и нет смысла говорить о состояниях в модах **a** и **b** по отдельности. Таким образом, нельзя утверждать, что мода a находится в суперпозиционном состоянии (3)!

Замечание. Проделанные вычисления (Путь II) вовсе не доказывают, что состояние в моде **a** неполяризованное. Например, при наличии в этой моде циркулярно-поляризованного света, результат получился бы таким же. Строгое доказательство - например, через параметры Стокса (в разделе V).

Заметим, что действуя таки же образом, можно доказать, что состояние в моде a до элемента CNOT - поляризованное.



Здесь усреднение нужно проводить по волновой функции исходного состояния (3). Результат получается таким:

$R_a \sim \langle \Psi | a^\dagger a | \Psi \rangle = \frac{1}{2}(1+\sin 2\alpha)$, т.е. максимум отсчетов достигается при $\alpha = 45^0$.

Информация и энтропия.

Не вводя пока “операционального” термина “информация” будем рассуждать, пользуясь “бытовым” языком. Т.е. информация - это некое знание об объекте.

За то, что понятия информация и энтропия тесно связаны, говорит следующий пример. Рассмотрим идеальный газ, находящийся в термодинамическом равновесии. Газ состоит из огромного количества молекул, которые двигаются в объеме V. Параметрами состояния являются давление, температура. Число состояний такой системы огромно. Энтропия газа при ТД равновесии максимальна и как следует из формулы Больцмана, определяется числом микросостояний системы. При этом мы ничего не знаем о том, какое конкретно состояние имеет система в данный момент времени у нас нет - информация минимальна. Допустим, что каким-то образом нам удалось с помощью очень быстрого прибора “подсмотреть состояние системы в данный момент времени. Значит мы получили о ней какую-то информацию. Можно даже представить, что мы сфотографировали не только координаты молекул, но и их скорости (например, сделав несколько фотографий одну за другой). При этом в каждые моменты времени, когда нам доступна информация о состоянии системы, энтропия стремится к нулю, т.к. система находится лишь в каком-то одном определенном состоянии из всего огромного их многообразия и это состояние сильно неравновесное. Этот пример показывает, что действительно информация и энтропия как-то связаны, причем уже вырисовывается характер связи: чем больше информация, тем меньше энтропия.

Сведения из термодинамики и статистической физики.

Физические величины, характеризующие макроскопические состояния тел (много молекул), называют термодинамическими (в том числе, энергия, объем). Существуют, однако, и величины, появляющиеся как результат действия чисто статистических закономерностей и имеющие смысл в применении только к макроскопическим системам. Такова, например, энтропия и температура.

Классическая статистика

*Теорема Лиувилля. Функция распределения постоянна вдоль фазовых траекторий подсистемы (речь идет о квазизамкнутых подсистемах, поэтому теорема справедлива только для не очень больших промежутков времени, в течение которых подсистема ведет себя как замкнутая).

$$\frac{d\rho}{dt} = \sum_i \left(\frac{\partial \rho}{\partial q_i} \dot{q}_i + \frac{\partial p}{\partial p_i} \dot{p}_i \right) = 0$$

Здесь - ρ - функция распределения или плотность вероятности. Она вводится через вероятность w обнаружить подсистему в элементе фазового пространства dpdq ***в данный момент времени: dw = ρ (p₁,...,pₛ, q₁,...,qₛ)dpdq, причем***

$$\int \rho dpdq = 1. \qquad (4)$$

Нахождение статистического распределения ρ для любой подсистемы и является основной задачей статистики. Если статистическое распределение известно, то можно вычислить вероятности различных значений любых физических величин, зависящих от состояний этой подсистемы (т.е. от значений координат и импульсов):

$$\overline{f} = \int f(p,q)\rho(p,q)dpdq .$$

****Микроканоническое распределение.***

Распределение ρ_{12} для совокупности двух подсистем (они полагаются замкнутыми, т.е. слабовзаимодействующими) равно $\rho_{12} = \rho_1\rho_2$. Поэтому $\ln\rho_{12} = \ln\rho_1 + \ln\rho_2$ - логарифм функции распределения - величина *аддитивная*. Из теоремы Лиувилля следует, что функция распределения должна выражаться через такие комбинации переменных p и q, которые при движении подсистемы, как замкнутой, должны оставаться постоянными (такие величины называются интегралами движения). Значит сама функция распределения является интегралом движения. Более того, ее логарифм - тоже интеграл движения, причем *аддитивный*. Всего в механике существует семь интегралов движения - энергия, три компоненты импульса и три компоненты момента импульса - (для подсистемы a: $E_a(p, q)$, $\boldsymbol{P}_a(p, q)$, $\boldsymbol{M}_a(p, q)$). Единственная аддитивная комбинация этих величин есть

$$\ln\rho_a = \alpha_a + \beta_a E_a(p,q) + \gamma P(p,q) + \delta M(p,q), \qquad (*)$$

причем коэффициенты β, γ, δ (их семь штук)- должны оставаться одинаковыми для всех подсистем данной замкнутой системы, а α выбирается из условий нормировки (4). Чтобы выполнялось условие нормировки (4), необходимо, чтобы функция ρ*(p,q)* обращалась в точках E_0, $\boldsymbol{P_0}$, $\boldsymbol{M_0}$ в бесконечность. Более точная формулировка дает выражение

$\rho = \text{const}\ \delta(E - E_0)\delta(P - P_0)\delta(M - M_0)$. - микроканоническое распределение.

Наличие δ - функций обеспечивает обращение ρ в нуль для всех точек фазового пространства, в которых хотя бы одна из величин *E,* ***P, M*** не равна своему заданному (среднему) значению E_0, $\boldsymbol{P_0}$, $\boldsymbol{M_0}$.

От шести интегралов ***P*** и ***M*** можно избавится, заключив систему в твердый ящик, в котором она покоится.

Тогда

$\rho = \text{const}\ \delta(E - E_0)$.

Физическая энтропия

Опять используем понятие идеального газа.

Пусть одноатомный идеальный газ с плотностью *n* и температурой *T* занимает объем *V*. Будем измерять температуру в энергетических единицах - не будет фигурировать постоянная Больцмана. Каждый атом газа имеет среднюю кинетическую энергию теплового движения, равную *3T/2*. Поэтому полная тепловая энергия газа равна

$$E = \frac{3}{2} TnV$$

Известно, что давление газа равно $p = nT$. Если газ может обмениваться теплом с внешней средой, то закон сохранения энергии газа выглядит так:

$$dE = -pdV + dQ. \qquad (5)$$

Таким образом, изменение внутренней энергии газа может происходить как за счет совершаемой им работы, так и вследствие поступления некоторого количества тепла dQ извне. Это уравнение выражает первое начало термодинамики, т.е. закон сохранения энергии. При этом предполагается, что газ находится в равновесии, т.е. $p = const$ по всему объему.

Если же допустить, что газ находится и в состоянии ТД равновесия, $T = const$, то соотношение (5) можно рассматривать как элементарный процесс вариации параметров газа при их очень медленном изменении, когда ТД равновесие не нарушается. Именно для таких процессов и вводится понятие энтропии S с помощью соотношения

$$dS = \frac{dQ}{T} \qquad (6)$$

Таким образом, утверждается, что у равновесного газа кроме внутренней энергии есть еще одна внутренняя характеристика, связанная с тепловым движением атомов. Согласно (5, 6) при постоянном объеме $dV = 0$, изменение энергии пропорционально изменению температуры, а в общем случае

$$dE = -pdV + TdS$$

Так как $p = nT = \frac{N}{V}T, \quad E = \frac{3}{2}NT,$ где $N = nV = const$ есть полное количество атомов газа, то последнее соотношение можно записать в виде

$$dS = N\left(\frac{3}{2}\frac{dT}{T} + \frac{dV}{V}\right).$$

После интегрирования получаем

$$S = N\left[\ln\left(VT^{3/2}\right) + \text{const}\right] \equiv NS.$$

Выражение в квадратных скобках представляет собой энтропию, приходящуюся на одну частицу.

Таким образом, если и температура и объем изменяются таким образом, что $VT^{3/2}$ остается постоянным, то и энтропия S не изменяется. Согласно (6) это означает, что газ не обменивается теплом с внешней средой, т.е. газ отделен от нее теплоизолирующими стенками. Такой процесс называется *адиабатическим*.

Поскольку

$$VT^{3/2} = \text{const}, \quad p = \frac{N}{V}T \to T = \frac{pV}{T} \to pV^{\gamma} = \text{const}.$$

где $\gamma = 5/3$ называется показателем адиабаты. Таким образом при адиабатическом процессе температура и давление изменяются с плотностью по закону

$$T = \text{const}\ \ n^{\gamma-1}, \quad p = \text{const}\ \ n^{\gamma}.$$

Формула Больцмана

Как следует из теоремы Лиувилля, функция распределения ? имеет резкий максимум при $E = E_0$ (среднее значение) и отлична от нуля только в окрестности этой точки. Если ввести ширину ΔE кривой $\rho(E)$, определив ее как ширину прямоугольника, высота которого равна значению функции $\rho(E)$ в точке максимума, а площадь равна единице $\rho(E_0 = \bar{E})\Delta E = 1$ (при надлежащей нормировке). Можно перейти от интервала значений

энергии к числу состояний $\Delta\Gamma$ с энергиями, принадлежащими ΔE (это, фактически, средняя флуктуация энергии системы). Тогда величина $\Delta\Gamma$ характеризует степень размазанности макроскопического состояния системы по ее микроскопическим состояниям. Другими словами, для классических систем $\Delta\Gamma$ - это размер той области фазового пространства, в которой данная подсистема проводит почти все время $\rho(E_0 = \bar{E})\Delta p\Delta q = 1, \quad \Delta\Gamma \square \Delta p\Delta q.$ В квазиклассической теории устанавливается соответствие между объемом области фазового пространства и приходящимся на него числом квантовых состояний.. А именно, на каждое квантовое состояние в фазовом пространстве приходится клетка с объемом $(2\pi\hbar)^s$, где s - число степеней свободы

Величину $\Delta\Gamma$ называют статистическим весом макроскопического состояния, его можно записать в виде:

$$\Delta\Gamma = \frac{\Delta p\Delta q}{(2\pi\hbar)^s}.$$

Логарифм статистического веса называется энтропией:

$S = \kappa \ln \Delta\Gamma$.

где $\Delta\Gamma$ - статистический вес = число микросостояний, охватываемых рассматриваемым макросостоянием системы.

$$\frac{S}{\kappa} = \ln\Delta\Gamma \to e^{\frac{S}{\kappa}} = \Delta\Gamma \to \Delta\Gamma = e^{\frac{TS}{\kappa T}}.$$

В квантовой статистике показывается, что $\rho(E_0)\Delta\Gamma = 1 = 1$. Тогда

$S = \ln\Delta\Gamma = -\ln\rho(E_0)$, где под ρ понимается статистическая матрица (плотности). Ввиду линейности логарифма функции распределения по энергии (*) $S = \ln\Delta\Gamma = -\ln\rho(E_0) = -\langle\ln\rho(E)\rangle$, где усреднение проводится по функции распределения ρ.

Поскольку число состояний $\Delta\Gamma$ во всяком случае не меньше единицы, то энтропия не может быть отрицательной. S определяет густоту уровней энергетического спектра макроскопической системы. Ввиду аддитивности энтропии можно сказать, что средние расстояния между уровнями макроскопического тела экспоненциально убывают с увеличением его размеров (т.е. числа частиц в нем). Наибольшее значение энтропии соответствует полному статистическому равновесию.

Характеризуя каждое макроскопическое состояние системы распределением энергии между различными подсистемами, можно сказать, что ряд последовательно проходимых системой состояний соответствует все более вероятному распределению энергии. Это возрастание вероятности велико в силу его экспоненциального характера e^S - в экспоненте стоит аддитивная величина - энтропия. Т.о. процессы, протекающие в неравновесной замкнутой системе, идут таким образом, что система непрерывно переходит из состояний с меньшей энтропией в состояния с большей энтропией. В итоге энтропия достигает наибольшего возможного значения, соответствующего полному статистическому равновесию.

Таким образом, если замкнутая система в некоторый момент времени находится в неравновесном макроскопическом состоянии, то наиболее вероятным следствием в последующие моменты времени будет монотонное возрастание энтропии системы. Это - *второй закон термодинамики* (Р.Клаузиус, 1865г.). Его статистическое обоснование дано Л.Больцманом в 1870г. Другое определение:

если в некоторый момент времени энтропия замкнутой системы отлична от максимальной, то в последующие моменты энтропия не убывает. Она

увеличивается или в предельном случае остается постоянной. Соответственно этим двум возможностям все происходящие с макроскопическими телами процессы принято делить на ***необратимые*** и ***обратимые***. ***Необратимые*** - те процессы, которые сопровождаются увеличением энтропии всей замкнутой системы (процессы, которые бы являлись их повторениями в обратном порядке, не могут происходить, так как при этом энтропия должна была бы уменьшаться). Заметим, что уменьшение энтропии может быть вызвано флуктуациями. ***Обратимыми*** называются процессы, при которых энтропия замкнутой системы остается постоянной и которые, следовательно, могут проходить и в обратном направлении. Строго обратимый процесс представляет собой идеальный предельный случай.

При адиабатических процессах система не поглощает и не отдает тепло $\delta Q = 0$.

Замечание: (существенное). Утверждение о том, что замкнутая система должна в течение достаточно длительного времени (большего, чем время релаксации) перейти в состояние равновесия относится лишь к системе, находящейся в стационарных внешних условиях. Пример - поведение доступной нашему наблюдению большой области Вселенной (свойства природы не имеют ничего общего со свойствами равновесной системы).

Информация.

Рассмотрим ленту, разбитую на ячейки - классический регистр. Если в каждой ячейке может быть помещен только один из двух символов, то говорят, что в ячейке содержится бит информации. Очевидно (см. лекцию 1), что в регистре, содержащем N ячеек содержится N бит информации и в нем можно записать 2^N сообщений. Итак, информационная энтропия измеряется в битах:

$$H_B \equiv N \equiv \log_2 Q_N. \qquad (7)$$

Здесь $Q_N = 2^N$ - полное число различных сообщений. Из (7) ясно, что ***информационная энтропия просто равна минимальному числу двоичных ячеек, с помощью которых можно записать некую информацию.***

Определение (7) можно переписать по-другому. Пусть у нас имеется множество Q_N различных сообщений. Найдем вероятность того, что необходимое нам сообщение совпадет со случайно выбранным из общего числа Q_N различных сообщений. Она равна, очевидно, $P_N = 1/Q_N$. Тогда определение (7) запишется как:

$$H_B \equiv N \equiv -\log_2 P_N. \qquad (8)$$

Чем больше число ячеек N, тем меньше вероятность P_N и тем больше информационная энтропия H_B, содержащейся в данном конкретном сообщении.

Пример. Число букв алфавита равно 32 (без буквы ё). Число 32 есть пятая степень двойки $32 = 2^5$. Чтобы каждой букве сопоставить определенную комбинацию двоичных чисел необходимо иметь 5 ячеек. Добавив к строчным буквам заглавные, мы удваиваем число символов, которые хотим закодировать - их станет $64 = 2^6$ - т.е. добавляется лишний бит информации $H_B = 6$. Здесь H_B - объем информации, приходящийся на одну букву (строчную или заглавную). Однако такой прямой подсчет информационной энтропии не совсем точен, поскольку в алфавите есть буквы, которые встречаются реже или чаще. Тем буквам, которые встречаются реже, можно отдать большее количество ячеек, а на часто встречающихся буквах - сэкономить и отдать им те состояния регистра, которые занимают меньшее количество ячеек. Точное определение информационной энтропии было дано Шенноном:

$$H \equiv -\sum_i p_i \ln p_i. \qquad (9)$$

Формально вывод этого соотношения можно обосновать следующим образом.
Мы показали выше, что

$$S = \ln \Delta\Gamma = -\ln \rho(E_0) = -\langle \ln \rho(E) \rangle$$

из-за аддитивности логарифма функции распределения и его линейности по энергии.
Пусть p - функция распределения какой-нибудь дискретной величины f_i (например, буквы “о” в этом тексте). Если с помощью функции p построить функцию распределения вероятностей различных значений величины $f = f_1, f_2,...f_N$, то эта функция будет иметь максимум при $f = \bar{f}$, где $\bar{f} = \int f p d\Gamma$ и $\int p d\Gamma = 1$ (нормировка). Тогда $p(\bar{f})\Delta\Gamma = 1$ и $H \equiv -\ln p(\bar{f}) = -\langle \ln p(f_n) \rangle = -\sum_i p_i \ln p_i$. (вообще говоря, это справедливо для класса функций, удовлетворяющих условию (*))
Суммирование ведется по всем символам (буквам алфавита), а p_i означает вероятность появления символа с номером i. Как видно это выражение охватывает как часто используемые буквы, так и буквы, вероятность появления которых в данном сообщении мала.

Поскольку в выражении (9) используется натуральный логарифм, соответствующую единицу информации называют “нат”.
Выражение (9) можно переписать в виде

$$H \equiv -\langle \ln p_i \rangle, \qquad (10)$$

где скобки означают обычное классическое усреднение с помощью функции распределения p_i.
Замечание. В следующих лекциях будет показано, что для квантовых состояний

$$H_{quant} \equiv -\langle \ln p_i \rangle_\rho = -Sp\rho \ln p_i. \qquad (11)$$

где ρ - матрица плотности. Формально выражения (10) и (11) совпадают, однако есть и существенная разница. Классическое усреднение производится по ортогональным (собственным) состояниям системы, в то время как для квантового случая состояния могут быть и неортогональные (суперпозиции). Поэтому всегда $H_{quant} \le H_{class}$!
В формулах (8) и (9) используются логарифмы при разных основаниях. В (8) - по основанию 2, а в (9) - по основанию e. Соответствующие этим формулам информационные энтропии можно легко выразить друг через друга. Воспользуемся соотношением, в котором M - произвольное число

$$M = 2^{\log_2 M} = e^{\ln M}.$$

Тогда, учтя, что $H_{Bit} = \log_2 M$, а $H_{Nat} = \ln M$, получаем

$$e^{H_{Nat}} = 2^{H_{Bit}} \to H = H_{Nat} = \ln 2^{H_{Bit}} = H_{Bit} \ln 2.$$

Откуда

$$H_{Bit} = \frac{H_{Nat}}{\ln 2} = 1.44 H_{Nat}$$ - число бит почти в полтора раза больше числа нат!

Рассуждая аналогично, можно получить соотношение между энтропиями, выраженными в тритах и битах:

$$M = 2^{\log_2 M} = 3^{\log_3 M} \to 2^{H_{Bit}} = 3^{H_{Trit}} \to H_{Bit} = \frac{H_{Trit}}{\log_3 2} = \frac{H_{Trit}}{0.631} = 1.58 H_{Trit}.$$

В компьютерной технике пользуются информацией по двоичному основанию (в битах). Для рассуждений в физике удобнее пользоваться информацией по Шеннону (в натах), которой можно характеризовать любую дискретную информацию. Всегда можно найти число соответствующих бит.

СВЯЗЬ ЭНТРОПИИ И ИНФОРМАЦИИ. Демон Максвелла

Этот парадокс впервые был рассмотрен Максвеллом в 1871г (см. рис.1). Пусть некая “сверхъестественная” сила открывает и закрывает заслонку в сосуде, перегороженном на две части и содержащем газ. Заслонка управляется по правилу: она открывается, если быстрые молекулы, двигающиеся справа налево, соприкасаются с ней или, если медленные молекулы ударяют в нее, двигаясь в противоположном направлении. Таким образом демон вводит разницу температур между двумя объемами без совершения работы, что нарушает второе начало термодинамики.

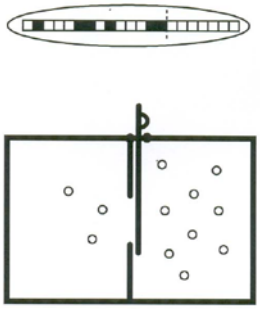


Рис.1.

Демон Максвелла. Демон устанавливает разность давления открывая заслонку, когда число молекул газа, ударивших в нее слева превышает число ударов справа. Это можно сделать полностью обратимым способом до тех пор, пока в памяти демона сохраняются случайные результаты его наблюдений за молекулами. Поэтому память демона (или его голова) нагревается. Необратимый шаг состоит не в том, что накапливается информация, а в том, что информация теряется, когда демон потом очищает память. Сверху: заполнение памяти демона битами информации – это случайный процесс. По правую сторону от пунктира – незаполненная область памяти (все ячейки находятся в состоянии 0, слева – случайные биты). Внизу – демон.

Был предпринят целый ряд попыток разрешить парадокс или изгнать демона. Например, предполагалось, что демон не может извлечь информацию без совершения работы или без возмущения (т.е. нагрева) газа – но, оказалось, что это не так! Другие попытки сводились к тому, что второе начало может нарушаться под действием неких «разумных» или “мыслящих” сил (существ). В 1929г. Лео Сцилард существенно «продвинул» решение проблемы, сведя ее к минимальной формулировке и выделив существенные компоненты. Главное, что нужно сделать Демону это установить находится ли единичная молекула справа или слева от скользящей заслонки, что позволило бы извлекать тепло. Такое устройство было названо двигателем Сциларда. Однако Сцилард не разрешил парадокса, поскольку его анализ не учитывал, как измерение, посредством которого демон узнает находится ли молекула справа или слева, влияет на увеличение энтропии (см рисунок Szilard_demon.pdf). Двигатель работает по шести-шагвому циклу. Двигатель представляет собой цилиндр, в торцах которого помещены поршни. В середину вставляется заслонка. Работа по вдвиганию перегородки может быть сведена к нулю (это показал Сциллард). Также имеется устройство памяти (УП). Оно может находиться в одном из трех состояний. «Пусто», «Молекула справа» и «Молекула слева». Исходное состояние: УП= «Пусто», поршни – отжаты, перегородка – выдвинута, у молекулы есть средняя скорость, которая определяется температурой термостата (слайд 1).

1. перегородка вставляется, оставляя молекулу справа или слева (слайд 2).
2. Устройство памяти определяет, где находится молекула и переходит в состояние «справа» или «слева».

3. Сжатие. В зависимости от состояния УП происходит вдвигание поршня со стороны, где нет молекулы. Этот этап не требует совершение работы. Поскольку сжимается вакуум (слайд 3).
4. Перегородка удаляется. Молекула начинает оказывать давление на поршень (слайд 4).
5. Рабочий ход. Молекула ударяется в поршень, заставляя его двигаться в обратном направлении. Энергия молекулы передается поршню. При движении поршня ее средняя скорость должна уменьшаться. Однако этого не происходит, поскольку стенки сосуда находятся при постоянной температуре. Поэтому тепло от термостата передается молекуле, поддерживая ее скорость постоянной. Таким образом во время рабочего хода происходит преобразование тепловой энергии, поступаемой из термостата в механическую работу, совершаемую поршнем (слайд 6).
6. Очищение УП, возвращая ее в состояние «Пусто» (слайд 7). Цикл завершен (слайд 8 = слайд 1).

Удивительно, что этот парадокс не был разрешен до 80-ых годов 20-го века. За это время было установлено, что в принципе, любой процесс можно сделать обратимым образом, т.е. без «оплаты» энтропией. Наконец, Беннетт в 1982г. установил окончательную связь между этим утверждением и парадоксом Максвелла. Он предложил, что демон на самом деле может узнать, где находится молекула в двигателе Сциларда без совершения работы или увеличения энтропии окружения (термостата) и таким образом, совершить полезную работу за один цикл работы двигателя. Однако, информация о положении молекулы должна оставаться в памяти демона (рси.1). По мере выполнения большего числа циклов все больше и больше информации накапливается в памяти. Для завершения термодинамического цикла демон должен стереть информацию, запасенную в памяти. Именно эту операцию стирания информации приходится классифицировать как процесс увеличения энтропии окружения, как требуется вторым началом. На этом завершается принципиально физическая часть устройства демона Максвелла.

Некоторое развитие этих идей получило в работах Д.Д.Кадомцева.

Рассмотрим идеальный газ, состоящий только из одной частицы (Кадомцев, «динамика и информация»). Это не абсурд. Если одна частица заключена в сосуде объемом V со стенками, находящимися при температуре Ò, то рано или поздно она придет в равновесие с этими стенками. В каждый момент времени она находится во вполне определенной точке пространства и с вполне определенной скоростью. Будем проводить все процессы настолько медленно, что частица успеет в среднем заполнить весь объем и многократно поменять величину и направление скорости при неупругих столкновениях со стенками сосуда. Таким образом, частица оказывает на стенки среднее давление, имеет температуру T и ее распределение по скоростям является максвелловским с температурой T. Эту систему из одной частицы можно адиабатически сжимать, можно менять ее температуру, давая ей возможность прийти в равновесие со стенками сосуда.

Среднее давление на стенку при $N = 1$, равно $p = T/V$, а средняя плотность n = $1/V$. Рассмотрим случай изотермического процесса, когда $T = const$. Из первого начала при $T = const$. и $p = T/V$ получаем

$\Delta Q = TdS = pdV = T\dfrac{dV}{V}$, поскольку $dE = 0$.

Отсюда находим, что изменение энтропии не зависит от температуры, так что

$$TdS = T\frac{dV}{V} \to S = \ln\frac{V}{V_0}.$$

Здесь введена постоянная интегрирования: “размер частицы”<<V_0<<V - чтобы не нарушалось приближение идеального газа.

Работа при изотермическом процессе

$$W = \int pdV = T\int\frac{dV}{V} = T\ln\frac{V_2}{V_1} = T(S_2 - S_1)$$

работа определяется разностью энтропий.

Пусть у нас имеются идеальные перегородки, которыми можно поделить сосуд на части без затраты энергии. Разделим наш сосуд на две равные части с объемом *V/2* каждая. При этом частица будет находиться в одной из половин - но мы не знаем в какой. Допустим, что у нас есть прибор, который позволяет определить в какой из частей находится частица, например, прецизионные весы. Тогда из симметричного распределения вероятностей 50% на 50% нахождения в двух половинках мы получаем 100% вероятности для одной из половин - происходит “коллапс” распределения вероятностей. Соответственно, новая энтропия $S = \ln\frac{V}{2V_0}.$ окажется меньше исходной энтропии на величину $\Delta S = S_1 - S_2 = \ln\frac{V}{V_0} - \ln\frac{V}{2V_0} = \ln V - \ln V_0 - \ln V + \ln 2 + \ln V_0 = \ln 2.$

За счет уменьшения энтропии можно совершить работу. Для этого достаточно двигать перегородку в сторону пустого объема вплоть до его исчезновения. Работа будет равна $W = T\Delta S = T\ln 2.$ Если бы во внешнем мире ничего не менялось, то повторяя эти циклы, можно построить вечный двигатель второго рода. Это и есть демон Максвелла в варианте Сцилларда. Но второй закон термодинамики запрещает получение работы только за счет тепла. Значит во внешнем мире должно что-то происходить. Что же это? Обнаружение частицы в одной из половин ***меняет информацию о частице*** - из двух возможных половинок указывается только одна, в которой находится частица. Это знание соответствует одному биту информации. Процесс измерения уменьшает энтропию частицы (перевод в неравновесное состояние) и ровно настолько же увеличивает информацию о системе (частице). Если совершать повторные деления пополам полученной ранее половинки, четвертушки, восьмушки и т.д., то энтропия будет последовательно уменьшаться, а информация - увеличиваться! Другими словами $S + I = \text{const}.$

Чем больше известно о физической системе, тем меньше ее энтропия. Если о системе известно все - это значит, что мы перевели ее в сильнонеравновесное состояние, когда ее параметры максимально удалены от равновесных значений. Если в нашей модели частицу удастся поместить в элементарную ячейку объема V_0, то при этом $S = 0$, а информация достигает своего максимального значения $I_{\max} = -\ln p_{\min} = \ln\frac{V}{V_0},$ поскольку вероятность p_{min} найти частицу в данной ячейке равна V_0/V. Если в последующие моменты времени частица начнет заполнять больший объем, то информация будет утрачиваться, а энтропия - расти. Подчеркнем, что за информацию нужно платить (по второму началу) увеличением энтропии S_e внешней системы, причем $\Delta S_e > I$. Действительно, если бы за один бит информации прибор (внешняя система) увеличивал свою энтропию на величину ΔS_e меньшую одного бита, то мы могли бы обратить тепловую машину. А именно, расширяя объем, занятый частицей, мы бы увеличивали ее энтропию на величину *ln2*, получая работу *Tln2*, а суммарная

энтропия системы частица плюс прибор уменьшилась бы. Но это невозможно по второму началу. Формально, $S_{e+syst} \geq S_{syst} + S_e$, поэтому уменьшение энтропии системы (частицы) ΔS_{syst} сопровождается увеличением энтропии прибора ΔS_e.

Итак, информационная энтропия - это мера недостатка (или степень неопределенности) информации о действительном состоянии физической системы.
Информационная энтропия Шеннона:
$H = \log_2 \Delta\Gamma = -\sum_n p_n \log_2 p_n$, где $\sum_n p_n = 1.$ (это относится к двухуровневым системам, типа бит: “0” и “1”. Если размерность равна *n*, то $H = log_n \Delta\Gamma$. Так, для $n = 3$, $H = log_3 \Delta\Gamma$ причем, $\Delta\Gamma = 3$.)

Количество информации *I* (или просто информация) о состоянии классической системы, получаемое в результате измерений внешним прибором, связанным с рассматриваемой системой некоторым каналом связи, определяется как разность информационной энтропии, соответствующей начальной неопределенности состояния системы H_0, и информационной энтропии конечного состояния системы после измерения *H*. Таким образом,

I + H = H₀ = const.

В идеальном случае, когда отсутствуют шумы и помехи, создаваемые внешними источниками в канале связи, конечное распределение вероятностей после измерения сводится к одному определенному значению $p_n = 1$, т.е. $H = 0$, а максимальное значение полученной при измерении информации будет определяться : $I_{max} = H_0$. Таким образом, информационная энтропия Шеннона системы имеет смысл максимальной информации, заключенной в системе; она может быть определена в идеальных условиях измерения состояния системы в отсутствие шумов и помех, когда энтропия конечного состояния равна нулю:

$H = 0$.

Рассмотрим классический логический элемент, который может находиться в одном из двух равновероятных логических состояний “0” и “1”. Такой элемент вместе с окружающей средой - термостатом и генерируемым внешним теплоизолированным объектом сигналом единую неравновесную замкнутую систему. Переход элемента в одно из состояний, например, в состояние “0”, соответствует уменьшению стат. веса его состояния по сравнению с начальным состоянием в 2 раза (для трехуровневых систем - в 3 раза). Найдем уменьшение *информационной энтропии* Шеннона, которое соответствует увеличению количества информации об элементе на единицу, которая называется *битом*:

$$\Delta H = -\Delta I = \log_2(\Delta\Gamma/2) - \log_2 \Delta\Gamma = \log_2(2/2) - \log_2 2 = -\log_2 2 = -1 \textit{бит.}$$

Следовательно, информационная энтропия определяет число битов, которое требуется для кодирования информации в рассматриваемой системе или сообщении.

ЛИТЕРАТУРА

1. Д.Ландау, И.Лифшиц. Статистическая физика. Часть 1. Наука, М 1976.
2. М.А.Леонтович. Введение в термодинамику. Статистическая физика. Москва, Наука, 1983. - 416с.
3. Б.Б.Кадомцев. Динамика и информация. УФН, 164, №5, 449 (1994).

Лекция 3.

1. Условная энтропия. Взаимная информация. Канал связи.
2. Сжатие классических данных. Типичные слова. Теорема Шеннона для незашумленного канала связи.
3. Двоичный симметричный канал связи. Емкость канала.
4. Коды, исправляющие ошибки. Код Хэмминга. Теорема Шеннона для зашумленного канала.

Обратимые логические операции. Универсальные ЛЭ Тоффоли и Фредкина.

(Из прошлой лекции - не успел)

Связь энтропии и информации.

Итак, информационная энтропия - это мера недостатка (или степень неопределенности) информации о действительном состоянии физической системы.

Информационная энтропия Шеннона:

$$H = \log_2 \Delta\Gamma = -\sum_n p_n \log_2 p_n, \text{ где } \sum_n p_n = 1. \qquad (1)$$

(это относится к двухуровневым системам, типа бит: “0” и “1”. Если размерность равна n, то $H = log_n \Delta\Gamma$. Так, для $n = 3$, $H = log_3 \Delta\Gamma$, причем, $\Delta\Gamma = 3$.)

В идеальном случае, когда отсутствуют шумы и помехи, создаваемые внешними источниками в канале связи, конечное распределение вероятностей после измерения сводится к одному определенному значению $p_n = 1$, т.е. $H = 0$, а максимальное значение полученной при измерении информации будет определяться : $I_{max} = H_0$. Таким образом, информационная энтропия Шеннона системы имеет смысл максимальной информации, заключенной в системе; она может быть определена в идеальных условиях измерения состояния системы в отсутствие шумов и помех, когда энтропия конечного состояния равна нулю:

$H = 0$.

Часто величину (1) называют информационным содержанием

Пусть X - случайная величина, принимающая значения $X = \{x_1, x_2 ... x_n\}$, а $p(x)$ - ее функция распределения. Тогда информационное содержание или информационная энтропия величины X:

$$H = \log_2 \Delta\Gamma = -\sum_x p(x) \log_2 p(x). \qquad (2)$$

Рассмотрим три примера.

Пример 1. Если мы знаем, что $X = 2$, то $p(2) = 1$ и в сумме (2) нет других слагаемых, то $H = 0$, т.е. информационное содержание величины X равно нулю.

Пример 2. Если величина X получается при подбрасывании кости с равновероятным распределением $p(x) = 1/6$ для $x \in \{1, 2, 3, 4, 5, 6\}$. Тогда $H = -\log_2\left(1/6\right) \approx 2.58$. Если X может принимать N различных значений, то ***информационное содержание величины X максимально, когда распределение вероятностей равномерное,*** т.е. $p(x) = 1/N$. Таким образом, для честной кости $H \cong 2.58$, а для нечестной, когда, например, $p(6) = 1/2$, $P(1, 2,...5) = 1/10$ получаем $H = 2.16$. Это утверждение можно строго доказать. Заметим, что оно сочетается с нашим пониманием физического смысла энтропии в том смысле, что информационное содержание (энтропия) максимально, если априорное знание об X минимально. Это свойство используется, например, в криптографии, где необходимо выбирать (неортогональные) базисы равновероятным образом.

Пример 3. Какое количество информации содержится в утверждении: “зимой холодно”? С одной стороны для жителей России в этом сообщении не содержится ничего нового - информация равна нулю. Однако, рассмотрим его с информационной точки зрения. Закодируем буквы русского алфавита (32 штуки с пробелом, без “ё”и без “й”) с помощью символов $\{x_n\}$. Например, с помощью таблицы:

а	б	в	г	д	е	ж	з	и	к	л	м	н	о	п	р	с
x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	x_9	x_{10}	x_{11}	x_{12}	x_{13}	x_{14}	x_{15}	x_{16}	x_{17}

т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я	_
x_{18}	x_{19}	x_{20}	x_{21}	x_{22}	x_{23}	x_{24}	x_{25}	x_{26}	x_{27}	x_{28}	x_{29}	x_{30}	$x3_1$	x_{32}

Тогда наше сообщение принимает вид

$$M_n = x_8x_9x_{12}x_{14}x_9x_{32}x_{21}x_{14}x_{11}x_{14}x_5x_{13}x_{14} \qquad (*)$$

Длина последовательности символов $\{x_n\}$ равна 13. Буква “о” (x_{14}) встречается 4 раза, поэтому $p(x_{14}) = 4/13 \approx 1/3$. Будем рассматривать последовательность (*) как функцию $M_n(X)$ случайной величин, где $X = \{x_k, p(x_k)\}$ принимает 32 значения с некоторыми вероятностями $p(x_k)$. (Здесь ошибка - буква “и” встречается два раза!)

Таким образом если в некотором сообщении, состоящем из *n* букв алфавита, содержащего *N* символов заданы вероятности $p(x_k)$ найти ту или иную букву x_n, то количество информации вычисляется как произведение число букв n на информацию, содержащуюся в одной букве *S(X)*:

$$S_n = nS(X) = -n\sum_k p(x_k)\log p(x_k).$$

В нашем примере *n* = 13, $p(x_{14}) = 4/13$, $p(x \neq x_{14}) = 1/13$, поэтому

$$S_n \approx -13\left[4/13*\log(4/13) + 9/13*\log(1/13)\right] \approx 13\left[4/13*1.71 + 9/13*3.7\right] \approx 13\left[0.53 + 2.56\right] = 40.2$$

.

Если бы мы взяли равновероятное распределение для появления буквы по всему алфавиту $p(x_k) = 1/32$ (что, конечно, не так!), то получили:

$$S_n = -13\left[\log 1/13\right] = 13\left[3.7\right] = 48.1 > 40.2$$

Заметим, что приведенный пример не вполне корректен. Мы использовали вероятность встретить ту или иную букву в коротком сообщении для малого числа n букв. На самом деле, необходимо брать длинные сообщения и использовать вероятности $p(x_k)$, характерные для всего русского языка.

Максимальная информация, которая может быть, в принципе, запасена в переменной, принимающей *N* различных значений, составляет $-\log_2\left(1/N\right) = \log_2(N)$ и достигается при равномерном распределении вероятностей. Выбор основания “2” у логарифма в теории информации обусловлен требованием *H(X)* = 1, когда *X* может принимать два значения с одинаковой вероятностью (*N* = 2). Двухуровневые переменные, таким образом, содержат единицу информации - *бит*, а величина *X*, принимающая два значения, называется бинарной.

Пусть для двухуровневой переменной X, вероятность того, что $X = 1$, равна p, а вероятность того, что $X = 0$ равна $1 - p$. Тогда информационная энтропия есть функция только p:

$$H = -p\log_2 p - (1-p)\log_2(1-p) \le 1. \quad (3)$$

Далее в этой лекции под $H(p)$ понимается именно энтропия бинарных сигналов.

Условная энтропия.

Рассмотрим условную вероятность $p(y|x)$ - вероятность того, что величина Y принимает значение y при условии, что величина X принимает значение x. Условной энтропией называется величина $S(Y|X)$:

$$S(Y \mid X) = -\sum_x p(x)\sum_y p(y \mid x)\log p(y \mid x) = -\sum_x \sum_y p(x,y)\log p(y \mid x) =$$

$$-\sum_x \sum_y p(x,y)\log\frac{p(x,y)}{p(x)} = S(X,Y) + \sum_x \sum_y p(x,y)\log p(x) = \quad (4)$$

$$S(X,Y) + \sum_x \log p(x)\sum_y p(x,y) = S(X,Y) + \sum_x \log p(x)p(x) = S(X,Y) - S(X)$$

где во втором равенстве использовано понятие совместной вероятности $p(x,y) = p(y \mid x)p(x)$ - есть вероятность того, что X принимает значение x, а Y принимает значение y. Также использовалось правило усреднения совместного распределения по лишним “переменным”: $\sum_y p(x,y) = p(x)$. Аналогично можно показать, что $S(X \mid Y) = S(X,Y) - S(Y)$. Кроме того, мы ввели энтропию совместного распределения:

$$S(X,Y) = -\sum_{x,y} p(x,y)\log p(x,y), \quad (4a)$$

Из определения (4) следует, что $S(Y|X)$ есть мера того, сколько информации, в среднем, оставалось бы в Y при условии, что мы бы знали X. Заметим, что всегда $S(Y|X) \le S(Y)$ и обычно $S(Y|X) \ne S(X|Y)$.

Понятие условной энтропии служит краеугольным камнем для другой величины - ***взаимной информации***, определяемой как

$$I(X:Y) = \sum_x \sum_y p(x,y)\log\frac{p(x,y)}{p(x)p(y)} = \sum_x \sum_y p(x,y)\log\frac{p(y \mid x)p(x)}{p(x)p(y)} =$$

$$\sum_x \sum_y p(x,y)\log p(y \mid x) - \sum_x \sum_y p(x,y)\log p(y) = -S(X \mid Y) + S(X) \quad . \quad (5)$$

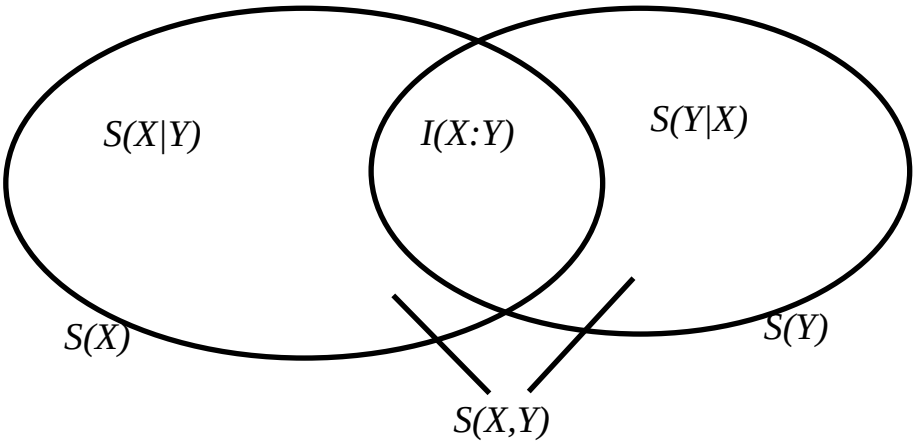
По определению величина $I(X:Y)$ есть мера того сколько информации содержат X и Y друг о друге. Например, если X и Y - независимые величины, то $p(x,y) = p(x)p(y)$, так что $I(X:Y) = 0$. Соотношения между основными мерами классической информации показаны на рисунке.

Можно показать, что $S(X,Y)$ - информационное содержание величин X и Y (информация, которую мы бы получили, если бы не зная ничего изначально, мы бы узнали значения X и Y) удовлетворяет

$S(X,Y) = S(X) + S(Y) - I(X:Y)$:

$$I(X:Y)=\sum_x\sum_y p(x,y)\log\frac{p(x,y)}{p(x)p(y)}=\sum_x\sum_y p(x,y)\log p(x,y)-$$

$$\sum_x\sum_y p(x,y)\log p(x)p(y)=-S(X,Y)+S(X)+S(Y)$$



Информация может исчезнуть, но она не может возникнуть из ничего. Этот важный факт отражается в математической формулировке “неравенства получения данных”:

$$\textit{если}\quad X\to Y\to Z,\quad \textit{то}\quad I(X:Z)\le I(X:Y)\le S(X). \qquad (6)$$

Символы со стрелками означают, что величины *X, Y, Z*, составляют марковский процесс, в котором *Z* зависит от *Y*, и не зависит непосредственно от *X*:

$p(x,y,z)=p(x)p(y\mid x)p(z\mid y)$.

Содержание “неравенства получения данных” состоит в том, что “data processor” *Y* может передать к *Z* информации не больше, чем он получил от *X*.

Сжатие данных (data compression)

Как доказать, что определение (1) служит хорошей мерой информации? На первый взгляд кажется непонятно, как разрешить эту задачу. Рассмотрим следующую простую ситуацию (см. рисунок).

Пусть некая персона *X* (традиционно ее зовут Алиса) хочет передать сообщение приятелю (его зовут Бобом). Ограничим себя только случаем, когда *X* имеет только два значения: “нет” и “да”. Мы говорим, что Алиса служит “источником” с “алфавитом” из двух символов. Алиса общается с Бобом посредством пересылки битов (нулей и единиц). Между Алисой и Бобом размещается “***канал связи***” - физическая система, передающая или преобразующая информацию. В качестве канала связи может выступать и логическое устройство.

Если *X* - дискретная случайная величина, принимающая значения на множестве $\Lambda=\{1,2...K\}$. Рассмотрим случайный источник (Алиса), который порождает последовательность независимых одинаково распределенных случайных величин с распределением *p*. Последовательность $\omega=(x_1,.....x_n)$ {всего *n* штук} букв алфавита K называется словом длины *n*. Общее число таких слов K^n. Например, K= {1, 2, 3}.

Пусть $n = 2$. Сколько всего слов, составленных из $n = 2$ символов 1, 2, 3? Очевидно их $3^2 = 9$ штук. Общее же число слов, составленных из n букв (символов) есть:

$$K^n = \left(2^{\log_2 K}\right)^n = 2^{n\log_2 K}.$$

Значит, чтобы закодировать все эти слова, используя двоичные последовательности, казалось бы что потребуется $n\log_2 K$ бит! (Если $K = \{0,1\} \to K = 2,\ K^n = 2^n$ - нужно n бит информации).

Однако есть лучший способ кодирования - сжатие данных - который использует то обстоятельство, что распределение p - неравномерная величина.

Будем измерять информационное содержание X, подсчитывая *в среднем* число битов, которое должна послать Алиса, для того чтобы Боб распознал X. Очевидно, она должна просто посылать “0” как “нет и “1” как “да”, обеспечивая “скорость битов” в один бит на X. Однако, что будет, если X является существенно случайной переменной, исключая случаи, когда нули идут чаще, чем единицы? Оказывается, что в этом случае Алиса может передавать сообщения Бобу более эффективно, используя следующую процедуру.

Пусть p - вероятность того, что $X = 1$ и $1 - p$ - вероятность того, что $X = 0$. Алиса ждет, пока n значений X будут готовы для того, чтобы их переслать (n - большое число). Среднее число единиц в такой последовательности n значений равно np. Это - наиболее вероятное число единиц в любой последовательности, которая содержит n символов, так что число единиц будет всегда близко к np. Пусть np - целое число. Найдем вероятность получения любой последовательности, содержащей np единиц. Это будет произведение того, что в последовательности есть np единиц (p^{np}) и того, что остальные элементы - $n(1-p)$ нули $\{(1-p)^{n(1-p)}\}$ - итого, $np + n - np = n$

$$p^{np}(1-p)^{n-np} = \left\{\textit{Используем соотношение } A = 2^{\log_2 A},\ \textit{где } A = p^{np}(1-p)^{n-np}\right\} =$$

$$= 2^{\log_2\left[p^{np}(1-p)^{n(1-p)}\right]} = 2^{np\log_2 p + n(1-p)\log_2(1-p)} \equiv 2^{-nH(p)}$$

где $H(p)$ - определена в (3) для двоичной кодировки. Такая последовательность называется *типичной последовательностью* или *типичным словом.* Более точно, определим типичное слово как последовательность, которая удовлетворяет условию

$$2^{-n(H(p)+\varepsilon)} \le p(\textit{слово}) \le 2^{-n(H(p)-\varepsilon)},$$

где $p(\textit{слово})$ - вероятность появления последовательности (слова) Т.е. типичная последовательность содержит наиболее вероятное число единиц (нулей).

Теперь можно показать, что вероятность образования типичной последовательности из n величин Алисы превосходит величину $1-\varepsilon$ для достаточно больших n, вне зависимости от того, насколько мало ε! ***Это означает, что Алисе не нужно передавать n бит Бобу для того, что бы он распознал n исходов***. Ей лишь нужно сказать Бобу *какова ее типичная последовательность*. Им нужно договориться заранее о том, как выделять (в смысле отмечать) эти типичные последовательности. Например, они могут нумеровать их в порядке увеличения бинарного значения. Алиса просто посылает свое обозначение (метку), но не саму последовательность.

Чтобы проследить, насколько хорошо работает этот метод можно показать, что все типичные последовательности имеют одинаковые вероятности и, следовательно, их существует $2^{nH(p)}$ штук. Для передачи одной из $2^{nH(p)}$ последовательностей, очевидно, Алиса должна послать $nH(p)$ бит. Ясно, что Алиса не может сделать ничего лучше этого (т.е. послать меньшее число бит) т.к. типичные последовательности равновероятны: никакой информации не может быть извлечено при дальнейших

манипуляциях. Поэтому информационное содержание или информационная энтропия каждого значения из множества *X* в оригинальной последовательности должно быть *H(p)*, что доказывает справедливость (2)!

Мы не вдаемся в математические детали доказательства. Отметим, лишь, что использован закон больших чисел, который гласит, что для произвольно малых ε и δ выполняется неравенство

$$P\left(\left|m-np\right|<n\varepsilon\right)>1-\delta$$

для достаточно больших *n*, где *m* - число единиц, содержащихся в последовательности длиной n. Для достаточно больших n число единиц *m* будет отличаться от среднего значения *np* на число как угодно малое по сравнению с *n*. Например, в рассмотренном выше случае нули и единицы будут распределены по биномиальному закону

$$P\left(n,m\right)=C\left(n,m\right)p^{m}\left(1-p\right)^{n-m}\approx\frac{1}{\sigma\sqrt{2\pi}}\exp\left\{-(m-np)^{2}\Big/2\sigma^{2}\right\},$$

где распределение Гаусса получается в пределе, когда *n, np* $\to\infty$, стандартное отклонение $\sigma=\sqrt{np(1-p)}$, а $C(n,m)=\dfrac{n!}{m!(n-m)!}$ - число сочетаний из *n* по m.

Все эти соображения, относящиеся к определению информационной энтропии (информационному содержанию) (2) имеют важное практическое значение. Оно состоит в том, что для передачи *n* значений величины *X* (определена на множестве {0, 1}) нам нужно послать через канал связи только $nH(X)\le n$ бит.

Этот алгоритм получил название *классического сжатия данных* или ***теоремы Шеннона для нешумящего канала связи.***

Пример. Пусть p = 1/4. Тогда по теореме Шеннона лучшее из того, что дает техника сжатия данных это передача каждого сообщения из четырех значений *X* посылкой в среднем $4H(1/4)\sim 3.245$ бит.

Техника сжатия данных нашла огромное применение в телекоммуникации. Например, при сжатии информации для передачи телевизионных изображений и сохранении их в памяти компьютера. С точки зрения инженерного дизайна канала связи сжатие данных может показаться фантастической техникой. Предположим у нас есть телефонная связь с гористой местностью, но скорость связи не очень высока для того, чтобы послать, скажем, видео-изображение. Обычное инженерное решение состоит в замене телефонной линии на более быструю, в то время как из теории информации следует, что можно использовать старую линию, но при условии (де)компрессии данных на одном из двух концов (компрессия на одном и декомпрессия на другом конце). Удивительно, что пригодность кабеля может быть улучшена “починкой” информации, а не самого кабеля.

Двоичный симметричный канал связи

До сих пор мы рассматривали случаи идеальной передачи сообщений посредством нешумящих каналов. Теорема Шеннона дает нам меру лучшей компрессии данных в условиях идеальной связи.

Теперь остановимся на случае передачи информации при наличии шума в канале. рассмотрим лишь простейшие случаи.

Предположим, что у нас имеется двоичный канал связи, т.е. когда Алиса посылает Бобу только нули и единицы. Нешумящий канал передает значения по схеме $0\to 0$ *и* $1\to 1$. Зашумленный канал иногда выдает нуль вместо единицы и наоборот.

Существует большое число разновидностей шума. Например, “инверсия бита” приводит к равновероятному перевороту бита $0 \to 1$ *и* $1 \to 0$. Иногда канал имеет тенденцию к релаксации, т.е. $1 \to 0$, в то время как обратный процесс $0 \to 1$ невозможен. Возможны случаи, когда такие процессы идут случайно от бита к биту или возникают и кончаются внезапно.

Очень важную разновидность шума представляет собой процесс, при котором воздействие на биты происходит независимо и ошибки возникают по схеме $0 \to 1$ *и* $1 \to 0$. Эти ошибки наиболее близки к реальным шумовым процессам. Если две ошибки $0 \to 1$ *и* $1 \to 0$ равновероятны, то канал связи называется ***двоичным симметричным каналом***. Такой канал характеризуется единственным параметром *p,* который есть просто вероятность ошибки на один посланный бит. Предположим, что Алиса посылает в канал сообщение *X*, а Боб получает зашумленное сообщение *Y*. Задача Боба состоит в оптимальном извлечении *X* из *Y*. Если *X* состоит из единственного бита, то Боб может использовать условные вероятности:

$0 \to 1$: $p\left(x = 0 \mid y = 1\right) = p$

$1 \to 0$: $p\left(x = 1 \mid y = 0\right) = p$

$0 \to 0$: $p\left(x = 0 \mid y = 0\right) = 1 - p$

$1 \to 1$: $p\left(x = 1 \mid y = 1\right) = 1 - p$

из которых можно найти *S(X|Y)* используя (3, 4):

$$S\left(X \mid Y\right) = -\sum_{x,y} p(x,y) \log p(x \mid y) = -\sum_{y} p(y) \sum_{x} p(x \mid y) \log p(x \mid y) = (\text{рассматриваем}$$

случай, когда вероятность появления нулей и единиц совпадает: $p(y) = 1/2$) =

$$-\frac{1}{2}\left[p(0 \mid 0) * \log p(0 \mid 0) + p(0 \mid 1) * \log p(0 \mid 1) + p(1 \mid 0) * \log p(1 \mid 0) + p(1 \mid 1) * \log p(1 \mid 1) \right] =$$

$p * \log p + (1 - p) * \log(1 - p)$ = *H(p)*. Тогда из определения (5) взаимной информации получаем:

$$I\left(X : Y\right) = -S\left(X \mid Y\right) + S\left(X\right) = -H(p) + S(X). \qquad (7)$$

Очевидно, что наличие шума в канале ограничивает информацию об Алисиной величине *X*, содержащейся в принятом Бобом сигнале *Y*. Кроме того из неравенства сжатия данных (6) Боб не может увеличить информацию об *X* манипулируя *Y*. Однако из (7) следует, что качество связи между Алисой и Бобом ***может улучшаться при росте S(X).*** Оказывается, что информация зависит как от свойств источника, так и от свойств канала. Было бы полезно ввести некую меру, характеризующую только канал связи для того чтобы знать насколько хорошо канал передает информацию. Такая величина называется ***емкостью канала связи***. Она определяется как максимальная взаимная информация *I(X:Y)* между входом и выходом, причем максимизация происходит по всем возможным источникам шума:

Емкость канала $C \equiv \max_{\{p(x)\}} I\left(X : Y\right)$ (8)

Емкость канала измеряется в битах на символ (или в битах на выходе на входной бит) и для двоичных каналов должна принадлежать интервалу $0 \le C \le 1$. Все это очень здорово, но определенная в (8) емкость не позволяет нам эффективно сравнивать каналы, поскольку процедура максимизации по источникам не вполне тривиальна. Определение емкости канала *C(p)* является одной из основных проблем теории

информации, но к счастью рассматриваемый случай симметричного бинарного канала достаточно прост. Из (7) и (8) можно вывести результат:

$$C(p) = 1 - H(p). \qquad (9)$$

При выводе (9) мы учли, что при передаче одного бита *S(X) = 1* ("0" или "1" могут появиться с равной вероятностью). Если же вероятность ошибки равна 0.5 (т.е. когда *p(x = 0) = p(x = 1) = ½),* то H(*1/2*) = 1 и информацию передать невозможно - сообщение полностью зашумляется!

Теорема Шенона для зашумленного канала связи утверждает, что при наличии шумов, которые описываются слагаемым $H(p)$ в (7) и (8), для увеличении взаимной информации нужно увеличивать *S(X)*, характеризующую источник информации.

Замечание. Из теоремы Шенона для зашумленного канала следует, что пропускная способность *C(p)* определяет оптимальную скорость передачи информации по каналу с шумом. Оказывается, что для сообщения, содержащего большое число букв *n,* вероятность ошибки приема оказывается порядка *1/n*, если передача идет со скоростью *C(p).* Эта вероятность стремится к нулю при $n \to \infty$.

Коды, исправляющие ошибки.

До сих пор мы интересовались тем как информация проходит по зашумленному каналу связи и как она теряется там. Алиса не может передать больше информации, чем *C(p)* на передаваемый символ. Предположим, что Боб обезвреживает мину, а Алиса, находясь на некоем расстоянии, кричит ему какой провод обрезать. Если она крикнет лишь один раз "режь синий провод", то не будет уверена в том, что он услышит ее правильно. Она будет повторять свои сообщения много раз, а Боб будет ждать пока не будет уверен, что получил правильное сообщение. Такой способ сообщений может быть достигнут даже через зашумленный канал. В этом примере можно добиться передачи желаемого сообщения жертвуя количеством передаваемой информации - число ошибок уменьшается при увеличении количества передаваемой информации. Рассмотрим более продвинутые стратегии.

Набор {0, 1} рассматривается как группа Галуа (GF(2)), в которой операции сложения, вычитания, умножения и деления выполняются по модулю 2 (т.е. 1 + 1 = 0). *n*- битовое слово (двоичное слово, состоящее из n битов) есть вектор, содержащий *n* компонент, например, 011 это вектор (0,1,1). Набор таких векторов образует векторное пространство относительно сложения, т.к., например, 011 + 101 значит (0,1,1) + (1,0,1) = (0 + 1,1 + 0,1 + 1) = (1,1,0) = 110 по стандартным правилам сложения векторов. Это аналогично выполнению операции XOR.

Эффект шума, действующего на слово *u*, можно записать в виде $u \to u' = u + e$, где вектор ошибки показывает какой бит в слове *u* перевернулся под действием шума. Например, *u* = 1001101 $\to$ *u'* = 1101110 можно переписать в виде *u'* = *u* + 0100011. Код, исправляющий ошибку, есть такой набор слов, что

$$u + e \neq v + f \quad \forall u,\ v \in C\left(u \neq v\right), \forall e, f \in E, \qquad (10)$$

где *E* - набор векторов ошибок, исправляемых кодом *C*, включая случай отсутствие ошибки (нулевой вектор *e* = 0). Чтобы использовать такой код Алиса и Боб договариваются какому кодовому слову *u* отвечает какое сообщение. Тогда Алиса будет посылать в канал только кодовые слова. Поскольку канал зашумлен, Боб получает не *u*, а *u* + *e*. Однако, Боб может однозначно извлечь *u* из *u* + *e* используя (10), т.к. по этому условию он не может принять слово *u* + *e* , если Алиса передаст какое-нибудь другое кодовое слово *v*.

Пример работы кода, исправляющего ошибки, приведен в таблице. Это т.н. код Хемминга. Обозначение [*n, k, d*] означает, что кодовые слова имеют длину *n* бит, всего

этих кодовых слов 2^k штук и все они отличаются друг от друга по крайней мере в d позициях. В силу некоей специфики условие (10) удовлетворяется для любой ошибки, которая воздействует не более чем на один бит. Другими словами, набор E исправляемых ошибок есть {0000000, 1000000, 0100000, 0010000, 0001000, 0000100, 0000010, 0000001}. Заметим, что E может содержать по крайней мере 2^{n-k} членов. Отношение k/n называется *нормой кода*, т.к. каждый блок из n передаваемых бит содержит k бит информации, т.е. k/n битов на бит.

Сообщение	Хаффман	Хамминг
0000	10	0000000
0001	000	1010101
0010	001	0110011
0011	11000	1100110
0100	010	0001111
0101	11001	1011010
0110	11010	0111100
0111	1111000	1101001
1000	011	1111111
1001	11011	0101010
1010	11100	1001100
1011	111111	0011001
1100	11101	1110000
1101	111110	0100101
1110	111101	1000011
1111	1111001	0010110

Левая колонка - 16 возможных 4-битовых сообщений. Две другие колонки-закодированные версии каждого сообщения. Код Хаффмана - сжатие данных. Наиболее часто встречающиеся сообщения имеют более короткую длину. Считается, что в каждом бите сообщения нули встречаются в три раза вероятнее, чем единице. Код Хемминга - исправляющий ошибки. Каждое кодовое слово отличается от всех других по крайней мере тремя позициями. Поэтому любая единичная ошибка может быть исправлена. Код Хемминга линеен: все слова даются линейными комбинациями 1010101, 0110011, 0001111, 1111111. Они удовлетворяют проверке четности 1010101, 0110011, 0001111.

Параметр d называется “минимальным расстоянием” кода. Он важен, когда кодируется сигнал в присутствии шума, действующего на биты независимо , как в двоичном симметричном канале. Код с минимальным расстоянием d может исправить все ошибки, действующие менее чем на $d/2$ бит передаваемого кодового слова и при шуме, действующем независимо на биты, это является наиболее вероятным набором ошибок. На самом деле вероятность, что n-битовое слово получит m ошибок дается биномиальным распределением, поэтому если код может исправить более чем среднее количество ошибок np, исправление будет вероятнее всего удачным.

Центральный результат классической теории информации состоит в том, что существует мощный исправляющий ошибки код:

> **теорема Шеннона**. Если норма кода удовлетворяет условию $k/n < C(p)$ и число битов n достаточно велико, то существует двоичный код, позволяющий осуществлять связь с произвольно малой вероятностью ошибки.

Здесь вероятность ошибки - это вероятность того, что происходит неисправленная ошибка, которая заставляет Боба неверно воспринять полученное слово. Теорема

Шеннона звучит очень многообещающе, поскольку из нее следует, что не нужно разрабатывать низкошумящие каналы, что является дорогостоящей и трудновыполнимой задачей. Вместо этого мы компенсируем шум техникой коррекцией ошибок при кодировании и раскодировании, т.е. используя аппарат теории информации.

В заключение - об универсальных (классических) логических элементах.
Логический элемент осуществляет логически обратимую операцию, если сигнал на входе может быть однозначно определен по сигналу на выходе. Фредкин и Тоффоли показали, что существует два (по крайней мере) универсальных ЛЭ, с помощью которых можно организовать произвольные логические операции в компьютере. Это логически полные ЛЭ Controlled-Controlled-NOT (Тоффоли) и Controlled SWAP (Фредкин).

ТОФФОЛИ

a	**b**	**c**	**a**	**b**	**c**
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

Операция “НЕ” по выходу “c”, когда на входах a, b - логические единицы.

ФРЕДКИН

a	**b**	**c**	**a**	**b**	**c**
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	1	0
1	1	0	1	0	1
1	1	1	1	1	0

входы b, c - обмениваются значениями, когда на входе a -логическая единица.

ЛИТЕРАТУРА

1. A.Steane, Quantum Computing. Quant-ph/9708022
2. А.С.Холево. Введение в квантовую теорию информации. Москва, 2002. МЦНМО, 2002. - 228 с.
3. В.Н.Горбачев, А.И.Жилиба Физические основы современных информационных процессов. Ст.-Петербург, Издательство “Петербургский институт печати”, 2004.

Лекция 4

Основные понятия квантовой теории информации

1. Описание состояний в квантовой механике. Волновая функция. Принцип суперпозиции. Чистые и смешанные состояния. Вычисление средних величин. Матрица и оператор плотности. Свойства матрицы плотности, ее размерность. Аналогия с классическими поляризационными состояниями. Линейные операторы.
2. Энтропия фон Неймана. Случаи чистых и смешанных состояний. Вычисление энтропии фон Неймана и Шеннона для двухуровневой системы.

В квантовой механике физическим величинам ставятся в соответствие операторы. Пусть f физическая величина (координата, энергия, энтропия). Зная волновую функцию системы, можно предсказать моменты физической величины, например, ее среднее значение:

$\langle f \rangle = \int d\vec{r} \Psi^*(\vec{r},t)\, \hat{f}\, \Psi(\vec{r},t)$.

Волновая функция составляет основу математического аппарата квантовой механики. Каждое состояние системы может быть описано в данный момент времени определенной комплексной функцией, например, координат Ψ(r). Квадрат модуля этой функции определяет распределение вероятностей значения координат: $|\Psi|^2 d\vec{r}$ - есть вероятность того, что произведенное над системой измерение обнаружит значение координат в элементе объема $d\vec{r}$ конфигурационного пространства (об измерении будет разговор в дальнейшем). Ψ - волновая функция или амплитуда вероятности была введена Э.Шредингером в 1926г.

Вообще, квантовый объект, т.е. величина f в зависимости от предыстории может оказаться в одном из трех типов состояний:

1) ***в собственном состоянии φ_n какого-нибудь оператора*** (например, энергии), когда априори известно, что

$\langle f \rangle = f_{nn} \equiv \int d\vec{r} \varphi_n^*\, \hat{f}\, \varphi_n$ и, следовательно, f не флуктуирует. В этом случае квантовые флуктуации отсутствуют и моменты величины f:

$\langle f^k \rangle = \langle f \rangle^k$

В частности $\langle f^2 \rangle = \langle f \rangle^2$ и дисперсия $\langle f^2 \rangle - \langle f \rangle^2 = 0$.

Например, состояние $|V\rangle$ в вертикально-горизонтальном базисе представляется однозначно $|V\rangle = 1|V\rangle + 0|H\rangle$, т.е. при измерении этого состояния с помощью поляризационного светоделителя, отсчеты будут регистрироваться ***только*** $|V\rangle$-детектором. Квантовые флуктуации, обусловленные вероятностной природой волновой функции отсутствуют.

2) ***в чистом состоянии*** Ψ, образованном суперпозицией или разложением в базисе векторов φ_n

$\Psi(r,t) = \sum_n b_n \varphi_n(r)$.

В этом случае принципиальными становятся квантовые флуктуации величины f, поскольку известны лишь вероятности $|b|^2$ измерить то или иное значение f_{nn}:

$$\left\langle f^k \right\rangle = \sum_n |b_n|^2 \left(f_{nn} \right)^k .$$

Например, состояние $\left| +45^0 \right\rangle = 1/\sqrt{2} \left\{ \left| H \right\rangle + \left| V \right\rangle \right\}$. Соответствующие вероятности зарегистрировать отсчет равны 50% - проявляются квантовые флуктуации.
Здесь уместно напомнить о т.н. принципе суперпозиции - одном из основных утверждений квантовой механики, на котором строятся многие понятия квантовой информации.

Принцип суперпозиции (Ландау, Лифшиц)
Пусть в состоянии с волновой функцией $\psi_1(r)$ некоторое измерение приводит с достоверностью к определенному результату (I), а в состоянии $\psi_2(r)$ - к результату (II). Тогда принимается, что всякая линейная комбинация ψ_1 *и* ψ_2, т.е. всякая функция вида $\alpha\psi_1 + \beta\psi_2$ (α и β - комплексные числа) описывает такое состояние, в котором то же измерение дает либо результат (I), либо результат (II). Этот принцип без труда можно объединить на случай *n* состояний.
Итак, суперпозиция функций $\alpha\psi_1 + \beta\psi_2$ снова дает чистое состояние с определенной волновой функцией. В таком состоянии среднее значение оператора $\hat{f}$ содержит интерференционный член:

$$\left\langle f \right\rangle = \int dr \psi^* f \psi = \left\{ \textit{где } \psi = \alpha\psi_1 + \beta\psi_2 \right\} = p_1 f_{11} + p_2 f_{22} + 2\,\mathrm{Re}\left(\alpha^* \beta f_{12} \right), \quad (1)$$

$$\textit{где} \quad p_i = |\alpha|^2; \quad f_{ij} = \int dr \psi_i^* f \psi_j$$

3) ***В смешанном состоянии***. В таком состоянии добавляется неполнота информации о волновой функции, которую дает некогерентная смесь волновых функций. При этом отсутствуют интерференционные члены - третье слагаемое в сумме (1). Матричные элементы f_{ij} содержат квантово-механическое усреднение $f_{ij} = \int dr \psi_i^* f \psi_j$. К нему добавляется классическое усреднение с помощью распределений P_i и обычных правил теории вероятностей при вычислении средних величин:

$$\left\langle \overline{f} \right\rangle = \sum_n P_n f_{ij}^{(n)} = \sum_n P_n \int dr \psi^{(n)*} f \psi^{(n)},$$

где P_n - действительные положительные числа, и $\sum_n P_n = 1$.

Чистые и смешанные состояния имеют тесную аналогию с когерентными и некогерентными полями в оптике. Так, когерентное сложение полей приводит к возведению в квадрат суммы полей, в то время как некогерентная смесь полей от двух независимых источников со случайными флуктуациями фаз - к сложению интенсивностей, т.е. квадратов модулей соответствующих полей.

Вычисление средних величин

Рассмотрим задачу вычисления средних значений физических величин в квантовой теории в общем случае смешанного состояния, когда имеется ансамбль чистых состояний, распределенных с классической функцией распределения *P*. При вычислении средних значений в каждом из чистых состояний, составляющих смесь, добавляется индекс "*i*":

$$\left\langle L^{(i)} \right\rangle = \int d\tau \psi^{(i)*} \hat{L} \psi^{(i)}, \quad (2)$$

где $d\tau$ - набор дифференциалов пространственных переменных. После квантово-механического усреднения с помощью волновой функции необходимо усреднять выражения (2) по классическому распределению вероятностей *P(i)*:

$$\left\langle \bar{L} \right\rangle = \sum_i P(i) \left\langle L^{(i)} \right\rangle . \qquad (3)$$

Таким образом, квантовый ансамбль подобен ансамблю Гиббса в статистической физике, который состоит из совокупности систем, распределенных с вероятностями *P(p,q)* по возможным состояниям системы.

В квантовой механике полагается. что P_1N систем ансамбля находится в состоянии Ψ_1, P_2N систем - в состоянии Ψ_2,..... P_iN систем - в состоянии Ψ_i, где N - общее число систем. Видно, что в смешанном состоянии волновая функция не определена, но имеется набор чисел P_i, определяющих вероятность того, что система находится в чистом состоянии Ψ_i.

Пусть соответствующее чистое состояние определяется конечным набором собственных функций какого-нибудь оператора (например, поляризации - это две ортогональные поляризации). Тогда произвольное чистое состояние:

$$\Psi^{(i)} = \sum_n a_n^{(i)} \Psi_n , \quad \sum_n a_n^{(i)} * a_n^{(i)} = 1. \qquad (*)$$

Вообще говоря $a_n = a_n(t)$. Векторы (волновые функции) Ψ_n называются базисными, а представление (*) - базисным или *n*-представлением.

Подставим эту волновую функцию в выражение для среднего значения (2):

$$L^{(i)} = \sum_{nn'} L_{nn'} a_n^{(i)} * a_{n'}^{(i)}, \quad \text{где} \quad L_{nn'} = \int \Psi *_n \hat{L} \Psi_{n'} d\tau$$

Усредним это выражение по статистическому ансамблю (3):

$$\left\langle \bar{L} \right\rangle = \sum_i P(i) \sum_{n,n'} L_{nn'} a *_n^{(i)} a_{n'}^{(i)} .$$

Тогда

$$\left\langle \bar{L} \right\rangle = \sum_{n,n'} L_{nn'} \rho_{n'n} = \sum_n \left(L\rho \right)_{nn}, \quad \textit{или}$$

$$\left\langle \bar{L} \right\rangle = Sp\left(L\rho \right) = Sp\left(\rho L \right), \ \rho_{nn'} = \sum_i P\left(i \right) a_n^{*(i)} a_{n'}^{(i)}$$

- сумма диагональных элементов. Здесь ρ: $\rho^{(i)}{}_{mn} = P_i a_m^{(i)} a_n^{(i)*}$ - квадратная матрица - матрица плотности, которая полностью задает смешанное состояние. Зная матрицу плотности, можно вычислять средние значения операторов. Иногда говорят об операторе плотности

$$\hat{\rho} = \sum_i P_i \hat{\rho}_i , \quad \rho_{mn} = a_m a_n * \qquad (4)$$

<u>Свойства матрицы плотности</u>

1. $\rho_{mn} = \rho *_{nm}$ - эрмитовость
2. $Sp(\rho) = 1$ - нормировка
3. $\left(\rho^2 \right)_{mn} = \rho_{mn}$ - только для чистых состояний (одно слагаемое в статистическом усреднении)
4. $0 \le \rho_{nn} \le 1$ - это следствие второго свойства.

<u>Замечание</u>. В энергетическом представлении диагональные элементы ρ_{nn} - населенности уровней, а недиагональные характеризуют степень корреляции

$\overline{a_m^* a_n}$ состояний n и m в статистическом ансамбле. Поэтому условие $Sp(\rho)=1$ эквивалентно “вероятность найти систему на каком-то уровне = 1”. В то же время если амплитуды состояний различных систем ансамбля содержат случайный фазовый множитель $a_n^{(i)} \sim \exp i\left(\varphi_n^{(i)}\right)$, то при $m \neq n$

$\rho_{mn} \sim \overline{\exp i\left(\varphi_m - \varphi_n\right)} = 0$

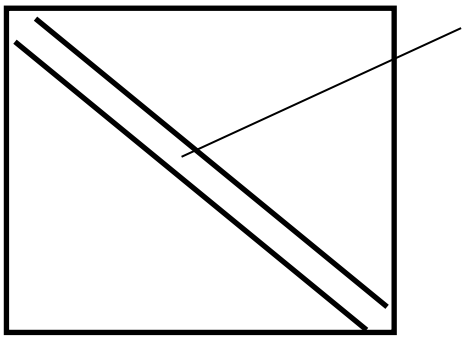
и состояние ансамбля полностью характеризуется населенностями состояний ρ_n.

Свойство $0 \le \rho_{nn} \le 1$ - неотрицательность вероятности. Свойство эрмитовости (1) - обеспечивает действительность наблюдаемых величин.

Из определения следует, что для чистого состояния $\rho_{nn}\rho_{mm} = \left|\rho_{nm}\right|^2$. Для смешанного состояния элементы матрицы плотности удовлетворяют неравенству Коши-Буняковского:

$\left|\rho_{nm}\right|^2 < \rho_{nn}\rho_{mm}$.

Размерность матрицы плотности.



n - диагональных элементов - действительные. Остается (n^2-n) - комплексных. Эрмитовость дает (n^2-n)/2 - комплексных, т.е.(n^2-n) действительных. Добавляем к ним n диагональных. Остается n^2 - действительных. Нормировка $Sp(\rho)=1$ дает n^2 - 1 действительных.

Если состояние чистое, то описание возможно с помощью волновой функции, отсюда - n комплексных чисел, $2n$ - действительных. Нормировка - $2n$ - 1. Общая фаза ВФ не важна - $2n$ - 2. Например, двухуровневая система:

$$\begin{pmatrix} a_1^2 & a_1 a_2 e^{i\varphi} \\ a_1 a_2 e^{-i\varphi} & 1-a_1^2 \end{pmatrix}. \quad \varphi_1 + \varphi_2 = \text{const}., \quad \varphi - \textit{относительная фаза}.$$

Два числа: a_1 *и* φ.

Если замкнутая система находится в одном из чистых энергетических состояний:

$\Psi = \varphi_1 \exp\left\{-i\,\mathrm{E}_1/\hbar\right\}$. (5)

Тогда из определения м.п. (4) лишь один ее элемент отличен от нуля: $\rho_{mn} = \delta_{mn}\delta_{n1}$.

Обычно свойство третье свойство матрицы плотности или матричное уравнение

$\hat{\rho}^2 = \hat{\rho}$ (6)

используется для проверки “чистоты” состояния. Другими словами, нарушение равенства (6) может служить признаком смешанного состояния. Однако существует другая более удобная мера смешанности квантовых состояний. Эта мера является статистической величиной и широко используется в квантовой информации - энтропия.

Энтропия фон Неймана

До сих пор мы говорили о классической энтропии или об энтропии Шеннона (информационное содержание). Эта характеристика показывает неопределенность, возникающую при описании с помощью классического распределения вероятностей. Обобщим это понятие на квантовый случай

Определим оператор энтропии через оператор плотности $\hat{\rho}$:

$\hat{S} \equiv -\ln\hat{\rho}$,

по аналогии с тем, как это делалось в статистической физике, где роль $\hat{\rho}$ играла функция распределения. тогда, очевидно, физическая величина “энтропия” или S есть среднее значение этого оператора $\langle\hat{S}\rangle$ или по правилам вычисления средних величин в квантовой механике:

$$S = -\langle\ln\hat{\rho}\rangle = -Sp(\hat{\rho}\ln\hat{\rho}). \qquad (7)$$

Встает вопрос, как вычислять логарифм оператора (например, недиагональные элементы матрицы плотности - вообще могут быть комплексными величинами, для которых логарифм не определен).

Некоторые полезные сведения о линейных операторах в квантовой теории.

1. Наблюдаемые и динамические величины представляются *линейными* операторами, т.е. линейными преобразованиями, связывающие два вектора (начальный и конечный). Если A - оператор, а $|\psi\rangle$ - вектор, то преобразованным вектором будет $A|\psi\rangle$. Этот преобразованный вектор в общем случае имеет другую длину и направление в гильбертовом пространстве.
2. Скалярное произведение этого преобразованного вектора на вектор $|\varphi\rangle$ будет $\langle\varphi|A|\psi\rangle$.
3. Операторы можно складывать, умножать на комплексное число - так получаются другие операторы.
4. Единичный оператор $\hat{I}$ оставляет все операторы без измерений.
5. Если для всех нормированных векторов $|\psi\rangle$ и $|\varphi\rangle$ выполняется $\langle\varphi|A|\psi\rangle \le b < \infty$, то оператор A называется ограниченным, а наименьшее значение b - нормой оператора A и обозначается $\|A\|$. В конечномерном гильбертовом пространстве каждый оператор ограничен; но это не так для бесконечномерного пространства.
6. Оператору А соответствует матрица $\{A_{mn}\}$ с элементами $A_{mn} = \langle m|A|n\rangle$ - m-ая компонента вектора $A|n\rangle$ для некоторого ортонормированного базиса $\langle m|n\rangle = \delta_{mn}$
7. Разложение единицы: $\hat{I} = \sum_{n=1}^{D} |n\rangle\langle n|$. Это верно для произвольного полного ортонормированного базиса $\{|n\rangle\}$.

Следствие. Вектор $A|\psi\rangle$ можно представить с помощью последовательности $\{(A\psi)_m\}$, где $\{(A\psi)_m\}$

$$\left(A\psi\right)_m = \left\langle m\middle|A\middle|\psi\right\rangle = \sum_{n=1}^{D}\left\langle m\middle|A\middle|n\right\rangle\left\langle n\middle|\psi\right\rangle = \sum_{n=1}^{D} A_{mn}\psi_n \ .$$

8. Оператор $A^\dagger$, ***сопряженный*** оператору *A*, определяется соотношением $\left\langle\varphi\middle|A^\dagger\middle|\psi\right\rangle = \left\langle\psi\middle|A\middle|\varphi\right\rangle^*$ - для всех ψ,φ.
9. ***Нормальным*** называется оператор, для которого $AA^\dagger = A^\dagger A$.Для них справедлива теорема о спектральном разложении: *Любой нормальный оператор M, определенный на векторном пространстве V, имеет диагональное представление в некотором базисе принадлежащем V*. Справедливо и обратное утверждение. Следствие: $M = \sum_n \lambda_n \left|n\right\rangle\left\langle n\right|$, где λ_n - собственные значения, а $\left|n\right\rangle$ - ортонормированный базис (на *V*).
10. ***Унитарным*** называется оператор, для которого $AA^\dagger = A^\dagger A = \hat{I} \to A^\dagger = A^{-1}$. Для унитарных операторов норма $\left\|A\psi\right\| = \left\|\psi\right\|$
11. ***Эрмитовым*** называется оператор A , для которого $A^\dagger = A$. Эрмитовы операторы - нормальные. Для эрмитовых операторов значение $\left\langle\varphi\middle|A\middle|\psi\right\rangle$ всегда действительно. Физическим величинам (наблюдаемым) соответствуют эрмитовы операторы. Эрмитов оператор *A*, удовлетворяющий условию $\left\langle\psi\middle|A\middle|\psi\right\rangle \geq 0$ для всех ψ называется положительным.
12. В конечномерном гильбертовом пространстве каждому эрмитовому оператору соответствует полный набор ортогональных собственных векторов и действительных собственных значений, для которых имеет место соотношение $A\left|a_n\right\rangle = a_n\left|a_n\right\rangle$. Если оператор положителен, то собственные значения неотрицательны. Важно заметить, что в представлении базиса $\left|a_n\right\rangle$ (в собственном представлении) оператор A диагонален, т.е. $\left\langle a_m\middle|A\middle|a_n\right\rangle = a_n\delta_{nm}$. В гильбертовом пространстве бесконечным числом измерений можно диагонализовать не каждый эрмитов оператор, даже если он ограничен.

Оказывается, что энтропия фон Неймана, определяемая через матрицу плотности, инвариантна относительно выбора базиса или представления. Тогда, переходя к диагональному представлению, получим:

$$S = -\sum_n \rho_n \ln\rho_n \ . \qquad (8)$$

В диагональном представлении элементы $\rho_n \equiv \rho_{nn}$ совпадают с собственными значениями матрицы.

Собственные значения матрицы находятся по правилу:

<u>*Напоминание:*</u> Пусть *A* - квадратная матрица *n* x *n*, тогда любой вектор *x*, из пространства V^n для которого выполняется $Ax = \lambda x$ называется собственным вектором, а λ - собственным значением матрицы. Это уравнение эквивалентно уравнению $(A-\lambda I)x = 0$. Это однородная система линейных уравнений. Нетривиальные решения имеются тогда, когда определитель равен нулю:

$det(A-\lambda I) = 0$. Или $\det\left\{a_{mn} - \delta_{mn}\lambda\right\} = \det A_{mn} = 0$, *где* $A_{mn} = a_{mn} - \delta_{mn}\lambda$.

Рассмотрим две ситуации.

1. *Чистое состояние*. В этом случае возможно описание квантовой системы с помощью волновой функции (*) в базисном представлении (т.е. В.Ф. - это когерентная суперпозиция базисных состояний какого-нибудь оператора):

$$\Psi^{(i)} = \sum_n a_n^{(i)} \Psi_n, \quad \sum_n a_n^{(i)} * a_n^{(i)} = 1.$$

В этом случае, конечно матрица плотности недиагональна. Наличие недиагональных элементов в базисном представлении как раз и отражает факт когерентности суперпозиции базисных состояний. Вообще же матрица плотности любой физической системы должна быть положительно определена, т.е. все ее собственные значения должны лежать в интервале [0,1]. Из теоремы о спектральном разложении следует, что матрица плотности может быть представлена в диагональном виде. Физически, это осуществляется при переходе к другому базису с помощью унитарных преобразований: $\tilde{A} = T * AT$. Таким образом, чистое состояние системы всегда может быть представлено в виде собственного состояния какого-нибудь оператора. Например, рассмотрим когерентную суперпозицию двух состояний или кубит:

$$\Psi = a|0\rangle + b|1\rangle, \ |a|^2 + |b|^2 = 1.$$

Пусть $a = b = 1/\sqrt{2}$. Полным аналогом такого состояния является состояние поляризации света, когда поляризация составляет угол 45^0 с вертикалью. Действительно, измерения поляризации отдельных фотонов в этом состоянии будут давать либо горизонтальную, либо вертикальную поляризации с вероятностью 1/2. В то же время. Измерения, проводимые в базисе $+45^0$ - всегда будут давать достоверный результат.

Эти рассуждения можно обобщить на случай произвольной (эллиптической) поляризации, когда в разложении волновой функции отличны от нуля два комплексных коэффициента.

Но в чистом состоянии (*), как было показано в примере[1], лишь один элемент матрицы плотности отличен от нуля, т.е. $\rho_n = 0$ *или* 1, а значит $S = 0$. Как было показано на предыдущих лекциях, равенство нулю энтропии интерпретируется как минимальная неопределенность (хаотичность). Вопрос: а когда неопределенность будет максимальна?

2. *Смешанное состояние*. Рассмотрим однородную смесь состояний: $\rho_n = \text{const.} = 1/\Gamma$, где, как обычно, Γ - число состояний с данной энергией, т.е. микроканонический ансамбль Гиббса.

В смешанном состоянии, как было показано выше, недиагональные элементы матрицы плотности равны нулю - матрица имеет диагональный вид с диагональными элементами $\rho_n = \text{const.} = 1/\Gamma$ [2].

Известно, что в диагональном представлении функции от операторов удовлетворяют соотношению:

---

[1] Матрицу плотности чистого состояния всегда можно привести к диагональному (или собственному) виду, когда лишь один диагональный элемент равен единице, а остальные диагональные элементы равны нулю (недиагональные элементы тоже равны нулю).

[2] Матрицу плотности смешанного состояния всегда можно привести к диагональному виду, но по диагонали будут стоять классические вероятности p_1.....p_n

$\left[F\left(\hat{f}\right)\right]_{nn} = F\left(f_{nn}\right)$, где функционал F в данном случае - логарифм.

Тогда, $\hat{\rho} = \hat{I}/\Gamma$, $\hat{\rho}^2 = \hat{I}/\Gamma^2$ и из (8) следует, что

$$S = -\sum_{n=1}^{\Gamma}(1/\Gamma)\ln(1/\Gamma) = \ln\Gamma .$$

Отсюда видно, что выполняется неравенство $0 \le S \le \ln\Gamma$.

Рассмотрим двухуровневую систему, когда волновая функция имеет вид:

$$\Psi = a|0\rangle + b|1\rangle . \qquad (9)$$

Такой волновой функцией описываются, например, электронные или ядерные спины, двухуровневые атомы и проч. Это объект, который называется кубит - квантовый бит. Пусть основному состоянию атома приписывается значение собственного вектора |0>, а возбужденному - собственный вектор |1> (или значение проекции на ось *z* спина). Эти векторы в квантовой механике записываются в виде столбцов|α> (α = 0, 1)

$$|0\rangle = \begin{pmatrix}1\\0\end{pmatrix}, \quad |1\rangle = \begin{pmatrix}0\\1\end{pmatrix}.$$

Собственные “бра” векторы <α| образуют эрмитово-сопряженные строки:

$\langle\alpha| = |\alpha\rangle^{+}$. Вектор состояния оканчивается на окружности единичного радиуса в двухмерном гильбертовом пространстве. Измерение такого состояния состоит в определении коэффициентов разложения, или проекций измеряемого состояния на базисные состояния:

$a = \langle 0|\Psi>,\ b = \langle 1|\Psi>$.

Собственному представлению оператора плотности двухуровневой системы, находящейся в чистом состоянии, соответствует диагональная матрица, выраженная через собственные векторы:

$$\hat{\rho}(\alpha) \equiv |\alpha\rangle\langle\alpha|,$$

причем двум возможным (собственным) состояниям отвечают следующие матрицы плотности:

$|0\rangle\langle 0| = \begin{pmatrix}1 & 0\\0 & 0\end{pmatrix}$, $|1\rangle\langle 1| = \begin{pmatrix}0 & 0\\0 & 1\end{pmatrix}$. (Видно, что $Sp\hat{\rho}(\alpha) = 1$). Т.о. для каждого α = 0, 1 у двухуровневой системы, находящейся в чистом состоянии, имеется только одно ненулевое значение матрицы, равное 1

Для смешанного состояния и выбранного базиса матрица плотности имеет диагональный вид, поскольку недиагональные элементы, отвечающие за “когерентность” суперпозиции (9) равны нулю:

$$\hat{\rho} = \sum_{\alpha} p_\alpha \hat{\rho}(\alpha) = \begin{pmatrix}p_0 & 0\\0 & p_1\end{pmatrix}, \quad \sum_{\alpha} p_\alpha = 1.$$

Отсюда сразу следует, что энтропия S совпадает с классической энтропией Шеннона случайной величины p_α. Забегая вперед, можно сказать, что энтропия фон Неймана совпадает с энтропией Шеннона.

Рассмотрим когерентную суперпозицию (9). Тогда вектор ее состояния:

$$|\Psi\rangle = a|0\rangle + b|1\rangle = \begin{pmatrix} a \\ b \end{pmatrix}$$

$$\langle\Psi| = a^*\langle 0| + b^*\langle 1| = \begin{pmatrix} a^* & b^* \end{pmatrix}$$

Матрица плотности этого чистого состояния уже недиагональна и в базисном представлении имеет вид:

$$\hat{\rho} = |\Psi\rangle\langle\Psi| = \begin{pmatrix} |a|^2 & ab^* \\ a^*b & |b|^2 \end{pmatrix}. \qquad (10)$$

Составим уравнение для собственных значений матрицы (10):

$$\det(A-\lambda I) = \det\begin{pmatrix} |a|^2-\lambda & ab^* \\ a^*b & |b|^2-\lambda \end{pmatrix} = (aa^*-\lambda)(bb^*-\lambda) -$$

$$(ab^*)(a^*b) = 0. \rightarrow aa^*bb^* + \lambda^2 - \lambda(aa^* + bb^*) - (ab^*)(a^*b) = \lambda^2 - \lambda = 0$$

и, тогда $\lambda_{1,2} = 0,1$.

Этот результат носит общий характер в силу произвольности выбора рассматриваемого чистого состояния (9) - собственные значения матрицы плотности чистого состояния (размерности d) равны: $\lambda_n (n = 2,...d) = 0,\ \lambda_1 = 1$.

Далее, найдем энтропию Шеннона чистого состояния суперпозиции (9), исходя из формального определения, в котором фигурируют некие вероятности. Она похожа (совпадает) с энтропией смешанного состояния с заданными классическими вероятностями заполнения или населенностями $\rho_{00} = |a|^2$, $\rho_{11} = |b|^2 = 1 - |a|^2$, поскольку не учитывает вклада недиагональных членов

$\rho_{01} = \rho^*_{10} = ab^*$. Итак, энтропия Шеннона оказывается:

$$H\left(|a|^2\right) = -|a|^2 \log_2 |a|^2 - \left(1-|a|^2\right)\log_2\left(1-|a|^2\right).$$

Максимальное значение эта величина достигает при $|a|^2 = |b|^2 = \frac{1}{2}$,

когда $\rightarrow$ $H = \log_2 2 = 1$ *бит*.

Отметим, что отличие матрицы плотности чистого состояния от смешанного состоит в том, что матрица плотности чистого состояния имеет только одно ненулевое собственное значение, равное единице, в то время как для смешанного состояния у матрицы плотности отличны от нуля несколько собственных значений - т.н. парциальные (т.е. взвешенные с классическими вероятностями) населенности соответствующих чистых состояний.

Энтропия фон Неймана, определяемая через матрицу плотности, согласно (8), в отличие от энтропии Шеннона, инвариантна относительно выбора представления матрицы плотности. Из (8) видно, что

$$S = -\sum_n \rho_n \ln \rho_n, \quad \textit{где} \quad \lambda_n = 0,1 \rightarrow \ S(\rho) = 0 < H.$$

Таким образом, кодирование информации в суперпозиционных состояниях вида $\Psi = a|0\rangle + b|1\rangle$ бессмысленно - их информационное содержание равно нулю. Кодирование с помощью чистых ортогональных состояний $|0\rangle,\ |1\rangle$ не дает ничего

нового в информационном смысле по сравнению с классической кодировкой. Остается одна возможность - кодирование при помощи чистых и неортогональных состояний. В канал запускается смесь таких состояний (с вероятностями $p_1....p_n$); их информационное содержание $S(\rho) \le H$.

Приложения. (необязательно)

В квантовой механике доказывается, что любой эрмитов оператор, действующий в гильбертовом пространстве двухуровневой системы, можно представить в виде суммы:

$$\hat{f} = aI + b\sigma_x + c\sigma_y + d\sigma_z , \qquad (П1)$$

где *a, b, c, d* - вещественные числа, а $\sigma_{x,y,z}$ - операторы Паули:

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Операторы Паули удовлетворяют следующим коммутационным соотношениям:

$$\sigma_x\sigma_y = -\sigma_y\sigma_x = i\sigma_z,$$

$$\sigma_y\sigma_z = -\sigma_z\sigma_y = i\sigma_x, \quad \sigma_\alpha = I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\sigma_z\sigma_x = -\sigma_x\sigma_z = i\sigma_y.$$

Подставляя выражения для операторов Паули в разложение для *f*, находим:

$$\hat{f} = \begin{pmatrix} a+d & b-ic \\ b+ic & a-d \end{pmatrix}. \qquad (П2)$$

Часто разложение для *f* пишут в другом (эквивалентном) виде:

$$\hat{f} = \frac{1}{2}\left(I + a_x\sigma_x + a_y\sigma_y + a_z\sigma_z\right) \equiv \frac{1}{2}\begin{pmatrix} 1+a_z & a_x+ia_y \\ a_x-ia_y & 1-a_z \end{pmatrix} = \frac{1}{2}\left(\hat{I} + a\hat{\sigma}\right). \qquad (Ё)$$

Заметим, что коэффициенты разложения (П1) произвольного оператора *f* по матрицам Паули имеют непосредственный физический смысл. Они определяют *два разрешенных значения*, которые принимает наблюдаемая *f* при отдельных измерениях (проблема измерений квантовых состояний - будет рассмотрена ниже). Составим уравнение для собственных значений (П2):

$$\det(A-\lambda I) = \begin{pmatrix} (a+d)-\lambda & (b-ic) \\ (b+ic) & (a-d)-\lambda \end{pmatrix} = (a+d-\lambda)(a-d-\lambda) -$$

$$(b+ic)(b-ic) = 0$$

и, тогда

$$\lambda_{1,2} = a \pm \sqrt{d^2+b^2+c^2} .$$

ЛИТЕРАТУРА:

1. К.А.Валиев, А.А.Кокин Квантовые компьютеры: надежда и реальность. Ижевск: НИЦ “Регулярная и хаотическая динамика”, 2001. - 352 с.

2. Д.Н.Клышко. Физические основы квантовой электроники. Москва, Наука, 1986, 293с.

Лекция 5

II. Основные понятия квантовой теории информации (продолжение)

1. Энтропия фон Неймана, ее неотрицательность, максимальное значение. Квантовая относительная энтропия. Неравенство Клейна.
2. Композиционные системы. Субаддитивность и вогнутость энтропии. Энтропия смеси состояний. Совместная энтропия. Условная энтропия. Взаимная информация. Примеры. Различие между классической и квантовой информацией.
3. Достижимая информация.
4. Теорема о запрете клонирования квантовых состояний. Ее связь с достижимой информацией.

На прошлых лекциях было введено понятие классической (Шенноновской) и квантовой (фон Неймана) энтропий. Шенноновская энтропия (далее будем обозначать ее буквой *H*) дает меру неопределенности, связанную с **классическим** распределением вероятностей. Квантовые состояния описываются схожим образом, только вместо распределения вероятностей используются операторы плотности. Важно, что квантовые состояния могут быть неортоганальными. Мы определили энтропию фон Неймана квантового состояния ρ соотношением:

$$S(\rho) \equiv -Sp\left(\rho \log \rho\right). \qquad (5.1)$$

Напомним, что в теории информации логарифмы принято брать по основанию “2” (а в статистической физике - по основанию “e” - “наты”).

Если λ_x - собственные значения матрицы плотности ρ, то выражение (5.1) для энтропии фон Неймана можно переписать по-другому:

$$S(\rho) \equiv -\sum_x \lambda_x \log \lambda_x, \qquad (5.2)$$

где, как обычно, считается, что *0 log0 ≡ 0* (как и для Шенноновской энтропии). При вычислениях удобнее пользоваться последней формулой. Например, как было показано на прошлой лекции для полностью смешанного состояния в *N*-мерном пространстве энтропия равна log*N*.

Пример. Сравнение квантовой и классической энтропии. Вычислим энтропию смеси состояний

$\rho = p|0\rangle\langle 0| + (1-p)\dfrac{\left(|0\rangle+|1\rangle\right)\left(\langle 0|+\langle 1|\right)}{2}$. (Сравнить результат с Шенноновской энтропией *H(p, 1-p)*). Приведенное состояние есть проектор (с вероятностью *p*) на состояние $|0\rangle$ или (с вероятностью *1-p*) на состояние $\left|45^0\right\rangle = 1/\sqrt{2}\left(|0\rangle+|1\rangle\right)$.

Решение.

Учтем, что

$$|0\rangle\langle 0| = \begin{pmatrix}1\\0\end{pmatrix}\begin{pmatrix}1 & 0\end{pmatrix} = \begin{pmatrix}1 & 0\\0 & 0\end{pmatrix}, \qquad |1\rangle\langle 1| = \begin{pmatrix}0\\1\end{pmatrix}\begin{pmatrix}0 & 1\end{pmatrix} = \begin{pmatrix}0 & 0\\0 & 1\end{pmatrix},$$

$$|0\rangle\langle 1| = \begin{pmatrix}1\\0\end{pmatrix}\begin{pmatrix}0 & 1\end{pmatrix} = \begin{pmatrix}0 & 1\\0 & 0\end{pmatrix}, \qquad |1\rangle\langle 0| = \begin{pmatrix}0\\1\end{pmatrix}\begin{pmatrix}1 & 0\end{pmatrix} = \begin{pmatrix}0 & 0\\1 & 0\end{pmatrix}.$$

$$\rho = p\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}+\frac{1-p}{2}\left[|0\rangle\langle 0|+|0\rangle\langle 1|+|1\rangle\langle 0|+|0\rangle\langle 1|\right]=$$

Тогда $$= p\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}+\frac{1-p}{2}\left[\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}+\begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix}+\begin{pmatrix}0 & 0\\ 1 & 0\end{pmatrix}+\begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}\right]=$$

$$= p\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}+\frac{1-p}{2}\left[\begin{pmatrix}1 & 1\\ 1 & 1\end{pmatrix}\right]=\begin{pmatrix}\frac{1+p}{2} & \frac{1-p}{2}\\ \frac{1-p}{2} & \frac{1-p}{2}\end{pmatrix}.$$

Ур-ие на собственные значения:

$$\left(\frac{1+p}{2}-\lambda\right)\left(\frac{1-p}{2}-\lambda\right)-\left(\frac{1-p}{2}\right)^2=0$$

$$\lambda_{1,2}=\frac{1\pm\sqrt{p^2-(1-p)^2}}{2}$$

Пусть, например, p = 1/2. Тогда $\lambda_{1,2}=0.854;\ 0.146$

$$H(p,1-p)=-\left(\frac{1}{2}\log_2\frac{1}{2}+\frac{1}{2}\log_2\frac{1}{2}\right)=1\textit{бит}.$$

$$S(1/2)=S(p=1/2)=-\left[0.854\log_2(0.854)+0.146\log_2(0.146)\right]\approx$$

$$0.854*0.24+0.146*2.8\approx 0.21+0.41\approx 0.6<1\textit{бит}$$

(Видно, что *S*, вычисленная из последней матрицы отличается от *H(p, 1-p)*).

<u>Квантовая относительная энтропия.</u>

Как и для энтропии Шеннона, полезно ввести квантовый аналог относительной энтропии. Пусть ρ и σ -два оператора плотности. Относительная энтропия состояний (операторов) ρ и σ (ρ относительно σ) называется величина:

$$S(\rho\|\sigma)\equiv Sp(\rho\log\rho)-Sp(\rho\log\sigma)=-S(\rho)-Sp(\rho\log\sigma). \qquad (5.3)$$

Как и соответствующая классическая величина, квантовая относительная энтропия может принимать бесконечные значения.

Так, относительная энтропия определяется как бесконечная, если *ядро* (*kernel*) оператора σ (векторное пространство собственных векторов σ с нулевыми собственными значениями) имеет нетривиальное пересечение с *основанием* (*support*) оператора ρ (векторное пространство образованное собственными векторами ρ с ненулевыми собственными значениями). В других случаях относительная энтропия конечна.

Квантовая относительная энтропия неотрицательна (неравенство Клейна):

$$S(\rho\|\sigma)\geq 0, \qquad (5.4)$$

равенство достигается, когда ρ = σ.

Перечислим основные свойства энтропии фон Неймана.

1. Энтропия неотрицательна. Она принимает нулевые значения только для чистых состояний (доказательство следует из определения).
2. В *N* - мерном гильбертовом пространстве максимальное значение энтропии log*N*. Энтропия равна log*N* только если система находится в (полностью) смешанном состоянии *I/N*.

3. Предположим, что композиционная система *AB* находится в чистом состоянии. Тогда *S(A) = S(B).*
4. Предположим, что p_i - это вероятности, а состояние ρ - раскладывается по собственным векторам с ненулевыми собственными значениями (имеют *основание)* в ортогональном базисе. Тогда

$$S\left(\sum_i p_i\rho_i\right) = H\left(p_i\right) + \sum_i p_i S\left(\rho_i\right).$$

Док-во. Пусть λ_i^j и $\left|e_i^j\right\rangle$ - собственные значения и собственные векторы состояния ρ_i (в прошлой лекции было использовано инверсное обозначение верхних и индексов, но по-прежнему, i нумеровал классическую выборку, а j – собственные векторы). Видно, что $p_i\lambda_i^j$ и $\left|e_i^j\right\rangle$ - собственные значения и собственные векторы состояния $\sum_i p_i\rho_i$, поэтому

$$S\left(\sum_i p_i\rho_i\right) = -\sum_{i,j} p_i\lambda_i^j \log p_i\lambda_i^j = -\sum_i \lambda_i^j \sum_j p_i \log p_i - \sum_j p_i \sum_i \lambda_i^j \log \lambda_i^j =$$

$$H\left(p_i\right) + \sum_i p_i S(\rho_i).$$

Видно, что если ρ_I – чистые состояния, то $S \to H\left(p_i\right)$

5. Теорема о совместной энтропии: Предположим, что p_i - вероятности, $\left|i\right\rangle$ - ортогональные состояния для системы A и ρ_i - любой набор операторов плотности для другой системы B, Тогда

$$S\left(\sum_i p_i \left|i\right\rangle\left\langle i\right| \otimes \rho_i\right) = H\left(p_i\right) + \sum_i p_i S\left(\rho_i\right).$$

(Доказывается аналогично (4)).

6. Субаддитивность энтропии . Пусть различные квантовые системы A и B имеют общее состояние ρ^{AB}. Тогда совместная энтропия для двух систем удовлетворяет следующим неравенствам:

$S\left(A,B\right) \le S(A) + S(B)$ - причем равенство имеет место только если системы А и В некоррелированы, т.е. $\rho^{AB} = \rho^A \otimes \rho^B$

$S\left(A,B\right) \ge \left|S(A) - S(B)\right|$ - т.н. неравенство треугольника или Араки-Льеба. Это, фактически, квантовый аналог неравенства $H(X,Y) \ge H(X)$ для энтропии Шеннона.

7. Вогнутость энтропии. Пусть p_i - неотрицательные действительные числа, такие, что $\sum_i p_i = 1$, а ρ_i - соответствующие операторы плотности. Тогда энтропия удовлетворяет неравенству:

$S\left(\sum_i p_i\rho_i\right) \ge \sum_i p_i S\left(\rho_i\right)$ - следует из св-ва (4).

Интуитивно ясно, что $\sum_i p_i \rho_i$ выражает состояние квантовой системы, которая находится в неизвестном состоянии ρ_i с вероятностью p_i. Неопределенность нашего знания о такой смеси состояний должна быть больше, чем средняя неопределенность состояний ρ_i, поскольку состояние $\sum_i p_i \rho_i$ дает вклад в неопределенность не только из-за наличия состояний ρ_i но и благодаря усреднению по индексу i.

8. Энтропия смеси квантовых состояний. Обратная сторона условия вогнутости проявляется в некоей полезной теореме, дающей верхнюю границу для энтропии смеси квантовых состояний. А именно, что для смеси $\sum_i p_i \rho_i$ квантовых состояний ρ_i выполняется следующее неравенство:

$$\sum_i p_i S(\rho_i) \le S\left(\sum_i p_i \rho_i\right) \le \sum_i p_i S(\rho_i) + H(p_i)$$

Что можно сказать о верхней границе или о правой части неравенства? Интуитивно ясно, что неопределенность состояния $\sum_i p_i \rho_i$ не может быть больше, чем средняя неопределенность состояния ρ_i плюс дополнительный вклад за счет $H(p_i)$, который представляет собой максимально возможный вклад в неопределенность об индексе i в общую неопределенность. Сформулируем теперь теорему о верхней границе

Теорема. Предположим, что $\rho = \sum_i p_i \rho_i$, где p_i - некоторый набор вероятностей, а ρ_i - операторы плотности. Тогда

$$S(\rho) \le \sum_i p_i S(\rho_i) + H(p_i), \qquad (**)$$

причем равенство достигается, если состояния ρ_i образуют ортогональный набор.

По аналогии с классическим случаем (энтропия Шеннона) для композиционных систем можно определить *квантовые совместную* и *условную энтропии*, а также *квантовую взаимную информацию*. ***Совместная энтропия*** *S(A, B)* для композиционной системы, состоящей из двух компонент *A* и *B*, определяется как и в классике:

$$S(A,B) \equiv -Sp\left(\rho^{AB} \log\left(\rho^{AB}\right)\right), \qquad (5.5)$$

где ρ^{AB} - матрица плотности системы *AB*. Напоминание:

в классике условной энтропией называлась величина

$$S(Y \mid X) = -\sum_x p(x) \sum_y p(y \mid x) \log p(y \mid x) = -\sum_x \sum_y p(x,y) \log p(y \mid x), \qquad (+)$$

где во втором равенстве использовано понятие совместной вероятности $p(x,y) = p(y \mid x) p(x)$ - есть вероятность того, что *X* принимает значение *x*, а *Y* принимает значение *y*.

Из определения (+) следует, что *S(Y|X)* есть мера того, сколько информации, в среднем, оставалось бы в *Y* при условии, что мы бы знали *X*. Заметим, что всегда $S(Y|X) \le S(Y)$ и обычно $S(Y|X) \ne S(X|Y)$. (конец напоминания)

Определим ***условную энтропию***, как

$$S(A|B) \equiv S(A,B) - S(B). \qquad (5.6)$$

Определим ***взаимную информацию***, как

$$S(A:B) \equiv S(A) + S(B) - S(A,B) = S(A) - S(A|B) = S(B) - S(B|A). \qquad (5.7)$$

Некоторые свойства энтропии Шеннона не переносятся на энтропию фон Неймана и отсюда следуют интересные следствия квантовой теории информации. Например, для случайных переменных *X* и *Y* имеет место неравенство: $H(X) \le H(X, Y)$. Интуитивно, это понятно: не может быть большей неопределенности состояния *X*, чем для совместного состояния *X* и *Y*. Это интуитивное понимание не годится для квантовых состояний. Рассмотрим систему *AB* двух кубитов в перепутанном состоянии :

$$\left(|00\rangle + |11\rangle\right)/\sqrt{2}. \qquad (*)$$

Это чистое состояние, поэтому *S(A, B) = 0*. С другой стороны, система *A* имеет оператор плотности *I/2* (*I* - единичный оператор) и поэтому ее энтропия равна единице. Действительно, волновой функции состояния системы *A* (или *B*)(*) не существует, это состояние максимально смешанное. Другой способ озвучивания этого результата состоит в том, что для этой системы величина (условная энтропия) $S(B|A) \equiv S(A,B) - S(A)$ - отрицательная. Это соотношение может трактоваться как критерий перепутывания: Если |*AB*> - чистое состояние композиционной системы, то |*AB*> находится в перепутанном состоянии если и только если *S(A|B) < 0*.

$$|\Psi\rangle_{AB}\langle\Psi|_{AB} = \frac{1}{2}\left\{\left(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B\right)\otimes\left(\langle 0|_A\langle 0|_B + \langle 1|_A\langle 1|_B\right)\right\} =$$

$$\frac{1}{2}\left\{|0\rangle_A|0\rangle_B\otimes\langle 0|_A\langle 0|_B + |0\rangle_1|0\rangle_B\otimes\langle 1|_A\langle 1|_B\right\} + \qquad (12.5)$$

$$+\frac{1}{2}\left\{|1\rangle_B|1\rangle_B\otimes\langle 0|_A\langle 0|_B + |1\rangle_A|1\rangle_B\otimes\langle 1|_A\langle 1|_B\right\}$$

Тогда

$$\rho_2 = Sp_1(\rho_{12}) = \frac{1}{2}\left\{|V\rangle_2\langle V|_2 + |H\rangle_2\langle H|_2\right\}, \qquad (12.6)$$

т.е. представляет собой взвешенную смесь. Следовательно, состояние второй подсистемы нельзя описывать волновой функцией; оно не является полностью определенным. Аналогично, матрица плотности первой подсистемы находится как след по индексам второй подсистемы:

$$\rho_1 = Sp_2(\rho_{12}) = \frac{1}{2}\left\{|V\rangle_1\langle V|_1 + |H\rangle_1\langle H|_1\right\}. \qquad (12.7)$$

Классическая теория информации, в основном, затрагивает проблему пересылки классических сообщений - букв алфавита, текстов, строк битов - через каналы связи, которые работают в соответствии с законами классической физики. Как изменится картина, если будут использоваться квантовые каналы связи? Можно ли передать информацию более эффективно? Можно ли использовать законы квантовой механики для того, чтобы передавать секретную информацию, защищенную от

подслушивания? Такого рода вопросы возникают, когда мы используем каналы связи, работающие по законам квантовой механики. Такое переопределение того, что же есть канал связи вызвано необходимостью переосмысления основных положений классической теории информации .

Квантовая теория информации нацелена на исследование каналов связи, но она имеет гораздо более широкую область применения. Можно обозначить три фундаментальные цели, которые стоят перед теорией квантовой информации:

- идентифицировать элементарные классы статических ресурсов в квантовой механике (или типы "информации")
- идентифицировать элементарные классы динамических процессов в квантовой механике (или типы информационных процессов)
- характеризовать ресурсы, с помощью которых можно реализовать элементарные динамические процессы.

Оказывается, что квантовая теория информации гораздо глубже и богаче классической теории информации потому, что квантовая механика включает в себя гораздо больше элементарных классов статических и динамических ресурсов, которые не просто соответствуют известным классическим типам, но и описывают целые новые типы состояний, например, перепутанные состояния, которые не имеют аналога в классике.

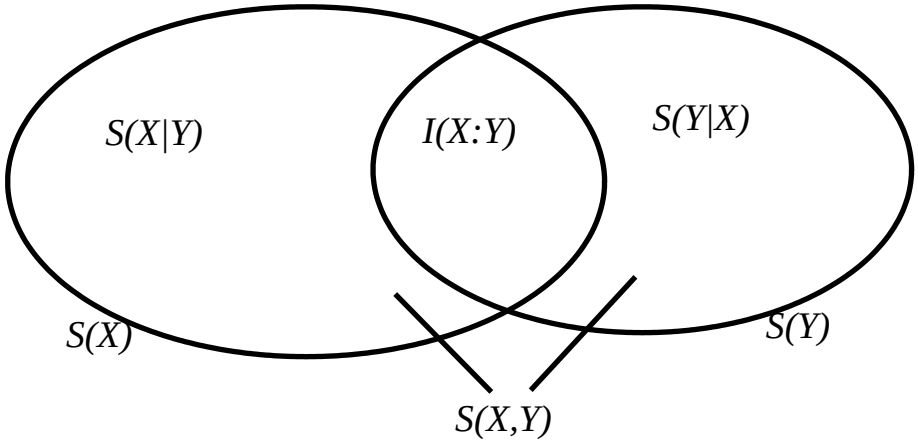
Рассмотрим на некоторых примерах разницу в описании между квантовой и классической информацией.

Принцип соответствия. "Законы квантовой физики должны быть сформулированы таким образом, что в классических границах, когда в процесс вовлечено много квантов, эти законы приводили бы к классическим уравнениям для усредненных величин." (Д.Бом. Квантовая теория)

Предположим, что Алиса имеет классический источник информации, который выдает символы $X = 0, \ldots n$ с соответствующим распределением вероятностей $p_0, \ldots, p_n$. Цель Алисы и Боба состоит в том, чтобы Боб смог определить величину X наилучшим образом. Для того, чтобы достигнуть этого. Алиса приготавливает квантовое состояние ρ_X выбирая его из некоторого фиксированного набора $\rho_0, \ldots \rho_n$, и посылает это состояние Бобу, который выполняет квантовое измерение над этим состоянием. Затем, он пытается сделать лучшее предположение о том, как идентифицировать X, основываясь над результатах своих измерений Y.

Хорошей мерой того, сколько информации получено Бобом о величине X из его измерений - это взаимная информация между X и результатом измерения Y. Мы помним из предыдущих лекций, что Боб может сделать заключение об X по результатам измерения Y только, если и только если $H(X:Y) = H(X)$, и что в общем случае $H(X:Y) \leq H(X)$. Далее мы покажем, что близость величины $H(X:Y)$ к $H(X)$ не самом деле дает хорошую меру того, как Боб смог определить X. Цель Боба - выбрать измерение, которое максимизирует величину $H(X:Y)$ и тем самым приближая ее к $H(X)$. Для этого, определим *достижимую информацию* (*accessible information*), как максимальную величину *взаимной информации*. **Достижимая информация - это мера того, насколько хорошо Боб смог сделать вывод о приготовленном Алисой состоянии, которая она послала ему.**

КЛАССИКА (см. лекцию 3)



Квантовая информация	Классическая информация
Условная энтропия: $S(A\|B) \equiv S(A,B) - S(B).$ МОЖЕТ БЫТЬ ОТРИЦАТЕЛЬНОЙ!!	Условная энтропия: $H(A\|B) \equiv H(A,B) - H(B).$ $H(B\|A) \le H(B)$
Совместная энтропия: $S(A,B) \equiv -Sp\left(\rho^{AB} \log\left(\rho^{AB}\right)\right)$	Совместная энтропия: $H(A), H(B) \le H(B,A)$
Взаимная информация: $S(A:B) \equiv S(A) + S(B) - S(A,B) =$ $S(A) - S(A\|B) = S(B) - S(B\|A).$	Взаимная информация: $H(A:B) \equiv H(A) + H(B) - H(A,B) =$ $H(A) - H(A\|B) = H(B) - H(B\|A).$

В теории классической информации, достижимая информация не так интересна. Если на практике различение пары классических состояний может встретить определенные трудности, то в принципе, это всегда можно проделать. В отличие от этого, в квантовом случае, далеко не всегда возможно различить два состояния даже в принципе. Например, не существует однозначной процедуры, позволяющей различить два неортогональных состояния. Будем “выражаться” в терминах достижимой информации. Если Алиса готовит состояние $|\psi\rangle$ с вероятностью *p* и другое неортогональное состояние $|\varphi\rangle$ с вероятностью *1 - p*, то достижимая информация при таком приготовлении уж точно меньше, чем *H(p)*, поскольку Боб не может определить принадлежность состояния с полной достоверностью. В классике - если Алиса готовит два классических состояния, например, бит - в состоянии “0” с вероятностью *p* или “1” с вероятностью *1 - p*, то не существует фундаментального закона, запрещающего Бобу различить эти состояния; поэтому достижимая информация оказывается такой же как и энтропия приготовления, т.е. *H(p)*.

Существует важное замечание, относящееся к этой дискуссии - когда концепция достижимой информации имеет классический смысл. Суть его - в различении распределений вероятностей. Представим, что Алиса готовит состояние “0” или “1” с двумя распределениями вероятностей либо с (*p, 1 - p*) либо с (*q, 1 - q*). Получая состояние Боб должен определить, какое распределение вероятности использовала Алиса для приготовления состояния.

Очевидно, что Боб не всегда способен определить это с достоверностью 100%. Тем не менее, этот пример (по аналогии с достижимой информацией для квантовой системы, приготавливаемой в одном состоянии из набора смешанных состояний) очень важен. Что является наиболее важным и замечательным - так это то, что фундаментальные объекты в квантовой механике - чистые квантовые состояния - обладают свойствами различимости, что является существенно отличным и существенно богатым свойством, нежели чем для фундаментальных объектов классической теории информации, таких как “0” и “1”.

Теорема о запрете копирования (клонирования)

Теорема о запрете клонирования сулит другую перспективу в плане ограничения на достижимую квантовую информацию, по сравнению с классической. Классическая информация, безусловно, может быть копирована. Это точно можно сделать с цифровой информацией, например. создавая копии файлов с текстами, заложенными в компьютер. Теорема о запрете клонирования утверждает, что квантовая механика не позволяет точно копировать неизвестное квантовое состояние и накладывает некоторые ограничения на возможность создания примерных копий.

На первый взгляд, теорема о запрете клонирования выглядит довольно странно. В конце концов, не является ли классическая физика частным случаем квантовой механики? Почему мы можем копировать классическую информацию, если нельзя копировать квантовую? Ответ состоит в том, что эта теорема не запрещает копировать все квантовые состояния. Она лишь утверждает, что нельзя копировать неортогональные квантовые состояния. Далее, теорема подразумевает, что невозможно построить квантовый прибор так, что бы при наличии на входе состояний $|\psi\rangle$ и $|\varphi\rangle$, на выходе будет две копии входного состояния $|\psi\rangle|\psi\rangle$ или $|\varphi\rangle|\varphi\rangle$. С другой стороны, если $|\psi\rangle$ и $|\varphi\rangle$ ортогональны, то теорема не запрещает их копирование. Действительно, довольно просто сконструировать квантовые схемы, которые копируют такие состояния. Это замечание разрешает кажущееся противоречие между теоремой о запрете клонирования и способностью копировать классическую информацию. Для различных состояний классическая информация может восприниматься как представляемая ортогональными состояниями!

Доказательство теоремы.

Предположим, что у нас есть квантовое устройство с двумя портами (slots), обозначенными *A* и *B*. Порт *A* - это *порт данных*. В него помещается неизвестное, но чистое квантовое состояние $|\psi\rangle$. Это состояние требуется скопировать на порте *B* - это т.н. *порт - мишень*. Предположим, что порт - мишень изначально находится в некоем стандартном чистом состоянии $|s\rangle$.Таким образом, начальное состояние всего копирующего устройства есть:

$$|\psi\rangle\otimes|s\rangle. \qquad (5.8)$$

Процедура копирования подвергается некоторой унитарной эволюции *U*. В идеальном случае

$$|\psi\rangle\otimes|s\rangle\rightarrow(U)\rightarrow U\left(|\psi\rangle\otimes|s\rangle\right)=|\psi\rangle\otimes|\psi\rangle. \qquad (5.9)$$

Предположим, что процедура копирования работает для каких-нибудь двух особых чистых состояний $|\psi\rangle$ и $|\varphi\rangle$. Тогда,

$$U\left(|\psi\rangle\otimes|s\rangle\right)=|\psi\rangle\otimes|\psi\rangle. \quad (5.10)$$

$$U\left(|\varphi\rangle\otimes|s\rangle\right)=|\varphi\rangle\otimes|\varphi\rangle. \quad (5.11)$$

Находя скалярное (= внутреннее) произведение этих двух уравнений, получаем, что

$$\left(\langle s|\otimes\langle\varphi|\right)U^{\dagger}U\left(|\psi\rangle\otimes|s\rangle\right)=\left(\langle\psi|\otimes\langle\psi|\right)\left(|\varphi\rangle\otimes|\varphi\rangle\right).$$

Унитарность дает $U^{\dagger}U=I$, а раскрывая прямое произведение векторов, и учитывая, что $\langle s|s\rangle=I$ получаем:

$$\langle\psi|\varphi\rangle=\left(\langle\psi|\varphi\rangle\right)^2. \quad (5.12)$$

Но уравнение $x^2 = x$ имеет только два решения: $x = 0$ и $x = 1$, поэтому $|\psi\rangle = |\varphi\rangle$ или $|\psi\rangle$ и $|\varphi\rangle$ - ортогональны! Следовательно, копирующее устройство может копировать только состояния ортогональные друг другу. Отсюда - в общем случае квантовые состояния нельзя копировать (клонировать). Например, квантовый клонер не может клонировать состояния кубита $|\psi\rangle = 0$ и $|\varphi\rangle=\left(|0\rangle+|1\rangle\right)/\sqrt{2}$ т.к. эти состояния неортогональны.

Напоминание.

Прямым (внешним) произведением двух векторов $|a\rangle=\begin{pmatrix}a_1\\ \dots\\ a_n\end{pmatrix}$ и $|b\rangle=\begin{pmatrix}b_1\\ \dots\\ b_n\end{pmatrix}$ называется вектор, размерности $1\times n^2$ вида $|a\rangle\otimes|b\rangle=\begin{pmatrix}a_1b_1\\ a_1b_2\\ \dots\\ a_2b_1\\ \dots\\ a_nb_n\end{pmatrix}$.

Скалярным (внутренним) произведением векторов называется число $\langle a|b\rangle=a_1^{*}b_1+a_2^{*}b_2+\dots+a_n^{*}b_n$

Лекция 6

II. Основные понятия квантовой теории информации (продолжение)

1. Унитарные преобразования и их свойства
2. Теорема о запрете клонирования квантовых состояний. Ее связь с достижимой информацией и различимостью состояний.
3. Граница и информация Холево. Примеры. Априорная и апостериорная энтропии.
4. Передача (transposition) квантовой информации. Понятие квантового канала связи. Точность воспроизведения информации (fidelity). Теорема Б.Шумахера о кодировании при отсутствии шума.

Рассмотрим другое доказательство теоремы о запрете клонирования (W.Wooters W.Zurek 1982).

Пусть квантовый источник (квантовая система *M*) генерирует состояния $|a_M\rangle$.

При квантовом копировании мы хотим создать копии этих состояний в другой квантовой системе *X*. Итак, при копировании исходный сигнал (состояние) квантовой системы *M* не возмущается, а состояние системы *X* становится его копией. Другими словами состояние комбинированной системы развивается по закону:

$$|a_M, 0_X\rangle \to |a_M, a_X\rangle, \qquad (6.1)$$

где $|0_X\rangle$ - это некоторое начальное (“нулевое”) состояние системы *X*.

Доказательство. Пусть существует устройство, которое приготавливает копии произвольного состояния системы *M* в системе *X*. Тогда для двух различных состояний системы *M* $|a_M\rangle$ и $|b_M\rangle$ копирующая машина работает следующим образом:

$$|a_M, 0_X\rangle \to |a_M, a_X\rangle,$$

$$|b_M, 0_X\rangle \to |b_M, b_X\rangle.$$

Рассмотри теперь состояние суперпозиции (согласно принципу суперпозиции такое состояние существует):

$|c_M\rangle = |a_M\rangle + |b_M\rangle$ (не будем следить за нормировкой). Если конечное состояние системы *X* есть точная копия, то

$|c_X\rangle = |a_X\rangle + |b_X\rangle$. Но из общих принципов квантовой механики следует, что эволюция квантовой системы должна происходить по линейному закону, т.е. под действием унитарных преобразований.

Замечание. Свойства унитарности преобразований (Д.Бом. Квантовая теория)

1. Нормировка произвольной волновой функции остается неизменной при унитарном преобразовании (т.е. УП соответствует классической операции поворота, при которой сохраняется длина вектора).
2. Унитарное преобразование не меняет ортогональности исходных волновых функций.
3. Связи между преобразованными при УП операторами остаются такими же как и между непреобразованными операторами.

4. Собственные значения матриц не изменяются при УП. В частности не меняется след матрицы, что позволяет вычислять его в удобных представлениях.

Из унитарности преобразований следует, что

$$|c_M, 0_X\rangle = |a_M, 0_X\rangle + |b_M, 0_X\rangle \rightarrow$$

$$\rightarrow |a_M, a_X\rangle + |b_M, b_X\rangle \neq |c_M, c_X\rangle, \qquad (6.2)$$

Видно, что знак равенства во второй строчке (6.2) невозможен, т.к. $|c_M, c_X\rangle = |a_M, a_X\rangle + |a_M, b_X\rangle + |b_M, a_X\rangle + |b_M, b_X\rangle$. Следовательно, если два различных состояния могут быть копированы точно, то их линейная суперпозиция - нет!

Заметим, что копирование может быть выполнено, если состояния являются взаимно ортогональными (второе и третье слагаемые в 6.2). Например, можно копировать наблюдаемую, у которой собственные состояния являются состояниями системы *M*, а затем, использовать классическую информацию о конечных состояниях для изготовления необходимого количества копий. С другой стороны, квантовый сигнал, представляющий собой набор неортогональных состояний не может быть в точности скопирован.

Мы остановились на теореме о запрете клонирования. Было показано, что квантово-механическая машина, приготавливающая копии квантовых состояний может это сделать лишь для совпадающих или ортогональных состояний. Происходит это из-за того, что как и все квантовые операции, операция клонирования должна быть унитарной и сохранять скалярное (внутреннее) произведение. Мы доказали, что невозможно приготовить совершенную копию неизвестного квантового состояния используя унитарное преобразование (эволюцию). При этом возникает несколько вопросов.

- Что будет, если мы попытаемся копировать смешанное состояние?
- Что будет, если мы захотим получить неточные копии, которые, тем не менее достаточно хороши, с точки зрения потребности конкретной задачи?

Ответ на них составляет предмет отдельной главы теории квантовой информации, которого мы касаться не будем. Лишь вкратце заметим, что даже если в копирующей машине используются неунитарные операции, то по-прежнему невозможно копировать неортогональные чистые состояния, до тех пор пока мы не задумываемся об удовлетворительности соответствия копируемых состояний исходным. То же относится и к смешанным состояниям, хотя для доказательства используется более умозрительный подход даже в таком вопросе “что означает понятие копирования смешанного состояния?”

Рассмотрим проблему копирования несколько с другой стороны. В криптографии при обмене секретными сообщениями необходимо заботиться в возможности перехвата. Тот, кто перехватывает сообщения (обычно, этот персонаж носит имя Ева) должен уметь различить неортогональные состояния, поскольку именно их и передает Алиса.

Пусть Ева приготавливает свой измерительный прибор в исходном состоянии $|F\rangle$. Ее цель - различить неортогональные состояния $|\psi\rangle$ и $|\varphi\rangle$ не возмущая их. Другими словами, она хочет выполнить унитарную операцию:

$$\begin{aligned}|\psi\rangle|F\rangle &\to |\psi\rangle|F_\psi\rangle \\ |\varphi\rangle|F\rangle &\to |\varphi\rangle|F_\varphi\rangle\end{aligned} \qquad (6.3)$$

Из унитарности операции следует, что $\langle\psi|\varphi\rangle\langle F|F\rangle = \langle\psi|\varphi\rangle\langle F_\psi|F_\varphi\rangle$, т.е. $\langle F_\psi|F_\varphi\rangle = 1$. Отсюда видно, что конечное значение измерительного прибора будет одинаковым в обоих случаях! Ева не возмутила (не исказила) два неортогональных состояния, но она и не получила никакой информации ою этих состояниях, т.к. $\langle F_\psi|F_\varphi\rangle = 1.$ Более общее измерение (но все еще не самое общее!), которое возмущает исходные состояния, так что $|\psi\rangle \to |\psi'\rangle$ и $|\varphi\rangle \to |\varphi'\rangle$, дает

$$\begin{aligned}|\psi\rangle|F\rangle &\to |\psi'\rangle|F_\psi\rangle \\ |\varphi\rangle|F\rangle &\to |\varphi'\rangle|F_\varphi\rangle\end{aligned} \qquad (6.4)$$

Из унитарности следует, что $\langle\psi|\varphi\rangle = \langle\psi'|\varphi'\rangle\langle F_\psi|F_\varphi\rangle.$ Самый лучший вариант для Евы, в смысле оптимального различения двух состояний, соответствует минимуму выражения $\langle F_\psi|F_\varphi\rangle$. Минимум осуществляется, когда $\langle\psi'|\varphi'\rangle = 1$, что как раз означает неразличимость исходных состояний $|\psi\rangle$ и $|\varphi\rangle$ после операции, выполняемой Евой. Этот пример служит наглядной иллюстрацией связи между *информацией*, извлекаемой при измерении *и возмущением исходных состояний*.

Напоминание (из прошлой лекции)

Хорошей мерой того, сколько информации получено Бобом о величине *X* из его измерений - это взаимная (классическая!) информация между *X* и результатом измерения *Y*. Мы помним из предыдущих лекций, что Боб может сделать заключение об *X* по результатам измерения *Y* только, если и только если *H(X:Y) = H(X)*, и что в общем случае *H(X:Y) ≤ H(X)*. Далее мы покажем, что близость величины *H(X:Y)* к *H(X)* не самом деле дает хорошую меру того, как Боб смог определить *X*. Цель Боба - выбрать измерение, которое максимизирует величину *H(X:Y)* и тем самым приближая ее к *H(X)*. Для этого, определим *достижимую информацию* (*accessible information*), как максимальную величину *взаимной информации*. **Достижимая информация - это мера того, насколько хорошо Боб смог сделать вывод о приготовленном Алисой состоянии, которая она послала ему.**

Существует важное замечание, относящееся к этой дискуссии - когда концепция достижимой информации имеет классический смысл. Суть его - в различении распределений вероятностей. Представим, что Алиса готовит состояние “0” или “1” с двумя распределениями вероятностей либо с (*p, 1 - p*) либо с (*q, 1 - q*). Получая состояние Боб должен определить, какое распределение вероятности использовала Алиса для приготовления состояния. Очевидно, что Боб не всегда способен определить это с достоверностью 100%. Тем не менее, этот пример (по аналогии с достижимой информацией для квантовой системы, приготавливаемой в одном состоянии из набора смешанных состояний) очень важен. Что является наиболее важным и замечательным - так это то, что фундаментальные объекты в квантовой механике - чистые квантовые

состояния - обладают свойствами различимости, что является существенно отличным и существенно богатым свойством, нежели чем для фундаментальных объектов классической теории информации, таких как “0” и “1”.

Какова связь между копированием и достижимой информацией? Пусть Алиса приготавливает одно из двух неортогональных состояний $|\psi\rangle$ и $|\varphi\rangle$ с соответствующими вероятностями *p* и *(1 - p)*. Предположим, что в этом случае достижимая информация Боба есть *H(p)*, т.е. законами квантовой механики Бобу разрешается получить достаточно информации при его измерении о том, какое из двух состояний $|\psi\rangle$ или $|\varphi\rangle$ было приготовлено Алисой. Боб может копировать состояния очень простым способом. Он бы выполнил измерение, определив, какое состояние $|\psi\rangle$ или $|\varphi\rangle$ было приготовлено Алисой и как только он завершил идентификацию он бы приготовил копии состояний, которые получил от Алисы. Таким образом, теорема о запрете копирования явилась бы следствием того факта, что достижимая информация об этих состояниях строго меньше, чем *H(p)*. Можно обратить эти рассуждения и показать, что из теоремы о запрете клонирования следует, что достижимая информация меньше чем *H(p)*! Это делается так. Представим, что возможно клонировать неортогональные состояния. После получения состояния $|\psi\rangle$ или $|\varphi\rangle$ от Алисы, Боб смог бы повторно применить клонирующее устройство для получения состояния $|\psi\rangle^{\otimes n}$ или $|\varphi\rangle^{\otimes n}$. В пределе больших n эти два состояния становятся практически ортогональными и возможно различить их с произвольной точностью при проективных измерениях.

Таким образом, если было бы возможным копирование, то Боб мог бы идентифицировать с произвольно высокой вероятностью успеха какое из двух состояний $|\psi\rangle$ или $|\varphi\rangle$ было приготовлено Алисой и, таким образом, достижимая информация была бы *H(p)*. Следовательно, теорему о запрете клонирования можно рассматривать как эквивалент утверждения о том, что в квантовой механике достижимая информация для неортогональных состояний в общем случае меньше, чем энтропия приготовления.

Хочется подчеркнуть, что скрытая природа квантовой информации играет центральную роль в мощности квантовых вычислений и достижимая информация есть количественное проявление природы квантовой информации. К сожалению не существует общего рецепта вычисления достижимой информации (по крайней мере он неизвестен). В то же время имеется ряд важных достижимых границ, которые строго обоснованы. Наиболее важная из них - т.н. граница Холево.

Граница Холево. Она играет очень важную роль в теории квантовой информации.

Теорема о границе Холево. Предположим, что Алиса приготавливает состояние ρ_X, где $X = 0,...n$ с вероятностями $p_0,...p_n$. Пусть Боб выполняет некое измерение этого состояния (т.н. *POVM* - probability-operator-valued measure - дающее максимальное относительно всех вероятностных мер значение взаимной информации = при наилучшем измерении сигнала на выходе) описываемое множеством элементов $\{E_y\} = \{E_0,...,E_m\}$. Результат измерения Боба есть *Y*. Граница Холево утверждает, что при любых измерениях Боб может достигнуть:

$$H(X:Y) \le S(\rho) - \sum_x p_x S(\rho_x), \qquad (6.5)$$

где $\rho = \sum_x p_x \rho_x$.

Таким образом, граница Холево является верхней границей достижимой информации. Величина, фигурирующая в правой части (6.5) настолько важна в квантовой теории информации, что получила отдельное имя - *информация (или количество) Холево*. Иногда ее обозначают как χ.

Граница Холево играет ключевую роль при доказательстве многих положений квантовой теории информации. Рассмотрим несколько примеров.

Пример 1. В теории квантовой информации доказывается теорема (см.**), что

$$S(\rho) - \sum_x p_x S(\rho_x) \le H(X), \qquad (6.6)$$

где равенство достигается только для тех состояний ρ_x, которые имеют ортогональные основания (т.е. определены на множестве ортогональных состояний). Здесь $\rho = \sum_x p_x \rho_x$, а p_x - набор вероятностей для состояний ρ_x (т.е. $\rho_x = |x_i\rangle\langle x_i|$) . Предположим, что неравенство в (6.6) - строгое.

Тогда, из теоремы о границе Холево сразу следует, что *H(X:Y)* строго меньше *H(X)*. Следовательно невозможно достоверно определить *X*, исходя из результатов измерений *Y*. Это обобщает наше понимание того, что если состояния, приготавливаемые Алисой неортогональны, то Боб не может определить с достоверностью, какое состояние было приготовлено Алисой.

Пример 2. (конкретный)

Пусть Алиса приготавливает единичный кубит в одном из двух квантовых состояний, в соответствии с результатом подбрасывания монеты. При выпадении орла Алиса готовит состояние |0>, если же выпадает решка, то она готовит состояние $\cos\theta|0\rangle + \sin\theta|1\rangle$, где θ - некоторый действительный параметр. Цель Боба - определить какое из двух состояний было послано.

В базисе |0>, |1> состояние ρ можно записать следующим образом:

$$\rho = \frac{1}{2}\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} + \frac{1}{2}\begin{bmatrix} \cos^2\theta & \cos\theta\sin\theta \\ \cos\theta\sin\theta & \sin^2\theta \end{bmatrix}. \qquad (6.7)$$

Чтобы вычислить границу $S(\rho) - \sum_x p_x S(\rho_x)$, найдем S($\rho$). Для этого найдем собственные значения матрицы ρ:

$$\rho = \begin{bmatrix} \frac{1+\cos^2\theta}{2} & \frac{\cos\theta\sin\theta}{2} \\ \frac{\cos\theta\sin\theta}{2} & \frac{\sin^2\theta}{2} \end{bmatrix}$$

Уравнение на собственные значения:

$$\left(\frac{1+\cos^2\theta}{2}-\lambda\right)\left(\frac{\sin^2\theta}{2}-\lambda\right)-\frac{\cos^2\theta\sin^2\theta}{4}=0$$

$$\frac{\left(1+\cos^2\theta-2\lambda\right)\left(\sin^2\theta-2\lambda\right)}{2}-\frac{\cos^2\theta\sin^2\theta}{4}=0$$

$$\sin^2\theta-2\lambda+\cos^2\theta\sin^2\theta-2\lambda\cos^2\theta-2\lambda\sin^2\theta+4\lambda^2-\cos^2\theta\sin^2\theta=0$$

$$\sin^2\theta-2\lambda-2\lambda\left(\cos^2\theta+\sin^2\theta\right)+4\lambda^2=0$$

$$\sin^2\theta-4\lambda+4\lambda^2=0$$

$$\lambda_{1,2}=\frac{1\pm\cos\theta}{2}$$

Тогда $S(\rho)=-\sum_x \lambda_x \log\left(\lambda_x\right)$ (см. 5.2):

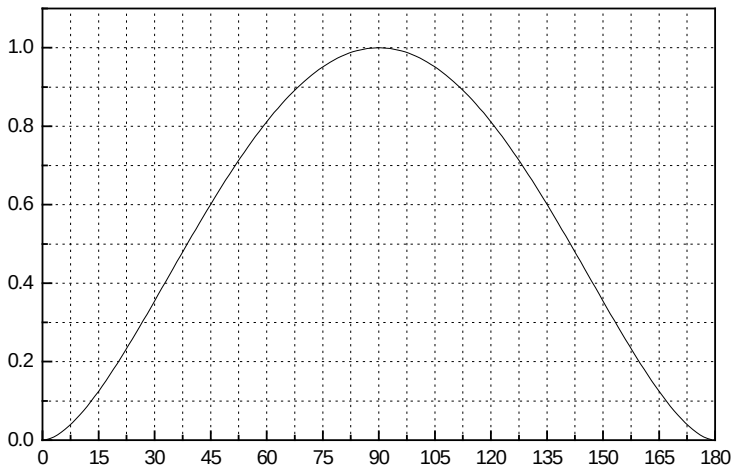
$$S(\rho)=-\left[\frac{1+\cos\theta}{2}\log\left(\frac{1+\cos\theta}{2}\right)+\frac{1-\cos\theta}{2}\log\left(\frac{1-\cos\theta}{2}\right)\right]=$$

$$=H\left(\frac{1\pm\cos\theta}{2}\right)$$

Теперь найдем величину $\sum_x p_x S\left(\rho_x\right)$. Собственные значения каждой из двух матриц плотности, задающих исходное состояние (5.15) и входящих в эту сумму равны $\lambda_x^{(1)}=(0,\,1)$ и $\lambda_x^{(2)}=(0,1)$. Поэтому

$$\sum_x p_x S\left(\rho_x\right)=\frac{1}{2}\left[-\sum_x \lambda_x^{(1)}\log\lambda_x^{(1)}\right]+\frac{1}{2}\left[-\sum_x \lambda_x^{(2)}\log\lambda_x^{(2)}\right]=\left[-\sum_x \lambda_x\log\lambda_x\right]=0$$

Отсюда, граница Холево определяется бинарной энтропией Шеннона $H\left(\frac{1\pm\cos\theta}{2}\right)$. Из рисунка видно, что максимум границы достигается при $\theta = \pi/2$ и отвечает уровню 1 бит.



По вертикали отложено значение границы Холево (фактически - это бинарная энтропия). По горизонтали - значение параметра θ в град.

Это, в свою очередь, означает, что Алиса готовит состояния, которые выбирает из ортогонального набора |0> либо |1> с равной вероятностью. Значит Боб может достоверно определить какое из (ортогональных) состояний было приготовлено Алисой. Для других значений θ граница Холево строго меньше единицы, т.е. Боб не может определить достоверно, какое из неортогональных состояний было приготовлено. С другой стороны, ясно, что при θ = 9 два состояния неразличимы. Поэтому при этом значении параметра Боб может угадать, какое состояние было послано с вероятностью 50%.

Границу (или информацию Холево) можно ввести несколько по-другому. Переобозначим величины, входящие в определение (6.5): $H\left(X:Y\right) \le S(\rho) - \sum_x p_x S\left(\rho_x\right)$:

$$S(\rho) = S(\rho)_{apr} \le H,$$

$$\sum_x p_x S\left(\rho_x\right) = S(\rho)_{aps} \ge 0.$$

Первая величина называется априорной (безусловной) энтропией. Она описывается соответствующими диагональными элементами матрицы плотности.

Апостериорная (условная) энтропия - определяет вносимую каналом связи ошибку в классической схеме. В квантовой теории она отвечает за квантовую недетерминированность сигналов, связанную с соотношением неопределенности... В отсутствие классических шумов и помех апостериорная энтропия обращается в нуль. Сигналы на входе и на выходе канала при этом коррелированы и взаимная информация $I(\rho) = S = H$.

Достижимая информация определяется выражением $I_{acc} = S(\rho) = H$, что соответствует случаю, когда сигнал формируется из ортонормированных собственных состояний ψ_n, а операторы на выходе коммутируют с оператором плотности, т.е. когда $S(\rho)_{aps} = H(\rho)_{aps} = 0$.

В случае, когда сигналы $\rho_a = \pi_a$ - это чистые состояния с нулевой энтропией, граница Холево просто сводится к утверждению, что

$H\left(X:Y\right) \le S(\rho)$,

где $\rho = \sum_a p(a)\pi_a$ - оператор плотности для ансамбля чистых сигналов (состояний). И хотя Шенноновская энтропия $H(X)$ сообщения, посылаемого источником в общем случае больше, чем энтропия фон Неймана $S(\rho)$ ансамбля сигналов, достижимая информация (классическая) ограничена величиной $S(\rho)$. Таким образом ясно, что граница Холево устанавливает связь между энтропией фон Неймана квантового ансамбля и (***классической***) взаимной Шенноновской информацией ***квантового*** канала связи.

Такая связь, однако, является довольно слабой. Дело в том, что теорема Холево формулируется в виде неравенства. Поэтому, в принципе, можно сконструировать такой источник квантовых сигналов, для которого взаимная информация $H(X:Y)$ и близко не достигает $S(\rho)$ при любом выборе наблюдаемой Y при декодировании. Поэтому, хотя из теоремы Холево и следует информационно-теоретическое значение величины $S(\rho)$, она не дает интерпретации $S(\rho)$ в терминах классической теории информации. Например, мы не могли бы использовать теорему Холево при интерпретации квантовой

теории некоторого макросостояния термодинамической системы, как дающую меру ресурсов, необходимых для представления информации о микросостояниях системы.

Ответ на этот вопрос дает квантовая теорема кодирования Б.Шумахера (1995). В ней классическая идея о двоичной логике в терминах битов заменяется моделью квантовых битов - двухуровневых систем. Эти квантовые биты являются фундаментальными единицами квантовой информации. В теореме утверждается, что ***энтропия фон Неймана*** $S(\rho)$ ***ансамбля является просто средним числом кубитов, необходимых для кодирования состояний ансамбля при помощи идеальной кодирующей системы***. Теорему можно рассматривать как краеугольный камень альтернативного подхода в квантовой теории информации. Вместо использования классической теории информации к вероятностям, вычисленным по законам квантовой механики (подход Левитина и Холево), мы пересмотрим понятия кодирования и мер информации, которые сами по себе определенно являются квантовыми величинами.

Теорема о квантовом кодировании при отсутствии шума (*quantum noiseless coding theorem*)

Пусть *M* - источник квантового сигнала, который представляется ансамблем. Этот ансамбль описывается оператором плотности ρ **(**тогда можно задать $S(\rho)$**)**. Пусть имеются два числа $\delta,\ \varepsilon > 0$.

1. Предположим, что имеется $S(\rho)+\delta$ кубитов. Тогда для достаточно большого *N*, группы из *N* сигналов из источника *M* могут быть переданы с помощью имеющегося набора кубитов с качеством $F > 1 - \varepsilon$.
2. Предположим, что имеется $S(\rho)-\delta$ кубитов. Тогда для достаточно большого *N*, при передаче групп из *N* сигналов от источника с помощью имеющегося набора кубитов, качество передачи будет $F < \varepsilon$.

Комментарии к теореме.

N - это число независимых испытаний с функцией распределения p_n.

Энтропию фон Неймана ансамбля сигналов (чистых состояний) можно интерпретировать как число кубитов на сигнал, необходимое для передачи с качеством, близким к единице. Если имеется больше, чем $S(\rho)$ кубитов, при увеличении группы сигналов можно добиться произвольно высокого качества *F*. Если же доступно меньше, чем $S(\rho)$ кубитов, качество *F* стремиться к нулю.

Более того, $S(\rho)$ является (в некотором смысле) количеством кубитов, необходимым для передачи части перепутанной системы при поддержании качества *F* всего состояния близким к единице

Таким образом, энтропия *S* является мерой физических ресурсов, необходимых для представления информационного содержания о системе смешанных состояний. Неважно каким образом получена эта система смешанных состояний - из стохастического процесса или при выбрасывании части перепутанных состояний. **Квантовая энтропия фон Неймана измеряется в кубитах.**

При доказательстве теоремы используется в основном классический аппарат с небольшими изменениями. Вместо распределения вероятностей - рассматривается набор собственных значений оператора плотности. Кроме того используется две (вспомогательных) леммы, доказанных Б.Щумахером.

Заметим, что в квантовой теории информации рассматриваются и соответствующие теоремы для зашумленных каналов. Кроме того вводится понятие качества для смешанных состояний.

Кратко рассмотрим логику доказательства. Прежде всего, заметим, что под кубитом в квантовой теории информации понимается нечто большее, чем просто состояние двухуровневой системы. А именно, утверждается, что квантовая система состоит из *n* кубитов если

- размерность ее гильбертова пространства 2^n и/или
- имеется 2^n взаимно ортогональных квантовых состояний.

Если, например, записать ортогональные состояния одного кубита как $\{|0\rangle,|1\rangle\}$, то 2^n взаимно ортогональных состояний n кубитов запишутся как $\{|i\rangle\}$, где *i* это *n*-битовое число. Например, для трех кубитов, получается:
$\{|000\rangle,|001\rangle,|010\rangle,|011\rangle,|100\rangle,|101\rangle,|110\rangle,|111\rangle\}$.

Кстати, в классике *n* бит тоже задают 2^n различных состояний. Это свойство кубита непосредственно используется при доказательстве теоремы Шумахера. Там рассматривается задача о хранении или передаче состояния квантовой системы *q* с матрицей плотности ρ. Идея состоит в том, собрать *n > 1* этих квантовых систем и закодировать их информацию в маленькой системке. Маленькая квантовая системка передается по каналу связи, и на принимающей стороне канала состояние декодируется в *n* систем q' такого же типа, как и *q*. Конечная матрица плотности каждой системы q' есть ρ'. Весь процесс считается проведенным успешно, если ρ' достаточно близко к ρ. Мерой близости двух матриц плотности (fidrlity) (по Ульману) выступает величина

$$f(\rho,\rho') = \left[Sp\sqrt{\sqrt{\rho}\rho'\sqrt{\rho}} \right]^2 .$$

Она (статистически) интерпретируется как вероятность того, что система q' пройдет тест на то, что она была в состоянии ρ. Для чистых состояний $\rho = |\phi\rangle|\phi\rangle$, $\rho' = |\phi'\rangle|\phi'\rangle$ фиделити сводится к простому «перекрытию» состояний:

$$f = |\langle\phi|\phi'\rangle|^2 .$$

Цель того, что сделал Шумахер – найти минимальную передаваемую квантовую систему, удовлетворяющую условию $f == 1-\varepsilon$ для ε 1. Его идея аналогична аргументации, использованной нами при выделении типичных последовательностей (см. Лекцию 3). Ограничимся случаем двухуровневых квантовых систем. Общее состояние *n* таких систем представляется вектором в 2^n-мерном гильбертовом пространстве. Однако энтропия фон Неймана в общем случае $S(\rho) < 1$ (поскольку состояния могут быть неортогональны). Очень вероятно, что в пределе больших n для данной реализации вектор состояния буде принадлежать некоему типичному подпространству из этого пространства. Шумахер (и Джозса) показали, что размерность такого типичного подпространства равна $2^{nS(\rho)}$. *Отсюда, следует, что нужно лишь* $nS(\rho)$ *кубитов для адекватного представления квантовой информации. Кубит как логарифм размерности гильбертова пространства служит удобной мерой*

квантовой информации. Более того, и передающая и принимающая стороны не нуждаются в знании того, какими именно состояниями была передана информация.. Это правило самого общего вида именно потому, что мы не делали никаких предположений о природе рассматриваемых квантовых состояний. Заметим, что если передаваемые состояния взаимно ортогональны, то задача сводится к классической.

Перенос (transposition) квантовой информации. Понятие квантового канала связи.

В квантовой теории информации необходимо различать понятия *копирования* состояний и *перенос* (transposition) информации из системы *M* в систему *X*. При переносе состояние системы *M* передается к системе *X* без сохранения копии начального состояния:

$$|a_M, 0_X\rangle \to |0_M, a_X\rangle, \qquad (6.8)$$

где $|0_X\rangle$ и $|0_M\rangle$ - некоторые “нулевые” состояния систем *X* и *M*. После переноса сигнал полностью возникает в кодирующей системе *X*, исчезая в системе *M*. Одним из экзотических примеров переноса служит явление квантовой телепортации.

Перенос является унитарной операцией для произвольных состояний из системы *M*. Это обеспечивает сохранение скалярного (внутреннего) произведения:

$\langle a_X | b_X \rangle = \langle a_M | b_M \rangle$ для любых сигналов (состояний) $|a_M\rangle$ и $|b_M\rangle$. Это может происходить только, если размерность гильбертова пространства системы *X* H_X не меньше чем размерность гильбертова пространства системы *M* H_M. Как происходит процесс переноса с помощью унитарного преобразования U? Для ответа на этот вопрос необходимо понять как ортогональный базис из гильбертова пространства системы *M* переходит в ортогональный базис гильбертова пространства системы *X* (свойство 2 УП). После этого эволюция других состояний будет очевидна из-за линейности.

Перенос является *обратимой операцией*, поскольку состояние сигнала может быть передано назад из *X* в *M* посредством унитарного преобразования U^{-1}. Поэтому система связи, основанная на переносе, представляется в следующем виде. Со стороны кодирования, сигнал (квантовое состояние), исходящий из системы *M*, поступает в процессе унитарного преобразования U в кодирующую систему *X*. Система *X* переправляется от передатчика к получателю. С декодирующей стороны выполняется унитарное преобразование U^{-1} для возвращения сигнала из *X* в *M** - как идентичной копии системы *M*. В символьном виде:

$$M \xrightarrow[U]{} X \xrightarrow[U^{-1}]{} M^*.$$

Система *X* называется квантовым каналом связи и поддерживает перенос состояний из системы *M* в систему *M**. В общем случае для совершенной передачи (переноса) квантовый канал должен быть достаточно емким: необходимо, чтобы $dim H_X \geq dim H_M$. Впрочем, иногда совершенная передача (перенос) не является необходимой; требуется лишь приближенный перенос информации из системы *M* в систему *M**. В зависимости от характеристик сигнала можно требовать от канала связи меньшей емкости - смотря насколько качественно нам нужно его воспроизвести.

Под сигналом далее будем понимать передаваемое квантовое состояние вида:

$$\rho = \sum_a p(a)\pi_a ,$$

где $\pi_a = |a_M\rangle\langle a_M|$ - оператор плотности (для чистого состояния - это оператор проецирования), отвечающий векторам-состояниям $|a_M\rangle$ квантовой системы *M*, передаваемым с вероятностью *p(a)*.

Для того чтобы определить эффективность канала нам нужно ввести меру качества передачи или фиделити (fidelity) В русском языке этот термин не имеет устоявшегося отображения. Будем называть его *качеством* (передачи информации). Пусть начальный передаваемый сигнал системы *M* есть $|a_M\rangle$. Он представляется оператором плотности $\pi_a = |a_M\rangle\langle a_M|$. Конечное состояние *M** будет состоянием, представленным оператором плотности w_a. В общем случае это состояние не является чистым, поэтому w_a - необязательно оператор проецирования. Для того, чтобы проверить насколько близко состояние w_a находится к состоянию π_a можно произвести контрольное измерение наблюдаемой π_a. Это измерение имеет два возможных исхода: “1” - показывающее, что конечное состояние совпадает с начальным и “0” - показывающее, что конечное состояние отлично от начального. Тогда вероятность того, что конечное состояние w_a прошло испытание есть $Sp(\pi_a w_a)$. Определим точность воспроизведения информации - *качество* как общую вероятность того, что набор сигналов (или ансамбль сигналов) приготовленный в *M* и переданный в *M** прошел контрольный тест, сравнивающий его с начальным состоянием:

$$F = \sum_a p(a) Sp(\pi_a w_a). \qquad (6.9)$$

Ясно, что *качество* лежит в интервале между 0 и 1. Оно равна единице только в случае, когда передача всех возможных сигналов является совершенной (идеальной). *F* будет близко к единице если:

- сигналы с большой вероятностью *p(a)* искажены несильно при передаче, поэтому w_a приблизительно совпадает с π_a;
- набор сигналов, который сильно возмущен, т.е. имеющий w_a сильно отличную от π_a имеет малую вероятность появления *p(a)*.

Замечание. В другом виде fidelity определяется как:

$$F = \langle \Psi^{in} | \rho | \Psi^{in} \rangle = \left\{ \rho \xrightarrow{\text{чист. сост.}} |\Psi^{out}\rangle\langle\Psi^{out}| \right\} =$$
$$= \langle \Psi^{in} | \Psi^{out} \rangle \langle \Psi^{out} | \Psi^{in} \rangle \equiv \left| \langle \Psi^{in} | \Psi^{out} \rangle \right|^2 \equiv \left| \langle \Psi^{out} | \Psi^{in} \rangle \right|^2 \qquad (6.10)$$

т.е. для чистых состояний эта величина есть квадрат модуля скалярного произведения начального и конечного состояний.

ЛИТЕРАТУРА

1. Д.Бом. Квантовая теория
2. Benjamin Schumacher Quantum coding. Phys.Rev.A, 51, №4, 2738 - 2747 (1995).

ЛЕКЦИЯ 7.

III. Квантовые двухуровневые информационные ячейки - кубиты (qubits).

1. Представление состояния двухуровневой системы в виде суперпозиции. Чистые и смешанные состояния, разница между ними. Оптическая реализация кубитов. Аналогия между степенью поляризации и чистотой состояния.
2. Квантовые логические элементы (ЛЭ) и логические операции (ЛО). Одно-кубитовые ЛЭ: фазовращатель, тождественное преобразование, «НЕ» и др. Оптическая реализация ЛО Адамара – светоделитель. Последовательности одно-кубитовых ЛЭ – интерферометры. Двух- и трех-кубитовые ЛО: CNOT и Тоффоли. Обратимость и унитарность квантовых ЛО.
3. Принцип суперпозиции, квантовая интерференция, “неразличимость” путей переходов, квантовый стиратель.

Кубиты

Элементарной единицей в квантовой теории информации являются кубиты (qubits). По-видимому, впервые, в этом контексте кубиты были введены Б.Шумахером в 1995г (статья была подана в Phys.Rev.A в 1993г). Единичный кубит представляет собой состояние двухуровневой системы. В качестве примеров такого рода состояний можно указать

- двухуровневые атомы,
- частица со спином 1/2,

Говоря о кубитах как о мере квантовой информации, мы имеем в виду следующее. Квантовая система состоит из *n* кубитов, если ее гильбертово пространство имеет размерность 2^n и при этом имеется 2^n *взаимно ортогональных* квантовых состояний. Заметим, что n классических бит могут представлять 2^n различных состояний.

Далее, говоря о двух ортогональных состояниях единичного кубита мы будем пользоваться обозначениями: $\{|0\rangle,|1\rangle\}$. Если речь пойдет о состояниях конкретной системы, например, поляризация света, то будем пользоваться другими представлениями, такими как $\{|H\rangle,|V\rangle\}$ - это будет ясно из контекста. В общем случае 2^n взаимно ортогональных состояний *n* кубитов можно представить в виде $\{|i\rangle\}$, где i - это *n*-ое двоичное число. Например, для трех кубитов *n* = 3: $\{|000\rangle,|001\rangle,|010\rangle,|011\rangle,|100\rangle,|101\rangle,|110\rangle,|111\rangle\}$ - всего 2^3 состояний.

Итак, состояние двухуровневой системы - кубита представляется в виде

$$|S\rangle = \alpha|0\rangle + \beta|1\rangle, \qquad (7.1)$$

где комплексные коэффициенты - амплитуды состояний удовлетворяют условию нормировки $|\alpha|^2 + |\beta|^2 = 1$. Заметим, что запись (7.1) не означает, что значение кубита “распределено” между состояниями “0” и “1”. Выражение (7.1) означает, что кубит - это когерентная суперпозиция двух ортогональных состояний. Измерение кубита в базисе двух собственных состояний “0” и “1” будет давать значение “0” с вероятностью $|\alpha|^2$ и значение “1” - с вероятностью $|\beta|^2 = 1 - |\alpha|^2$.

В чем же состоит отличие между когерентной суперпозицией и смесью (между чистым состоянием и смешанным)? Дело в том, что для чистого состояния S всегда можно указать базис, в котором значение кубита строго определено, т.е. является собственным. Для

смешанного состояния такого базиса не существует. Например, рассмотрим чистое состояние

$$|S\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right). \qquad (7.2)$$

При измерениях в базисе "0" и "1", очевидно, что состояния "0" и "1" будут обнаружены с 50%-ой вероятностью. Однако, если в качестве базисных использовать состояния $|+45\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)$ и $|-45\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)$, то состояние (7.2) строго определено и не флуктуирует при измерениях.

Замечание. Легко убедиться, что новые базисные состояния $|+45\rangle$ и $|-45\rangle$ - ортогональны: $\langle +45|-45\rangle = 0$.

Утверждение об определенности значения кубита в новом базисе доказывается следующим образом. Применим к кубиту (7.2) преобразование вида:

$$H|0\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right),$$
$$H|1\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right). \qquad (7.3)$$

Тогда $H|S\rangle = |0\rangle$, т.е. получается, что значение кубита строго определено.

Прямая аналогия рассмотренным преобразованиям - состояния поляризации в оптике. Если степень поляризации равна единице (в общем случае - эллиптическая), то всегда можно с помощью фазовой пластинки, действие которой описывается унитарным преобразованием *SU(2)*

$$\hat{D} = \begin{pmatrix} t & r \\ -r^* & t^* \end{pmatrix}, \quad t = \cos\delta + i\sin\delta\cos 2\chi, \quad r = i\sin\delta\sin 2\chi \qquad (7.4)$$

привести это состояние к линейной поляризации (*H* или *V*). Этого, очевидно, нельзя сделать с неполяризованным светом. Преобразования (7.3) переводят горизонтальную поляризацию в $+45^0$, а вертикальную - в -45^0. Такое преобразование можно выполнить с помощью пластинки λ/2 ($\delta = \pi/2$, $\chi = 22.5^0$, $t = \frac{i}{\sqrt{2}}$, $r = \frac{i}{\sqrt{2}}$):

$$\hat{D}(\lambda/2) = \frac{i}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad \hat{D}(\lambda/2)\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{i}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix}.$$

Квантовые логические элементы

Мы опять сталкиваемся с примером, когда англоязычному термину нет адекватного русского перевода. Будем называть "gate" логическим элементом (ЛЭ). Итак, унитарные логические операции над кубитами выполняются с помощью ЛЭ (введены Д.Дойчем в 1985, 1989гг.).

Одно-кубитовые операции.

Например, рассмотрим следующее преобразование кубита: $|0\rangle \to |0\rangle$, $|1\rangle \to \exp(i\omega t)|1\rangle = \exp(i\theta)|1\rangle$. Тогда состояние кубита по прошествии времени *t* после действия операции $P(\theta)$ (фазовращатель):

$$P(\theta) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix} \qquad (7.5)$$

изменится. Таким образом, ЛЭ к кубиту была приложена операция $P(\theta)$. В другом виде это можно записать так:

$$P(\theta) = |0\rangle\langle 0| + \exp(i\theta)|1\rangle\langle 1|. \quad (7.6)$$

Перечислим некоторые основные квантовые ЛЭ:

$$I \equiv |0\rangle\langle 0| + |1\rangle\langle 1| \rightarrow \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{- тождественное преобразование} \quad (7.7)$$

$$X \equiv |0\rangle\langle 1| + |1\rangle\langle 0| \rightarrow \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{- ЛЭ “НЕ”} \quad (7.8)$$

Оптический эквивалент - пластинка λ/2, (45^0, t = 0, r = i)

$$Z \equiv P(\pi) \rightarrow \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad (7.9)$$

Оптический эквивалент - пластинка λ/2, (0^0, $t = i$, $r = 0$)

$$Y \equiv XZ \rightarrow \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad (7.10)$$

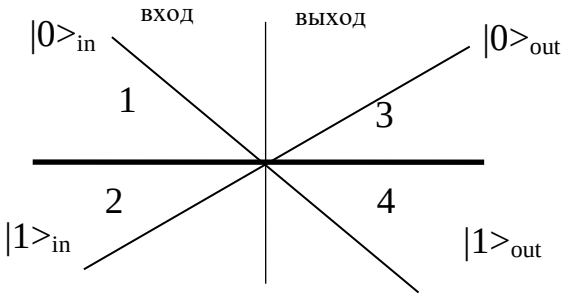
$$H \equiv \frac{1}{\sqrt{2}}\left[\left(|0\rangle + |1\rangle\right)\langle 0| + \left(|0\rangle - |1\rangle\right)\langle 1|\right] \rightarrow \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \text{ - ЛЭ Адамара} \quad (7.11)$$

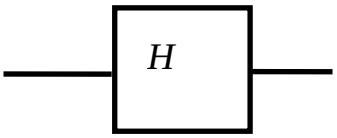
Оптический эквивалент - пластинка λ/2, (22.5^0, $t = r = \frac{i}{\sqrt{2}}$)

Все они -одно-кубитовые операции, которые действуют на единичный кубит.

Поскольку их действие можно описать действием некоторых гамильтонианов в уравнении Шредингера, то все они являются унитарными операциями. Таким образом, мы будем говорить о логических операциях (ЛО) и о ЛЭ, с помощью которых эти операции выполняются. Ниже мы рассмотрим подробно физический аналог операции Адамара *H*. Вообще говоря существует бесконечное множество одно-кубитовых ЛО (и, соответственно ЛЭ). Напомним, что для классических битов существует только две ЛО. Это операции “тождественного преобразования” и “НЕ”. В квантовом случае, для операции “НЕ” состояния $|0\rangle$ и $|1\rangle$ меняются местами, т.е. существует прямая аналогия с классикой. Поскольку такая операция представляется оператором Паули σ_x, то она часто обозначается символом *X* (но это - не общепринятое обозначение). То же относится и к обозначениям *Z* и *Y*.

Рассмотрим подробнее ЛО Адамара для случая, когда имеется две пространственные моды (а не поляризационные, как было выше)





Частица, падающая на один из двух входов делителя может с одинаковой вероятностью оказаться как в верхнем, так и в нижнем выходном пучке.

Действие светоделителя без потерь должно описываться унитарным преобразованием. Из унитарности следуют определенные фазовые соотношения, возникающие между прошедшими и отраженными пучками.

$$|t|^2+|r|^2=1\rightarrow (I_3+I_4)_{out}=(I_1+I_2)_{in}$$

Так, в случае оптических преобразований для напряженностей полей в модах 1, 2, 3 и 4 имеем:

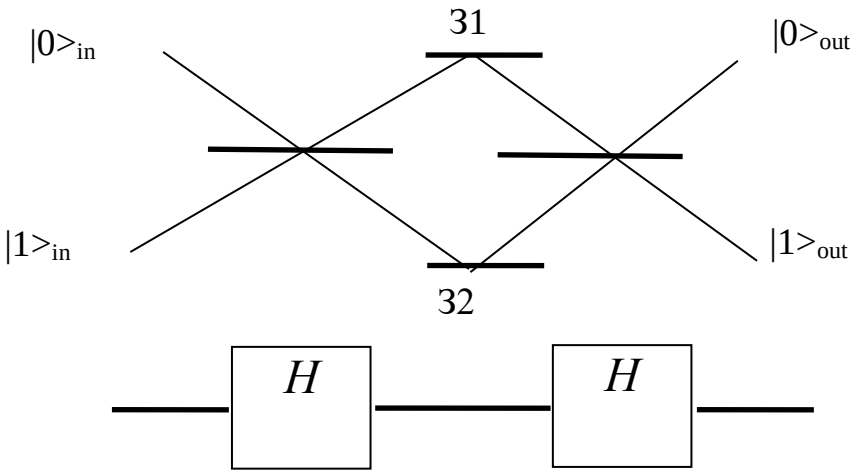
$$E_3=-r^*E_1+t^*E_2,\quad \begin{pmatrix}E_4\\E_3\end{pmatrix}=\begin{pmatrix}t & r\\ -r^* & t^*\end{pmatrix}\begin{pmatrix}E_1\\E_2\end{pmatrix}$$
$$E_4=tE_1+rE_2.$$

Если на входе состояние - кубит $|S\rangle_{in}=\alpha|0\rangle_{in}+\beta|1\rangle_{in}$, т.е. вероятности обнаружить частицу (фотон) на верхнем и на нижнем входе светоделителя, соответственно, равны $|\alpha|^2$, *и* $|\beta|^2$, то после светоделителя состояние преобразуется к виду:

$$|S\rangle_{out}=H|S\rangle_{in}=\frac{1}{\sqrt{2}}\left\{(\alpha+\beta)|0\rangle_{out}+(\alpha-\beta)|1\rangle_{out}\right\}. \qquad (7.12)$$

Отсюда сразу следует, что амплитуда вероятности найти частицу в верхнем плече теперь равна $\alpha+\beta$, а в нижнем $\alpha-\beta$. Так, если $\alpha=0$ или $\beta=0$ (частица падала определенно сверху либо снизу - известно откуда), то имеется одинаковая вероятность обнаружить ее в любом из выходных плечей. Однако, если $\alpha=\beta$, то частица обязательно будет обнаружена в верхнем плече и никогда - в нижнем! Заметим, что в данном примере речь идет о четырех пространственных модах. Две из них - входные и две - выходные. Так два ортогональных входных состояния обозначены как $|0\rangle_{in}$ и $|1\rangle_{in}$. Аналогичным образом можно рассматривать другие моды, например, поляризационные.

Следующий важный этап рассмотрения одно-кубитовых ЛЭ - последовательность нескольких ЛЭ. Если два преобразователя Адамара стоят последовательно, то физически это эквивалентно действию интерферометра с фиксированной фазовой задержкой между двумя плечами.:



В данном случае зеркала (31 и 32) нужны только для того, чтобы перенаправить пучки. Действие интерферометра как последовательность двух ЛЭ Адамара представляется в виде:

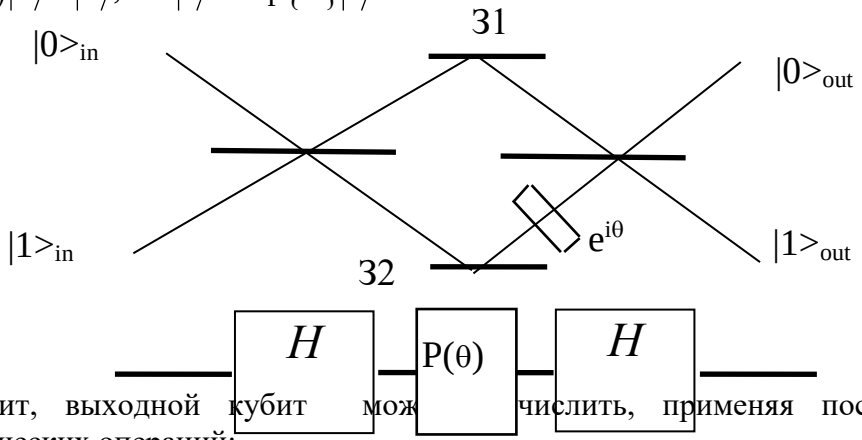
$$|S\rangle_{out} = HH\,|S\rangle_{in} = H\left[\frac{1}{\sqrt{2}}\left\{(\alpha+\beta)|0\rangle_{out} + (\alpha-\beta)|1\rangle_{out}\right\}\right] = |S\rangle_{in} \qquad (7.13)$$

Результат прямо следует из того факта, что двойное действие преобразования Адамара есть тождественное преобразование - на выходе интерферометра воспроизводится входное состояние. В частном случае, когда на входе имеется только одно состояние (α = 1, β = 0).Тогда, согласно (7.13) на выходе частица будет обнаружена в верхнем плече. Хотя внутри интерферометра эта частица имеет одинаковые вероятности оказаться в каждом из плеч. Дело в том, что выходные амплитуды вероятностей определяются относительной фазой, набегающей в интерферометре. В оптике этот эффект изучен досконально и не вызывает удивления. С массивными частицами, поведение которых можно описывать волнами де-Бройля дело происходит точно также.

На языке теории квантовой информации рассмотренный эффект формулируется так. Кубит на выходе интерферометра имеет определенное значение, если и только если кубит на входе имеет определенное значение. Внутри интерферометра его состояние максимально неопределено!

Действие двух операций Адамара можно дополнить ЛЭ “фазовращатель” (7.5). Как видно, его действие состоит в том, чтобы вносит сдвиг фаз у одного из пучков (будем считать, что это происходит в нижнем пучке, хотя это не важно - важна только относительная фаза).

$$P(\theta)|0\rangle = |0\rangle, \quad P|1\rangle = \exp\{i\theta\}|1\rangle.$$



Значит, выходной кубит можно вычислить, применяя последовательность трех логических операций:

$$|S\rangle_{out} = HP(\theta)H\,|S\rangle_{in} \qquad (7.14)$$

Например, если на входе имеется только один пучок, (α = 1, β = 0), т.е. $|S\rangle_{out} = |0\rangle$, то состояние кубита на выходе окажется:

$$|S\rangle_{out} = HP(\theta)H|S\rangle_{in} = \frac{1}{2}\left\{\left[e^{i\theta}+1\right]|0\rangle + \left[e^{i\theta}-1\right]|1\rangle\right\}. \qquad (7.15)$$

Из этого выражения видно, что если $\theta = 0$, то значение кубита определено: $|S\rangle_{out} = |0\rangle$. Если $\theta = \pi$, то $|S\rangle_{out} = |1\rangle$. Таким образом ЛЭ НРН может переключать состояние кубита между двумя значениями. Видно, что вероятность того, что кубит имеет значение $|0\rangle$ равна $P_{|0\rangle} = \cos^2(\theta/2)$, а вероятность того, что он имеет значение $|1\rangle$ равна $P_{|0\rangle} = \sin^2(\theta/2)$.

Двух-кубитовые операции.

Среди всех возможных двухкубитовых ЛО интересно рассмотреть такие, которые могут быть записаны в виде:

$$|0\rangle\langle 0|\otimes I + |1\rangle\langle 1|\otimes U, \qquad (7.16)$$

где I - тождественная операция, а U - некоторый оператор, описывающий ЛЭ. Такие двух-кубитовые операции получили название “управляемое U”, поскольку действие I или U на второй кубит управляется состоянием первого кубита - находится ли он в состоянии $|0\rangle$ или $|1\rangle$. Например, уже рассмотренная нами операция “CNOT” выглядит так:

$$\begin{aligned} &|0\rangle\langle 0|\otimes I + |1\rangle\langle 1|\otimes NOT \rightarrow \{|0\rangle\langle 0|\otimes|0\rangle\langle 0| + |0\rangle\langle 0|\otimes|1\rangle\langle 1|\} + \\ &\{|1\rangle\langle 1|\otimes|0\rangle\langle 1| + |1\rangle\langle 1|\otimes|1\rangle\langle 0|\} = \{|0\rangle\langle 0| + 0\} + \{0 + |1\rangle\langle 0|\} = |0\rangle\langle 0| + |1\rangle\langle 0| \end{aligned} \qquad (7.17)$$

Тогда, например, $\{|0\rangle\langle 0|\otimes I + |1\rangle\langle 1|\otimes NOT\}|00\rangle \rightarrow \{|0\rangle\langle 0| + |1\rangle\langle 0|\}|00\rangle = |00\rangle$

Следовательно, полная таблица действия оператора CNOT представляется:

$$\begin{aligned} &|00\rangle \rightarrow |00\rangle, \\ &|01\rangle \rightarrow |01\rangle, \\ &|10\rangle \rightarrow |11\rangle, \\ &|11\rangle \rightarrow |10\rangle. \end{aligned} \qquad (7.18)$$

Второй кубит подвергается операции “НЕ” если и только если первый находится в состоянии $|1\rangle$.

Трех-кубитовые операции.

Некоторые ЛО требуют участия большего количества кубитов. Так, операция “AND” выполняется при использовании трех-кубитового ЛЭ “дважды управляемое НЕ”. Здесь третий кубит подвергается действию ЛО “НЕ” только и только, если оба других кубита находятся в состоянии $|1\rangle$. Мы уже рассматривали такую ЛЭ, получившую название Тоффоли (1980). Ее действие над состоянием $|a\rangle|b\rangle|0\rangle$ описывается выражением: $a \rightarrow a,\ b \rightarrow b,\ 0 \rightarrow a\&b.$ Или можно сказать, что если третий кубит приготавливается в состоянии $|0\rangle$ то этот ЛЭ производит ЛЭ “AND” над первыми двумя кубитами! Заметим, что использование третьего кубита необходимо для того чтобы вся операция в целом была унитарной, т.е. была разрешенной с точки зрения квантово-механической эволюции (была обратимой - reversible). Обратимость - важнейшее свойство квантовых логических операций!

Квантовая интерференция. Принцип суперпозиции.

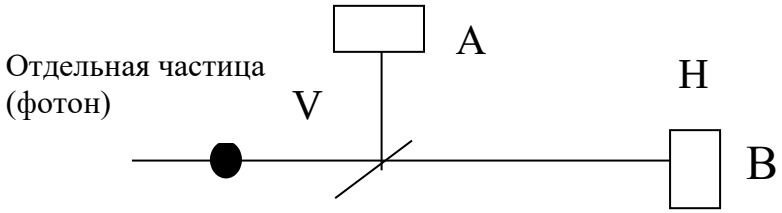
Прежде, чем приступить к изложению понятия «квантовая интерференция», вспомним основное положительное утверждение, на котором строится квантовая механика – принцип суперпозиции (Л.Ландау, Е.Лифшиц. Квантовая механика).

Пусть в состоянии с волновой функцией $\Psi_1(q)$ *некоторое измерение приводит с достоверностью к результату 1, а в состоянии с волновой функцией* $\Psi_2(q)$ *к результату 2. Тогда принимается (это утверждение – аксиома), что всякая линейная комбинация* $\Psi_1(q)+\Psi_2(q)$ *т.е. всякая линейная комбинация вида* $c_1\Psi_1(q)+c_2\Psi_2(q)$ *дает состояние, в котором то же измерение дает либо разультат 1, либо результат 2. Здесь* c_1 *и* c_2 *– два комплексных числа. Кроме того, можно утверждать, что если нам известна зависимость состояний от времени, которая для одного случая дается функцией* $\Psi_1(q)$

а для другого – функцией $\Psi_2(q)$*, то любая их линейная комбинация тоже дает возможную зависимость от времени. Эти утверждения непосредственно обобщаются на случай произвольного числа состояний.*

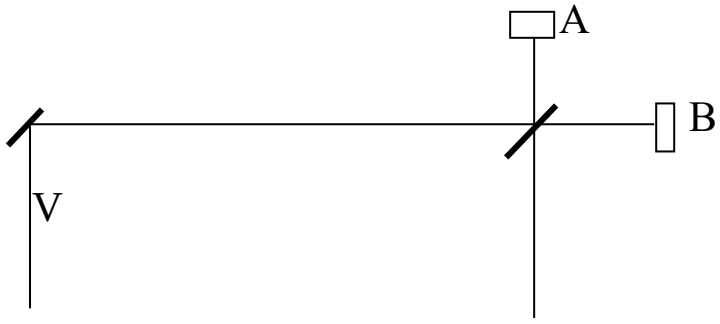
Из принципа суперпозиции, в частности, следует, что все уравнения, которым удовлетворяют волновые функции, должны быть линейными по этим функциям.

Итак, согласно принципу суперпозиции, если бит может находиться в одном из различимых состояний, то он может находиться и в состоянии их когерентной суперпозиции. Тогда, это новые состояния, которые не имеют аналога при классическом описании. Если двухуровневая система – это атом, то атом (в состоянии суперпозиции) описывается **обоими** значениями «0» и «1». Т.е. физическая величина одновременно может принимать два значения! Чтобы понять это, рассмотрим простейший мысленный эксперимент. Его схема показана на рисунке. В качестве частиц будем рассматривать однофотонные состояния, которые достаточно хорошо можно приготавливать в эксперименте.



Фотоны падают на полупрозрачное зеркала (поляризационный светоделитель), которое отражает вертикально поляризованную компоненту вверх с вероятностью 50%, и пропускает горизонтально поляризованную компоненту с вероятностью 50 %. При прохождении светоделителя фотон не расщепляется пополам: энергия (частота) фотонов в выходных плечах светоделителя не меняется (светоделитель – линейный прибор). Кроме того, светоделитель случайно распределяет фотоны в оба плеча – в среднем половина частиц пойдет вверх, а другая половина – вправо. Если, конечно исходное состояние частиц содержало равновесовой вклад этих двух ортогональных состояний, т.е. представляло собой свет, поляризованный по углом 45^0 в лабораторной системе. Однако последующие рассуждения показывают, что такая точка зрения по крайней мере спорна! Будет показано, что нет смысла утверждать, что фотон находится или в плече H или в плече V, т.е., что фотон априори находится в каком-то плече.

Чтобы продемонстрировать это рассмотрим другой эксперимент.



На рисунке изображена оптическая схема, представляющая собой последовательное соединение двух светоделителей, так, чтобы выходные плечи первого служили бы входными плечами для второго. В таком интерферометре относительная фаза между двумя плечами равна нулю.

Предположим, что фотон, который с вероятностью 50% распределяется на первом светоделителе, попадает в плечо H. Но тогда, он опять же с вероятностью 50% распределится и на втором светоделителе, как это было рассмотрено в предыдущем примере. Следовательно, два детектора A и B будут давать отсчеты с одинаковой частотой. Те же рассуждения можно привести для случая, когда после первого делителя фотоно направляется по пути V. Таким образом, если фотон двигался бы по строго определенным путям внутри интерферометра - неважно, вдоль какого - каждый из детекторов срабатывал бы одинаково часто - в половине всех случаев. Эксперимент и расчет показывает, что это не так. А именно, когда оптические пути в интерферометре одинаковы, фотон всегда попадает в детектор A и никогда - в B! Более того, известно, что если перекрыть любой из путей движения фотонов, оба детектора начинают давать одинаковое количество отсчетов, причем, каждый, в среднем, в четыре раза реже, чем количество фотонов на входе. Рассуждая в терминах фотонов - неделимых частиц - можно прийти к выводу, что фотон должен в некотором смысле находиться в обоих плечах одновременно при движении через интерферометр. Так, если отркрыты оба плеча, фотон немедленно узнает о том, что он не должен попасть в B. Иногда говорят о том, что фотону B доступна некая информация, которая распространяется вдоль другого пути со скоростью света, отражаясь от зеркал также как и сам фотон. Часто этому свойству квантовой интерференции приписывается существование двойников, которые оказывают влияние на движение частиц, причем касается это не только фотонов, но и других массивных частиц, с которыми проводятся интерференционные опыты.

Замечание.

Рассмотренный выше эксперимент имеет тривиальное объяснение, как только мы перестаем оперировать понятием “фотон = частица”. Физическое описание эффекта оптической интерференции основывается на сложении амплитуд полей - напряженностей с различными фазами. При этом нет необходимости рассматривать интерференцию вероятностей - формально, волновой функции фотона ставится в соответствие напряженность поля.

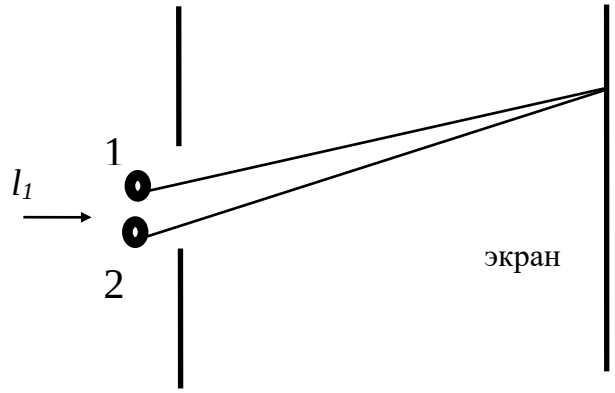
Квантовый стиратель (Quantum eraser).

Процедура *измерения*, включающая воздействие измерительного прибора (наблюдателя) на измеряемый объект, как и процедура *приготовления* состояния лежит в основе квантовой механики. С этими двумя понятиями связано основное расхождение на уровне интерпретации классической и квантовой механики. Ниже будет рассмотрен пример “парадоксальноый” с точки зрения классической физики, когда сам факт наличия некоего дополнительного знания (или его отсутствия) о квантовом объекте принципиально влияет на результат измерения. Другими словами “стирание” этой информации воздействует на результат измерения. Парадокс усугубляется тем, что это знание оказывается принципиальным с точки зрения приготовления состояния. Процесс как бы субъектизируется: экспериментатор может отложить свой выбор, сделав его существенно позже акта физического приготовления состояния. Рассмотри это на примере “дуализма волна-частица”. Экспериментатор решает о том, что хочет обнаружить (волну или частицу) после того, как сам объект (в нашем случае фотонв) был приготовлен. Эта

позиция согласуется с копенгагенской трактовкой квантовой механики. Согласно ей до измерения определенного состояния просто не существует.

Пример “квантового стирателя” рассматривается в работах М.Скалли и соавторов в 80-ых годах.

Рассматривается интерференция света, испущенного двумя атомами, локализованными в положениях 1 и 2. Атомы возбуждаются внешними электромагнитными волнами (импульс l_1).

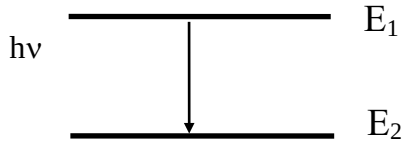


По Фейнману если каким-либо способом мы можем узнать какой из атомов излучил фотон, интерференционная картина не наблюдается. Однако, если наблюдатель решает “стереть” эту информацию из своей памяти (т.е. в принципе), интерференционная картина восстанавливается. Процесс стирания при этом может происходить гораздо позднее, чем процесс испускания. Другими словами экспериментатор может решить какие свойства квантового объекта (атомы) он желает подчеркнуть: волновые (есть интерференция) или корпускулярные (ее нет).

Все эти проблемы обсуждаются до сих пор в квантовой и атомной оптике, но математический аппарат их весьма схожий. Он построен на вычислении корреляционных функций.

Напоминание. **Интерференция одного фотона.**

Когда в интерферометре находится много фотонов, то наблюдаемые интерференционные явления имеют классическое объяснение - это результат наложения и последующей интерференции классических световых волн. Однако, как показывает опыт, интерференция возникает и в том случае, когда фотоны (электроны) проходят через интерферометр поодиночке. Хотя само понятие фотон являнтся неоднозначным и нуждается в уточнении. Следуя Бору, под фотоном будем понимать квант излучения, испущенного при квантовом переходе между двумя уровнями



Рассмотрим интерферометр Юнга - экран с двумя отверстиями, который освещается пучком света. После экрана находится фотопластинка или детектор. Такой интерферометр аналогичен тому, который будет рассмотрен ниже. Известн, что интерференционная картина наблюдается. Когда открыты две щели:

$$I \sim \sin c^2\left(\frac{\lambda}{a/2}\right)\cos^2\left(\frac{\lambda}{b/2}\right), \qquad (7.19)$$

где a - ширина щели, a b - расстояние между центрами щелей. Если одну из щелей перекрыть, то останется лишь первый сомножитель - модуляция пропадет.

Примечательно, что интерференция будет наблюдаться, когда щель освещается единичными фотонами. Аналогичные опыты выполнялись и с массивнами частицами - нейтронами, α-частицами, электронами. В случае одиночных частиц нельзя полагать, что фотон проходит через одно отверстие или через второе случайным образом (мы уже рассматривали эту ситуацию на примере интерферометра Маха-Цандера). Если бы такая независимость имелась, то при прохождении фотона, например, через отверстие 1, было бы безразлично, открыто или закрыто отверстие 2. Опыт же показывает, что призакрывании отверстия 2 интерференционная картина пропадает. Предположение о том, что фотон проходит через оба отверстия одновременно, также не годится, поскольку в таком случае, его энергия должна разделиться пополам:

$\hbar\omega_1 + \hbar\omega_2 = \hbar\omega$ - т.е. частота меняется в линейном процессе!

Квантово-механическое обяснение интерференции отдельных частиц следующее.

Пусть w_1 - вероятность фотону оказаться зарегистрированным в некотором месте фотослоя, когда открыта щель 1, а щель 2 - закрыта. Пусть w_2 - наоборот (щель 2 - открыта, а 1 - закрыта). Пусть w - вероятность регистрации при обеих открытых щелях. Если бы фотоны проходили через щели независимо, что

$$w = w_1 + w_2 \qquad (7.20)$$

Согласно квантовой механике трем вышеописанным ситуациям отвечают волновые функции ψ_1, ψ_2, ψ или амплитуды вероятностей, причем,

$$|\psi_1|^2 = w_1, \quad |\psi_2|^2 = w_2, \quad |\psi|^2 = w \qquad (7.21)$$

Вместо сложения вероятностей в микромире скоадываются волновые амплитуды вероятностей, а затем находится квадрат модуля:

$$\psi = \psi_1 + \psi_2 \rightarrow w = |\psi|^2 = |\psi_1 + \psi_2|^2 = w_1 + w_2 + \left(\psi_1\psi_2^* + \psi_1^*\psi_2\right). \qquad (7.22)$$

Таким образом, в вероятности, отвечающей случаю, когда открыты обе щели появился интерференционный член.

По Фейнману интерференционный член дает вклад лишь, когда рассматриваемые альтернативы, отвечающие прохождению фотона либо через одну щель, либо - через другую, неразличимы. Если же принять какие-то меры к их различению, т.е. выяснить через какую щель прошел фотон, то интерференционный член обратиться в нуль. Это можно делать разными способами - закрывать одну из щелей, помещать дополнитеотный детектор вблизи какой-нибудь щели и т.д. Важно при этом знание **в принципе**! Т.е. всякая индивидуализация частицы (т.е. ее различимость) приводит к потере интерференции. Заметим, что условие

$$\psi_1\psi_2^* + \psi_1^*\psi_2 = 0 \qquad (7.23)$$

означает ортогональность состояний. Ортогональные состояния не интерферируют! Т.е. для полной системы мы знаем о ней все, если укажем, через какую щель прошел фотон. Таким образом, вопрос через какую щель прошел фотон, не имеет смысла. Итак, интерференция при прохождении одиночных частиц через щель, является принципиально квантовым явлением. При прохождении фотонов через интерферометр, рассмотренный выше, можно говорить об амплитудах вероятностей, отвечающим двум альтернативам. Как только альтернативы различаются, например. фотоны отличаются по поляризации - интерференция пропадает. Чтобы восстановить ее нужно уничтожить знание поляризации - поставить поляроид, ориентированный под 45^0, если фотоны были поляризованы как *H* и *V*.

Проблема квантового стирателя. (если есть время)

Лекция 8. Основные понятия теории измерения.

1. Классические вероятностные модели. Приготовление и измерение классического состояния. Аналог смешанного состояния. Маргинальные моменты. Связь моментов и вероятностей. Проблема моментов.
2. Квантовые вероятностные модели. Прямые и косвенные измерения. Опыты Штерна и Герлаха. Двухуровневые системы (примеры). Формула Раби для вероятности перехода.
3. Измерительный (Борна) и проекционный постулаты (фон Неймана).
4. Понятие квантовой томографии.

Обычно рассматриваемые в учебниках и методических работах по квантовой физике схемы оказываются слишком далекими от лабораторной реальности. Это относится и к работам по так называемой *квантовой теории измерения.* Эта теория уделяет мало внимания реальным приборам, регистрирующим элементарные квантовые события -- детекторам элементарных частиц и фотодетекторам (счетчики Гейгера, камера Вильсона, ФЭУ, и т.д.). В значительной мере игнорируются и реальные процедуры *приготовления*, вместо этого приготовление традиционно отождествляется с *измерением*.

В этой лекции проведен элементарный логический анализ ряда терминов квантовой физики исходя из реальных измерительных процедур. В частности, сделана попытка операционального обоснования тезиса о том, что волновая функция ψ **данного индивидуального** объекта -- атома, электрона, α-частицы -- имеет четкий операциональный смысл. При этом предлагается тщательно разделять процедуры *приготовления*, *измерения*, *фильтрации*.

Можно выделить три типа квантовых экспериментов.

1) Измерение спектров -- энергетической структуры молекул, атомов, ядер,..(здесь теория часто дает содержательную информацию исходя лишь из симметрии объекта)

2) Измерение вероятностей переходов, сил осцилляторов, относительных весов различных каналов распада

3) Динамические эксперименты, измерение распределения вероятностей каких либо наблюдаемых, реконструкция состояния или томография.

Ниже нас будут интересовать в основном именно динамические эксперименты, которые являются в некотором смысле наиболее фундаментальными.

Классические вероятностные модели

1. Приготовление классического состояния.

При бросании обычной игральной кости возможно шесть *элементарных* событий: выпадение цифр n = 1, 2, 3, 4, 5 или 6 на верхней грани. Назовем совокупность этих шести возможностей *пространством элементарных событий* кости. Это пространство состоит из дискретных пронумерованных точек, n = 1,... N, N = 6. Каждому событию припишем из физических соображений определенную вероятность p_n, при этом выполняются колмогоровские аксиомы $p_n \geq 0$, $\sum_n p_n = 1$. Эту совокупность назовем *вектором состояния* или, короче, *состоянием* и будем ее записывать так:

$\Psi \equiv (p_1, p_2, p_3, p_4, p_5, p_6) \equiv \{p_n\}$. Если кость сделана из однородного материала, то естественно принять p_n = 1/6, т.е. $\Psi \equiv c(1, 1, 1, 1, 1, 1)$, c = 1/6. Но в общем случае это не так. Можно изготовить или, как говорят в квантовой

физике, *приготовить* фальшивую кость, у которой 6-ая грань сделана из очень тяжелого материала, капелька которого попала и на пятую грань, так что

$\Psi \equiv (0{,}01;\ 0{,}01;\ 0{,}01;\ 0{,}01;\ 0{,}02;\ 0{,}94).$ (8.1)

Таким образом, **каждой** кости можно приписать определенное состояние Ψ, который содержит полную вероятностную информацию о данной кости.

Каждое возможное состояние можно *отобразить* в виде точки в воображаемом 6-мерном *пространстве состояний*, если вдоль базисных осей этого пространства откладывать p_n или $c_n = \sqrt{p_n}$. В последнем случае в силу условия нормировки точка принадлежит сфере и вектор состояния можно записывать так:

$\Psi = \{c_n\}$

Пусть теперь $N = 2$. Можно представить себе набор из фальшивых монет, приготовленных из намагниченного железа. При этом монеты бросаются на намагниченный стол, так что вероятности выпадания орла p_1 или решки p_2 для данной монеты зависит от силы и направления ее намагниченности.

2. Измерение классического состояния.

Измерить (определить) состояние данной монеты с помощью одного *испытания* невозможно. Выпадение, например, орла может соответствовать любому состоянию, кроме Ψ = (1, 0). Надо или бросать одну и ту же монету много раз, $M >> 1$, или изготовить большое множество одинаково приготовленных монет - *ансамбль* монет. Если считать, что монеты при бросании не меняют свойств, не изнашиваются, то эти способы эквивалентны (свойство *эргодичности* вероятностной модели).

Бросив монету 10 раз и получив каждый раз орла, можно с некоторой надежностью утверждать, что $\Psi_{10} = (0, 1)$. Однако, не исключено, что при следующих 90 испытаниях монета выпадет решкой вверх. Теперь мы будем более или менее уверены, что $\Psi_{100} = (0{,}9;\ 0{,}1)$, -- и опять можем ошибиться, потому что, скажем, после следующих 10^3 испытаний может, в принципе, оказаться $\Psi_{1000} = (0{,}1;\ 0{,}9)$. Таким образом, измерить истинное (приготовленное) состояние Ψ со 100% надежностью (как, впрочем, и приготовить) вообще невозможно, можно лишь надеяться, что при увеличении числа бросков M вероятность сильно ошибиться уменьшается (это обстоятельство количественно выражают через *доверительный интервал*) и Ψ_M все же приближается к истинному значению Ψ. Итак, мы видим, что принципиального различия между одним испытанием и множеством испытаний нет, результаты эксперимента всегда имеют лишь вероятностный характер.

Таким образом в вероятностных моделях классической физики при операциональном подходе возникает принципиальное различие в возможности приписывания понятия состояния индивидуальному объекту: при *приготовлении* объекта это четко определенная операция, в то время как при *измерении* она не имеет смысла, состояние можно приписать с некоторой ограниченной степенью надежности лишь большому набору одинаково приготовленных объектов.

Аналогичный вывод можно сделать и в квантовой физике. Конечно, приведенная аналогия ограничена, под приготовлением кубика можно понимать и его свойства и параметры начального толчка, которые согласно законам класси-

ческой механики определяют будущий исход. Начальное состояние ψ_0 в квантовой теории определяет и начальные условия и вероятности различных исходов.

3. Аналог смешанного состояния в классике. Маргинальные моменты.

3.1.Рассмотрим два набора монет. Пусть каждый набор характеризуется вероятностями выпадения орла и решки:

$$\Psi_1 = \{p_1(орел), p_1(решка)\},$$
$$\Psi_2 = \{p_2(орел), p_2(решка)\}. \qquad (8.2)$$

Пусть общее число монет равно N, а в каждом наборе, соответственно, N_1 и N_2. При подбрасывании наугад взятой монеты из полного набора, вероятности выпадания орла и решки окажутся взвешенными:

$$p(орел) = \frac{p_1(орел)N_1 + p_2(орел)N_2}{N},$$
$$p(решка) = \frac{p_1(решка)N_1 + p_2(решка)N_2}{N}. \qquad (8.3)$$

Эти вероятности определяются не только индивидуальными свойствами монет (*вероятностями выпадения орла и решки в данном наборе*), но и свойствами ансамбля - числами N_1 и N_2. Существует, как бы, двойная стохастичность - случайность выпадения орла или решки данной монеты и случайность выбора монеты из двух наборов. Этот пример можно рассматривать как *аналог квантового смешанного состояния*, когда к чисто квантовой неопределенности чистого состояния добавляется классическое усреднение по наборам таких состояний. Смешанное состояние не характеризует индивидуальные свойства каждой из подсистем - оно относится ко всему ансамблю в целом.

3.2. *Маргинальные (частные) вероятности* - определяются через элементарные вероятности, характеризующие состояние через суммирование. Они также характеризуют свойства индивидуального состояния объекта. Для примера, приведенного выше (8.1), например, маргинальные вероятности выпадения четных и нечетных чисел кубика составят, соответственно:

$$p_{четн.} = 0.96,$$
$$p_{нечетн.} = 0.04.$$

4. Связь моментов и вероятностей.

Эти связи окажутся полезными при анализе неравенств Белла.

Рассмотрим две разные монеты, которые подбрасываются одновременно. Введем две случайные величины S_1 и S_2, каждая из которых характеризуется двумя значениями (дихотомная переменная) s_1, $s_2 = \pm 1$. Это удобная параметризация выпадения орла и решки. Полная система, состоящая из двух монет, описывается набором вероятностей $p(s_1, s_2)$. Это - вероятности выпадения четырех парных комбинаций: $\left(+1\ +1,\ +1\ -1,\ -1\ +1,\ -1\ -1\right)$. Например, если монеты не взаимодействуют при подбрасывании, то двумерные вероятности определяются $p(s_1, s_2)$ произведением одномерных вероятностей:

$$p(s_1, s_2) = p_1(s_1)\, p_2(s_2). \qquad (8.4)$$

Предположим, что монеты при подбрасывании взаимодействуют, так что условие (8.4) больше не выполняется. Тогда в исходах испытаний будет наблюдать-

ся некая корреляция выпадения орлов и решек двух монет, которая определяется характером взаимодействия. Полное состояние, описывающее всевозможные исходы дается набором четырех вероятностей $p(s_1, s_2)$. Рассмотрим маргинальные вероятности. Вероятность того, что определенная монета выпадет определенной стороной складывается из двух вероятностей:

$$p_n(s_n) = p(s_n, +1) + p(s_n, -1). \qquad (8.5)$$

В среднем n-ая (n = 1, 2) монета будет выпадать “орловой” стороной:

$$\langle S_n \rangle = p_n(+1) - p_n(-1) = p_n(+1) - \{1 - p_n(+1)\} = 2\,p_n(+1) - 1. \qquad (8.6)$$

В среднем обе монеты упадут орлом или решкой, а не разными сторонами:

$$\langle S_1 S_2 \rangle = p(+1,+1) + p(-1,-1) - p(+1,-1) - p(-1,+1). \qquad (8.7)$$

Видно, что

$$|\langle S_n \rangle| \le 1, \quad |\langle S_1 S_2 \rangle| \le 1. \qquad (8.8)$$

В этом случае можно решить обратную задачу, т.е. выразить вероятности через моменты (т.н. *проблема моментов*):

$$p_n(s_n) = \frac{1 + s_n \langle S_n \rangle}{2}, \qquad (8.9)$$

$$p(s_1, s_2) = \frac{1}{4}\left[1 + s_1 \langle S_1 \rangle + s_2 \langle S_2 \rangle + s_1 s_2 \langle S_1 S_2 \rangle\right]. \qquad (8.10)$$

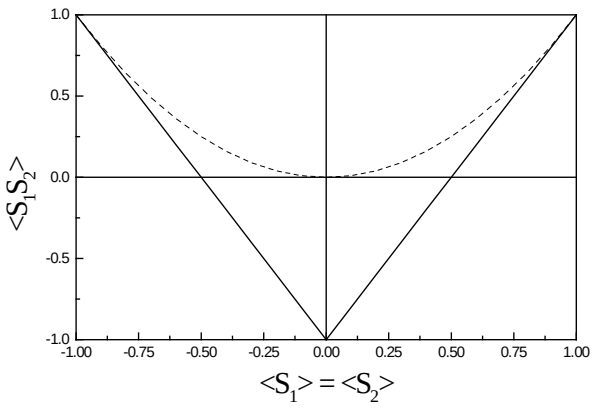
Из (8.10), а также из того, что $p(s_1, s_2) \ge 0$, следует, что моменты не являются независимыми величинами. Они должны удовлетворять некоторым соотношениям (неравенствам). Например, если заданы первые моменты $\langle S_n \rangle$, то второй момент или коррелятор $\langle S_1 S_2 \rangle$ будет ограничен:

$$S_{\min} \le \langle S_1 S_2 \rangle \le S_{\max}. \qquad (8.11)$$

Здесь

$$\begin{aligned} S_{\min} &= \max\{-1 - \langle S_1 \rangle - \langle S_2 \rangle, -1 + \langle S_1 \rangle + \langle S_2 \rangle\} \\ S_{\max} &= \min\{1 + \langle S_1 \rangle - \langle S_2 \rangle, 1 - \langle S_1 \rangle + \langle S_2 \rangle\}. \end{aligned} \qquad (8.12)$$

Например, в важном частном случае, когда $\langle S_1 \rangle = \langle S_2 \rangle$ получается ограничение на коррелятор: $2|\langle S_1 \rangle| - 1 \le \langle S_1 S_2 \rangle \le 1$. Так, коррелятор не может равняться нулю при $\langle S_1 \rangle > 1/2$, т.е. при (см.8.6) $p \ge \frac{1}{2}(\langle S_1 \rangle + 1) = \frac{1}{2}\left(\frac{3}{2}\right) = \frac{3}{4}$.



На рисунке показана зависимость между коррелятором $\langle S_1 S_2 \rangle$ и первыми моментами, когда $\langle S_1 \rangle = \langle S_2 \rangle$. Центральная треугольная часть с вершиной в нуле - область разрешенных значений коррелятора. Два прямоугольных треугольника по бокам - запрещенная область, где вероятности, выраженные через моменты принимают отрицательные значения. Пунктирная парабола - связь между коррелятором и моментами для независимых исходов подбрасывания монет: $\langle S_1 S_2 \rangle = \langle S_1 \rangle \langle S_2 \rangle$

Квантовые вероятностные модели

Считается, что квантовая случайность, лежащая в основе вероятностной интерпретации волновой функции (по Борну) имеет фундаментальный характер (“бог играет в кости”). До сегодняшнего дня все попытки свести эту случайность к детерминированности (например, теория скрытых параметров) не привели к успеху.

В квантовой теории также можно пытаться исходя из набора квантовых моментов построить соответствующие им распределения вероятностей. Однако в случае некоммутирующих операторов эта процедура может оказаться неоднозначной. Более того, она приводит к функциям, принимающим неопределенные или отрицательные значения, как, например, функции Вигнера W(x, p) и распределение Глаубера-Сударшана P(α). Неопределенность последней функции часто рассматривают как критерий неклассичности поля.

Одной из важных особенностей квантовых вероятностных моделей является тот факт. что в некоторых случаях нельзя говорить об элементарных вероятностях при существовании маргинальных. Часто этот факт относят к неколмогоровости квантовой механики. Ей соответствует отказ от концепции *априорных* (т.е. до измерений) значений у наблюдаемых. Например, из соотношения неопределенностей следует, что можно измерить или вычислить через волновую функцию распределения координат и для импульса частицы в данный момент времени. Однако нельзя измерить их совместное распределение. Такое распределение неоднозначно и приводит в некоторых случаях к отрицательным вероятностям. В этом случае приписывание частице априорных значений координат и импульсов теряет смысл.

1. Полуклассические этапы в квантовых моделях.

В квантовой теории измерения можно выделить две актуальные задачи. Прежде всего, это фундаментальная проблема объединения квантовой и классической физики, единого подхода к квантовому объекту и измеряющего его свойства макроскопическому прибору. Эта глобальная задача, требующая, очевидно, выхода за рамки стандартного квантового формализма, до сих пор не решена. Другая задача -- создание в рамках квантовой теории реалистических моделей существующих измерительных процедур. Эта задача теории измерения, как правило, игнорируется.

Рассмотрим логическую структуру современных квантовых динамических моделей, допускающих сопоставление с экспериментом. Формально квантовая теория может описывать действительность лишь с помощью общей волновой функции Ψ некоторой изолированной *системы*, которая должна включать как операторы изучаемой подсистемы, так и операторы

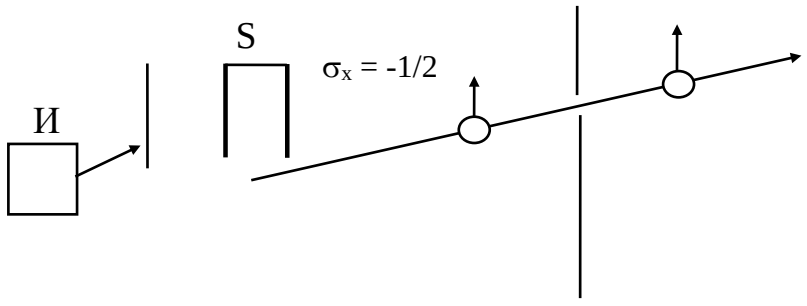
приготовительной и измерительной аппаратуры, взаимодействующей с частицей. При желании можно включить в систему и экспериментаторов. В этом смысле чисто квантовый мир является невидимым, вещью в себе.

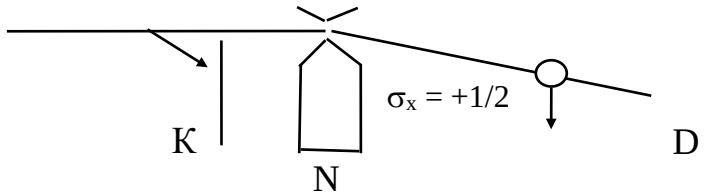
Поэтому необходимо на основании дополнительных, интуитивных соображений как то ограничить число учитываемых степеней свободы и дополнительно постулировать соответствие между математическими символами и макроскопическими приборами -- приготовительным и измерительным. Фактически мы вынуждены на двух этапах использовать полуклассический подход: на "входе" -- при определении начального состояния квантовой системы ψ_0, задаваемого классическими силами, -- и на "выходе" -- при выборе "крайнего" оператора B_m, влияющего на классический измерительный прибор. Задавая ψ_0 мы исключаем операторы приготовительного прибора, а выбирая B_m мы исключаем операторы измерительного прибора. Примеры этих двух полуклассических этапов расчета будут даны ниже. Между входом и выходом система предоставлена самой себе и эволюционирует согласно уравнению Шредингера.

Рассмотрим подробней последний, выходной этап -- процедуру измерения. Различают *прямые* и *косвенные* квантовые измерения. При прямом измерении имеется один квантовый объект **A**, который описывается с помощью ВФ $\psi(a,b,c,...)$. Для простоты выписываем только один аргумент ВФ и считаем состояние чистым; в случае смешанного состояния добавляется тривиальное классическое усреднение, учитывающее несовершенство приготовительной процедуры, см. ниже. Связь с внешним миром устанавливается выбором (на основании физических, интуитивных соображений) какого-либо оператора A в качестве "наблюдаемого". Параметры измерительной аппаратуры при этом исключаются из рассмотрения. С экспериментом можно сравнивать распределение $p(a) = |\psi(a)|^2$ или его моменты $\langle a^k \rangle$. Как уже отмечалось, разумное подтверждение расчета возможно лишь при многократном повторении приготовительной и измерительной процедур.

При косвенном измерении кроме исследуемого объекта имеется по крайней мере еще одно "пробное тело" **B (квантовая считывающая система)**, взаимодействующее (или взаимодействовавшее) с **A** и служащее посредником между **A** и макромиром. Рассматривается общая ВФ $\Psi(a, b)$ системы **A** + **B**, при этом взаимодействие **A** и **B** рассчитывается по формальным правилам квантовой теории. В качестве *наблюдаемого* оператора B теперь уже выбирается оператор, относящийся к **B**. Теория дает общее совместное распределение $p(a, b) = |\Psi(a, b)|^2$. Классическое суммирование по вероятностям ненаблюдаемых событий приводит к наблюдаемому *маргинальному* распределению $p(b) = \sum_a p(a, b)$, которое несет информацию о $p(a)$.

Операторы A и B могут относиться к разным степеням свободы одного объекта: например, в эксперименте Штерна-Герлаха $A \equiv S_x$ и $B \equiv X$ -- операторы проекции спина и поперечные координаты одной частицы, которые становятся коррелированными при движении в неоднородном магнитном поле.





И - источник частиц со спином $\sigma_x = \pm 1/2$, К - коллиматор, формирующий пучок, S-N - постоянный магнит, создающий неоднородное магнитное поле, D - экран, на месте которого можно установить фотопластинку или дырочку, пропускающую отселектированный по спинам пучок в данном направлении.

В результате по непосредственно наблюдаемой (на фотопленке, например) поперечной *классической* координате частицы x_1 косвенно, на основании теоретической модели, описывающей влияние магнитного поля на ВФ частицы со спином, определяется значение проекции спина $\sigma_x = \sigma_x (x_1)$ на поперечное направление у данной частицы. Полученное число принимается за априорную (до измерения) координату частицы. Точность измерения ограничена размером атома серебра, поглотившего частицу. Значит, непосредственно наблюдаемым оператором является оператор координаты X. Отсюда при известных других параметрах можно рассчитать (исходя из уравнения Шредингера и начальной волновой функции частицы) априорную проекцию спина частицы. Если вместо фотопленки установить экран с отверстием в точке x_1, то получим аппарат, приготавливающий частицы в состоянии $|\sigma_x\rangle$ с определенной проекцией спина. Магнит и экран служат *фильтром* или *спектральным анализатором*, который можно считать частью или приготовительной или измерительной аппаратуры. Но целесообразно отличать процедуру фильтрации от приготовления и измерения. Заметим, что фильтрация в общем случае описывается неунитарным преобразованием, при котором система переходит в смешанное состояние.

Обычно термины *наблюдаемая* и *оператор* отождествляются; однако, в любой квантовой модели для сравнения с экспериментом какой то оператор необходимо выделить в качестве "более наблюдаемого". Связь с внешним миром устанавливается выбором (на основании физических, интуитивных соображений) какого-либо оператора B_m в качестве “наблюдаемого”. Параметры макроскопической измерительной аппаратуры при этом исключаются из рассмотрения.

Характерно, что при общем формальном рассмотрении выбор "крайнего" оператора не критичен, он не сказывается на правильности предсказаний теории, Иначе говоря, границу между двумя мирами можно расположить произвольно, иногда ее располагают в сетчатке глаза наблюдателя или в его мозге. Как известно, космонавты воспринимают космические частицы непосредственно глазом; при этом "крайние" операторы надо, очевидно, располагать в нервных клетках *наблюдателя* и этот традиционный субъективный термин получает некоторое оправдание. Формально можно рассматривать ВФ всей измерительной аппаратуры или всей вселенной. Но подобные модели не допускают количественного сравнение с реальными экспериментами. Для этой цели необходимо сократить число степеней свободы модели и выбрать некоторый оператор в качестве *наблюдаемого.*

В качестве такого "более наблюдаемого" оператора часто выбирается оператор энергии атома, который принадлежит детектору типа счетчика Гейгера или фотоумножителя. Представляется, что такой выбор соответствует многим реальным детекторам микрособытий, которые служат по-

средниками между нашим макромиром и "невидимым" миром индивидуальных квантовых объектов.

Измерительный и проекционный постулаты

Около 70 лет назад Дирак и фон Нейман ввели понятие редукции или коллапса волновой функции (ВФ). Они постулировали, что если в эксперименте измерение какого либо оператора *A* дало некоторое значение a_1, то ВФ системы независимо от исходного состояния становится равной $|a_1\rangle$ -- собственной функции *A*, соответствующей измеренному собственному значению. Этот постулат (его называют *проекционным*) иногда оправдывают *принципом повторяемости* -- при повторном измерении *A* через достаточно короткое время должно обнаружиться то же самое значение a_1 -- иначе понятие измерения относится лишь к прошлому. Было предложено также множество различных динамических моделей процесса измерения, учитывающих влияние большого числа степеней свободы макроскопического измерительного прибора, однако, пока они не получили экспериментального подтверждения. Похоже, что из всех выводов квантовой теории измерения лишь постулат Борна-Дирака допускает сравнение с экспериментом.

Постулат Борна-Дирака.
Чтобы вычислить вероятность наблюдения какого-либо собственного значения a_1 оператора *A* в момент времени t_1, надо найти проекцию вектора состояния $|\psi_1\rangle$ на вектор $\langle a_1|$ и возвести ее модуль в квадрат:

$$p(a_1,t_1)=\left|\langle a_1|\psi(t_1)\rangle\right|^2=\left|\langle a_1,t_1|\psi_0\rangle\right|^2=\langle\psi_0|P(a_1,t_1)|\psi_0.\rangle \qquad (8.13)$$

В двух последних равенствах использовано представление Гейзенберга. Под оператором P понимается оператор редукции или проекционный оператор:
$P(a,t)\equiv|a,t\rangle\langle a,t|$,
а собственный вектор оператора *A(t)*:
$|a,t\rangle\equiv U^{\dagger}(t)|a\rangle$,
где $U\equiv\exp\left\{-\frac{iHt}{\hbar}\right\}$ - оператор эволюции, а *H* - не зависящий от времени оператор Гамильтона. Напомним, что проекторы обладают свойством
$P^2 = P$ и двумя собственными векторами 0 и 1.
Согласно постулату *Б-Д* среднее значение какой-либо наблюдаемой *A* в момент времени *t* имеет следующий вид:
$\langle A(t)\rangle\equiv\langle\psi(t)|A|\psi(t)\rangle=\left\langle\psi_0U(t)^{\dagger}\right|A\left|U(t)\psi_0\right\rangle$,
где $\psi(t)=U(t)\psi_0$. В представлении Гейзенберга:
$A(t)\equiv U(t)^{\dagger}AU(t)$ и для средних значений в представлении Гейзенберга:
$\langle A(t)\rangle\equiv\langle\psi_0|A(t)|\psi_0\rangle$.
Постулат Борна (8.13) дает возможность сравнить предсказания теории и эксперимент, однако ничего не говорит о том, что происходит с самим объектом или с его волновой функцией в результате измерения. Происходит редукция ВФ в точке, где находится детектор (где производилось измерение). Чтобы узнать состояние объекта необходимо провести повторное измерение!

Постулат Дирака-фон Неймана.
В результате регистрации собственного значения a_1 происходит проецирование волновой функции системы $|\psi(t_1)\rangle$ на вектор $|a_1\rangle$. Пусть показание a_1 возникло в момент t_1, тогда P можно представить в виде:

$$|\psi(t_1)\rangle \to |\psi'(t_1)\rangle = P(a_1,t_1)|\psi_0\rangle. \qquad (8.14)$$

Очевидно, для проверки этого утверждения надо в последующий момент $t_2 > t_1$ произвести измерение еще какого-либо оператора системы *B.* Пусть это измерение описывается оператором $P(b_2,t_2)$. Второй измеритель "видит" измененную ВФ $|\psi'(t_1)\rangle$, поэтому усреднять $P(b_2,t_2)$ надо с ее помощью. В результате получаем формулу Вигнера для совместного распределения:

$$p(a_1,t_1,b_2,t_2) = \langle\psi'|P(b_2,t_2)|\psi'\rangle = \langle\psi_0|P(a_1,t_1)P(b_2,t_2)|\psi_0\rangle. \qquad (8.15)$$

Можно обобщить этот результат на случай нескольких наблюдаемых.

В соответствии с проекционным постулатом часто утверждается, что *измерение* является в то же время *приготовлением.* Однако, это отождествление противоречит практике реальных квантовых экспериментов, в которых для приготовления ВФ и для измерения используются совершенно различные процедуры. Формально первое из двух последовательных наблюдений можно считать приготовлением новой ВФ, но лучше последний термин сохранить для обозначения процедур, не связанных с регистрирующими приборами (например, приготовления атома в определенном состоянии с помощью лазера - далее).

С чисто операциональной точки зрения последняя формула допускает сравнение с экспериментом лишь целиком, сама P как промежуточный этап не наблюдаема, поэтому (8.15) можно принять в качестве *измерительного постулата*. Это, по-существу, обобщение постулата Борна-Дирака (который применительно к данному случаю имеет вид

$$p(a_1,t_1) = \langle\psi_0|P(a_1,t_1)|\psi_0\rangle$$

на случай двух последовательных измерений.

Хотя использование понятия P при описании некоторых экспериментов удобно, однако, не имеет смысла задаваться вопросом о том, что происходит "на самом деле". Можно полагать для наглядности, что при образовании трека в камере Вильсона происходит цепочка редукций -- каждый затравочный атом, около которого возникла капелька воды, приготавливает новую ВФ для следующего атома. При этом каждой капельке воды в реальном треке частицы следует сопоставить свою пару проекторов P_k в обобщение формулы (2) на множество последовательных измерений. Подчеркнем, однако, что это лишь возможная интерпретация, фактически P не нужна для описания трека.

Хотя P считается основным понятием квантовой физики, он по-видимому никогда не использовался для конкретных практических расчетов, допускающих сравнение с экспериментом. Более того, в ряде работ оспаривается необходимость этого понятия. Однако он действительно необходим для **количественного** описания некоторых экспериментов (имеются в виду практические расчеты, допускающие сравнение с экспериментов -- в отличие от общих моделей квантовой теории измерения или рассуждений о ВФ всей аппаратуры). В таких экспериментах должны выполняются три усло-

вия: в каждом испытании последовательно проводится измерение двух или более операторов, эти операторы в представлении Гейзенберга не коммутируют и измерения проводятся с достаточно высоким временным разрешением.

К этому классу относятся так называемые время-пролетные эксперименты, широко используемые для измерения скорости элементарных частиц. Частица с достаточно большой энергией последовательно пролетает через два детектора, например, два счетчика Гейгера. Расстояние между детекторами $z_2 - z_1$, деленная на задержку во времени появления импульса на выходе второго детектора $t_2 - t_1$, дает скорость пакета частицы (потерей энергии в детекторах пренебрегается). Пусть частица каждый раз приготавливается в состоянии с достаточно хорошо определенным импульсом, при этом она описывается протяженным волновым пакетом. В результате моменты регистрации t_1, t_2, отсчитываемые от характерного приготовительного момента $t_0 \equiv 0$, будут флуктуировать. При многократном повторении процедуры можно измерить распределение $p(t_1,t_2)$ или плотность распределения $w(t_1,t_2) = \partial^2 p/\partial t_1 \partial t_2$.

Итак, для большинства наблюдаемых квантовых эффектов понятие P является лишь удобным для наглядной интерпретации вспомогательным понятием, однако для некоторого узкого класса эффектов оно действительно необходимо -- для вывода правила Вигнера. Альтернативный операциональный подход заключается в принятии этого правила в качестве исходного постулата.

Двухуровневая система.

На первых этапах квантовой физики рассматривались лишь атомы с определенной энергией, E_g и E_e, при этом если ограничиться двумя уровнями (*двухуровненвый атом*), то у атома остается только две возможности и его пространство состояний эквивалентно пространству намагниченной монеты или ячеек памяти компьютера. Однако, если учесть так называемые *когерентные состояния* с неопределенной энергией, то пространство состояний двухуровневого атома становится непрерывным и имеет вид $|\psi\rangle = a|g\rangle + b|e\rangle$. Теперь состояние задается двумя комплексными числами, $\Psi = (a, b)$ и пространство событий обозначается $\mathbf{Z}^2 = \mathbf{R}^4$. Однако, если учесть нормировку $|a|^2 + |b|^2 = 1$ и игнорировать общую фазу $|\psi\rangle$, то состояние задается двумя вещественными параметрами, например, сферическими координатами точки (θ, φ) на *сфере Блоха* . Это же пространство состояний (в терминах теории групп оно называется SU(2)-пространством) описывает также спин 1/2 и поляризацию фотона. В последние годы большой интерес привлекает возможность создания *квантовых компьютеров,* в которых вместо электронных ячеек с дихотомным спектром состояний (0,1) будут использоваться системы -- атомы, фотоны -- с SU(2)-пространством, что произведет революцию в компьютерной технике.

Рассмотрим процедуру приготовления. Современная лабораторная техника позволяет поместить одиночный атом в ловушку и охладить его до сверхнизких температур, при этом он переходит в основное состояние $|g\rangle$. В момент времени $t_0 \equiv 0$ на него действует короткий лазерный импульс с опреде-

ленной амплитудой и длительностью. Лазерное излучение с большой точностью можно рассматривать классически. Частота лазера совпадает с боровской частотой перехода между $|g\rangle$ и одним из возбужденных $|e\rangle$ состояний атома. Согласно теории атом под действием лазерного импульса переходит в заданное состояние $|\psi\rangle$, где коэффициенты *a, b* определяются "площадью" лазерного импульса -- произведением амплитуды на длительность. Вероятность перехода под действием внешнего монохроматического поля дается формулой Раби:

$$P = \left[\frac{\Omega}{\tilde{\Omega}}\sin\left(\tilde{\Omega}t/2\right)\right]^2, \qquad (8.16)$$

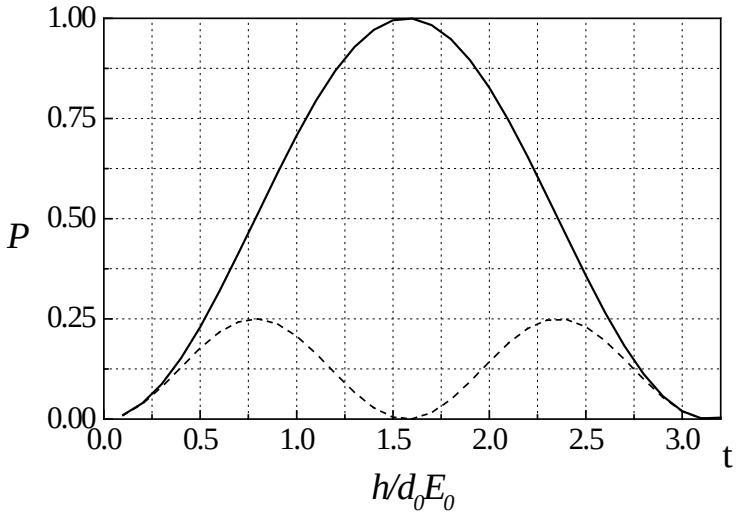
где $\Omega \equiv \left|\vec{d}_0\vec{E}_0\right|/\hbar$ - частота Раби (8.17)

$\tilde{\Omega} = \sqrt{\Omega^2 + \left(\omega - \omega_0\right)^2}$ - отстройка.

Эта формула показывает, что квантовая система под действием резонансного возмущения $\left(\omega \to \omega_0, \quad \tilde{\Omega} \to \Omega\right)$периодически переходит с нижнего уровня на верхний и обратно. Время перехода (из min в max), согласно (8.16), составляет:

$$\frac{t\Omega}{2} = \frac{\pi}{2}. \to t_\pi = \frac{\pi}{\Omega} = \frac{\pi\hbar}{d_0E_0}. \qquad (8.18)$$

Формула Раби дает рецепт приготовления двухуровневой системы в заданном состоянии. Например. для перевода системы из основного в когерентное состояние необходимо подействовать на нее т.н. “π/2”-импульсом, когда $\frac{t\Omega}{2} = \frac{\pi}{4}. \to t_{\pi/2} = \frac{\pi}{2\Omega} = \frac{\pi\hbar}{2d_0E_0}.$



Пунктиром отложена зависимость вероятности перехода от времени в нерезонансном случае, когда $\omega - \omega_0 = \sqrt{3}\Omega$.

Таким образом, данный атом при $t_0 \equiv 0$ приготавливается в заданном состоянии -- аналогично фальшивой игральной кости или монете. В дальней-

шем состояние эволюционирует в соответствии с уравнением Шредингера: $|\psi_0\rangle = a|g\rangle + b|e\rangle\exp(-i\omega_0 t)$, где ω_0 -- боровская част перехода.

Отметим, что описанная процедура *приготовления* не является *измерением* чего либо, так что эти процедуры не эквивалентны, как это часто полагают. Существенным допущением явилось классическое описание лазерного поля, которое играет роль заданной внешней силы, действующей на атом. Как и при описании измерения, на стадии приготовления необходимо "рукой" установить разумную границу между классическим и квантовым мирами.

До сих пор мы пренебрегали взаимодействием атома с невозбужденными, вакуумными модами поля, что допустимо в случае достаточно короткого лазерного импульса. Учет этого взаимодействия приведет к спонтанному излучению фотона (точнее, экспоненциального волнового пакета со средней частотой ω_e и длительностью t_e) - *релаксации*. Отображающая состояние точка на сфере Блоха движется по спирали от одного полюса к другому. Спустя время, много большее t_e атом с большой вероятностью оказывается в основном состоянии, а поле -- в однофотонном состоянии. Таким образом, наша модель дает также пример процедуры приготовления поля в определенном состоянии.

Итак, современная техника позволяет приготовлять достаточно надежно определенные состояния атомов и поля. Как уже отмечалось, эта техника привлекает сейчас большое внимание в связи с идеей квантового компьютера.

Существует целый класс эффектов, позволяющих говорить о фазе волновой функции, относящейся к индивидуальной частице. Такие эксперименты позволяют говорить об операциональном смысле ВФ отдельного квантового объекта. На прошлой лекции мы рассматривали воздействие двух ЛЭ Адамара на двухуровневую систему - кубит. Мы показали, что управляя относительной фазой можно перенаправить частицу из одного плеча в другой. В основе этого эффекта лежит явление квантовой интерференции. Другими словами, по желанию экспериментатора амплитуду ВФ в том или ином выходном плече можно обратить в нуль. Следовательно, манипулируя задержкой мы управляем волновой функцией.

Интерферометр $HP(\theta)H$ действует как унитарный преобразователь. При этом чистое состояние преобразуется в чистое состояние.

Итак полную информацию об измеримых статистических свойствах (в данный момент времени) дает вектор состояния в каком-то представлении. Например, в координатном представлении $\langle x|\psi\rangle \equiv \psi(x)$. Другими словами, оператор координаты $\hat{X}$ в единственном числе составляет полный набор операторов, необходимых для задания состояния. То же можно сказать и об импульсе $\hbar\hat{K}$ - состояние можно задать вектором состояния в импульсном представлении $\langle k|\psi\rangle \equiv \psi(k)$ или фурье-образом $\psi(x)$.

Замечание. Оператор энергии $\hat{H} = \hat{K}^2/2m$ не образует полного набора, поскольку оставляет неопределенным знак импульса (зависит от его квадрата).

Для *задания* чистого состояния достаточно указать собственные значения всех операторов полного набора. Например, если известно, что $k = k_1$, то волновая функция полностью определена:

$\psi(x) = \exp\{ik_1 x\}$. Если спектр операторов дискретный, то состояние задается набором квантовых чисел (для двухуровневой системы $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ - это пара комплексных чисел α и β).

Для измерения чистого состояния необходимо произвести многократное измерение (например, координаты) с помощью идеального детектора. При этом измеряется лишь модуль волновой функции - ее огибающая $|\psi(x)|$. Фаза волновой функции непосредственно не наблюдаема. Значит нужно производить дополнительные измерения (хотя оператор $\hat{X}$ и представляет полный набор). Например, можно измерить огибающую волновой функции в импульсном представлении $|\psi(k)|$

ЛИТЕРАТУРА

1. Д.Н.Клышко Основные понятия квантовой физики с операциональной точки зрения. УФН, 168, №9, 975-1016 (1998).
2. Д.Н.Клышко Физические основы квантовой электроники. М.,”Наука”, 1986, 293с.

ЛЕКЦИЯ 9. Квантовые (неклассические) состояния света и их использование в квантовой информатике.

1. Роль неклассических полей в физике квантовой информации. Определение (I) неклассического света и его недостатки.
2. Элементарная полуклассическая теория фотодетектирования. Фактор Фано и параметр группировки. Супер- и субпуассоновский свет. Одномодовый детектор. Формула Манделя. Гомодинирование. Связь распределений энергии и комплексной амплитуды. Квазивероятность. Распределение Глаубера-Сударшана.
3. Наблюдаемые признаки неклассичности света. Мера Ли. Операциональное определение (II) неклассического света. g_2 - и D -критерии. Примеры: лазерный свет, тепловое излучение, смесь вакуумного и K-фотонного состояний.

Использование световых сигналов закономерно вызывает интерес при решении проблемы передачи квантовой информации. Дело в том, что определенные типы световых полей обладают рядом свойств, которые непосредственно используются в квантовых коммуникационных протоколах, например, таких как квантовая телепортация и сверхплотная кодировка. В квантовой криптографии сообщения между удаленными пользователями осуществляются на основе специфических световых полей, рассматриваемых как системы с квантовыми свойствами. Поэтому возникает вопрос количественного описания излучения и выделения его отличительных признаков. Особенно полезно выделить т.н. операциональные критерии, которые можно было бы применить в эксперименте. Грубо говоря, под неклассическим понимается свет, свойства которого нельзя описать классическим образом, т.е. такой свет, который не имеет классических аналогов.

Свойства световых полей можно исследовать анализируя свойства фототока, порождаемых ими. При этом логично анализировать как средний ток, так и его флуктуации. Известно, что средний ток пропорционален интенсивности света, падающего на фотодетектор. Флуктуации фототока можно объяснить случайностью рождения фотоэлектронов в процессе детектирования (фотоэффекта), поэтому долгое время им не придавали существенного значения. Такие флуктуации были названы *пуассоновскими* или *дробовыми*. Тривиальность флуктуаций такого рода объяснялась тем, что даже абсолютно стабилизированное по амплитуде и фазе электромагнитное излучение, которое описывается плоской волной, будет вызывать случайные флуктуации тока, вызванные случайностью рождения фотоэлектронов.

Наблюдение флуктуаций фототока, превышающими по величине пуассоновские флуктуации было выполнено Брауном и Твиссом в середине 50-х годов. В этих экспериментах исследовался свет, излучаемый звездами или ртутной лампой. (Избыточные флуктуации наблюдались с помощью двух детекторов, т.е. в этих экспериментах анализировались четвертые моменты поля.) Такие избыточные флуктуации имеют объяснение в классической теории: поскольку амплитуда электромагнитной волны. падающей на детекторы случайно изменяется, то и флуктуации фототока также будут иметь дополнительную (по отношению к пуассоновскому уровню) синхронно изменяющуюся компоненту. В этом случае говорят о *группировке* фотонов в пучке, приводящей к *суперпуассоновской* статистике тока. Следовательно и

свет, исследовавшийся Брауном и Твиссом, впоследствии названный тепловым, можно отнести к разряду “классических”. Тем не менее, эксперименты, выполненные Брауном и Твиссом, считают первыми экспериментами, положившими начало квантовой оптике.

Несколько позже были исследованы и истинно неклассические состояния поля, такие как излучение при *двухквантовых переходах* в атомах или *спонтанном параметрическом рассеянии* света. Еще позднее был зарегистрирован свет, у которого флуктуации тока оказались ниже, чем пуассоновский уровень - это эффект *антигруппировки* фотонов, приводящий к *субпуассоновской* статистике фототока или сжатые состояния.

С помощью неклассических состояний света стало возможным продемонстрировать известный парадокс, рассмотренный А.Эйнштейном, Б.Подольским и Н.Розеном, поскольку именно в таких состояниях реализовывались необходимые корреляционные свойства излучения. Впоследствии эти же состояния были использованы в экспериментах по нарушении неравенств Белла. Это позволило говорить о неприменимости классических моделей, в которых вероятностная интерпретация квантовой теории обосновывалась введением скрытых параметров.

Перед тем, как перейти к количественному описанию нелассических полей, заметим, что многие из них образуются в результате нелинейных оптических процессов.

Замечание. В квантовой криптографии используется метод получения “однофотонных” состояний, который осуществляется с помощью ослабления лазерных импульсов. При этом, конечно возникающие состояния не являются однофотонными - всегда существует вероятность, что в импульсе окажется 0 или, скажем, 2 фотона.

Определение I. Свет, для которого *P*-распределение Глаубера-Сударшана принимает отрицательные значения или является нерегулярной функцией, называется неклассическим. Здесь под *P*-распределением понимается квантовый аналог классического распределения вероятности для амплитуд поля.

Это определение, очевидно, нельзя отнести к непосредственно применяемым в эксперименте, т.е. операциональному. В экспериментах измеряется статистика фототока (или распределение импульсов фототока), связанная со статистическими свойствами падающего на детектор светового поля посредством формулы Л.Манделя.

Будем считать, что фотодетектор работает в “режиме счета фотонов”, когда на его выходе образуется последовательность не перекрывающихся импульсов фототока. Периодически подсчитывается число таких импульсов m за малое время T. В силу случайности, это число флуктуирует - можно вычислить моменты, т.е. определить полные вероятностные характеристики дискретной случайной величины m. Зададим их с помощью распределения вероятностей p_m, когда выполняются требования колмогоровской теории вероятностей

$$\left(\sum_{m=0}^{\infty} p_m = 1, \quad p_m \geq 0 \right) \tag{9.1}$$

или моментов:

$$\left\langle m^k \right\rangle = \sum_{m=0}^{\infty} m^k p_m, \quad k = 1, 2, 3.. \tag{9.2}$$

По определению, средним числом отсчетов и дисперсией называются моменты:

$$\langle m\rangle = \sum_{m=0}^{\infty} m p_m, \tag{9.3}$$

$$\left\langle \Delta m^2 \right\rangle = \left\langle m^2 \right\rangle - \langle m\rangle^2 . \tag{9.4}$$

Через них можно определить ввести фактор Фано:

$$F = \frac{\left\langle \Delta m^2 \right\rangle}{\langle m\rangle} \tag{9.5}$$

и параметр группировки фотонов:

$$g_2 = 1 + \frac{\left\langle \Delta m^2 \right\rangle - \langle m\rangle}{\langle m\rangle^2} = 1 + \frac{F-1}{\langle m\rangle}. \tag{9.6}$$

Нетрудно заметить, что эти два параметра характеризуют отличие статистики от пуассоновской. Действительно, в случае пуассоновской статистики $\left\langle \Delta m^2 \right\rangle = \langle m\rangle$, поэтому $F = g_2 = 1$. Для теплового поля $\left\langle \Delta m^2 \right\rangle = \langle m\rangle + \langle m\rangle^2$, поэтому $F = 1 + \langle m\rangle, g_2 = 2.$

Если F < 1 или g_2 < 1, то статистика является *субпуассоновской*, а излучение - *субпуассновским* (неклассическим) светом или антигруппированным светом.

С точки зрения простейшей “корпускулярной” модели фотоэффекта эффект антикорреляции можно объяснить следующим образом. Пусть квантовая эффективность детектора η = 100%. Тогда прибытие каждого фотона вызывает появление фотоэлектрона. Таким образом поток фотоэлектронов “повторяет” поток фотонов, т.е. условие $\left\langle \Delta m^2 \right\rangle \neq \langle m\rangle$ означает, что в потоке фотонов имеется некая регулярность, по сравнению с хаотическим пуассоновским распределением, где все события равноправны. Тогда условие g_2 > 1 интерпретируется как группировка, а g_2 < 1 - как отталкивание. Например, известен способ получения антигруппированного света, когда одиночные атомы возбуждаются резонансным излучением, после чего они флюоресцируют. Акт следующего поглощения атомом энергии не может произойти раньше некоторого времени, поэтому и в излученном свете фотоны антигруппированы, что и дает субпуассоновскую статистику. В идеальном случае атом излучает в строго определенные моменты времени, поэтому $F = g_2 = \left\langle \Delta m^2 \right\rangle = 0$. Заметим, что в рамках корпускулярной модели света (фотоны- шарики) эффект антикорреляции имеет простое объяснение.

При использовании квантовых моделей для описания света число фотонов является оператором:

$$\hat{n} = a^{\dagger} a . \tag{9.7}$$

Можно рассчитать распределение числа фотонов p_n и моменты этого распределения $\left\langle n^k \right\rangle$. Последовательное квантовое описание очень хорошо согласуется с экспериментом, но встречаются трудности с его интерпретацией. Так, на сегодняшний день общепринятой является “копенгагенская” трактовка, которая не допускает априорного существования некоторых физических

величин. Операциональные свойства неклассического света возникают в рамках *полуклассического подхода*, когда атомы детектора описываются квантовым образом, а падающее поле - классическим. В рамках этого подхода не удается описать ряд оптических экспериментов. Именно в этих случаях и принято говорить о неклассических состояниях света.

Одномодовый детектор.

Пусть площадь детектора $A<<A_{coh}$ падающего света, а интервалы выборки $T << \tau_{coh} \equiv 2\pi/\Delta\omega = 1/\Delta f$. Таким образом детектор регистрирует одну моду поля, т.е. одну независимую колебательную степень свободы. Динамическое (или статистическое) описание тогда совпадает с описанием гармонического осциллятора. Для стационарного квазимонохроматического поля

$$E = E_0 \sin\left(\omega_0 t + \varphi\right),$$

где E_0 и φ - случайные (медленно меняющиеся) функции времени. Характерное время изменения этих параметров и называется временем когерентности τ_{coh}.

Замечание. Если детектор многомодовый, то необходимо дополнительно проводить усреднение по времени и пространству, что в пределе многих мод дает опять тривиальную пуассоновскую статистику, которая не зависит от свойств падающего поля.(*конец*)

Если от амплитуды перейти к числу фотонов - энергии, приходящейся на объем когерентности (в нашем случае $V_{coh} \equiv c\tau_{coh}A_{coh} = V_{\det} \equiv cTA$) и деленный на энергию одного фотона:

$$n \equiv \frac{энергия\ \ поля}{энергия\ \ кванта} = \left\{ энергия\ \ поля = \frac{E_0^2 V}{8\pi} \right\} = \frac{E_0^2 V_{coh}}{8\pi\hbar\omega_0}. \qquad (9.8)$$

$$\left(интенсивность\ \ I = \frac{cE_0^2}{8\pi} \right)$$

Эта величина принимает любые действительные неотрицательные значения. Поэтому и статистика фотоэлектронов в полуклассическом случае определяется непрерывным распределением *P(n)*.

Замечание. В квантовой теории этой классической переменной соответствует оператор числа фотонов в одной моде $\hat{n}$, который имеет спектр собственных значений в виде набора целых чисел 0, 1, 2... Статистика определяется дискретным распределением *p(n)*. (*конец*)

Замечание. Среднее число фотонов в одной моде связано с интенсивностью I эффективной полосой частот света $\Delta\omega$ (для одной поперечной моды):

$$I = \frac{\hbar\omega\Delta\omega\langle n\rangle}{2\pi}$$ (*конец*)

В качестве примера рассмотрим световой поток, который имеет мощность $W = 10^{-9}$ *Вт*, спектральная ширина излучения $\Delta f = \Delta\omega/2\pi = 10^9$ *Гц* с центральной длиной волны $\lambda = 0.5$*мкм*. Тогда, подставляя в (9.8), получаем:

$$n = \frac{E_0^2}{8\pi}\frac{V_{coh}}{\hbar\omega_0} = \frac{E_0^2}{8\pi}\frac{c\tau_{coh}A}{\hbar\omega_0} = \frac{E_0^2 cA}{8\pi}\frac{\tau_{coh}}{\hbar\omega_0} =$$

$$\left\{ I = \frac{E_0^2 c}{8\pi},\ W = \frac{E_0^2 cA}{8\pi} \right\} = W\frac{\tau_{coh}}{\hbar\omega_0} =$$

$$= 10^{-9}\times 10^{7}\frac{1/\Delta f}{\hbar\left[2\pi c/\lambda\right]} = 10^{-2}\frac{10^{-9}}{10^{-27}\left[6*3*10^{10}/5*10^{-5}\right]} \approx \ 2.8\ \textit{фотона}.$$

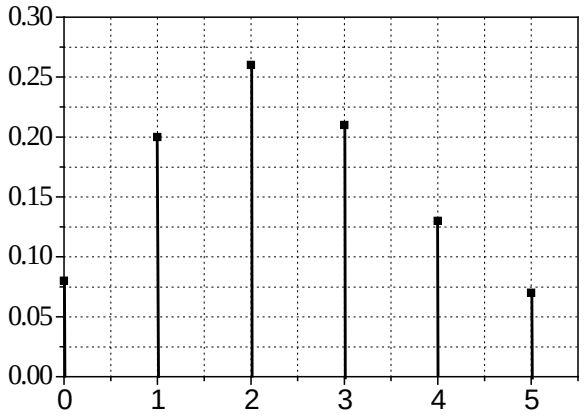
Формула Манделя (полуклассическая)

Если квантовая эффективность детектора равна η, то вероятность появления фотоэлектрона в интервале *(t, t + dt)*. Поскольку фотоэлектроны рождаются случайно, то среднее их число за время T:

$\langle m\rangle = \eta\langle n\rangle$, где символ *m* относится к электронам, а *n* - к фотонам. Если интенсивность поля постоянна, то *n* не флуктуирует**. Будем считать детектор идеальным, т.е. η = 100%.** Поскольку все моменты времени рождения фотоэлектрона эквивалентны, то он может с одинаковой вероятностью *<n>dt/T* возникнуть в любом интервале *dt*, принадлежащем *T*. Тогда статистика числа отсчетов будет определяться распределением Пуассона:

$$p_m = \frac{\langle n\rangle^m \exp\{-\langle n\rangle\}}{m!}. \qquad (9.9)$$

Формула (9.9) показывает, что в среднем за время *T* наблюдается *m* отсчетов. Для примера, разобранного выше ($\langle m\rangle = \langle n\rangle = 2.8$) получаем: p_0 = 0.08, p_1 = 0.2, p_2 = 0.26, p_3 = 0.21, p_4 = 0.13, p_5 = 0.07 (для чисел *m* = 0, 1, 2, 3, 4, 5,...)



Замечание. Даже для стабилизированного по амплитуде излучения с $E_0 = const$ (идеального лазера) имеем пуассоновское распределение фотоэлектронов - т.н. дробовой шум. (*конец*)

Все другие источники света, у которых величина *n=<n>* флуктуирует, будут характеризоваться избыточными флуктуациями фототока, вызванными флуктуациями интенсивности. Такие флуктуации можно описать, введя функцию распределения “интенсивности”: *P(n)*. Т.е. вероятность того, что интенсивность излучения (выраженная в единицах *n*) принимает значение в интервале *(n, n + dn)* равна *P(n)dn*. Очевидно, что классическая плотность вероятности *P(n)* должна удовлетворять аксиомам Колмогорова:

$$\int_0^\infty P(n)dn = 1, \quad P(n) \geq 0. \tag{9.10}$$

Тогда распределение наблюдаемой дискретной величины p_m оказывается связанным с распределением интенсивности поля $P(n)$ через преобразование Пуассона:

$$p_m = \frac{1}{m!}\int_0^\infty n^m \exp\{-n\} P(n)dn \tag{9.11}$$

Наблюдается как бы двойная стохастичность. Во-первых, за счет случайности образования фотоэлектрона (постоянная величина - электромагнитное поле - порождает дискретный набор фотоэлектронов). Во-вторых, за счет флуктуаций самой интенсивности падающего света, что и приводит к *избыточному шуму*.

Тепловой (хаотический) свет.

Свет с тепловой статистикой возбуждается многими независимыми источниками со случайными амплитудами и фазами. Примером служит излучение нагретого тела, свет звезд. При этом распределение комплексной амплитуды $z = z' + iz'' = E_0{}' + iE_0{}''$ является гауссовым (или нормальным) с независимыми z' и z''. Распределение интенсивности описывается экспоненциальным законом:

$$P_T(I) = \frac{1}{\langle I \rangle}\exp\left\{-I/\langle I \rangle\right\}. \tag{9.12}$$

Видно, что средняя интенсивность <*I*> полностью определяет статистику одной моды стационарного хаотического поля. Из (9.12) следует связь между дисперсией и средней интенсивностью:

$$\left\langle \Delta I^2 \right\rangle_T = \left\langle I^2 \right\rangle_T - \langle I \rangle^2{}_T = \langle I \rangle^2{}_T. \tag{9.13}$$

Для фотоотсчетов при этом справедливо:

$$\left\langle \Delta m^2 \right\rangle = \langle m \rangle + \eta^2 \left\langle \Delta I^2 \right\rangle \rightarrow$$
$$\left\langle \Delta m^2 \right\rangle_T = \langle m \rangle \left(1 + \langle m \rangle\right). \tag{9.14}$$

<u>Гомодинное детектирование.</u>

До сих пор рассматривалось лишь распределение энергии (интенсивности) падающего поля $P(n)$ и игнорировались флуктуации фазы φ. Их можно измерить с помощью *гомодина*, смешивая исследуемое излучение с излучением стабильного по фазе лазерным пучком (т.н. опорный генератор). Пусть $z = z' + z''$ комплексная амплитуда волны.

По определению когерентными состояниями $|z\rangle$ называются собственные функции (неэрмитова) оператора уничтожения фотона:

$$\hat{a}|z\rangle = z|z\rangle,$$

$$\langle z|a^\dagger = z^*\langle z|.$$

<u>Замечание.</u> Из этих формул сразу следует, что среднее число фотонов в когерентном состоянии $\langle n \rangle \equiv \langle z|n|z\rangle = |z|^2$.

Связь между *n* и *z* дается условием нормировки:

$$|z|^2 \equiv n = \frac{E_0^2 V_{coh}}{8\pi\hbar\omega_0}. \qquad (9.15)$$

Двумерная вероятность $P_z(z)$ полагается нормированной

$\int P_z(z) d^2 z = 1$, где $d^2 z \equiv dz' dz'' = |z| d|z| d\varphi$.

(9.16)

Функция $P_z(z)$ играет роль квазивероятности вероятности того, что осциллятор имеет комплексную амплитуду z, т.е. $\left(q = \sqrt{2} z', \quad p = \sqrt{2} z''\right)$.

Тогда формула Манделя (9.11) приобретает вид:

$$p_m = \frac{1}{m!} \int_0^\infty |z|^{2m} \exp\left\{-|z|^2\right\} P_z(z) d^2 z.$$

Эту формулу называют квантовым аналогом формулы Манделя.

Замечание. Если квантовая эффективность меньше 100%, то (9.17) переходит в:

$$p_m = \frac{1}{m!} \int_0^\infty \left(\eta |z|^2\right)^m \exp\left\{-\eta |z|^2\right\} P_z(z) d^2 z. \text{ (\textit{конец})} \qquad (9.17)$$

Можно выразить распределение энергии $P(n)$ через распределение комплексной амплитуды $P_z(z) \equiv P_z(z', z'')$. Тогда

$$P(n) = P_z(|z|) \frac{d|z|}{dn} = \frac{1}{2} \int_0^{2\pi} d\varphi P_z\left(\sqrt{n}\cos\varphi, \sqrt{n}\sin\varphi\right). \qquad (9.18)$$

В случае стационарного поля P_z не зависит от фазы, следовательно,

$$P(n) = \pi P_z\left(\sqrt{n}\right). \qquad (9.19)$$

При гомодинировании (смешении) двух независимых по фазе колебаний распределение результирующего поля равно свертке исходных распределений:

$$P_z(z) = \int d^2 z_1 P_z^{(1)}(z - z_1) P_z^{(2)}(z_1) = \int d^2 z_1 P_z^{(1)}(z_1) P_z^{(2)}(z - z_1). \qquad (9.20)$$

Одно из этих колебаний описывает лезерное поле со стабильной амплитудой z_0:

$$P^{(2)}(z) = \delta^{(2)}(z - z_0) = \delta\left(z' - z_0'\right) \times \delta\left(z'' - z_0''\right) \qquad (9.21)$$

Тогда $P_z(z) = P_z^{(1)}(z - z_0)$. Теперь наглядно видно, что при гомодинировании исходное распределение $P_z^{(1)}(z)$ просто смещается в комплексной плоскости z *без изменения своей формы*! **Согласно "Определению I" статус состояния не меняется - классическое распределение остается классическим, а неклассическое - неклассическим!**

Замечание. Функция $P_z(z)$ может принимать отрицательные значения и даже в случае чистого состояния $P^{(2)}(z) = \delta^{(2)}(z - z_0)$ координата q и импульс p испытывают нулевые флуктуации, поэтому функцию $P_z(z)$ называют квазивероятностью. (*конец*)

Используя формулу (9.17) можно найти распределение числа отсчетов для теплового и когерентного излучений.

1. Когерентное поле. $P^{(2)}(z) = \delta^{(2)}(z - z_0)$, откуда

$P_z(m) = \langle m \rangle^m e^{-\langle m \rangle} / m!$.

2. Тепловое поле. $P_T(z) = \dfrac{\exp\left(-|z|^2 / \langle N \rangle\right)}{\pi \langle N \rangle}$, откуда

$P_T(m) = \langle m \rangle^m / \left(1 + \langle m \rangle\right)^{m+1}$.

где $\langle m \rangle = \eta \langle N \rangle$.

Квантовая теория.

В квантовой теории статистика фотоотсчетов определяется оператором плотности ρ для свободного поля, падающего на детектор. При использовании (дискретного) фоковского базиса диагональный матричный элемент (детектор считается идеальным) дает вероятность наблюдения *n* отсчетов:

$p_n = \rho_{nn} \equiv \langle n | \rho | n \rangle$. (*)

В случае чистого состояния $\rho \equiv |\psi\rangle\langle\psi|$, так что $p_n = |\langle n | \psi \rangle|^2$.

Обычные моменты определяются в соответствии с правилами квантовой теории:

$$\langle n^k \rangle = \left\langle \left(a^\dagger a\right)^k \right\rangle = Sp\left(\rho n^k\right) = \sum_n \rho_{nn} n^k.$$

Что же общего между квантовой формулой (*) и полуклассической формулой Манделя (9.11)? Оказывается связь между вероятностью и матрицей плотности $p_n = \rho_{nn}$ просто преобразуется к виду (9.11). Для этого надо использовать непрерывное представление векторов и операторов по когерентным состояниям $|z\rangle$. При этом оператор плотности изображается некоей функцией, называемой представлением Глаубера-Сударшана. Эта функция определяет распределение отсчетов p_m посредством преобразования Пуассона, совпадающим по форме с формулой Манделя (9.11) или (9.17). Отличие состоит только в том, что функция $P_z(z)$ или $P(n) = \pi P_z\left(\sqrt{n}\right)$ определена теперь через оператор плотности и может быть отрицательной и нерегулярной, т.е. является квазираспределением.

Наблюдаемые признаки неклассического света.

Только что было продемонстрировано, что свойство неклассичности инвариантно к гомодинированию с *когерентным состоянием* (лазерное поле с постоянной комплексной амплитудой). Оказывается, что это утверждение не выполняется в случае подмешиваемого поля с произвольной статистикой, например, с тепловой. Такое поле (тепловое) имеет экспоненциальное распределение интенсивности. Поэтому исходное распределение “портится” тем быстрее, чем больше интенсивность теплового поля. При этом сингулярные и отрицательные участки исчезают, так что исходное неклассическое поле может стать классическим.

Мера Ли.

Пусть N_T - среднее число фотонов в одной моде вспомогательного теплового поля. Под мерой Ли понимают минимальное число фотонов, $N_0 = N_T$, при котором распределение $P_z(z)$ остается неотрицательной регулярной функцией в

смысле “Определения I”. Можно показать, что N_0 изменяется от 1 (для максимально неклассических полей - K-фотонных) до 0 (для классических). Важно то, что величину N_0 можно, в принципе, измерить. Для этого следует к исследуемому свету добавить с помощью светоделителя тепловой свет с регулируемой интенсивностью.

Операциональное определение неклассического света.

Для идеального лазера, статистика которого описывается распределением Пуассона, $\left\langle \Delta m^2 \right\rangle = \left\langle m \right\rangle$.Следовательно, для такого излучения $F = g_2 = 1$. Поэтому представляется, что другие источники света из-за нестабильности их параметров могут лишь увеличить шумы фототока. Отсюда следует вывод, что наблюдение субпуассоновской статистики с $g_2 < 1$ в полуклассической теории невозможно! Значение $g_2 = 1$ является нижней границей в случае полуклассической теории фотоотсчетов: $g_{2\ class} = 1$. **Условие $g_2 < 1$ также называют g_2 - критерием неклассичности света.**

Определение II. Если наблюдаемая статистика фотоотсчетов не согласуется с полуклассической формулой Манделя (9.11) при $P(n) \geq 0$, т.е. если падающий на детектор свет нельзя описать некоторым распределением энергии $P(n)$, то свет называется неклассическим.

Замечание. Если свет порождает антигруппировку отсчетов, то он неклассичен.

Как же применить “Определение II” к результатам эксперимента? Очевидно, для этого нужно обратить формулу Манделя (9.11), т.е. определить функцию $P(n)$ через измеренный набор чисел $\{p_m\}$. Если это удастся, то проверить условие неотрицательности $P(n) \geq 0$.

В общем случае эта процедура неоднозначна. Она восходит к математической *проблеме моментов* - выражение вероятностей через моменты, которая рассматривалась на прошлой лекции.

Пусть в эксперименте измерен набор (чисел) отсчетов $\{m\}$. Из них можно построить наборы вероятностей $\{p_m\}$ или факториальных моментов:

$$G_k \equiv \left\langle m(m-1)(m-2)...(m-k+1) \right\rangle =$$

$$= \sum_{m=k}^{\infty} \frac{m!}{(m-k)!} p_m = \sum_{m=0}^{\infty} \frac{(m+k)!}{m!} p_{m+k}. \qquad (9.22)$$

Они являются комбинациями обычных моментов $\langle m^k \rangle$, например, $G_2 = \left\langle m(m-1) \right\rangle = \left\langle m^2 \right\rangle - \left\langle m \right\rangle$.

Замечание. Если известны обычные моменты $\langle m^i \rangle$ для $1 \leq i \leq k$, то можно вычислить и факториальные G_k. (*конец*)

Замечание. Факториальные моменты дискретного распределения отсчетов p_m, определяемого по формуле Манделя (9.11) совпадают с обычными моментами непрерывного распределения энергии $P(n)$:

$$G_k = \left\langle n \right\rangle^k \int n^k P(n) dn. \text{ (конец)} \qquad (9.23)$$

Замечание. Нормированные факториальные моменты вводятся так:

$$g_k \equiv \frac{G_k}{G_1^k}. \text{ (конец)} \qquad (9.24)$$

Из чисел отсчета $\{m_k\}$ можно составить комбинации моментов G_k некоторой неотрицательной функции, следовательно, моменты должны удовлетворять некоторым неравенствам.

Оказывается, что в общем случае для неклассичности света **достаточно** выполнение хотя бы одного из бесконечного набора условий вида

$$D_k < 1, \quad (k = 1, 2...). \tag{9.25}$$

Замечание. Выполнение условий (9.25) является достаточным условием, т.е. при невыполнении ни одного из этих условий свет может быть неклассическим. Необходимым условием ***классичности*** служит неравенство:

$$g_k g_l \le g_{k-1} g_{l+1}, \quad (k, l = 1, 2...).$$

В частности, при $k = l$, получаем:

$$D_k = \frac{g_{k-1} g_{k+1}}{g_k^2} \ge 1, \quad k = 1, 2..$$

Например, при $k = 1$, $g_2 \ge g_1^2$.

Итак, упомянутые выше неравенства имеют вид:

$$D_k(1) = \frac{(k+1)\, p_{k-1} p_{k+1}}{k p_k^2} < 1, \tag{9.26}$$

$$D_k(0) = \frac{g_{k-1} g_{k+1}}{g_k^2} < 1. \tag{9.27}$$

Эти условия называются D_k - критериями. Рассмотрим, например, условие $D_1(0) = g_2 < 1$. Оно совпадает с наиболее известным критерием неклассичности - антигруппировкой фотоотсчетов. Условие $D_k(0) < 1$ при $k \ge 2$ иногда называют антигруппировкой высших порядков. Введенные величины могут служить и количественными мерами степени неклассичности. Так случай $D_k = 0$ соответсвует максимальной неклассичности, а $D_k = 1$ - минимальной. Рассмотрим некоторые примеры.

1. Идеальный лазерный свет дает пуассоновское распределение числа отсчетов (9.9) с параметром $\langle n \rangle = N = |z_0|^2$:

$$p_m = \frac{\langle n \rangle^m \exp\{-\langle n \rangle\}}{m!}.$$

При этом $g_k = G_k = N^k$. Поэтому $D_k(0) = D_k(1) = 1$. Это распределение является промежуточным между классическим и квантовым.

2. Тепловое поле дает

$$G_k = k! N^k,$$

$$g_k = k!$$

откуда $D_k(0) = D_k(1) = \frac{k+1}{k} > 1.$

3. Рассмотрим такие распределения числа отсчетов для которых вероятность некоторого числа отсчетов κ равна нулю: $p_{k-1} \ne 0, \quad p_k = 0, \quad p_{k+1} \ne 0.$ Тогда

$D_{k-1}(1) = D_{k+1}(1) = 0$ - распределение неклассично.

Аналогично, если $p_{k-1} = 0, \quad p_k \ne 0, \quad p_{k+1} = 0$, то $D_k(1) = 0$.

Возникает вопрос, не исчерпывает ли условие антигруппировки $g_2 < 1$ (или g_2 -критерий) все случаи неклассического света, т.е. не является ли это условие достаточным?

Рассмотрим в качестве примера шумовое излучение вырожденного по частоте параметрического усилителя света - параметрическое рассеяние света. Состояние света при этом называют сжатым вакуумом. Из квантовой теории следует, что $\langle m\rangle = \sinh^2 \Gamma$, и $\left\langle \Delta m^2 \right\rangle = 2\langle m\rangle\big(\langle m\rangle + 1\big)$. Здесь Г - коэффициент параметрического усиления, который зависит от расстройки синхронизма, $\chi^{(2)}$, интенсивности накачки и проч. Тогда

$$D_1(0) = g_2 = 3 + \frac{1}{\langle m\rangle} > 3. \qquad (9.28)$$

Следовательно статистика параметрического рассеяния - сверхпуассоновская, и согласно g_2-критерию свет является классическим! Более того, обычно в эксперименте $g_2 \sim 10^2 - 10^8$ и имеет место сверхгруппировка, когда $g_2 > 2$. Именно такое излучение часто используется в квантовых коммуникационных протоколах. Почему же его относят к неклассическим?

Теоретически это следует из “Определения I”. Можно показать, что регулярного P_z- распределения Глаубера Сударшана не существует.

С другой стороны, расчет матрицы плотности дает значения ее диагональных компонент $\rho_{nn} = 0$ для нечетных n. Таким образом, сжатый вакуум состоит четного числа фотонов, когда $p_{2k+1} = 0$. Такие резкие провалы в распределении вероятностей противоречат полуклассической формуле Манделя (9.11), согласно которой соседние вероятности p_{m-1}, p_m, p_{m+1} должны иметь, по-видимому, сравнимые величины. Это подтверждается и D-критериями (9.26, 9.27): при четных m получаем

$$D_m(1) = p_{m-1}p_{m+1} \big/ p_m^2 = 0 .$$

Излучение при параметрическом рассеянии света неклассично, даже при отсутствии антигруппировки! В предельном случае Г<<1 параметрический усилитель излучает смесь вакуумного (преобладающего) состояния и двухфотонного фоковского:

$$P(N) = P(0)\delta_{N0} + P(K)\delta_{NK}, \quad K = 2.$$

Среднее число фотонов $\langle N\rangle = KP(K)$, и моменты можно выразить через него.

$$P(0) = 1 - P(K), \quad \left\langle N^m \right\rangle = K^m P(K) = K^{m-1}\langle N\rangle, \quad 0 \le N \le K . \qquad (9.29)$$

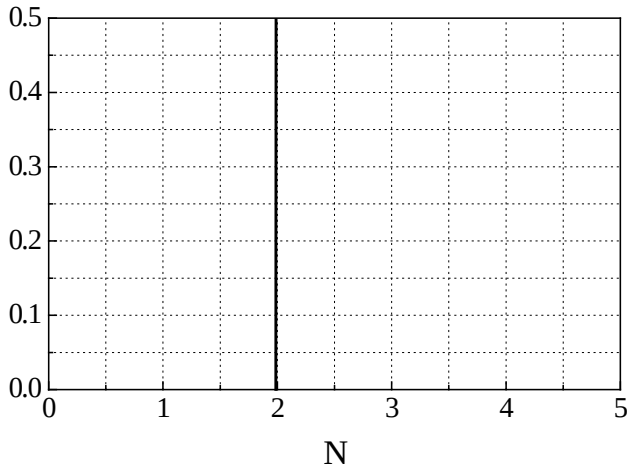
В случае $\langle N\rangle = K$, получаем чистое энергетическое состояние с K фотонами, когда в объеме когерентности заведомо присутствует K фотонов. В зависимости от соотношения между $\langle N\rangle$, K и N можно получить разные типы статистики K-фотонного света.

Из (9.29) следует, что параметр группировки для K-фотонного равен:

$$g_2 = \frac{(K-1)}{\langle N\rangle}. \qquad (9.30)$$

1. Пусть $\langle N\rangle << K - 1$, (смесь K-фотонного состояния и вакуума). Отсюда получаем сверхгруппировку, $g_2 >> 1$.

Ниже изображено распределение числа фотонов для $\langle N \rangle = 1.$



2. Пусть $\langle N \rangle > K - 1,$ получаем антигруппировку. В частности при однофотонном распаде (К = 1), $g_2 = 0$.
3. В чистом К-фотонном состоянии флуктуации числа фотонов N отсутствуют, $P(N) = \delta_{NK}$, $\langle N^m \rangle = \langle N \rangle^m \rightarrow$

$$g_2 = \frac{\langle N^2 \rangle - \langle N \rangle}{\langle N \rangle^2} = 1 - \frac{1}{K} < 1.$$

В заключение отметим, что излучение при параметрическом рассеянии света (смесь вакуума и двухфотонного света) используется для демонстрации более общей неклассичности света. Этот тип неклассичности противопоставляется не с классической статистической оптикой, а с вероятностной моделью, предложенной Беллом, основанной на наличии “скрытых” параметров у квантовых объектов.

На будущее: подробно остановиться на анализе неклассичности основных типов полей, используемых в квантовой информации: К-фотонных и их смеси с вакуумом (это есть); сжатых (этого почти нет), а также классических - тепловых и когерентных (это есть)

ЛИТЕРАТУРА.

1. Д.Н.Клышко. Неклассический свет. УФН, т.166, №6, 613-638 (1996).
2. Д.Н.Клышко. Квантовая оптика: квантовые, классические и метафизические аспекты. УФН, т.164, № 11, 1187-1214 (1994).
3. Д.Н.Клышко Физические основы квантовой электроники. М.,”Наука”, 1986, 293с.

ЛЕКЦИЯ 10. Парадокс Эйнштейна - Подольского - Розена и неравенства Белла.

1. Парадокс ЭПР в варианте Бома. Антисимметричные состояния. Их инвариантность относительно поворота базиса. Аналогия между состояниями частиц со спином 1/2 и поляризационными состояниями света.
2. Неравенства Белла. Классическая модель с двумя дихотомными переменными. Измеряемая Белла. Модель скрытых параметров. Квантовая модель: спонтанное параметрическое рассеяние из двух кристаллов. Роль некоммутирующих операторов.
3. *Парадокс Белла для трех наблюдаемых. Состояния Гринберга - Хорна - Цайлингера. Теорема Белла без неравенств.

В 1935 году А.Эйнштейн, Б.Подольский и Н.Розен предложили мысленный эксперимент, на основании результатов которого они пришли к выводу, что квантовомеханическое описание не является полным и что существуют элементы реальности, которые не учитываются в квантовой механике.

Будем рассматривать т.н. парадокс ЭПР в варианте, предложенном Д.Бомом.
Пусть имеется система двух частиц, так что полный спин системы равен нулю. Например, это может быть электрон-позитронная пара. Другим примером служит двухфотонный распад атома, когда поляризации фотонов ортогональны. И, наконец, при спонтанном параметрическом рассеянии можно так ориентировать кристалл (или пару кристаллов), что излучение в двух пространственных модах будет удовлетворять этому условию.
Совместное состояние пары частиц записывается в виде антисимметричной комбинации спиновых состояний со спином 1/2:

$$\left|\Psi^-\right\rangle = \frac{1}{\sqrt{2}}\left[\left|\uparrow\right\rangle_1\left|\downarrow\right\rangle_2 - \left|\downarrow\right\rangle_1\left|\uparrow\right\rangle_2\right]. \qquad (10.1)$$

Здесь $\left|\uparrow\right\rangle_i, \left|\downarrow\right\rangle_i$ - собственные состояния *z*-компонент спина *i*-ой частицы с собственными значениями 1/2. Антисимметричное состояние (10.1) инвариантно относительно вращений. Докажем это утверждение для поляризационного состояния Белла

$$\left|\Psi^-\right\rangle = \frac{1}{\sqrt{2}}\left[\left|B_x\right\rangle\left|C_y\right\rangle - \left|B_y\right\rangle\left|C_x\right\rangle\right], \qquad (10.2)$$

где B и C обозначают частицы, а x y - компоненты линейного поляризационного базиса. Запись $\left|B_x\right\rangle\left|C_y\right\rangle$ означает двукратное действие оператора рождения на вакуум (в разных поляризационных модах):

$$\left|B_x\right\rangle\left|C_y\right\rangle = b_x^\dagger c_y^\dagger\left|0\right\rangle. \qquad (10.3)$$

Замечание. Формальная аналогия между состояниями частиц со спином 1/2 и поляризационными состояниями света основывается на тождественности коммутационных соотношений операторов проекций момента количества движения j_k частицы со спином $J = (1/2)S_0$ (операторы Паули) и Стокса, подчиняющимися алгебре Ли (или SU2):
Для операторов Паули:

$$\left[\sigma_x,\sigma_y\right] = 2i\sigma_z,\ \left[\sigma_y,\sigma_z\right] = 2i\sigma_x,\ \left[\sigma_z,\sigma_x\right] = 2i\sigma_y.$$

Для операторов Стокса:

$s_0 \equiv a^\dagger a + b^\dagger b, \quad (I)$

$s_1 \equiv a^\dagger a - b^\dagger b, \quad (HV)$

$s_2 \equiv a^\dagger b + a b^\dagger, \quad (+45^0, -45^0)$

$s_3 \equiv -i\left(a^\dagger b - a b^\dagger\right) \quad (RL).$

$[s_1, s_2] = i s_3, \ [s_2, s_3] = i s_1, \ [s_3, s_1] = i s_2, \ [s_0, s_m] = 0.$ (*конец*)

Пусть при произвольном преобразовании поляризационного базиса $B_{x,y} \to B_{1,2}, \quad C_{x,y} \to C_{1,2}$ его компоненты определяются элементами эрмитовой матрицы:

$$D = \begin{pmatrix} t & r \\ -r^* & t^* \end{pmatrix}, \quad |t|^2 + |r|^2 = 1, \tag{10.4}$$

т.е. в матричном виде:

$$D\begin{pmatrix} B_1 \\ B_2 \end{pmatrix} = \begin{pmatrix} B_x \\ B_y \end{pmatrix}, \ D^\dagger \begin{pmatrix} B_x \\ B_y \end{pmatrix} = \begin{pmatrix} B_1 \\ B_2 \end{pmatrix}. \tag{10.5}$$

Тогда компоненты базисов преобразуются по правилам:

$$\begin{aligned} &|B_x\rangle = t|B_1\rangle + r|B_2\rangle, \qquad |C_x\rangle = t|C_1\rangle + r|C_2\rangle, \\ &|B_y\rangle = -r^*|B_1\rangle + t^*|B_2\rangle, \ |C_y\rangle = -r^*|C_1\rangle + t^*|C_2\rangle. \end{aligned} \tag{10.6}$$

Подставив эти выражения в (10.2), получим:

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}\left[|B_x\rangle|C_y\rangle - |B_y\rangle|C_x\rangle\right] =$$

$$= \frac{1}{\sqrt{2}}\left[\left(t|B_1\rangle + r|B_2\rangle\right)\left(-r^*|C_1\rangle + t^*|C_2\rangle\right) - \left(-r^*|B_1\rangle + t^*|B_2\rangle\right)\left(t|C_1\rangle + r|C_2\rangle\right)\right] =$$

$$= \frac{1}{\sqrt{2}}\left[-tr^*|B_1\rangle|C_1\rangle + |t|^2|B_1\rangle|C_2\rangle - |r|^2|B_2\rangle|C_1\rangle + rt^*|B_2\rangle|C_2\rangle\right] +$$

$$+ \frac{1}{\sqrt{2}}\left[r^*t|B_1\rangle|C_1\rangle + |r|^2|B_1\rangle|C_2\rangle - |t|^2|B_2\rangle|C_1\rangle - rt^*|B_2\rangle|C_2\rangle\right] =$$

$$= \frac{1}{\sqrt{2}}\left[|B_1\rangle|C_2\rangle - |B_2\rangle|C_1\rangle\right].$$

Т.о. синглетное состояние (10.1) инвариантно при произвольных преобразованиях базиса. Другими словами, это состояние имеет один и тот же вид независимо от того, какая ось используется для определения проекции спина. В частности, если выбрано направление "*x*", то состояние (10.1) переходит в:

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}\left[|\rightarrow_1\rangle|\leftarrow_2\rangle - |\leftarrow_1\rangle|\rightarrow_2\rangle\right], \tag{10.7}$$

где $|\rightarrow_i\rangle|\leftarrow_i\rangle$ - собственные состояния x-компоненты спина.

Теперь предположим что две частицы разлетелись настолько далеко, что взаимодействием между ними можно пренебречь. Будем производить измерение *z*-компоненты спина одной частицы (вертикальной поляризации в одном пучке). Это измерение, в соответствии с (10.1), может дать либо значение +1/2 либо -1/2. Если измерение дало результат +1/2, то коррелированная с ней частица должна оказаться в состоянии -1/2. Объясняется это

действием проекционного постулата: После проведения измерения над системой, она проецируется на состояние данной наблюдаемой. В данном случае наблюдаемой служит проекция на ось *z* первой частицы. Поскольку какое-либо влияние между частицами исключено по условию эксперимента, то отсюда делается вывод. что вторая частица имела такое значение проекции спина и *до измерения* над первой частицей. Т.е. *априори* существовал элемент физической реальности в виде определенного значения проекции спина второй частицы на ось *z*.

Теперь предположим, что в эксперименте измеряется *x*-компонента первой частицы. Согласно инвариантности состояния (10.1) относительно вращений будем рассматривать состояние (10.7), т.е. эквивалентное представление исходного состояния (10.1).

Аналогичные рассуждения приводят к тому, что у второй частицы априори существует определенное значение *x*-компоненты спина, в зависимости от результата измерения над первой частицей. Наблюдаемой в данном случае является значение x-компоненты спина первой частицы, а полное состояние системы проецируется либо на состояние $\left|\rightarrow_1\right\rangle\left|\leftarrow_2\right\rangle$, либо на состояние $\left|\leftarrow_1\right\rangle\left|\rightarrow_2\right\rangle$.

Поскольку две проекции спина - несовместные переменные, они соответствуют некоммутирующим операторам, то не существует такого состояния системы, в котором обе переменные имелт бы определенные значения. Отсюда ЭПР сделали вывод о неполноте квантово-механического описания, в которое следует добавить “скрытые” параметры.

Парадокс разрешается в рамках аппарата стандартной квантовой механики. Прежде всего, замети, что поскольку рассматриваемые частицы “1” и “2” взаимодействовали в прошлом, то им нельзя по отдельности приписать волновую функцию. Существует лишь совместная волновая функция $\left|\Psi^-\right\rangle$. На языке поляризационной оптики это означает, что у обоих пучков степень поляризации равна нулю. Т.о. состояние каждой частицы (в каждом из) пучков является смешанным и его следует описывать с помощью матрицы плотности. Из свойств матрицы плотности следует, что состояние одной из взаимодействующих частиц можно найти, взяв след по “лишним” переменным от матрицы плотности общей системы. Тогда *до измерения* его состояние есть:

$$\rho_2 = Sp_{(1)}\rho_{12} = Sp_{(1)}\left(\left|\Psi\right\rangle\left\langle\Psi\right|\right). \qquad (10.8)$$

Здесь мы учли, что общее состояние описывается волновой функцией, т.е. является чистым. Тогда из (10.8) следует:

$$\rho_2 = Sp_{(1)}\left(\left|\Psi^-\right\rangle\left\langle\Psi^-\right|\right) = \frac{1}{2}\left[\left|\uparrow\right\rangle\left\langle\uparrow\right| + \left|\downarrow\right\rangle\left\langle\downarrow\right|\right]. \qquad (10.9)$$

Замечание. При выводе (10.9) мы воспользовались тем, что операция *Sp* оставляет только те компоненты выражения $\left|\Psi^-\right\rangle\left\langle\Psi^-\right|$, которые содержат диагональные элементы по первой частице, т.е. вида $\left|\uparrow_1\right\rangle\left|\downarrow_2\right\rangle\left\langle\downarrow_2\right|\left\langle\uparrow_1\right|$.

С другой стороны, то же состояние описывается выражением (10.7):

$$\rho_2 = Sp_{(1)}\left(\left|\Psi^-\right\rangle\left\langle\Psi^-\right|\right) = \frac{1}{2}\left[\left|\rightarrow\right\rangle\left\langle\rightarrow\right| + \left|\leftarrow\right\rangle\left\langle\leftarrow\right|\right]. \qquad (10.10)$$

Видно, что оператор плотности второй частицы представляется в виде единичного оператора с точностью до 1/2 (поскольку $\hat{I} = \sum_n \left|n\right\rangle\left\langle n\right|$).

Что происходит со второй частицей **после измерения**? Если измерялась *z*-компонента первой частицы, то состояние второй было с равной вероятностью либо $\left|\uparrow\right\rangle$, либо $\left|\downarrow\right\rangle$, причем с равной вероятностью. Если же измеряется *x*-компонента первой частицы, то с равной вероятностью состояние второй частицы оказывается либо $\left|\rightarrow\right\rangle$, либо $\left|\leftarrow\right\rangle$. Таким

образом оператор плотности до и после измерения имеет один и тот же вид, хотя и описывает результаты разных экспериментов. Значит экспериментально невозможно отличить все эти состояния.

Неравенства Белла

Доказательство неприменимости скрытых параметров для описания некоторых предсказаний квантовых моделей называют теоремой Белла.

Ниже будут рассмотрены случаи двух и трех наблюдателей и дихотомной (или телеграфный сигнал, т.е. сигнал, принимающий два значения) наблюдаемой. Однако если число наблюдателей N растет, то отношение квантового и классического пределов для некоторой наблюдаемой величины S_N растет как $2^{(N-1)/2}$ (Д.Клышко, Д.Мермин)

Неравенство Белла для двух наблюдателей.

Рассмотрим некоторый случайный процесс, который можно характеризовать четырьмя переменными A, A', B, B'. Каждая дискретная случайная величина может принимать два значения, например: $A' \to a' = \pm 1$, и т.д. (В квантовой теории такой параметризации отвечают операторы некой физической величины и принимаемые собственные значения). Иногда мы будем писать $A' = \pm 1$ и т.д.

Для наглядности будем полагать, что имеется передатчик, который посылает сообщения двум наблюдателям А и В. У каждого наблюдателя имеется по одной ручке, с помощью которой он может менять свою наблюдаемую: $A \to A',\ B \to B'$. В общем случае число положений ручки - произвольно, т.е. наблюдаемые А и В зависят от параметров А(α), В(β). Например, сообщение состоит в команде зажечь лампу красного (-) или зеленого (+) цвета. Одна передача может содержать четыре исхода: $(++), (+-), (-+), (--)$. Передачи повторяются многократно, а исход каждой из них случаен. Т.е. независимо от выбора наблюдаемой A или A', B или B' у каждого наблюдателя загорается красная или зеленая лампа. Эксперимент состоит в выяснении корреляции цвета ламп у разных наблюдателей. Опишем этот процесс математически.

Предположим, что существует положительно определенная нормированная функция совместного распределения вероятностей этих четырех величин:

$$P\left(A, A', B, B'\right) \geq 0, \qquad (10.11)$$

удовлетворяющая условию нормировки:

$$\sum_{a,a',b,b'} P\left(A, A', B, B'\right) = 1. \qquad (10.12)$$

Для функций распределения можно вычислять маргинальные вероятности по правилам:

$$P\left(+1, A', B, B'\right) + P\left(-1, A', B, B'\right) = P\left(A', B, B'\right). \qquad (10.13)$$

Введем величину S - т.н. наблюдаемая Белла, которая выражается через моменты наблюдаемых величин:

$$\left\langle S \right\rangle \equiv \frac{1}{2}\left\{\left\langle AB \right\rangle + \left\langle A'B \right\rangle + \left\langle AB' \right\rangle - \left\langle A'B' \right\rangle\right\}. \qquad (10.14)$$

Докажем неравенство Белла (часто его называют неравенством Белла типа Гринберга -Хорна - Шимони - Хольта):

$$\left|\left\langle S \right\rangle\right| \leq 1. \qquad (10.15)$$

Функция распределения вероятностей (10.11) состоит из $2^4 = 16$ совместных вероятностей вида:

$$\begin{aligned} P_{A,A',B,B'}(++++) &\equiv P(a=+1, a'=+1, b=+1, b'=+1), \\ P_{A,A',B,B'}(-+++) &\equiv P(a=-1, a'=+1, b=+1, b'=+1), \end{aligned} \qquad (10.16)$$

и т.д. Выразим через эти вероятности средние величины или вторые моменты, входящие в неравенство (10.15) (см. также лекцию 8):

$$\langle AB\rangle = P_{AB}(++) + P_{AB}(--) - P_{AB}(+-) - P_{AB}(-+). \qquad (10.17)$$

Напомним, что этот момент показывает превышение доли коррелированных сигналов (--) или (++) над некоррелированными (+-) или (-+).

В другом виде (10.17) выглядит так:

$$\langle AB\rangle = \sum_{a,a',b,b'} abP_{A,A',B,B'}(a,a',b,b') = \sum_{a,b} abP_{AB}(a,b).$$

В это выражение входят маргинальные вероятности, которые можно выразить через совместную функцию распределения (10.11). Например,

$$P_{AB}(--) = P_{AA'BB'}(----) + P_{AA'BB'}(-+--) + P_{AA'BB'}(-+-+) + P_{AA'BB'}(---+).$$

Записывая таким образом все входящие в (10.14) моменты, получаем

$$\begin{aligned} S &\equiv \frac{1}{2}\left\{\langle AB\rangle + \langle A'B\rangle + \langle AB'\rangle - \langle A'B'\rangle\right\} = \\ &= P(++++) + P(+++-) - P(++-+) - P(++--) + \\ &+ P(+-++) - P(+-+-) + P(+--+) - P(+---) - \\ &- P(-+++) + P(-++-) - P(-+-+) + P(-+--) - \\ &- P(--++) - P(--+-) + P(---+) + P(----). \end{aligned} \qquad (10.18)$$

В правой части (10.18) стоит знакопеременная сумма. Если бы все знаки были “+”, то мы получили бы условие нормировки (10.12). Но половина слагаемых входит со знаками “-“, и, следовательно, в силу неотрицательности распределения вероятностей (10.11), получаем, что сумма в (10.18) распределена в интервале [-1, +1]. Неравенство (10.15) доказано.

Еще более простой способ доказательства основан на следующем подходе.

Выразим среднее значение случайной величины S, определенной в (10.14), через элементарные вероятности:

$$\langle S\rangle = \sum_{a,a',b,b'} P_{AA'BB'}(a,a',b,b')s(a,a',b,b'). \qquad (10.19)$$

Здесь $s(a,a',b,b') \equiv (ab + a'b + ab' - a'b')/2$.

Покажем, что эта функция содержит четыре различных множителя и поэтому принимает лишь два значения: ±1. Действительно, сгруппируем слагаемые следующим образом: $s = \left[a(b+b') + a'(b-b')\right]/2$. Поэтому, если , например, b = b′, то $s = ab = \pm 1$; если же b = -b′, то $s = a'b = \pm 1$.

Модуль суммы не превышает суммы модулей, поэтому из (10.19) и условий

$$s = \pm 1, \quad P \geq 0, \quad \sum P = 1,$$

получаем искомое неравенство Белла (10.15):

$$|\langle S\rangle| \leq \sum |sP| = \sum |s|P = \sum P = 1.$$

Таким образом исходя из классического распределения вероятности четырех наблюдаемых величин мы пришли к некоторому соотношению, которому должны удовлетворять моменты (или корреляции) этих величин. Оказывается, что при квантовом описании рассмотренного эксперимента неравенство (10.15) может нарушаться). Происходит это потому, что в классическом случае мы пользуемся понятием совместных вероятностей событий, а в квантовом - с помощью специфической волновой функции, учитывающей возможность парных корреляций. Именно такие корреляции и рассматривались в парадоксе ЭПР.

Почему же этот элементарный вывод теряет силу при квантовом описании? Как только мы ввели совместные вероятности (10.11), мы неявно сделали предположение об априорном существовании и возможности одновременного измерения (в одном испытании) всех четырех величин *A, A′, B, B′*. В квантовых моделях такое предположение

не всегда допустимо, когда, например, состояние, записанное на одном фотоне, не может клонироваться или разветвляться по двум каналам. Т.о. два регистрирующих устройства никогда не измеряют такое состояние - фотон не может быть зарегистрирован двумя детекторами. Если говорить о ферми-частицах с полуцелым спином (как при описании парадокса ЭПР в варианте Бома), то наблюдаемым A и A' соответствуют разные проекции спина.σ_z σ_x. Следовательно A и A' нельзя измерить в одном испытании.

С формальной точки зрения невозможность одновременного измерения каких-либо наблюдаемых величин в квантовой теории связана с некоммутативностью соответствующих операторов. В нашем случае это $\hat{A}$ и $\hat{B}$.Поскольку они не коммутируют, то им нельзя априори приписывать собственные значения +1 или -1. Также не имеют смысла и элементарные вероятности $P(a, a', b, b')$.

Можно ли избавиться от неравенства $\left|\langle S\rangle\right| \le 1$, оставаясь в рамках классических представлений об априорных вероятностях? У нас остается лишь две альтернативы.

1. Отказаться от условия неотрицательности вероятностей $P \ge 0$;
2. Избавиться от равенства s = ±1. Это равенство нарушается если предположить существование каких-то взаимодействий между измерительными приборами. Другими словами выбор наблюдаемой у первого наблюдателя (A или A′) “нелокально” влияет на показания прибора другого наблюдателя и наоборот. Тогда во всех использованных формулах учесть эту зависимость в виде $a(\alpha, \beta)$, $b(\alpha, \beta)$ и т.д.

Тогда s будет зависеть не от четырех, а от восьми множителей:

$$s = \frac{1}{2}\left[A(B)B(A) + A'(B)B(A') + A(B')B'(A) - A'(B')B'(A')\right]. \qquad (10.20)$$

Тогда s может принимать значения 0, ± 1, ± 2. Следовательно в выражении для среднего значения (10.19) должны фигурировать другие элементарные вероятности, которые определяют статистику всех восьми множителей.

Однако теперь все четыре слагаемых в (10ю20) могут быть статистически независимы. При этом (10.20) переходит в

$$s = \frac{1}{2}\left[AB + A'B' + A''B'' - A'''B'''\right].$$

Значит универсальное соотношение (10.15): $\left|\langle S\rangle\right| \le 1$ уже не возникает и при отсутствии дополнительных условий величина $\left|\langle S\rangle\right|$ оказывается ограниченной $\left|\langle S\rangle\right| \le 2$.

Часто при обсуждении неравенств Белла в качестве элементарных вероятностей выбирают не совместные распределения $P(a, a', b, b')$, а другие вероятности вида P(λ), где $\lambda \equiv \{\lambda_1, \lambda_2 ...\}$ - множество т.н. “скрытых” параметров. Эти параметры определяют неким причинным образом, например, по законам классической электродинамики, все свойства посылаемых сообщений. Следовательно, существуют некоторые однозначные зависимости вида $a(\lambda)$ и $b(\lambda)$. При этом предположение о нелокальности не используется! Приведенное выше доказательство остается в силе. Просто под усреднением надо понимать:

$$\langle S\rangle = \int d\lambda P(\lambda) s(\lambda). \qquad (10.21)$$

Здесь под интегралом стоит величина $s(\lambda)$, которая равна:

$$s(\lambda) \equiv \frac{1}{2}\left[a(\lambda)b(\lambda) + a'(\lambda)b(\lambda) + a(\lambda)b'(\lambda) - a'(\lambda)b'(\lambda)\right]. \qquad (10.22)$$

Эта величина опять зависит от четырех переменных и поэтому она ограничена $s(\lambda) = \pm 1$. Отсюда из условий

$$\int d\lambda P(\lambda) = 1, \quad P(\lambda) \ge 0. \qquad (10.23)$$

снова получается (10.15): $\left|\langle S\rangle\right| \le 1$.

Предположение о существовании плотности распределения для скрытых параметров P(λ) и однозначных причинных связей *a(λ)* и *b(λ)* подразумевает и существование совместного распределения *P*(*a, a′, b, b′*):

$$P_{ABA'B'} = \int_{\Lambda(a,b,a',b')} d\lambda P(\lambda). \qquad (10.24)$$

Здесь множество $\Lambda(a,b,a',b')$ - одно из 2^4 = 16 непересекающихся множеств всего множества скрытых параметров Λ ≡ {λ}, порождающее причинным образом определенную комбинацию знаков *a, a′, b, b′.*

Таким образом ода приведенных вывода (со скрытыми параметрами и без) неравенства $\left|\langle S\rangle\right| \le 1$ предполагают возможность описания наблюдаемых эффектов в терминах элементарных вероятностей $P_{AA'BB'}(a,a',b,b')$. Его невыполнение в квантовых моделях можно объяснять именно нарушением этой возможности. Такое же заключение можно сделать из появления отрицательных и многозначных вероятностей, рассчитываемых с помощью формулы $\left|\langle S\rangle\right| \le \sum |sP| = \sum |s| P = \sum P = 1.$ при использовании квантовых средних значений для произведений некоммутирующих операторов.

Итак, рассмотрим логику использующихся рассуждений в предположении о нелокальности:

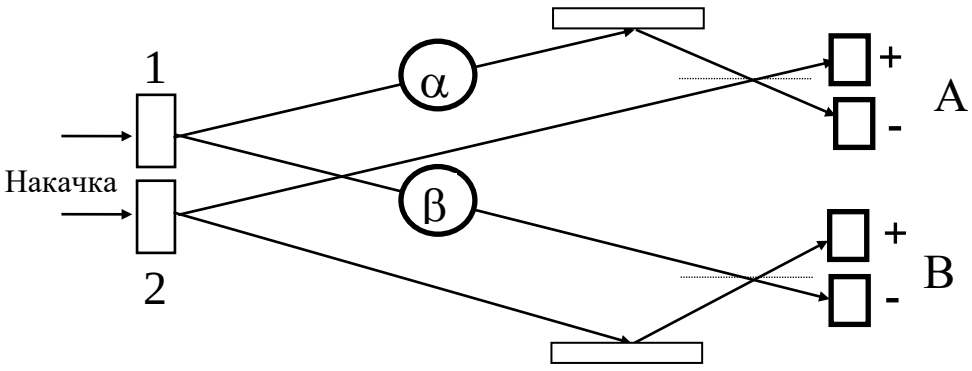
1. Классические локальные (в предположении о локальности, т.е. об отсутствии влияния аппаратуры на результаты измерения в другом канале) теории приводят к некоторым неравенствам.
2. Квантовая теория нарушает эти неравенства. Отсюда делается вывод, что
3. квантовая теория нелокальна.

Этот вывод противоречит правилам формальной логики:
для сравнения рассмотрим аналогичный силлогизм:

1. Все хорошие анекдоты - короткие
2. Этот рассказ - длинный. Значит (?!),
3. этот рассказ - плохой.

<u>Предсказания квантовой теории.</u>

Для вывода соотношения типа (10.20) необходимо рассмотреть конкретную модель и конкретные квантовые состояния по которым будут производиться усреднения. Рассмотрим процесс параметрического рассеяния света из двух кристаллов, которые возбуждаются когерентной накачкой. Коррелированные фотоны вылетают одновременно из двух кристаллов 1 и 2 в две пространственные моды. Один из фотонов задерживается при помощи линий задержки β или α. Моды, соответствующие сигнальному (холостому) излучению, родившемуся в разных кристаллах смешиваются на светоделителях, так что каждая пара детекторов A или B регистрирует только сигнальное или только холостое излучение. Значит корреляция возможна только между детекторами A и B, и невозможна между A^+ и A^- (B^+ и B^-).



Предполагается, что сохраняется поперечный импульс: $\left(k_{1,2}^a + k_{1,2}^b\right)_\perp = 0$. В итоге получаем четырех-пучковую схему или схему для наблюдения двухфотонной интерференции. Итак сигнальные (холостые) пучки после светоделителя направляются на пару детекторов D_+^a и D_-^a. Фазовая задержка α вводится в один из пучков. Аналогично строится вторая пара плеч. Светоделители преобразуют флуктуации фаз в флуктуации интенсивностей, которые регистрируются детекторами. Двухфотонная интерференция проявляется в том, что при наблюдении моментов четвертого порядка вида $\left\langle I_\pm^a I_\pm^b \right\rangle$ они будут зависеть по гармоническому закону от суммарной фазы $\varphi = \alpha + \beta$:

$\left\langle I^a I^b \right\rangle \propto 1 + V\cos\varphi$.

Видность интерференции интенсивностей при квантовом описании равна 100%. Теория скрытых параметров, которая рассмотрена выше дает оценку для видности:

$\left\langle S \right\rangle = \sqrt{2}V \to V \le 71\%$

В классической теории видность ограничена уровнем 50%.

Пусть детекторы работают в режиме счета фотонов. Считаем, что число истинных совпадений намного превышает число случайных, которыми можно пренебречь. Если также предположить, что квантовая эффективность детекторов равна 100%, то детекторы с индексами A и B щелкают одновременно. Отсчет (фотон), зарегистрированный детектором D_+^a обязательно сопровождается отсчетом либо в детекторе D_+^b, либо в детекторе D_-^b. Параметризуем результаты измерения так, что когда щелкает детектор D_+^a переменная A принимает значение “+”, когда D_-^a - то “-“. И, наконец, введем третью дихотомную переменную - $F_{\varphi i} \equiv A_{\alpha i} B_{\beta i} = \pm 1$.

Среднее значение (первый момент) величины *F*:

$$E \equiv \left\langle F_\varphi \right\rangle = \frac{1}{M}\sum_{i=1}^{M} F_{\varphi i}, \qquad (10.25)$$

$F_{\varphi i} \equiv A_{\alpha i} B_{\beta i}, \ \varphi = \alpha + \beta.$

Здесь M - полное число испытаний.

Заметим, что наблюдатель, регистрирующий только события в “канале A” не замечает изменений показаний, вызванных вариациями фазовых задержек α или β. Вероятность принять значение “+” или “-“ для переменной A (как и B) одинакова:

$P_A^+ = P_A^- = 1/2.$

В то же время, из результатов экспериментов и расчетов по квантовой модели следует, что вероятность наблюдения “+” или “-“ значения переменной F:

$$P_F^+ = \cos^2\varphi/2, \ \ P_F^- = \sin^2\varphi/2. \qquad (10.26)$$

Совместное распределение вероятностей двух наблюдаемых A и B:

$$P_{AB}^{++}(\varphi) = P_{AB}^{--}(\varphi) = \frac{1}{2}\cos^2\varphi/2,$$
$$P_{AB}^{+-}(\varphi) = P_{AB}^{+-}(\varphi) = \frac{1}{2}\sin^2\varphi/2. \qquad (10.27)$$

Тогда превышение числа коррелированных сигналов над антикоррелированными дается соотношением:

$$E_\varphi = P_{AB}^{++} + P_{AB}^{--} - P_{AB}^{+-} - P_{AB}^{-+} = \cos\varphi. \qquad (10.28)$$

Более строгое выражение величины E содержит множитель V, который имеет смысл видности интерференционной картины. В случае спонтанного параметрического

рассеяния, когда мощность накачки мала и детекторы регистрируют лишь сопряженные моды (сигнальные и холостые), $V \to 1$.

Пусть задержки, вносимые в канал A (или B) принимают два значения:

$\alpha, \alpha' \ (\beta, \beta')$:

$$\alpha' = \alpha + \frac{\pi}{2}, \quad \beta' = \beta + \frac{\pi}{2}. \tag{10.29}$$

Таким образом, в эксперименте исследуются сигналы в зависимости от четырех параметров: α, α' *и* β, β'. Будем записывать результаты четырех серий экспериментов, соответствующих следующим парам значений параметров:

$$\alpha, \beta \quad \alpha\beta' \quad \alpha'\beta \quad \alpha'\beta'. \tag{10.30}$$

Из (10.25) следует, что анализируется четыре наблюдаемых величины:

$$F^{(1)} = AB, \quad F^{(2)} = AB', \qquad F^{(3)} = A'B, \quad F^{(4)} = A'B'. \tag{10.31}$$

Назовем *измеряемой Белла* следующую комбинацию наблюдаемых величин:

$$S \equiv \frac{1}{2}\left\{F^{(1)} + F^{(2)} + F^{(3)} + F^{(4)}\right\}. \tag{10.32}$$

После усреднения по M испытаниям, получим:

$$\left\langle S \right\rangle_{эксперимент} \equiv \frac{1}{2}\left\{\left\langle F^{(1)} \right\rangle + \left\langle F^{(2)} \right\rangle + \left\langle F^{(3)} \right\rangle + \left\langle F^{(4)} \right\rangle\right\} =$$
$$= \frac{1}{2}\left\{E^{(1)} + E^{(2)} + E^{(3)} + E^{(4)}\right\} = \frac{1}{2}\left\langle AB + A'B + AB' - A'B' \right\rangle_{эксперим.}. \tag{10.33}$$

В то же время, согласно квантовой теории (10.28, 10.29):

$$\left\langle S \right\rangle_{\psi} = \frac{1}{2}\left[\cos\varphi + 2\cos\left(\varphi + \frac{\pi}{2}\right) - \cos\left(\varphi + \pi\right)\right] =$$
$$= \frac{1}{2}\left[\cos\varphi + 2\cos\left(\varphi + \frac{\pi}{2}\right) + \cos\left(\varphi + \pi\right)\right] = \sqrt{2}\cos\left(\varphi + \frac{\pi}{4}\right). \tag{10.34}$$

Замечание. В квантовой теории усреднение производится по перепутанному состоянию, которым является совместное состояние двух пар фотонов:

$$\psi \equiv \frac{1}{\sqrt{2}}\left[\left|1\right\rangle_1\left|0\right\rangle_2 + \left|0\right\rangle_1\left|1\right\rangle_2\right] = \Phi^{(+)}. \textit{(конец)} \tag{10.35}$$

Замечание. Можно показать, что квадрат наблюдаемой Белла определяется двумя коммутаторами:

$$S^2 = I - \left[A, A'\right]\left[B, B'\right] \to$$
$$\left|\left\langle S \right\rangle\right| = \sqrt{1 - \sin\left(\alpha - \alpha'\right)\sin\left(\beta - \beta'\right)} \le \sqrt{1+1} = \sqrt{2}. \textit{(конец)} \tag{10.36}$$

Максимальное значение наблюдаемая Белла принимает для значений аргумента $\varphi + \frac{\pi}{4} = \pi n$. Например, при $\varphi = -\frac{\pi}{4}$:

$$\left\langle S\left(A, A', B, B'\right)\right\rangle_{\psi,\max} \equiv \sqrt{2}. \tag{10.37}$$

Видно, что оценка наблюдаемой Белла, выполненная в рамках квантовой теории дает величину, превышающую (в некоторых случаях) классическую величину $\left|\left\langle S\left(A, A', B, B'\right)\right\rangle_{класс}\right| \le 1$.

Замечание. Видно, что нарушение неравенства Белла происходит при значениях параметров, не соответствующих максимальным корреляциям. *(конец)*

Формально, нарушение неравенств Белла объясняется тем, что коммутаторы в (10.36) не равны нулю, т.е. невозможно одновременно измерить величины A и A′ (B и B′). В нашей модели это утверждение эквивалентно тому, что у фотона *априори* не существует одновременно двух фаз (или двух значений поляризации) одновременно. В каждой реализации можно измерить лишь одну фазу (поляризацию) фотона!

Если есть время, рассказать про парадокс ГХЦ, теорему Кохена- Шпехера, неравенства Клышко-Мермина.

ЛИТЕРАТУРА

Противоречие с локальным реализмом

Гринберг, Хорн и Цайлингер показали, что квантово-механические предсказания некоторых результатов измерений над тремя перепутанными частицами противоречат локальному реализму в случаях, когда квантовая теория дает достоверные, т.е. нестатистические предсказания. Ситуация здесь отличается от случая с экспериментами типа Эйнштейна - Подольского - Розена с двумя перепутанными частицами по проверке неравенств Белла, где противоречие с локальным реализмом возникает только для статистических предсказаний.

Почему же трех-фотонные состояния ГХЦ находятся в более сильном противоречии с локальным реализмом, чем двух-фотонные состояния? Чтобы найти ответ на этот вопрос, рассмотрим состояние

$$\Psi_{ГХЦ} = \frac{1}{\sqrt{2}}\left(|H\rangle_1|H\rangle_2|H\rangle_3 + |V\rangle_1|V\rangle_2|V\rangle_3\right), \qquad (11.1)$$

где H и V обозначают горизонтальную и вертикальную поляризации. Это состояние показывает, что три фотона находятся в квантовой суперпозиции состояния $|H\rangle_1|H\rangle_2|H\rangle_3$ (все три фотона имеют горизонтальную поляризацию) и состояния $|V\rangle_1|V\rangle_2|V\rangle_3$ (три фотона имеют вертикальную поляризацию). Такое специфическое состояние симметрично по отношению к перестановкам всех фотонов, что упрощает аргументацию, приводимую ниже. Однако все рассуждения остаются справедливыми и для других максимально перепутанных трех-фотонных состояний.

Рассмотрим теперь некоторые специфические предсказания, следующие из вида состояния (11.1) и относящиеся к поляризационным измерениям, проводимыми над каждым фотоном либо в базисе, повернутом на 45^0 относительно $H-V$ и обозначенного $H'-V'$, либо циркулярном базисе, обозначенном $L-R$ (лево-циркулярный, право-циркулярный). Эти новые поляризационные базисы можно переписать в терминах исходного базиса:

$$|H'\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle + |V\rangle\right), \qquad |V'\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle - |V\rangle\right), \qquad (11.2)$$

$$|R\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle + i|V\rangle\right), \qquad |L\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle - i|V\rangle\right). \qquad (11.3)$$

Обратные преобразования имеют вид:

$$|H\rangle = \frac{1}{\sqrt{2}}\left(|H'\rangle + |V'\rangle\right), \qquad |V\rangle = \frac{1}{\sqrt{2}}\left(|H'\rangle - |V'\rangle\right), \qquad (11.4)$$

$$|H\rangle = \frac{1}{\sqrt{2}}\left(|L\rangle + |R\rangle\right), \qquad |V\rangle = \frac{i}{\sqrt{2}}\left(|L\rangle - |R\rangle\right). \qquad (11.5)$$

Обозначим состояние $|H\rangle$ вектором (1, 0), а состояние $|V\rangle$ вектором (0,1); эти вектора представляют два собственных состояния оператора Паули σ_z, с соответствующими собственными значениями +1 и -1. Можно просто удостоверится, что $|H'\rangle$ и $|V'\rangle$ или $|R\rangle$ и $|L\rangle$ являются собственными состояниями операторов Паули σ_x и σ_y с собственными значениями +1 и -1,

соответственно. Будем называть измерение в базисе $H'-V'$ - *x*-измерением, а в базисе $L-R$ - *y*-измерением.
Введем следующую параметризацию результатов измерений:

$$\begin{aligned} &H \to +1, \\ &V \to -1, \\ &R \to +1, \\ &L \to -1. \end{aligned} \qquad (11.6)$$

После представления состояния (11.1) в новых базисах можно получить предсказания измерений этих новых базисных поляризаций. Например, представим это состояние в базисах $1,2 \to R-L\ (y),\ 3 \to H'-V'\ (x)$. Такая запись будет означать, что первый и второй фотоны представляются в циркулярных базисах (y), а третий – в линейном, повернутом на 45^0 (x). Подставив преобразования (11.5) в исходное состояние (11.1), получим:

$$\Psi_{yyx} = \frac{1}{2}\left(|R\rangle_1|L\rangle_2|H'\rangle_3 + |L\rangle_1|R\rangle_2|H'\rangle_3\right) +$$

$$+\frac{1}{2}\left(|R\rangle_1|R\rangle_2|V'\rangle_3 + |L\rangle_1|L\rangle_2|V'\rangle_3\right). \qquad (11.7)$$

Такой вид нового представления состояния (11.1) означает, что при измерении линейной поляризации H' фотона 3, первые два фотона окажутся в состоянии циркулярной поляризации, причем для каждого из них поляризация не определена – она может оказаться как R, так и L, но разной у обоих фотонов (первые два слагаемых выражения (11.7.)) При измерении же V'- поляризации третьего фотона V', первые два оказываются опять в циркулярных, но совпадающих поляризациях (третье и четвертое слагаемые в (11.7)). Мы обозначили такие измерения как *yyx*-измерения. Из этого выражения можно получить ряд существенных следствий. Во-первых, его специфика состоит в том, что любое отдельное или двух-фотонное измерение имеет абсолютно случайный результат. Например, фотон 1 будет обнаружен либо с *R*, либо с *L* поляризациями с одинаковой вероятностью 50%.

Во-вторых, это выражение содержит только члены, составленные из произведений, принимающих значение -1 при *yyx*-измерении. Это дает возможность достоверно предсказать результат измерения третьего фотона, зная результат измерения над двумя другими фотонами. Например, предположим, что в результате измерения над фотонами 1 и 2 получилась право-циркулярная поляризация (R) (т.е. оба собственных значения равны +1). Из третьего слагаемого выражения (11.7) находим, что фотон 3 достоверно имеет V' -поляризацию (т.е. собственное значение -1).

При циклической перестановке можно получить аналогичные выражения для любых типов измерения циркулярной поляризации двух фотонов и V', H' - поляризаций оставшегося фотона. Например, рассмотрим измерение *yxy*. Производя тривиальную замену в выражении (11.7):

$R_2 \to H_2',\ L_2 \to V_2',\ H_3' \to R_1,\ V_3' \to L_3$, получаем:

$$\Psi_{yxy} = \frac{1}{2}\left(|L\rangle_1|H'\rangle_2|R\rangle_3 + |R\rangle_1|H'\rangle_2|L\rangle_3\right) +$$

$$+\frac{1}{2}\left(|R\rangle_1|V'\rangle_2|R\rangle_3 + |L\rangle_1|V'\rangle_2|L\rangle_3\right). \qquad (11.8)$$

И снова те слагаемые, которые представляются произведениями, дающими значение -1, являются результатами *yxy*-измерений. Аналогично получается и для *xyy*-измерений. Таким образом, результат измерения и циркулярной поляризации и линейной H', V' может быть предсказан с достоверностью для любого отдельного фотона при условии, что имеется соответствующий результат измерения двух других фотонов.

Попробуем проанализировать следствия таких предсказаний с точки зрения локального реализма. Сперва заметим, что эти предсказания не зависят ни от пространственного положения фотонов ни от очередности выполнения измерений во времени. Рассмотрим эксперимент, в котором три измерения выполняются одновременно в данной системе координат, скажем - для простоты - в системе координат источника. Применение Эйнштейновского понятия локальности означает, что информация не может распространяться быстрее скорости света. Отсюда, результат специфического измерения, выполненного над отдельным фотоном не должен зависеть ни от того, выполнено ли специфическое измерение над двумя другими фотонами одновременно, ни от исхода таких измерений. Единственный способ объяснить обсуждаемые полные корреляции с точки зрения локального реалиста состоит в предположении что каждый фотон несет элемент реальности всех рассмотренных измерений и что эти элементы реальности определяют результат специфического измерения.

Рассмотрим измерение линейной H', V' поляризации всех трех фотонов, т.е. *xxx*-измерения. Если элемент реальности существует, то какие исходы вообще возможны? Состояние (11.1) и его всевозможные циклические перестановки подразумевает, что какой бы результат $V'\left[H'\right]$ ни был получен для любого единичного фотона, другие два должны нести противоположные (для V') [идентичные (для H')] циркулярные поляризации. Учтем, что если какой-то фотон находится в состоянии R или L, то он может дать отсчет в базисе $H' - V'$, поскольку эти два базиса неортогональны. Предположим, что из каких-то трех фотонов, фотоны 2 и 3 были обнаружены в состоянии V'. Поскольку фотон 3 имеет V'-поляризацию, то фотоны 1 и 2 должны иметь идентичные циркулярные поляризации, а поскольку фотон 2 имеет V'-поляризацию, фотоны 1 и 3 опять должны нести идентичные циркулярные поляризации. Ясно, что если эти циркулярные поляризации являются элементами реальности, то все три фотона должны переносить идентичные циркулярные поляризации. Таким образом, если фотоны 2 и 3 имеют идентичные циркулярные поляризации, то фотон 1 должен достоверно иметь линейную поляризацию V'. Значит, существование элементов реальности приводит к заключению о том, что результат $|V_1'\rangle|V_2'\rangle|V_3'\rangle$ является одним из возможных исходов, если выбрано измерение H', V'-поляризации всех трех частиц, т.е. выполняется измерение *xxx*. Выполняя аналогичные рассуждения, можно проверить, что существует только четыре возможных исхода

$$\left|V_1'\right\rangle\left|V_2'\right\rangle\left|V_3'\right\rangle,\ \ \left|H_1'\right\rangle\left|H_2'\right\rangle\left|H_3'\right\rangle,\ \ \left|H_1'\right\rangle\left|V_2'\right\rangle\left|H_3'\right\rangle \text{ и } \left|V_1'\right\rangle\left|H_2'\right\rangle\left|H_3'\right\rangle. \quad (11.9)$$

Каким образом можно сравнить эти предсказания локального реализма с предсказаниями квантовой теории? Переписав состояние (11.1) в терминах H', V'-поляризаций, получим

$$\Psi_{xxx} = \frac{1}{2}(\left|H'\right\rangle_1\left|H'\right\rangle_2\left|H'\right\rangle_3 + \left|H'\right\rangle_1\left|V'\right\rangle_2\left|V'\right\rangle_3 +$$
$$+\left|V'\right\rangle_1\left|H'\right\rangle_2\left|V'\right\rangle_3 + \left|V'\right\rangle_1\left|V'\right\rangle_2\left|H'\right\rangle_3). \quad (11.10)$$

Сравнивая слагаемые, записанные в (11.9), со слагаемыми из (11.10) можно заметить, что всякий раз когда локальный реализм предсказывает достоверный специфический результат измерения одного фотона при данном результате измерений над двумя другими фотонами, квантовая физика достоверно предсказывает прямо противоположный результат. Таким образом, в то время как в случае неравенств Белла для двух фотонов, разница между локальным реализмом и квантовой физикой состоит в статистических предсказаниях теории, то здесь любая статистика возникает только благодаря неизбежным ошибкам в измерениях, свойственных и классической и квантовой физике.

ЛЕКЦИЯ 12. Перепутанные состояния, их физический смысл.

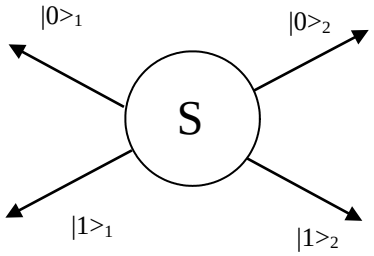
1. Составные квантовые системы, двухкомпонентные коррелированные системы. Роль ПС в квантовых алгоритмах. Примеры: ионы в ловушках, коррелированные ядерные спины в молекулах, атом в оптическом резонаторе.
2. Определение (I) перепутанных состояний. Пример приготовления двухчастичного ПС. Редуцированная матрица плотности компонент ПС. Состояния Белла, как частный случай ПС.
3. Оптическая реализация ПС. Отдельные фотоны и квадратурные компоненты поля. Спонтанное параметрическое рассеяние (СПР) света, волновая функция СПР, амплитуда бифотона, корреляционные свойства.
4. Перепутывание по времени, временная пост-селекция. Пространственно-частотные, поляризационно-частотные, поляризационно-угловые ПС. Амплитудная пост-селекция.
5. Перепутывание состояний с непрерывными переменными. Квадратурные компоненты поля. Реализация ПС с помощью светоделителя и квадратурно-сжатых полей. ПС поляризационно-сжатых полей.

Впервые понятие «перепутанных» состояний было введено Э.Шредингером в его работе от 29 ноября 1935г «Современное состояние квантовой механики». Известно, что появление этой статья было вызвано работой А.Эйнштейна, Б.Подольского и Н.Розена «Может ли квантово-механическое описание реальности быть полным?» (15 мая 1935г.) с дополнением, написанным Н.Бором. Русскоязычный перевод статьи Э.Шредингера появился в журнале Успехи химии в 1936г. Соответственно, первое упоминание термина «перепутанные состояния» на русском языке относится к этому переводу. Я придерживаюсь этого термина, следуя хронологическим соображениям[1]. Шредингер ввел понятие перепутанных состояний для описания состояния совокупной или составной системы, которая состоит из нескольких частей. Причем части общей системы могут быть пространственно разнесены.

Рассмотрим источник, испускающий пары частиц так, что одна из них (присвоим ей индекс 1) летит налево, а другая (индекс 2) - направо. Потребуем, чтобы сохранялась сумма импульсов частиц. Введем дополнительную параметризацию. Каждая частица может полететь и вверх (назовем это состоянием $|0\rangle$) и вниз ($|1\rangle$).

Но всякий раз сумма импульсов сохраняется. Если первая частица полетела налево вниз, то вторая полетит направо вверх. Или если первая частица полетела налево вверх, то вторая - направо вниз.

[1] Встречаются также термины «запутанные», «сцепленные», «переплетенные», которые на мой взгляд не многим лучше «перепутанных». В немецком языке термин «Verschrankung», использованный Шредингером, обозначает сильное переплетение, как при крепком рукопожатии. Английский перевод «entangled states» тоже вряд ли стоит считать удачным, поскольку в нем потерян первоначальный смыл «крепкого рукопожатия».



Полное состояние, которое приготавливает источник, записывается в виде суперпозиции двух “возможностей”:

$$\left|\Psi\right\rangle_{1,2} = c_1\left|0\right\rangle_1\left|1\right\rangle_2 + c_2\left|1\right\rangle_1\left|0\right\rangle_2 . \qquad (12.1)$$

Коэффициенты c_i (i = 1, 2) - это (комплексные) амплитуды двух “альтернатив”. Их физический смысл состоит в том, что соответствующие квадраты модулей $\left|c_i\right|^2$ определяют вероятности обнаружить пару частиц в состояниях $\left|0\right\rangle_1\left|1\right\rangle_2$, либо $\left|1\right\rangle_1\left|0\right\rangle_2$. Состояние (12.1) - пример т.н. перепутанного состояния двух частиц Позже будет дано четкое определение таких состояний и рассмотрены количественные меры перепутывания. Мы будем оперировать с разными видами перепутанных состояний. Например - ионы в ловушках, ядерные спины в молекуле при электронном парамагнитном резонансе, состояния атом-поле в резонаторе и др.

В прошлом семестре мы неоднократно рассматривали перепутанные состояния, когда говорили о простейших квантовых логических элементах, (в частности об операции CNOT), при выводе неравенств Белла. Напомню, что по определению перепутанными считаются состояния составной системы, которые не могут быть представлены в виде произведения волновых функций, описывающих ее части по отдельности. Так, для двухкомпонентной системы перепутанное состояние:

$$\Psi_{12} \neq \Psi_1 \otimes \Psi_2 \qquad (12.2)$$

Примером ПС служат т.н. состояния Белла. Они замечательны тем, что проецирование одной части системы в одно из двух возможных состояний, другая часть «мгновенно» приобретает определенное значение, несмотря на то, что она могла быть удалена на произвольное расстояние. Этот факт и был основной причиной, побудившей Эйнштейна к переосмыслению основных положений квантовой механики. Определение (12.2) не очень хорошо тем, что оно не содержит позитивного утверждения. Я умышленно вынесу математические аспекты в отдельную часть лекции, поскольку считаю, что в настоящее время математическое развитие квантовой информации и квантовых вычислений далеко опережает состояние дел в эксперименте и зачастую термины и понятия, используемые в математических кругах, не имеют четкого операционального смысла. Перед тем как перейти к физической стороне проблемы, я бы отметил важное свойство ПС, которое, опять же обсуждалось нами ранее. Оно состоит в том, что для чистых перепутанных состояний (т.е. тех, которые описываются ВФ) полное знание состояния составной системы не предполагает полного знания состояний

подсистем. Т.е. иногда вообще бессмысленно говорить о ВФ подсистем, поскольку они представляют собой некогерентную смесь, т.е. их можно описать классически в терминах статистической физики. Например, рассмотрим состояние Белла

$$\Psi^{+}=\frac{1}{\sqrt{2}}\left(\left|H\right\rangle_1\left|V\right\rangle_2+\left|V\right\rangle_1\left|H\right\rangle_2\right) \qquad (12.3)$$

системы, рассмотренной в начале лекции, когда $c_1=c_2=\frac{1}{\sqrt{2}}$. Чтобы найти матрицу плотности какой-нибудь подсистемы надо взять след по индексам другой системы от совместной матрицы плотности:

$$\rho_2=Sp_1\left(\rho_{12}\right)=Sp_1\left(\left|\Psi\right\rangle_{12}\left\langle\Psi\right|_{12}\right) \qquad (12.4)$$

Получаем:

$$\left|\Psi\right\rangle_{12}\left\langle\Psi\right|_{12}=\frac{1}{2}\left\{\left(\left|H\right\rangle_1\left|V\right\rangle_2+\left|V\right\rangle_1\left|H\right\rangle_2\right)\otimes\left(\left\langle V\right|_2\left\langle H\right|_1+\left\langle H\right|_2\left\langle V\right|_1\right)\right\}=$$

$$\frac{1}{2}\left\{\left|H\right\rangle_1\left|V\right\rangle_2\otimes\left\langle V\right|_2\left\langle H\right|_1+\left|H\right\rangle_1\left|V\right\rangle_2\otimes\left\langle H\right|_2\left\langle V\right|_1\right\}+ \qquad (12.5)$$

$$+\frac{1}{2}\left\{\left|V\right\rangle_1\left|H\right\rangle_2\otimes\left\langle V\right|_2\left\langle H\right|_1+\left|V\right\rangle_1\left|H\right\rangle_2\otimes\left\langle H\right|_2\left\langle V\right|_1\right\}$$

Тогда

$$\rho_2=Sp_1\left(\rho_{12}\right)=\frac{1}{2}\left\{\left|V\right\rangle_2\left\langle V\right|_2+\left|H\right\rangle_2\left\langle H\right|_2\right\}, \qquad (12.6)$$

т.е. представляет собой взвешенную смесь. Следовательно, состояние второй подсистемы нельзя описывать волновой функцией; оно не является полностью определенным. Аналогично, матрица плотности первой подсистемы находится как след по индексам второй подсистемы:

$$\rho_1=Sp_2\left(\rho_{12}\right)=\frac{1}{2}\left\{\left|V\right\rangle_1\left\langle V\right|_1+\left|H\right\rangle_1\left\langle H\right|_1\right\}. \qquad (12.7)$$

Говоря о перепутанных состояниях, мы, таким образом, выделяем следующие их атрибуты:

- наличие параметра, принимающего ряд фиксированных значений для каждой из подсистем;
- наличие корреляций между ***двумя*** подсистемами по этому параметру, или в более общем случае - синхронности флуктуаций этого параметра;

Сформулируем еще одно определение перепутанных состояний для ***двух подсистем***:

Перепутанными называются две подсистемы между которыми существуют квантовые корреляции по параметру, принимающему по крайней мере два значения для каждой из подсистем. Измерение состояния одной из подсистем однозначно определяет (проецирует) состояние другой. Совместное состояние двух подсистем тогда называется перепутанным.

Обращаю внимание, что корреляции должны носить квантовый характер, т.е. их нельзя описать классически. В противном (классическом) случае даже полные (т.е. 100%-ые) корреляции не дают результатов, к которым

ведет использование истинных перепутанных состояний - например, нарушение неравенств Белла.

Замечу также, что для трех подсистем однозначного определения перепутанных состояний ввести не удается. Связано это с тем, что в случае измерения состояния одной из подсистем две оставшиеся могут либо принять определенные значения (определение 1), либо оказаться в перепутанном состоянии (определение 2). К первому случаю, например, относится состояние ГХЦ трех кубитов: $\Psi_{1,2,3} = \frac{1}{\sqrt{2}}\left\{|0\rangle_1|0\rangle_2|0\rangle_3 + |1\rangle_1|1\rangle_2|1\rangle_3\right\}$. Как было показано в предыдущей лекции это же состояние, но записанное в XY- базисе (т.е. $+45^0$-45^0) имеет вид: $\Psi_{1,2,3} = c\left\{|0\rangle_1|0\rangle_2|1\rangle_3 + |0\rangle_1|1\rangle_2|0\rangle_3 + |1\rangle_1|0\rangle_2|0\rangle_3 + |1\rangle_1|1\rangle_2|1\rangle_3\right\}$, т.е. подпадает под второе определение. В то же время, ясно, что два определения относятся к совершенно различным физическим системам - в этом состоит одно из проявлений “парадокса ГХЦ”!

В этой лекции разговор, в основном, пойдет об оптической реализации ПС. На сегодняшний день именно оптические ПС удается приготовить с высоким качеством. Здесь под качеством я понимаю те признаки по которым можно судить о перепутанных состояниях в определенных экспериментах. Конкретно, имеются в виду эксперименты по двухфотонной интерференции, где видность интерференции четвертого по полю порядка непосредственно связана с качеством перепутанных состояний.

Для оптических систем различают ПС между отдельными фотонами и между квадратурными компонентами электромагнитного поля. В первом случае говорят о дискретных переменных, во втором - о непрерывных. Оба случая реализуются в процессе параметрического рассеяния света. В случае дискретных переменных используется спонтанный режим, когда пары фотонов излучаются в широком спектральном диапазоне (5-20нм) и практически не перекрываются в пространстве-времени. В случае непрерывных переменных используется режим параметрического усиления: кристалл, генерирующий пары фотонов помещается в резонатор, который работает как элемент обратной связи, т.е. и как фильтр частот.

Наиболее качественные ПС получаются при спонтанном режиме, т.е. для дискретных переменных.

Напомню, что в результате спонтанного параметрического рассеяния в нелинейной среде возникают пары коррелированных фотонов. Закон сохранения импульса (в нелинейно-оптических экспериментах его иногда называют условием фазового синхронизма) приводит к пространственной корреляции фотонов. Закон сохранения энергии дает жесткую корреляцию между частотами родившихся фотонов. Анизотропия среды накладывает строгие ограничения на поляризацию фотонов. Замечу, что понятие «корреляция» нужно уточнять в каждом конкретном эксперименте. Так, в нестационарном режиме, т.е. при использовании коротких импульсов накачки, когда ширина спектра накачки сравнима с шириной спектра СПР уже нет смысла говорить об однозначной связи частот сигнального и

холостого фотонов – эта связь определена лишь с точностью до ширины спектра накачки:

$\omega_s = \Omega_p - \omega_i \pm \Delta\omega_p$, где Ω_p – центральная частота в спектре накачки.

Аналогично, при рассеянии в ограниченных (в поперечном, либо в продольном направлениях) средах, импульс сохраняется с точностью до расстройки, обратно пропорциональной соответствующему масштабу среды. Поэтому игнорирование частотной или угловой формы линии параметрического рассеяния может привести к заметным погрешностям в процессе приготовлении перепутанных состояний. Иногда для их предотвращения используют процедуры т.н. пространственной или частотной *пост-селекции*, когда часть состояний отфильтровывается, не принимается в рассмотрение.

Статистические свойства СПР рассматривались в одной из предыдущих лекций.

Состояние света при СПР представляется в виде

$$\left|\Psi\right\rangle = \left|vac\right\rangle + \frac{1}{2}\sum_{k,k'} F_{k,k'}\left|1_k, 1_{k'}\right\rangle, \qquad (12.8)$$

где $\left|vac\right\rangle$ - вакуумное состояние, величина $F_{k,k'}$ называется амплитудой бифотона, а $\left|1_k, 1_{k'}\right\rangle$ - состояние с одним (сигнальным) фотоном в моде k и одним (холостым) фотоном в моде k$\mathbf{O}$. Смысл величины $F_{k,k'}$ состоит в том, что квадрат ее модуля дает вероятность регистрации двух фотонов в двух поляризационных модах k и k$\mathbf{O}$. Видно, что состояние (12.8) не факторизуется, а если рассматривать лишь два слагаемых в сумме (12.8), получим двух-компонентную (bipartite) систему из которой можно приготовить состояния Белла.

Итак, опираясь на пример спонтанного параметрического рассеяния света, рассмотрим разные типы перепутанных состояний, которые можно получить при рассмотрении разных мод k и k$\mathbf{O}$.

1. Состояния, перепутанные по времени (энергия -время).

Такой тип ПС был впервые предложен Дж.Фрэнсоном. Он основан на том, что сигнальный и холостой фотоны рождаются практически одновременно, с точностью до ширины спектра накачки. Однако каждый из них имеет конечный спектр, определяемый дисперсией и размерами кристалла. Сумма частот сигнального и холостого фотонов равна частоте накачке, т.е. остается постоянной для всех сопряженных спектральных компонент бифотонного поля. Суть схемы, предлженной Фрэнсоном состоит в следующем (Рис.1). Бифотоны генерируются в частотно-вырожденном неколлинеарном режиме при синхронизме типа I. При этом на пути сигнального и холостого фотона помещается по одинаковому разбалансированному интерферометру Маха-Цандера. Разность длин плеч должна превышать длину когерентности излучения СПР, которая при синхронизме типа I определяется второй производной закона дисперсии в окрестности половины частоты накачки:

$$l_{coh} = c\tau_{coh} = cD''L = c\frac{d^2k}{d\omega^2}\Big|_{\frac{\omega_p}{2}} L \qquad (12.9)$$

Интерференция в каждом из каналов не возникает, поскольку задержка превышает длину когерентности. Однако, при регистрации совпадений между детекторами, стоящими в разных плечах возможно наблюдение интерференции (четвертого порядка по полю). Это ясно из вида волновой функции, которая описывает состояние пары фотонов:

$$\Psi = \frac{1}{2}\left\{ \left|S\right\rangle_s \left|S\right\rangle_i + e^{i(\varphi_s+\varphi_i)} \left|L\right\rangle_s \left|L\right\rangle_i + e^{i(\varphi_i)} \left|S\right\rangle_s \left|L\right\rangle_i + e^{i(\varphi_s)} \left|L\right\rangle_s \left|S\right\rangle_i \right\} \quad (12.10)$$

Здесь символы S и L обозначают короткое и длинное плечо соответствующего интерферометра. Состояние (12.19) - факторизованное, поскольку представляет собой прямое произведение состояний сигнального и холостого фотонов:

$$\Psi_{s,i} = \frac{1}{\sqrt{2}}\left\{ \left|S\right\rangle_s + e^{i\varphi_s} \left|L\right\rangle_s \right\} \frac{1}{\sqrt{2}}\left\{ \left|S\right\rangle_i + e^{i\varphi_i} \left|L\right\rangle_i \right\} = \Psi_s \otimes \Psi_i \quad (12.11)$$

Но если регистрировать только факт одновременного прихода сигнального и холостого фотонов, что можно сделать, выбрав окно схемы совпадения меньше, чем задержка, возникающая между S и L путями в интерферометре, то последние два слагаемых в (12.10) исчезнут. Это - т.н. временная пост-селекция, когда отфильтровываются события, не принадлежащие определенному интервалу времени. В итоге состояние пары фотонов принимает нефакторизованный вид и отвечает суперпозиции

$$\Psi = \frac{1}{2}\left\{ \left|S\right\rangle_s \left|S\right\rangle_i + e^{i(\varphi_s+\varphi_i)} \left|L\right\rangle_s \left|L\right\rangle_i \right\}. \quad (12.12)$$

Такое ПС есть когерентная суперпозиция двух вкладов, когда оба фотона прошли по коротким плечам интерферометров, либо оба - по длинным плечам. Варьируя фазовые задержки, можно наблюдать интерференцию четвертого порядка.

2. Частотно-пространственные ПС (или перепутывание по импульсу).

Частотно-угловые ПС. Рассмотрим неколлинеарный невырожденный режим СПР, когда поляризация обоих фотонов одинакова (синхронизм типа I). Для малых частотных отстроек сигнального и холостого фотонов от половины частоты накачки:

$$\begin{aligned} \omega_s &= \omega_p/2 - \Delta\omega, \\ \omega_i &= \omega_p/2 + \Delta\omega. \end{aligned} \quad (12.13)$$

можно выделить такие направления рассеяния θ, θ′, в которых излучаются как сигнальный фотон с частотой ω_s, так и холостой фотон с частотой ω_i. При этом двухфотонная часть вектора состояния будет иметь вид

$$\left|(\omega_s)_\theta (\omega_i)_{\theta'}\right\rangle \pm \left|(\omega_s)_{\theta'} (\omega_i)_\theta\right\rangle. \quad (12.14)$$

Это состояния Белла $\Psi^{\pm}$, где перепутанными являются частотные и угловые степени свободы. Такие состояния (Белла) еще не были реализованы в эксперименте. Манипуляции с частотно-пространственными ПС осуществлялись в работах Д.Рарити и П. Тапстера.

3. Поляризационно-частотные ПС.

В этом случае будем говорить о нефакторизованных состояниях вида

$$\left|H_\omega H_{\omega'}\right\rangle + \exp\{i\varepsilon\}\left|V_\omega V_{\omega'}\right\rangle, \tag{12.15}$$

$$\left|H_\omega V_{\omega'}\right\rangle + \exp\{i\varepsilon\}\left|V_\omega H_{\omega'}\right\rangle \tag{12.16}$$

где перепутаны частотные и поляризационные моды. На практике такие состояния получаются в интерференционной схеме, показанной на рисунке 2.
В каждом плече интерферометра Маха-Цандера генерируется СПР в частотно-невырожденном, коллинеарном режиме, с синхронизмом типа I (Рис.3). В левом плече поляризация обоих фотонов поворачивается на 90^0 при помощи полу-волновой пластинки. Таким образом бифотоны, поступающие на поляризационный светоделитель, имеют ортогональные поляризации, что позволяет совместить их в одном пучке без потерь. Состояние света после светоделителя имеет вид (12.15). Фаза между компонентами состояния определяется задержкой ε, вносимой смещением зеркала М. Для получения состояния Белла Ψ^+ необходимо выполнить унитарные преобразования состояний $\Phi^\pm$ состоящие в повороте базиса. Подробно об этих преобразованиях будет рассказано на следующей лекции, которую мы договорились посвятить математическим аспектам перепутанных состояний. Сейчас заметим, что поворот базиса на 45^0 осуществляет преобразование $\Phi^- \to \Psi^+$. Другими словами состояние Белла Φ^- в лабораторном базисе (H,V) тождественно состоянию Белла Ψ^+ в 45^0-ом базисе (X, Y). Такое преобразование осуществляется пластинкой λ/2, ориентированной под углом 22.5^0.

Синглетное состояние Ψ^- не имеет аналога в вырожденном по частоте режиме, так как оно антисимметрично по отношению к перестановке фотонов в паре. Это значит, что состояние

$$\Psi_{12}^- = \frac{1}{\sqrt{2}}\left\{\left|a\right\rangle_1\left|b\right\rangle_2 - \left|b\right\rangle_1\left|a\right\rangle_2\right\} \tag{12.17}$$

- единственное из состояний Белла, которое меняет знак при перестановке индексов 1 и 2. Оставшиеся три состояния - триплетные - симметричны к перестановке индексов. Для приготовления этого состояния в эксперименте использовалась специальная фазовая пластинка из кристаллического кварца (QP), толщина которой удовлетворяла следующему условию: набег фаз между обыкновенной и необыкновенной волной на частоте ω отличается от соответствующего набега фаз на частоте ω′ на π. Если на входе в такую пластинку имеется состояние $\Psi^+ = \left|H_\omega V_{\omega'}\right\rangle + \left|V_\omega H_{\omega'}\right\rangle$, а ее оптическая ось ориентирована вертикально или горизонтально, то состояние после пластинки, с точностью до несущественной общей фазы, будет $\Psi^- = \left|H_\omega V_{\omega'}\right\rangle - \left|V_\omega H_{\omega'}\right\rangle$.

  Для получения состояния Ψ^- фаза ε в интерферометре устанавливалась равной π, так что на выходе из интерферометра получалось состояние $\Phi^- = \left|H_\omega H_{\omega'}\right\rangle - \left|V_\omega V_{\omega'}\right\rangle$. В базисе XY, повернутом на π/4 относительно базиса HV, как уже говорилось, состояние Φ^- переходит в Ψ^+:

$\left|H_{\omega}H_{\omega'}\right\rangle - \left|V_{\omega}V_{\omega'}\right\rangle = \left|X_{\omega}Y_{\omega'}\right\rangle + \left|Y_{\omega}X_{\omega'}\right\rangle$. Пластинка QP устанавливалась на выходе из интерферометра так, что ее оптическая ось была ориентирована по направлению X. После пластинки состояние в базисе XY превращалось в Ψ^{-}. Забегая вперед, отмечу, что синглетное состояние Белла инвариантно к любым преобразованиям базиса.

4. Поляризационно-угловые ПС. Этот тип ПС является в настоящее время самым распространенным. Сигнальный и холостой фотоны излучаются под различными углами θ, θ′ к волновому вектору накачки, причем для каждого из них поляризация не задана, однако имеется корреляция (перепутывание) между поляризациями. Двухфотонная часть вектора состояния имеет при этом вид

$$\left|H_{\theta}V_{\theta'}\right\rangle + \exp\left\{i\varepsilon\right\}\left|V_{\theta}H_{\theta'}\right\rangle \qquad (12.18)$$

или

$$\left|H_{\theta}H_{\theta'}\right\rangle + \exp\left\{i\varepsilon\right\}\left|V_{\theta}V_{\theta'}\right\rangle, \qquad (12.19)$$

где символы H и V обозначают горизонтальную и вертикальную поляризацию. Такие состояния были впервые реализованы за счет использования неколлинеарного частотно-вырожденного синхронизма типа II (Рис.4). Специфика ПС, приготавливаемых таким методом состоит в том, что в излучение СПР необходимо вносить групповую задержку между фотонами V и H поляризациями. Связано это с тем, что из-за дисперсии кристалла, в котором происходит генерация бифотонов, фотоны с обыкновенной поляризацией распространяются быстрее, чем с необыкновенной. Обратная ширина спектра СПР как раз и определяется этой величиной

$$\tau_{coh} = DL = \left(\frac{1}{u_e} - \frac{1}{u_o}\right) L. \qquad (12.20)$$

Здесь в скобках стоит разница обратных групповых скоростей необыкновенной и обыкновенной волн в нелинейном кристалле. Чтобы состояние (12.18) на выходе из кристалла было чистым, необходимо уничтожить возникшую в кристалле задержку, сделать вклады V и H поляризаций “неразличимыми”, т.е. добиться того, чтобы задержка между ними не превышала времени когерентности (12.20). Добиться этого можно, вводя после кристалла двулучепреломляющий элемент (пластинку из кристаллического кварца, например), которая компенсирует задержку:

$$\tau_{extra} = \frac{DL}{2} \qquad (12.21)$$

Впоследствии была предложена более удобная схема (Рис.5), при которой аналогичные состояния получались при интерференции бифотонов, рождающихся в двух последовательно расположенных кристаллах с синхронизмом типа I. На выходе такой схемы генерируется ПС вида (12.19), которое легко можно преобразовать ко всем четырем состояниям Белла. В частности, переход к состояниям вида (12.18) осуществляется с помощью полу-волновой пластинки, ориентированной под углом 45^0, помещенной в одну из угловых мод.

Перепутанные состояния квадратурных компонент поля

В заключение, рассмотрим оптический метод получения ПС непрерывных переменных. Типичные представители квантовых непрерывных переменных являются координата и импульс (частицы). Мы будем использовать тот факт, что одна поперечная мода квантованного электромагнитного поля излучения формально описывается так же, как и гармонический осциллятор.

Гамильтониан классического гармонического осциллятора имеет вид:

$$H = \frac{p^2}{2m} + \frac{m\omega^2 x^2}{2}. \qquad (12.22)$$

При квантово-механическом рассмотрении переменным x и p ставятся в соответствие операторы:

$$x \to \hat{x}, \quad p \to \hat{p} = i\hbar\partial / \partial x, \qquad (12.23)$$

которые удовлетворяют коммутационному соотношению:

$$\left[\hat{x}, \hat{p}\right] = i\hbar. \qquad (12.24)$$

Гамильтониан квантованного гармонического осциллятора принимает вид:

$$\hat{H} = \hbar\omega\left(a^{\dagger}a + \frac{1}{2}\right), \qquad (12.25)$$

где использована связь между операторами координаты, импульса и повышающим (a^+) и понижающим (a) операторами:

$$\hat{x} = \sqrt{\frac{\hbar}{2\omega m}}\left(a^{\dagger} + a\right), \qquad (12.26)$$

$$\hat{p} = \sqrt{\frac{\hbar}{2\omega m}}\left(a^{\dagger} - a\right). \qquad (12.27)$$

Для операторов a^+ и a действуют обычные коммутационные соотношения:

$$a\left|n\right\rangle = \sqrt{n}\left|n-1\right\rangle, \quad a\left|0\right\rangle = 0, \qquad (12.28)$$

$$a^{\dagger}\left|n\right\rangle = \sqrt{n+1}\left|n+1\right\rangle, \qquad (12.29)$$

$$\left[a, a^{\dagger}\right] = 1, \ \left[a, a\right] = \left[a^{\dagger}, a^{\dagger}\right] = 0, \qquad (12.30)$$

$$a^{\dagger}a = N. \qquad (12.31)$$

Символ $\left|n\right\rangle$ обозначает n-ое возбужденное состояние осциллятора, N - оператор числа частиц. Спектр собственных значений осциллятора дискретен: $E_n = \hbar\omega\left(n + 1/2\right)$.

Оператор электрического поля в точке r связан с операторами рождения и уничтожения фотонов. Если интересоваться только одной поперечной модой с частотой ω и одной поляризацией, то оператор электрического поля принимает вид:

$$\hat{E} = i\frac{\sqrt{\omega}}{c}\sqrt{\frac{2\pi\hbar c^2}{L^3}}\left[ae^{i(kr-\omega t)} - a^{\dagger}e^{-i(kr-\omega t)} \right], \qquad (12.32)$$

где L - размер ящика квантования. В общем виде, если рассматривать поле в начале координат (r = 0) и объединяя несущественные коэффициенты в один - E_0, получаем оператор поля в виде:

$$\hat{E} = E_0\left[ae^{i\omega t} + a^{\dagger}e^{-i\omega t} \right]. \qquad (12.33)$$

При квантовании поля по аналогии с гармоническим осциллятором, вводятся операторы X и P:

$$\hat{X} = a^{\dagger} + a, \qquad (12.34)$$

$$\hat{P} = i\left(a^{\dagger} - a \right). \qquad (12.35)$$

Соответственно, обратные преобразования дают

$$a = \frac{1}{2}\left(\hat{X} + i\hat{P} \right), \qquad (12.36)$$

$$a^{\dagger} = \frac{1}{2}\left(\hat{X} - i\hat{P} \right). \qquad (12.37)$$

В терминах операторов X и P, оператор поля приобретает вид

$$\hat{E} = E_0\left[\hat{X}\cos\omega t + \hat{P}\sin\omega t \right]. \qquad (12.38)$$

Собственные значения X и P оператора поля называются квадратурными компонентами. Их часто интерпретируют как синфазная и противофазная компоненты по отношению к фазе локального генератора (осциллятора). Коммутационные соотношения для них имеют вид:

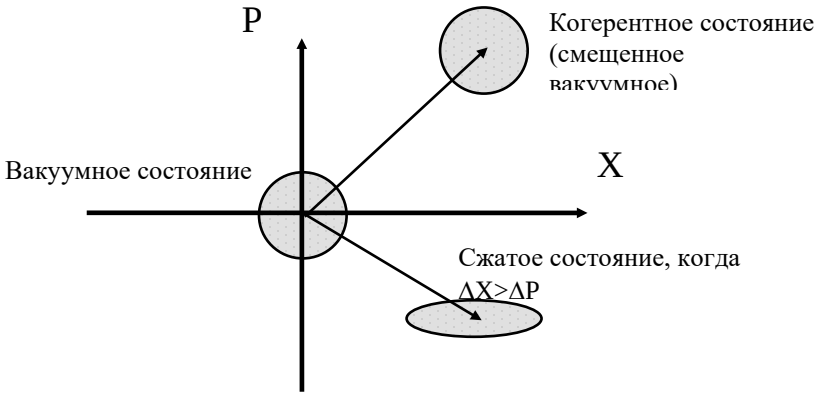
$$\left[\hat{X}, \hat{P} \right] = 2i. \qquad (12.39)$$

Отсюда сразу следуют соотношения для флуктуация квадратурных компонент:

$$\Delta X \Delta P = 1, \quad \left(\langle \Delta X \rangle^2 = \langle X^2 \rangle - \langle X \rangle^2 \right), \qquad (12.40)$$

из которых следует, что квадратурные компоненты не могут быть измерены одновременно и с произвольной точностью.

У сжатых состояний поля неопределенность одной из квадратурных компонент больше, чем у другой. На фазовой плоскости такие состояния изображаются эллипсами, вытянутыми вдоль X или Y осей.



Наконец, рассмотрим способ получения перепутанных состояний в непрерывных переменных. Пусть во входные моды неполяризационного светоделителя поступают поля E_1 и E_2, соответственно сжатые в X и P направлениях. (Я не рассматриваю случай т.н. поляризационного сжатия, когда подавлены флуктуации какого-нибудь параметра Стокса). Представим идеальную ситуацию, когда сжатие максимально, т.е. $X_1 = P_2 = 0$. Коэффициент сжатия определяется как отношение радиуса когерентного кружка к короткой полуоси эллипса неопределенности. В настоящее время (Mlynek) рекордное значение коэффициента сжатия составляет 20 (если не учитывать квант. эффективность детектора) и 30 (если учитывать). Для поляризационного сжатие коэффициент равен 3 (Bohar).

Поля на входе светоделителя

$$E_1 = E_0\left[0\cos\omega t + P_1\sin\omega t\right], \quad E_2 = E_0\left[X_2\cos\omega t + 0\sin\omega t\right]$$

Поля на выходе светоделителя

$$E_3 = \frac{1}{\sqrt{2}}\left(E_1 - E_2\right), \quad E_4 = \frac{1}{\sqrt{2}}\left(E_1 + E_2\right) \tag{12.41}$$

$$E_3 = E_0\left[X_3\cos\omega t + P_3\sin\omega t\right] = \frac{E_0}{\sqrt{2}}\left[P_1\cos\omega t - X_2\cos\omega t\right],$$

$$E_4 = E_0\left[X_4\cos\omega t + P_4\sin\omega t\right] = \frac{E_0}{\sqrt{2}}\left[P_1\sin\omega t + X_2\cos\omega t\right].$$

Тогда $X_3 = -X_4 = X_2/\sqrt{2}, \quad P_3 = P_4 = P_1/\sqrt{2}$.

Из последнего соотношения следует условие перепутанности состояний координат и импульсов (квадратурных компонент) в выходных модах светоделителя:

$$X_3 + X_4 = 0, \quad P_3 - P_4 = 0. \tag{12.42}$$

Из (12.42) следует, что свойства X_3, X_4, P_3, P_4 частиц (полей) не определены. Вместо этого определены их совместные свойства. Заметим, что хотя операторы X и P не коммутируют, операторы $X_3 + X_4, \quad P_3 - P_4$ коммутируют из-за знака

“-“! Поэтому для перепутанного состояния совместные свойства $X_3 + X_4, \quad P_3 - P_4$ могут быть измерены одновременно с любой точностью (как и для операторов $X_3 - X_4, \quad P_3 + P_4$).

Если же исходные поля были приготовлены не в максимально-сжатом состоянии, то условие (12.42) не выполняется. Таким образом качество приготовления сжатых состояний существенно определяет качество конечного перепутанного состояния в непрерывных переменных.

ЛЕКЦИЯ 13. ПЕРЕПУТАННЫЕ СОСТОЯНИЯ. МЕРЫ ПЕРЕПУТЫВАНИЯ: МАТЕМАТИЧЕСКИЕ АСПЕКТЫ.

1. Понятие пебита (ebit). Кубиты и пебиты как прямые и косвенные ресурсы квантовой информации.
2. Чистые перепутанные состояния. Разложение Шмидта двухкомпонентной системы. Энтропия перепутывания. Степень перепутывания. Локальные операции и классические сообщения.
3. Смешанные перепутанные состояния. Перепутывание создания. Пример: состояния Вернера.
4. Очищение перепутывания. Протоколы двустороннего и одностороннего обмена. Дистилляция и концентрация перепутывания.
5. Критерий Переса-Хородецки. Сепарабельность квантовых состояний. Пример: состояния Вернера. Свободное и граничное перепутывание.
6. Состояния Белла. Их преобразования при смене базиса. Инварианты.
7. Приложение: матрица плотности немаксимально перепутанных состояний.

Фундаментальной единицей квантовой теории информации является кубит. Напомню, что кубит представляет собой состояние двухуровневой системы, например, частицу со спином 1/2 или произвольная суперпозиция двух фоковских состояний. В представлении двух ортогональных состояний, таких как «0» и «1» кубит отличается от классического бита тем, что он может существовать в произвольной (комплексной) суперпозиции своих базисных состояний:

$$\Psi = c_1 |0\rangle + c_2 |1\rangle . \qquad (13.1)$$

Кроме того, кубит может оказаться в состоянии, которые мы назвали перепутанным и которое не имеет классической аналогии. В прошлом семестре мы рассматривали теорему Б.Шумахера об эффективном сжатии квантовых данных. Эта теорема утверждала, что для оптимального сжатия необходимо определенное количество кубитов, которое требуется для успешной передачи через квантовый канал неизвестных чистых состояний, полученных из источника, приготавливающего известный ансамбль состояний. Другими словами (см.лекцию 6) *энтропия фон Неймана* $S(\rho)$ *ансамбля является просто средним числом кубитов, необходимых для кодирования состояний ансамбля при помощи идеальной кодирующей системы*.

В некоторых протоколах квантовой информации речь идет о других квантовых ресурсах – не о кубитах, а о перепутанных состояниях. Например – в протоколах сверхплотного кодирования, квантовой телепортации, протоколе Экерта квантовой криптографии и многих других. В них речь идет о максимально перепутанных парах кубитов, которые распределены между излучателем и приемником, которые связаны между собой, в общем случае, и классическим и квантовым каналом связи. Так же как и Шумахер, определим *ebit(!) как количество перепутывания содержащейся в максимально перепутанной паре двухуровневых систем*, например, в паре частиц со спином 1/2, находящихся в синглетном состоянии:

$$\Psi = \frac{1}{\sqrt{2}} \left\{ |0\rangle_1 |1\rangle_2 - |1\rangle_1 |0\rangle_2 \right\}. \qquad (13.2)$$

Возникает вопрос, сколько ебитов (прости господи) необходимо для реализации

того или иного протокола.

Замечание: Предлагается произносить ebit как "пебит"! (от "перепутывание" и "бит")

Заметим, что кубиты являются прямыми ресурсами канала связи. Они посылаются в определенном направлении (от источника к приемнику). В то же время пебиты относятся к непрямым ресурсам – они распределены между источником и приемником. Например, если Алиса приготовила две частицы в синглетном состоянии (13.2) и отправила одну частицу Бобу, то результат будет таким же, как если бы Боб приготовил две частицы в таком же состоянии и послал одну из них Алисе.

В некотором смысле пебиты – более слабые ресурсы квантовой информации, чем кубиты, поскольку, передача одного кубита может быть использована для создания одного пебита перепутывания. Однако распределение между пользователями одного или нескольких пебитов само по себе не достаточно для передачи произвольного состояния двухуровневой (квантовой) системы или кубита в любом направлении. Для осуществления такой передачи необходимо дополнить пебит битами классической информации, как это имеет место при квантовой телепортации.

Возникает естественный вопрос. Можно ли в протоколах квантовой информации пользоваться частично перепутанными состояниями, например, в виде:

$$\Psi = \cos\theta \left|0\right\rangle_A \left|1\right\rangle_B - \sin\left|1\right\rangle_A \left|0\right\rangle_B \qquad (13.3)$$

вместо максимально ПС (13.2). А если можно, то сколько таких пар необходимо использовать вместо одной максимально перепутанной пары? Для ответа на эти вопросы нам необходимо количественно охарактеризовать перепутывание, что и составляет предмет этой лекции.

Разложение Шмидта.

Предположим, что у нас имеется две подсистемы A (размерности N) и B (размерности M ≤ N). Тогда утверждается, что совместное состояние этих двух подсистем может быть записано в виде ПС:

$$\Psi_{AB} = \sum_{i=1}^{M} c_i \left|\alpha_i\right\rangle \left|\beta_i\right\rangle, \qquad (13.4)$$

где $|\alpha_i\rangle = |\alpha_1\rangle, |\alpha_2\rangle,..|\alpha_M\rangle$ -базис для подсистемы A, $|\beta_i\rangle = |\beta_1\rangle, |\beta_2\rangle,\ldots|\beta_M\rangle$-базис для подсистемы B. Коэффициенты c_i – действительные, положительные числа. Мы включили фазы в определение базисных состояний для удобства.

Из разложения Шмидта следует, что с точки зрения каждого из двух наблюдателей перепутанные состояния являются смешанными состояниями. Так для наблюдателя A:

$$\rho_A = Sp_B\left(\Psi_{AB}\right) = Sp_B\left|\Psi_{AB}\right\rangle\left\langle\Psi_{AB}\right| = \sum_{i=1}^{M}\left|c_i\right|^2\left|\alpha_i\right\rangle\left\langle\alpha_i\right|. \qquad (13.5)$$

Аналогично, для другого наблюдателя:

$$\rho_B = Sp_A\left(\Psi_{AB}\right) = Sp_A\left|\Psi_{AB}\right\rangle\left\langle\Psi_{AB}\right| = \sum_{i=1}^{M}\left|c_i\right|^2\left|\beta_i\right\rangle\left\langle\beta_i\right|. \qquad (13.6)$$

Для количественного описания перепутывания в чистом состоянии *двух подсистем*

вводят следующую «меру» перепутывания.

Энтропия перепутывания.
Энтропией частично перепутанного чистого состояния – это энтропия фон Неймана

$$E = -Sp\left(\rho \ln \rho\right) \tag{13.7}$$

либо подсистемы А (ρ_A) либо В (ρ_B):

$$E \equiv -Sp\left(\rho_A \ln \rho_A\right) = -Sp\left(\rho_B \ln \rho_B\right) = -\sum_i c_i^2 \ln\left(c_i^2\right) \tag{13.8}$$

Последнее равенство легко проверить на примере двух кубитов:

$$\rho_A \ln \rho_A = \begin{pmatrix} c_1^2 & 0 \\ 0 & c_2^2 \end{pmatrix}\begin{pmatrix} \ln c_1^2 & 0 \\ 0 & \ln c_2^2 \end{pmatrix} = \begin{pmatrix} c_1^2 \ln c_1^2 & 0 \\ 0 & c_2^2 \ln c_2^2 \end{pmatrix}. \tag{13.9}$$

График зависимости энтропии (13.8) от степени перепутывания θ, введенной в (13.3) показан на рис. 1.

Замечание. Мы включили фазы в определение базисных состояний. Если этого не делать, то очевидно, последнее и предпоследнее соотношения будут записаны в виде:

$$E \equiv -Sp\left(\rho_A \ln \rho_A\right) = -Sp\left(\rho_B \ln \rho_B\right) = -\sum_i \left|c_i\right|^2 \ln\left(\left|c_i\right|^2\right) \tag{13.10}$$

Замечание. Представление энтропии в виде натурального логарифма содержит некий произвол. Можно встретить ее определение через логарифм по основанию «2». Тогда энтропия на рис.1 будет достигать единицы (1 пебит) в максимуме.

Величина E, которую часто называют просто «перепутывание», меняется от нуля (для факторизованных состояний, когда $\theta = 0$) до 1 пебита для максимально перепутанных состояний пары двух частиц (когда $\theta = \pi/4$). В более общем случае эта величина максимальна для равномерно распределенных коэффициентов c_i: $c_i^2 = \dfrac{1}{M}$, где M – число базисных векторов в разложении (13.5) или размерность гильбертова пространства для меньшей подсистемы. Так для двухуровневых систем имеем только два члена в разложении Шмидта (13.5)

$c_{1,2} = \dfrac{1}{\sqrt{2}}$ и для системы двух кубитов получаем:

$$\Psi = \frac{1}{\sqrt{2}}\left\{\left|0\right\rangle_1\left|0\right\rangle_2 + \left|1\right\rangle_1\left|1\right\rangle_2\right\} \equiv \Phi^+. \tag{13.11}$$

Здесь нужно сделать важное замечание о том, что разложение Шмидта нельзя осуществить более чем для двух перепутанных систем. Например, рассмотрим три перепутанных системы. Мы хотим записать их общее состояние так, чтобы при фиксации (скажем, в результате измерения) состояния одной из подсистем, этот результат достоверно указывал о состоянии каждой их двух оставшихся подсистем. Это происходит, например, в состоянии ГХЦ, рассмотренном в лекции 11:

$$\Psi_{GHZ} = \frac{1}{\sqrt{2}}\left\{\left|H\right\rangle_1\left|H\right\rangle_2\left|H\right\rangle_3 + \left|V\right\rangle_1\left|V\right\rangle_2\left|V\right\rangle_2\right\}. \tag{13.12}$$

В этом состоянии, измерив состояние первой частицы, которое оказалось, скажем

$|H\rangle_1$ мы достоверно узнаем, что вторая и третья окажутся в состояниях $|H\rangle_2|H\rangle_3$, соответственно. Но в общем случае этого сделать нельзя, поскольку при измерении состояния первой частицы два других окажутся в перепутанном состоянии. Действительно в Л11 было показано, что состояние ГХЦ (13.12), записанное в базисе $|+45^0\rangle, |-45^0\rangle = |H'\rangle, |V'\rangle$, где

$$|H\rangle = \frac{1}{\sqrt{2}}\left(|H'\rangle + |V'\rangle\right),$$
$$|V\rangle = \frac{1}{\sqrt{2}}\left(|H'\rangle - |V'\rangle\right). \qquad (13.13)$$

имеет вид:

$$\Psi_{GHZ} =$$
$$\frac{1}{2}\left(|H'\rangle_1|H'\rangle_2|H'\rangle_3 + |H'\rangle_1|V'\rangle_2|V'\rangle_3 + |V'\rangle_1|H'\rangle_2|V'\rangle_3 + |V'\rangle_1|V'\rangle_2|H'\rangle_3\right), \qquad (13.14)$$

Из (13.14) видно, что задавая состояние первой частицы, две другие проецируются в перепутанное белловское состояние Φ^+.

Частично перепутанными называются подсистемы, для которых величина $E < 1$. Оказывается, что использование таких состояний в протоколе квантовой телепортации приводит к неудачной передаче неизвестного состояния, т.е. с качеством (fidelity) $F < 1$. В протоколе сверхплотной кодировки их использование проявится в зашумленности классического канала связи.

Степень перепутывания. *(degree of entanglement)*
не путать с энтропией перепутывания.

Запишем перепутанное состояние в виде (ср. с (13.3), где использовалась другая параметризация перепутывания):

$$\Psi = \frac{|0\rangle_A|1\rangle_B + \varepsilon|1\rangle_A|0\rangle_B}{\sqrt{1+|\varepsilon|^2}}. \qquad (13.15)$$

Величина ε называется степенью перепутывания. Для максимально перепутанных состояний $\varepsilon = 1$. Вычислим, чему равна энтропия перепутывания состояния (13.15). Видно, что

$$c_1 = \frac{1}{\sqrt{1+|\varepsilon|^2}},\ c_2 = \frac{\varepsilon}{\sqrt{1+|\varepsilon|^2}} \qquad (13.16)$$

Тогда по Беннету,

$$E = -\sum_{i=1}^{2} c_i^2 \ln c_i^2,$$
$$E(\varepsilon) = -\left[\frac{1}{1+\varepsilon^2}\ln\left(\frac{1}{1+\varepsilon^2}\right) + \frac{\varepsilon^2}{1+\varepsilon^2}\ln\left(\frac{\varepsilon^2}{1+\varepsilon^2}\right)\right] =$$
$$= \frac{1}{1+\varepsilon^2}\ln\left(1+\varepsilon^2\right) - \frac{\varepsilon^2}{1+\varepsilon^2}\ln\varepsilon^2 + \frac{\varepsilon^2}{1+\varepsilon^2}\ln\left(1+\varepsilon^2\right) =$$

$$= \frac{1+\varepsilon^2}{1+\varepsilon^2}\ln\left(1+\varepsilon^2\right) - \frac{\varepsilon^2}{1+\varepsilon^2}\ln\varepsilon^2 \rightarrow$$

$$E\left(\varepsilon\right) = \ln\left(1+\varepsilon^2\right) - \frac{\varepsilon^2 \ln\left(\varepsilon^2\right)}{1+\varepsilon^2}. \qquad (13.17)$$

Если $\varepsilon = 1$, то $E(\varepsilon)$ – максимально. Если $\varepsilon = 0$, $E(\varepsilon) = 0$

Говоря о физической реализации состояния (13.15), следует упомянуть работы группы П.Квиата, подразумевая под состояниями $|0\rangle$, $|1\rangle$ пару кубитов, получающихся при неколлинеарном вырожденном по частоте параметрическом рассеянии типа I из двух кристаллов, оптические оси которых составляют друг с другом угол 90 град:

$|0\rangle \rightarrow |H\rangle$, $|1\rangle \rightarrow |V\rangle$

Вклад той или иной компоненты в общее состояние (13.15) регулируется поворотом полуволновой пластинки, установленной перед парой кристаллов ББО.

В этом случае вероятность регистрации совпадений зависит от ориентации поляризационных призм, уставленных перед детекторами по закону:

$$P_{12}\left(\theta_1, \theta_2\right) = \frac{\left|\cos\theta_1 \cos\theta_2 + \varepsilon e^{i\phi} \sin\theta_1 \sin\theta_2\right|^2}{1+\varepsilon^2}. \qquad (13.18)$$

Фаза ϕ регулируется задержкой между двумя поляризациями накачки.

От параметра ε будет меняться глубина модуляции в зависимости числа совпадений от фазы ϕ. Если при максимальной степени перепутывания минимум (в идеальном случае он равен нулю) должен наблюдаться при одинаковых ориентациях поляроидов θ_1, θ_2, то изменение параметра ε приводит не только к уменьшению видности, но к асимметрии зависимости положения минимума от ориентаций поляроидов. Этот эксперимент наглядно демонстрирует влияние степени перепутывания на экспериментально наблюдаемые величины – число совпадений как функция относительной фазы (пространственно-временная интерференция) и ориентации поляроидов (поляризационная интерференция).

Локальные операции и классические сообщения *(local operations and classical comminication LOCC)*

Часто эти два понятия встречаются при описании квантовых протоколов. Поясним, что имеется в виду.

Пусть изначально n частично перепутанных пар распределено между двумя партнерами (Алисой и Бобом). Алиса имеет одну частицу из каждой пары, а Боб – другую. Это *нелокальное* распределение частиц устанавливает начальное перепутывание *nE* между Алисой и Бобом. Теперь разрешим Алисе и Бобу действовать *локально*, т.е. независимо на свои частицы. Это может быть, например, унитарное преобразование, выполняемое Алисой (или Бобом) или обобщенное измерение (фон-Неймана) в гильбертовом пространстве ее т.е. Алисы частиц. То же может делать и Боб. Разрешим также Алису и Бобу координировать их действия путем обмена *классическими сообщениями*. Не разрешается лишь обмениваться

квантовыми системами, а также выполнять нелокальные операции (т.е. влияющие на состояния частиц партнера) после того, как было установлено начальное распределение перепутанными частицами.

К локальным операциям относят:

1. случайные билатеральные вращения. Эта операция выполняется над каждой частицей независимо и приводит начальное смешанное двухчастичное состояние в состояние Вернера. Ее относят к действию зашумленного канала.
2. Унилатеральные вращения на π. Выполняются над одной из частиц путем поворота вокруг осей *x, y* èëè *z*. Òàêèå îïåðàöèè ïîçâîëÿþò ïðåîáðàçîâûâàòü ñîñòîÿíèÿ Áåëëà äóã â äóãà (ïðåîáðàçîâàíèå ôàçîâûìè ìíîæèòåëÿìè):

$$\Psi^{\pm} \xrightarrow{\sigma_x} \Phi^{\pm},\ \Psi^{\pm} \xrightarrow{\sigma_z} \Psi^{\mp};$$

$$\Phi^{\pm} \xrightarrow{\sigma_z} \Phi^{\mp};\ \Psi^{\pm} \xrightarrow{\sigma_y} \Phi^{\mp}$$

3. Áèëàòåðàëüíûå âðàùåíèÿ íà π/2 (B_x, B_y, B_z) обеих частиц пары вокруг осей *x, y* èëè *z*. Òàêèå îïåðàöèè îñòàâëÿþò ñèíãëåòû èíâàðèàíòíûìè è ïðåîáðàçóþò òðèïëåòû äóã â äóãà:

$$\Phi^{+} \xrightarrow{B_x} \Psi^{+},\ \Phi^{-} \xrightarrow{B_y} \Psi^{+};$$

$$\Phi^{+} \xrightarrow{B_z} \Phi^{-};\ \Psi^{\pm} \xrightarrow{B_x, B_y, B_z} \Psi^{\pm}$$

4. Êâàíòîâûå îïåðàöèè XOR, выполняемые билатерально Алисой и Бобом над соответствующими членами распределенных пар. Унилатеральные операции XOR – это операции над двумя кубитами одного из наблюдателей (либо Алисы, либо Боба), когда условно переворачивается второй (мишень) спин если первый (источник) направлен вверх и не происходит ничего в противном случае:

$$U_{XOR} = \left|\uparrow_S \uparrow_T\right\rangle\left\langle\uparrow_S \uparrow_T\right| + \left|\uparrow_S \downarrow_T\right\rangle\left\langle\uparrow_S \downarrow_T\right| + \left|\downarrow_S \downarrow_T\right\rangle\left\langle\downarrow_S \downarrow_T\right| + \left|\downarrow_S \uparrow_T\right\rangle\left\langle\downarrow_S \uparrow_T\right|.$$

Áèëàòåðàëüíûå îïåðàöèè XOR (èëè BXOR) – äâóñòâîðíî àíàëîãè÷íî íà ñîîòâåòñòâóþùèå êîìïîíåíòû äâóõ ïàð, ðàñïðåäåëåííûõ ìåæäó Àëèñîé è Áîáîì. Åñëè ó Àëèñû íàõîäÿòñÿ ñïèíû 1 è 3, à ó Áîáà – ñïèíû 2 è 4, òî îïåðàöèÿ BXOR ñî ñïèíàìè 1 è 2 – êàê èñòî÷íèêàìè, à ñïèíàìè 3 è 4 – êàê ìèøåíÿìè, ïåðåâîðà÷èâàåò ñïèí 3 òîëüêî òîãäà, êîãäà ñïèí 1 íàïðàâëåí ââåðõ, â òî âðåìÿ êàê óñëîâíî ïåðåâîðà÷èâàåò ñïèí 4 òîëüêî òîãäà, êîãäà ñïèí 2 íàïðàâëåí ââåðõ. Видно, что BXOR над двумя состояниями Φ^{+} оставляет их без изменений. Результаты преобразований состояний Белла приведены в таблице:

До преобразования		После преобразования	
Источник	Мишень	Источник	Мишень
$\Phi^{\pm}$	Φ^{+}	без изменения	без изменения
$\Psi^{\pm}$	Φ^{+}	без изменения	Ψ^{+}
$\Psi^{\pm}$	Ψ^{+}	без изменения	Φ^{+}
$\Phi^{\pm}$	Ψ^{+}	без изменения	без изменения
$\Phi^{\pm}$	Φ^{-}	$\Phi^{\mp}$	без изменения
$\Psi^{\pm}$	Φ^{-}	$\Psi^{\mp}$	Ψ^{-}
$\Psi^{\pm}$	Ψ^{-}	$\Psi^{\mp}$	Φ^{-}
$\Phi^{\pm}$	Ψ^{-}	$\Phi^{\mp}$	без изменения

5. Кроме предыдущих четырех унитарных операций Алиса и Боб могут выполнять один тип измерений - измерение обоих спинов вдоль оси z. Такое измерение позволяет легко отличить состояний Ψ от Φ, но не позволяет отличить знак соответствующего состояния. Конечно, после того как проведено измерение, пара больше не является перепутанной.

Смешанные перепутанные состояния

До сих пор речь шла только о чистых перепутанных состояниях. Смешанные ПС возникают при воздействии шума на отдельные подсистемы, образующие составную систему, когда нарушается когерентность суперпозиции (13.3). Типичный сценарий образования (или создания) смешанного ПС показан на рис.3. В начальный момент времени в некоторой участке пространства две квантовые системы A и B взаимодействуют друг с другом. Затем они пространственно разделяются, одна подсистема направляется к Алисе, другая - к Бобу. Совместное состояние обеих подсистем принадлежит гильбертовому пространству $H = H_A \otimes H_B$, которое представляет собой тензорное произведение пространств подсистем. Однако само состояние составной системы не факторизуется – оно является перепутанным $\Psi \neq \Psi_A \otimes \Psi_B$. Впоследствии состояние системы Ψ испытывает воздействие шумовых процессов N_A и N_B, которые действуют независимо на составные части A и B системы, что переводит ее в смешанное состояние. Физически это происходит в зашумленных каналах. Для предотвращения таких процессов разрабатываются методы очищения перепутывания и соответствующие коды, исправляющие ошибки. Фундаментальной мерой перепутывания, которую мы по-прежнему будем обозначать символом E, является *перепутывание формирования* или *перепутывание создания или перепутывание приготовления (entanglement of formation).*

Итак, рассмотрим ансамбль чистых состояний, которые образуют смешанное состояние M. Вообще говоря таких ансамблей для выбранного смешанного состояния может быть несколько. Ансамбль характеризуется двумя наборами:
$\varepsilon = \{p_i, \Psi_i\}$.

Определение 1. Перепутыванием создания чистого двухчастичного состояния Ψ называется энтропия фон Неймана:

$$E(\Psi) = S\left(Sp_A\left|\Psi\right\rangle\left\langle\Psi\right|\right) \equiv S(\rho_A) \equiv S(\rho_B) = -\sum_i \left|c_i\right|^2 \log_2 \left|c_i\right|^2 \qquad (13.19)$$

редуцированной матрицы плотности Алисы или Боба (т.к. они совпадают).

Определение 2. Перепутыванием создания $E(\varepsilon)$ *ансамбля двухчастичных чистых состояний* $\varepsilon = \{p_i, \Psi_i\}$ называют *усредненное по ансамблю* «перепутывание создания» *всех чистых состояний*, составляющих ансамбль:

$$E(\varepsilon) = \sum_i p_i E(\Psi_i) \qquad (13.20)$$

Определение 3. Перепутыванием создания *смешанного состояния M* - *E(M)* называется минимальное значение $E(\varepsilon)$ по всем ансамблям $\varepsilon = \{p_i, \Psi_i\}$, которые могут реализовать данное смешанное состояние $M = \sum_i p_i \left|\Psi_i\right\rangle\left\langle\Psi_i\right|$.

Другими словами «перепутывание создания» – это мера перепутывания, определяемая как по крайней мере ожидаемое перепутывание любого ансамбля чистых состояний, реализующих *M*.

Замечание. Можно доказать, что локальные операции и классические сообщения не могут увеличить значения *E(M)*.

Перепутывание создания для смеси состояний Белла (пример)

Итак, ансамбль чистых состояний с минимальным средним перепутыванием по чистому состоянию и реализующим данную матрицу плотности определяет наиболее оптимальный способ создания или приготовления этой матрицы плотности.

Замечание. *Считается, что в общем случае неизвестно как найти такой ансамбль минимально перепутанных состояний для данной матрицы плотности*.

Однако в некоторых частных случаях это удается сделать, например, для подкласса ансамбля чистых состояний частиц со спином 1/2 , а именно – смешанному состоянию, которое диагонализуется в Белловском базисе.

Рассмотрим т.н. состояния Вернера. Это состояние, которое представляет ансамбль F частей чистых синглетов и (1-F) частей других состояний Белла:

$$W_F = F\left|\Psi^-\right\rangle\left\langle\Psi^-\right| + \frac{1-F}{3}\left(\left|\Psi^+\right\rangle\left\langle\Psi^+\right| + \left|\Phi^+\right\rangle\left\langle\Phi^+\right| + \left|\Phi^-\right\rangle\left\langle\Phi^-\right|\right). \qquad (13.21)$$

Такое представление состояния Вернера эквивалентно другому, когда $x = (4F-1)/3$ частей – это синглеты, а $(1-x)$ частей – т.н. полностью смешанное состояние, тождественное единичному оператору:

$$G = I = \frac{1}{4}\left(\left|\Psi^+\right\rangle\left\langle\Psi^+\right| + \left|\Psi^-\right\rangle\left\langle\Psi^-\right| + \left|\Phi^+\right\rangle\left\langle\Phi^+\right| + \left|\Phi^-\right\rangle\left\langle\Phi^-\right|\right). \qquad (13.22)$$

Именно в таком виде это состояние было определено Вернером. В представлении (13.21) фигурирует величина F, которая является качеством (fidelity) или чистотой состояния по отношению к идеальному синглету:

$$F = \left\langle\Psi^-\left|W_F\right|\Psi^-\right\rangle. \qquad (13.23)$$

Действительно, доля чистых синглетов в (13.21) составляет $x=(4F-1)/3$, а доля синглетов в единичном операторе составляет $(1-x)/4$. Итого в состоянии Вернера имеется $\frac{4F-1}{3}+\frac{1-x}{4}=\left(x=\frac{4F-1}{3}\right)=\frac{4F-1}{3}+\frac{1-\frac{4F-1}{3}}{4}=F$ синглетов, из которых чистых - ровно *x*.

Найдем, например, перепутывание создания для состояния Вернера $W_{5/8}$.

$$W_{5/8}=\frac{5}{8}\left|\Psi^-\right\rangle\left\langle\Psi^-\right|+\frac{1}{8}\left(\left|\Psi^+\right\rangle\left\langle\Psi^+\right|+\left|\Phi^+\right\rangle\left\langle\Phi^+\right|+\left|\Phi^-\right\rangle\left\langle\Phi^-\right|\right). \qquad (13.24)$$

Это состояние представляет собой 5/8 на 3/8 – синглет-триплетную смесь. Его можно приготовить, смешав равные порции синглетов и случайных некоррелированных спинов. На языке поляризаций – это равновзвешенная смесь синглетных пар и некоррелированных по поляризации пар частиц. Другими словами – состояние (13.24) получается при прохождении пары фотонов синглетном состоянии через 50%-ый зашумленный канал. (т.е. который каждую вторую коррелированную по поляризации пару делает некоррелированной).

Замечание. Вообще, по определению *x*-деполяризующим каналом связи называют такой канал, который пропускает входное состояние с вероятностью $1-x$ и заменяет его полностью случайными кубитами с вероятностью *x*.

Состояние Вернера (13.24) замечательно тем, что чистое перепутанное состояние может быть выделено из него с помощью двусторонних протоколов, но не может быть выделено с попощью односторонних протоколов

Видно, что для приготовления смешанного состояния $W_{F=5/8}$ необходимо $x=(4F-1)/3=0.5$ чистых синглетов; эта величина непосредственно входит в определение состояния Вернера. Казалось бы, что величина перепутывания создания составляет 0.5*x*1=0.5 пебит, поскольку на чистый синглет (максимально перепутанное состояние приходится по 1 пебиту). Однако численный расчет, производящий минимазацию по всем возможным ансамблям, составляющим состояние $W_{5/8}$ дает значение 0.117 пебит! Это значение дает смесь четырех чистых состояний с одинаковой вероятностью. Это означает, что равновероятная смесь чистых состояний, дающих $W_{5/8}$, более экономична.

Очищение перепутывания. *(entanglement purification).*

Под очищением перепутывания понимают асимптотическое создание (выделение) произвольного числа чистых синглетов, которые могут быть приготовлены локально из смешанного состояния M.

- является одной из главных алгоритмических задач теории квантовой информации. Кратко рассмотрим два основных протокола.

Наиболее мощный протокол – ***двустороннего обмена классическими сообщениями*.**

На рис. 4 показана схема протокола. Алиса и Боб имеют распределенное двухчастичное перепутанное смешанное состояние $\boldsymbol{M}=(M)^n$, состоящее из *n* перепутанных пар частиц. Каждая пара описывается матрицей плотности *M*. Протокол состоит в повторении трех операций:

Алиса и Боб выполняют унитарные преобразования над имеющимися у них состояниями (частицами);
Алиса и Боб выполняют измерения некоторых имеющихся у них частиц;
Алиса и Боб обмениваются результатами своих измерений. Они используют эту информацию для выбора следующего унитарного преобразования, которое они должны выполнить на следующем этапе.
Видно, что в этом протоколе приходится жертвовать некоторыми частицами, в то время как оставшиеся частицы переводятся в чистое максимально перепутанное состояние, например, в $\Psi = \left(\Psi^{-}\right)^{m}$, т.е. тензорное произведение m синглетов, причем $0 < m < n$.

Протокол одностороннего обмена классическими сообщениями.
Версия этого протокола показана на рисунке 5. Здесь участникам протокола разрешается выполнять лишь одно действие, состоящее в унитарной операции и измерении, сопровождаемым классическим, односторонним сообщением. Алиса выполняет унитарное преобразование U_1 и измерение *Mes*. Çàòåì, îíà ïîñûëàåò ðåçóëüòàò èçìåðåíèÿ â âèäå êëàññè÷åñêîãî ñîîáùåíèÿ ÁîáÓ. ÁîáÓ èñïîëüçóåò ýòîò ðåçóëüòàò â êîìáèíàöèè ñ ðåçóëüòàòîì ñâîåãî èçìåðåíèÿ äëÿ êîíòðîëÿ çà îêî÷àòåëüíûì óíèòàðíûì ïðåîáðàçîâàíèåì U_3. Главное преимущество этого протокола состоит в том, что компоненты итогового очищенного максимально перепутанного состояния (обозначенного звездочкой *) могут быть разнесены и в пространстве, и во времени!
Замечание. Иногда под очищением "*purification*" понимают процедуру, в которой увеличивается чистота состояния, т.е. уменьшается энтропия. Этот случай не относится к рассмотренной процедуре выделения чистых синглетов из смешанного состояния. Под энтропией здесь понимается мера чистоты состояния - энтропия матрицы плотности ρ:

$$S = -\sum_{i=1}^{4} \log_4 \lambda_i \ , \qquad \text{(S)}$$

где λ_i - собственные значения матрицы плотности

Замечание. *Distillation = purification = дистилляция = очищение*– ýòî óâåëè÷åíèå ïðåïóòñòâèÿ ñîñòîÿíèÿ в смысле выделения синглетов. Иногда под *Distillation* понимают увеличение степени перепутывания состояния.
Îïðåäåëåíèå. *Concentration* - это одновременное увеличение чистоты и перепутывания состояния. Изначально вводилось только для чистых перепутанных состояний вида (13.3)
Условно эти процессы манипуляций с перепутыванием можно изобразить в виде таблицы (Рис.5)

Критерий Переса-Хородецки.

Для того чтобы использовать перепутывание в протоколах квантовой информации, необходимо иметь их в чистой (например, синглетной) форме. Процедура преобразования смешанного перепутанного состояния ρ в синглетную форму называется дистилляцией или очищением (локальные операции + классические сообщения).

Смешанное состояние квантовой системы, состоящей из двух подсистем, является перепутанным, если оно несепарабельно, т.е. его нельзя записать в виде:

$$\rho = \sum_i p_i \rho_i^A \otimes \rho_i^B = \sum_i^k p_i \left|\alpha_i\right\rangle\left\langle\alpha_i\right| \otimes \left|\beta_i\right\rangle\left\langle\beta_i\right|, \quad p_i \geq 0, \quad \sum_i^k p_i = 1 \tag{A1}$$

где ρ_i^A, ρ_i^B - (смешанные) состояния двух подсистем.

Замечание. Часто говорят, что сепарабельные состояния являются “распутанными” (*disentangled*).

А.Перес доказал, что необходимым условием сепарабельности двух подсистем, состоит в том, что некая дополнительная матрица σ, полученная путем частичной перестановки индексов в ρ, имеет только неотрицательные собственные значения. Физический смысл критерия состоит в том, что он более чувствителен для распознавания (квантовой) несепарабельности, чем неравенства Белла.

В полном виде матрица плотности двухкомпонентной системы имеет вид:

$$\rho_{m\mu,n\nu} = \sum_i p_i \left(\rho_i^A\right)_{mn} \left(\rho_i^B\right)_{\mu\nu}. \tag{A2}$$

Здесь латинские индексы относятся к подсистеме *A*, а греческие – к подсистеме *B*.

Замечание – напоминание. Прямым произведением двух матриц размерностью 2x2 называется матрица размерности 4x4:

$$\alpha \otimes \beta = \begin{pmatrix} \alpha_{11}\beta & \alpha_{12}\beta \\ \alpha_{21}\beta & \alpha_{22}\beta \end{pmatrix} \equiv \begin{pmatrix} \alpha_{11}\beta_{11} & \alpha_{11}\beta_{12} & \alpha_{12}\beta_{11} & \alpha_{12}\beta_{12} \\ \alpha_{11}\beta_{21} & \alpha_{11}\beta_{22} & \alpha_{12}\beta_{21} & \alpha_{12}\beta_{22} \\ \alpha_{21}\beta_{11} & \alpha_{21}\beta_{12} & \alpha_{22}\beta_{11} & \alpha_{22}\beta_{12} \\ \alpha_{21}\beta_{21} & \alpha_{21}\beta_{22} & \alpha_{22}\beta_{21} & \alpha_{22}\beta_{22} \end{pmatrix}$$

Такая матрица плотности описывает, в частности, совместное состояние двух кубитов:

$$\Psi = \left(c_{11}\left|0\right\rangle_1 + c_{12}\left|1\right\rangle_1\right) \otimes \left(c_{21}\left|0\right\rangle_2 + c_{22}\left|1\right\rangle_2\right)$$

Замечание. Выражение (A2) напоминает таковое для классической функции Лиувилля, где дискретные индексы заменены на канонические переменные ***q*** и ***p***. Îäíàêî ôóíêöèÿ Ëèóâèëëÿ äîëæíà áûòü íåîòðèöàòåëüíîé, à ìû òðåáóåì îò ìàòðèöû ïëîòíîñòè ëèøü íåîòðèöàòåëüíûõ ñîáñòâåííûõ çíà÷åíèé, ÷òî ÿâëÿåòñÿ áîëåå ìÿãêèì óñëîâèåì.

Определим новую матрицу:

$$\sigma_{m\mu,n\nu} \equiv \rho_{n\mu,m\nu}, \tag{A3}$$

где латинские индексы в ρ были переставлены (матрица транспонирована), а греческие – нет. Такое преобразование не является унитарным, тем не менее, матрица σ - эрмитова. Если условия A1(или A2) выполняются, то

$$\sigma = \sum_i p_i \left(\rho_i^A\right)^T \otimes \left(\rho_i^B\right). \qquad \text{(A4)}$$

Поскольку транспонированные матрицы $\left(\rho_i^A\right)^T \equiv \left(\rho_i^A\right)^*$ -это неотрицательные матрицы с единичным следом, то они также могут выступать как матрицы плотности. Отсюда следует, что ни одно из собственных значений σ не может быть отрицательным. Это *необходимое условие* выполнения А1.

Пример. Рассмотрим пару частиц со спином 1/2 в состоянии Вернера, состоящем из части *x* синглетов и случайной части (*1-x*). Мы помним, что в случайной части *(1-x)* также присутствует равновероятная доля синглетов наряду с триплетами:

$$\rho = x\left|\Psi^-\right\rangle\left\langle\Psi^-\right| + \{1-x\}\left(\left|\Psi^-\right\rangle\left\langle\Psi^-\right| + \left|\Psi^+\right\rangle\left\langle\Psi^+\right| + \left|\Phi^+\right\rangle\left\langle\Phi^+\right| + \left|\Phi^-\right\rangle\left\langle\Phi^-\right|\right). \qquad \text{(A2)}$$

Оказывается, что дополнительная матрица σ имеет четыре собственных значения: три из них вырождены и равны $(1+x)/4$, а четвертое равно $(1-3x)/4$. Наименьшее собственное значение положительно, если

$$x < \frac{1}{3} \approx 0.33 \qquad \text{(A3)}$$

тогда условие сепарабельности выполняется. Этот результат можно сравнить с другим условием – выполнение неравенства Белла для тех же состояний. Оказывается, что неравенство Белла выполняется, если

$$x < \frac{1}{\sqrt{2}} \approx 0.71. \qquad \text{(A5)}$$

Это условие, очевидно, гораздо менее строгое, чем то, которое дается условием несепарабельности.

Таким образом, состояние может быть несепарабельным, но в то же время не нарушать неравенств Белла.

Замечание. В рассмотренном случае состояний Вернера условие $x < \frac{1}{3}$ также является достаточным условием сепарабельности – т.е. если $x < \frac{1}{3}$, то возможно записать ρ как смесь неперепутанных состояний. Этот результат предполагает, что необходимое условие, полученное выше (неотрицательность собственных значений матрицы σ)может также быть достаточным для любого состояния ρ. Для систем с размерностью выше 2X2 необходимое условие сепарабельности не является достаточным.

Можно показать (Хородецки 1997), что *любое несепарабельное двух-кубитовое состояние представляет собой перепутанное состояние, которое может быть дистиллировано в синглетную форму*.

Это утверждение оправдывает с операциональной точки зрения введение термина “(не)сепарабельность”.

Казалось бы, что из этого утверждения можно высказать гипотезу о том, что

«любое несепарабельное состояние можно дистиллировать в синглетную форму».

Оказывается, что это не так! Существуют несепарабельные состояния, которые нельзя очистить.

Любое состояние, которое может быть очищено должно нарушать критерий сепарабельности А.Переса. Дело в том, что существует два качественно разных типа перепутывания. Первый из них – «*свободное*» перепутывание, т.е. такое, которое может быть очищено в синглетную форму. Второй тип перепутывания – невозможно очистить. Его можно рассматривать по аналогии с термодинамикой как «*граничное*» перепутывание. Его нельзя использовать для выполнения «информационной работы», т.е. как подходящий ресурс для передачи квантовых данных или телепортации.

Состояния Белла. Их преобразования при смене базисов.

Под состояниями Белла понимают совместные двухмодовые состояния двухуровневых систем. Иногда их рассматривают как собственные состояния некого оператора, названного *оператором Белла*. Можно показать, что существует лишь четыре базисных ортогональных состояния, по которым можно разложить любую двухмодовую двухуровневую систему. Выпишем эти состояния, применительно к системе двух одинаковых фотонов в линейном поляризационном базисе (аналогично записывается состояние двухмодовой системы двух одинаковых частиц со спином 1/2):

$$\Psi_{12}^{(-)} = \frac{1}{\sqrt{2}}\left[\left|H_1\right\rangle\left|V_2\right\rangle - \left|V_1\right\rangle\left|H_2\right\rangle\right], \tag{13.25}$$

$$\Psi_{12}^{(+)} = \frac{1}{\sqrt{2}}\left[\left|H_1\right\rangle\left|V_2\right\rangle + \left|V_1\right\rangle\left|H_2\right\rangle\right], \tag{13.26}$$

$$\Phi_{12}^{(-)} = \frac{1}{\sqrt{2}}\left[\left|H_1\right\rangle\left|H_2\right\rangle - \left|V_1\right\rangle\left|V_2\right\rangle\right], \tag{13.27}$$

$$\Phi_{12}^{(+)} = \frac{1}{\sqrt{2}}\left[\left|H_1\right\rangle\left|H_2\right\rangle + \left|V_1\right\rangle\left|V_2\right\rangle\right]. \tag{13.28}$$

Видно, что состояния Белла являются максимально перепутанными состояниями, поскольку определенным совместным волновым функциям не отвечают определенные волновые функции отдельных систем. Термин “максимально перепутанный” формально возникает из-за условия нормировки, когда общее состояние представляется равновесовой суперпозицией двух компонент.

По иронии судьбы состояния Белла, впервые введенные в 1992 году А.Мэнном, М.Ривзеном и У.Шлейчем, по смыслу являлись прямо противоположными тем, которые широко используются в настоящее время (25-28). Изначально они определялись, как чистые квантовые состояния квантованного поля излучения, которые обладают фундаментальными атрибутами классических состояний (т.е. не приводят к квантовым корреляциям), и факторизуются на выходе светоделителя, а значит, никогда не нарушают неравенств Белла.

Рассмотрим, к примеру, состояние $\Phi^{(+)}$ (индексы 1,2 будем опускать там, где это не ведет к непониманию). Оно означает, что и сигнальный и холостой фотоны всегда имеют оба либо вертикальную, либо горизонтальную поляризации, причем вероятность зарегистрировать *H*- или *V*- поляризацию в каждой моде одинакова и равна 1/2. Другими словами, при совершенно неопределенной поляризации в каждой из мод, существует полная корреляция одинаковых поляризаций двух мод.

Рассмотрим преобразования состояний Белла при смене поляризационного базиса.

Для этого перепишем их в более общем виде:

$$\Psi_{BC}^{(\pm)} = \frac{1}{\sqrt{2}}\left[\left|B_x\right\rangle\left|C_y\right\rangle \pm \left|B_y\right\rangle\left|C_x\right\rangle\right], \tag{13.29}$$

$$\Phi_{BC}^{(\pm)} = \frac{1}{\sqrt{2}}\left[\left|B_x\right\rangle\left|C_x\right\rangle \pm \left|B_y\right\rangle\left|C_y\right\rangle\right], \tag{13.30}$$

где B и C обозначают две частицы, x и y - компоненты линейного поляризационного базиса, а запись $\left|B_x\right\rangle\left|C_y\right\rangle$ означает двукратное действие соответствующих операторов рождения на вакуум: $\left|B_x\right\rangle\left|C_y\right\rangle = b_x^\dagger c_y^\dagger\left|0\right\rangle$. Пусть при произвольном преобразования поляризационного базиса $B_{x,y} \to B_{1,2}$, $C_{x,y} \to C_{1,2}$ его компоненты определяются элементами матрицы преобразования

$$D = \begin{pmatrix} t^* & -r \\ r^* & t \end{pmatrix},\ |t|^2 + |r|^2 = 1, \tag{13.31}$$

т.е. в матричном виде $D\begin{pmatrix} B_1 \\ B_2 \end{pmatrix} = \begin{pmatrix} B_x \\ B_y \end{pmatrix}$, и $D^\dagger\begin{pmatrix} B_x \\ B_y \end{pmatrix} = \begin{pmatrix} B_1 \\ B_2 \end{pmatrix}$. Комплексные параметры t и r можно интерпретировать как коэффициенты пропускания и отражения, а матрицы являются эрмитово-сопряженными $D = D^\dagger$. Тогда, компоненты базисов преобразуются следующим образом:

$$\left|B_x\right\rangle = t^*\left|B_1\right\rangle - r\left|B_2\right\rangle, \quad \left|C_x\right\rangle = t^*\left|C_1\right\rangle - r\left|C_2\right\rangle, \tag{13.32}$$

$$\left|B_y\right\rangle = r^*\left|B_1\right\rangle + t\left|B_2\right\rangle, \quad \left|C_y\right\rangle = r^*\left|C_1\right\rangle + t\left|C_2\right\rangle. \tag{13.33}$$

После простых алгебраических вычислений получаем:

$$\Psi_{BC}^{-} = \frac{1}{\sqrt{2}}\left[\left|B_1C_1\right\rangle - \left|B_2C_2\right\rangle\right], \tag{13.34}$$

$$\Psi_{BC}^{+} = \frac{1}{\sqrt{2}}\left[2t^*r^*\left|B_1C_1\right\rangle - 2tr\left|B_2C_2\right\rangle + \left(tt^* - rr^*\right)\left(\left|B_1C_1\right\rangle + \left|B_2C_2\right\rangle\right)\right], \tag{13.35}$$

$$\Phi_{BC}^{-} = \frac{1}{\sqrt{2}}\left[\left(t^{*^2} - r^{*^2}\right)\left|B_1C_1\right\rangle + \left(r^2 - t^2\right)\left|B_2C_2\right\rangle - \left(t^*r + r^*t\right)\left(\left|B_1C_2\right\rangle + \left|B_2C_1\right\rangle\right)\right], \tag{13.36}$$

$$\Phi_{BC}^{+} = \frac{1}{\sqrt{2}}\left[\left(t^{*^2} + r^{*^2}\right)\left|B_1C_1\right\rangle + \left(t^2 + r^2\right)\left|B_2C_2\right\rangle + \left(r^*t - t^*r\right)\left(\left|B_1C_2\right\rangle - \left|B_2C_1\right\rangle\right)\right]. \tag{13.37}$$

Видно, что только одно (синглетное) состояние Белла инвариантно при произвольных преобразованиях базиса. ботах рассмотрены некоторые интересные особенности специфических поляризационных преобразований состояний Белла[1] и предложена экспериментальная процедура томографии таких состояний.

Частным случаем преобразований является поворот линейного базиса на угол $(-\alpha)$. Матрица D описывает поворот координат, если $t = \cos\alpha, \quad r = \sin\alpha$. Пусть a и b - декартовы оси нового базиса. Тогда

[1] Например, преобразование, в котором между x- и y-компонентами вносится задержка. Формально, такая процедура описывается матрицей D, у которой $t = e^{i\delta}, \quad r = 0$, где $\varphi_x - \varphi_y = 2\delta$.

$$\Psi^{-}_{xy}=\frac{1}{\sqrt{2}}\left[\left|B_xC_y\right\rangle-\left|B_yC_x\right\rangle\right]=\frac{1}{\sqrt{2}}\left[\left|B_aC_b\right\rangle-\left|B_bC_a\right\rangle\right], \tag{13.38}$$

$$\Psi^{+}_{xy}=\frac{1}{\sqrt{2}}\left[\left|B_xC_y\right\rangle+\left|B_yC_x\right\rangle\right]=\frac{1}{\sqrt{2}}\left[\sin 2\alpha\left\{\left|B_aC_a\right\rangle-\left|B_bC_b\right\rangle\right\}+\cos 2\alpha\left\{\left|B_aC_b\right\rangle+\left|B_bC_a\right\rangle\right\}\right]=$$

$$=\frac{1}{\sqrt{2}}\left[\sin 2\alpha\left|\Phi^{-}_{ab}\right\rangle+\cos 2\alpha\left|\Psi^{+}_{ab}\right\rangle\right]. \tag{13.39}$$

$$\Phi^{-}_{xy}=\frac{1}{\sqrt{2}}\left[\left|B_xC_x\right\rangle-\left|B_yC_y\right\rangle\right]=\frac{1}{\sqrt{2}}\left[\cos 2\alpha\left\{\left|B_aC_a\right\rangle-\left|B_bC_b\right\rangle\right\}-\sin 2\alpha\left\{\left|B_aC_b\right\rangle+\left|B_bC_a\right\rangle\right\}\right]=$$

$$=\frac{1}{\sqrt{2}}\left[\cos 2\alpha\left|\Phi^{-}_{ab}\right\rangle-\sin 2\alpha\left|\Psi^{+}_{ab}\right\rangle\right]. \tag{13.40}$$

$$\Phi^{+}_{xy}=\frac{1}{\sqrt{2}}\left[\left|B_xC_x\right\rangle+\left|B_yC_y\right\rangle\right]=\frac{1}{\sqrt{2}}\left[\left|B_aC_a\right\rangle+\left|B_bC_b\right\rangle\right]. \tag{13.41}$$

Замечательно, что при этом типе преобразований появляется еще один инвариант - состояние $\Phi^{+}_{xy}\equiv\Phi^{+}_{ab}$ (25), а два других преобразуются друг в друга при ориентации $\alpha=45^0$.

Приложение

Матрица плотности состояний Белла.

Формально вычисление матрицы плотности системы двух кубитов происходит следующим образом.

$\Psi=\left(c_{11}\left|0\right\rangle_1+c_{12}\left|1\right\rangle_1\right)\otimes\left(c_{21}\left|0\right\rangle_2+c_{22}\left|1\right\rangle_2\right)$.

Тогда М.П. имеет вид:

$$\rho=\left|\Psi\right\rangle\left\langle\Psi\right|=\left(c_{11}c_{21}\left|0\right\rangle_1\left|0\right\rangle_2+c_{11}c_{22}\left|0\right\rangle_1\left|1\right\rangle_2+c_{12}c_{21}\left|1\right\rangle_1\left|0\right\rangle_2+c_{12}c_{22}\left|1\right\rangle_1\left|1\right\rangle_2\right)\times$$

$$\times\left(c_{11}^{*}c_{21}^{*}\left\langle 0\right|_2\left\langle 0\right|_1+c_{11}^{*}c_{22}^{*}\left\langle 1\right|_2\left\langle 0\right|_1+c_{12}^{*}c_{21}^{*}\left\langle 0\right|_2\left\langle 1\right|_1+c_{12}^{*}c_{22}^{*}\left\langle 1\right|_2\left\langle 1\right|_1\right)$$

После перемножения получается 16 слагаемых при проекционных операторах, которые и являются компонентами М.П. Если принять следующие обозначения:

$$\left|0\right\rangle_1\left|0\right\rangle_2\to 1,\ \left|0\right\rangle_1\left|1\right\rangle_2\to 2,\ \left|1\right\rangle_1\left|0\right\rangle_2\to 3,\ \left|1\right\rangle_1\left|1\right\rangle_2\to 4$$

$$\left\langle 0\right|_2\left\langle 0\right|_1\to 1,\ \left\langle 1\right|_2\left\langle 0\right|_1\to 2,\ \left\langle 0\right|_2\left\langle 1\right|_1\to 3,\ \left\langle 1\right|_2\left\langle 1\right|_1\to 4$$

,

то М.П. примет окончательный вид:

$$\rho=\begin{pmatrix} c_{11}c_{21}c_{11}^{*}c_{21}^{*} & c_{11}c_{21}c_{11}^{*}c_{22}^{*} & c_{11}c_{21}c_{12}^{*}c_{21}^{*} & c_{11}c_{21}c_{12}^{*}c_{22}^{*} \\ c_{11}c_{22}c_{11}^{*}c_{21}^{*} & c_{11}c_{22}c_{11}^{*}c_{22}^{*} & c_{11}c_{22}c_{12}^{*}c_{21}^{*} & c_{11}c_{22}c_{12}^{*}c_{22}^{*} \\ c_{12}c_{21}c_{11}^{*}c_{21}^{*} & c_{12}c_{21}c_{11}^{*}c_{22}^{*} & c_{12}c_{21}c_{12}^{*}c_{21}^{*} & c_{12}c_{21}c_{12}^{*}c_{22}^{*} \\ c_{12}c_{22}c_{11}^{*}c_{21}^{*} & c_{12}c_{22}c_{11}^{*}c_{22}^{*} & c_{12}c_{22}c_{12}^{*}c_{21}^{*} & c_{12}c_{22}c_{12}^{*}c_{22}^{*} \end{pmatrix}$$

Теперь нетрудно вычислить матрицы плотности немаксимально перепутанных чистых состояний:

$$\left|\Phi^{\pm}\right\rangle=c_1\left|0\right\rangle_1\left|0\right\rangle_2\pm c_2\left|1\right\rangle_1\left|1\right\rangle_2,$$

$$\left|\Psi^{\pm}\right\rangle=c_1\left|0\right\rangle_1\left|1\right\rangle_2\pm c_2\left|1\right\rangle_1\left|0\right\rangle_2.$$

Для максимально перепутанных состояний (Белла): $c_1 = c_2 = \frac{1}{\sqrt{2}}$.

$$\left|\Phi^{\pm}\right\rangle\left\langle\Phi^{\pm}\right| = \begin{pmatrix} c_1^2 & 0 & 0 & \pm c_1 c_2 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \pm c_1 c_2 & 0 & 0 & c_2^2 \end{pmatrix}, \qquad \left|\Psi^{\pm}\right\rangle\left\langle\Psi^{\pm}\right| = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & c_1^2 & \pm c_1 c_2 & 0 \\ 0 & \pm c_1 c_2 & c_2^2 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Энтропия таких состояний выражается соотношением (S):

$$S = -\sum_{i=1}^{4} \log_4 \lambda_i .$$

Собственные значения λ_i вычисляются как корни характеристического уравнения. Например, для состояния Φ^+ это уравнение:

$$\det\begin{pmatrix} c_1^2 - \lambda & 0 & 0 & c_1 c_2 \\ 0 & -\lambda & 0 & 0 \\ 0 & 0 & -\lambda & 0 \\ c_1 c_2 & 0 & 0 & c_2^2 - \lambda \end{pmatrix} = 0 \rightarrow \left(c_1^2 - \lambda\right)\begin{Vmatrix} -\lambda & 0 & 0 \\ 0 & -\lambda & 0 \\ 0 & 0 & c_2^2 - \lambda \end{Vmatrix}(-1)^{1+1} + 0 + 0 + c_1 c_2 \begin{Vmatrix} 0 & 0 & c_1 c_2 \\ -\lambda & 0 & 0 \\ 0 & -\lambda & 0 \end{Vmatrix}(-1)^{1+4} =$$

$$\left(c_1^2 - \lambda\right)\left[\lambda^2\left(c_2^2 - \lambda\right)\right] - c_1 c_2\left(c_1 c_2 \lambda^2\right) = 0 ,$$

которое имеет решения: $\lambda_{1,2,3} = 0; \quad \lambda_4 = c_1^2 + c_2^2$. В силу нормировки:

$$\lambda_4 = c_1^2 + c_2^2 \equiv 1 .$$

Такие же собственные значения получаются и для других немаксимально перепутанных состояний.

Из последнего условия видно, что энтропия немаксимально перепутанных состояний равна нулю. Это представляется очевидным, поскольку речь идет о чистых состояний. Как показано на рис. 6 процедура discillation лишь увеличивает степень перепутывания, сохраняя энтропию (т.е. чистоту состояния0.

ЛИТЕРАТУРА:

1. Ch.Bennett, H.Bernstein, S.Popescu, B.Shumacher. Concentration partial entanglement by local operations. Phys.Rev.A, 53, 2046 (1996).
2. Ch.Bennett, D.DiVincenzo, J.Smolin, W.Wooters. Mixed-State entanglement and quantum error correction. Phys.Rev. A,54, 3824 (1996).
3. A.Peres. Separability Cryterion for Density Matrices. Phys.Rev.Lett. 77, 1413 (1996).
Michal Horodecki, Pavel Horodecki, Ryszard Horodecki. Separability of mixed states: necessary and sufficient conditions. Ph/9605038.
4. Michal Horodecki, Pavel Horodecki, Ryszard Horodecki. Mixed-state entanglement and distillation: is there a “bound” entanglement in nature?
5. R.T.Thew, W.Munro. Entanglement manipulation and concentration. Phys.Rev.A, 63, 030302 (2001).
6. A.G.White, D.F.V.James, P.H.Eberhard, and P.G.Kwiat, Non-maximally Entangled States: Production, Characterization and Utilization. LANL e-print quant-ph 99088081.

ЛЕКЦИЯ 14. ПЛОТНАЯ КОДИРОВКА.

1. Перепутывание – как информационный ресурс.
2. Идея плотной кодировки. Унилатеральные вращения. Протокол Ч.Беннета и С.Визнера. Преимущества плотной кодировки перед прямой передачей классических битов с помощью двух частиц.
3. Эксперимент группы А.Цайлингера по плотной кодировке с использованием двухчастичных поляризационно-угловых перепутанных состояний.

Утверждение, которое будет обсуждаться на ближайших лекциях, формулируется так:

- перепутывание является информационным ресурсом.

Известно, что кубиты могут быть использованы для хранения и передачи классической информации, поскольку они содержат в себе, как предельный случай, классические биты. Например, для передачи строки классических битов 00101, Алиса может послать пять кубитов (пять двухуровневых систем), приготовленных в состоянии $|00101\rangle$. Получатель сообщения – Боб – может извлечь информацию, измеряя каждый кубит в базисе $\{|0\rangle,|1\rangle\}$. Здесь под $|0\rangle,|1\rangle$ мы понимаем собственные состояния измеряемой наблюдаемой. Результат измерения дает строку классических битов. При этом с каждым кубитом передается не более одного классического бита.

Таким образом, можно записать, что $1\ bit \le 1\ qubit$.

Теперь предположим, что между Алисой и Бобом распределены пары максимально перепутанных кубитов в состоянии $|00\rangle+|11\rangle$. Мы будем опускать нормировочный множитель. На этом этапе между Алисой и Бобом нет никаких каналов связи – перепутанные состояния генерируются сторонним источником, который посылает один кубит Алисе, а другой – Бобу, а те, в свою очередь, имеют возможность манипулировать только своими частицами (т.е. локально). В такой схеме Алисе можно передать два классических бита информации, посылая затем Бобу лишь один кубит, точнее – половинку перепутанной пары. Эта идея, предложенная Визнером и Беннетом в 1992 году, получила название «***плотной кодировки***», поскольку лишь один квантовый бит поступает от Алисы к Бобу для передачи двух классических битов. В протокол вовлечены два квантовых бита, однако, Алисе доступен лишь один из них. При «***квантовой телепортации***» (следующая лекция) с помощью перепутанной пары частиц и двух битов классической информации можно *уничтожить* неизвестное квантовое состояние одной частицы (кубит) и *воссоздать* его на другой частице (Рис.1).

Напомню, что количественно, перепутывание характеризуется термином «пебит» (см. Лекцию 13), что характеризует квантовый ресурс, состоящий в распределенной паре максимально перепутанных состояний двухуровневых частиц. Тогда условно, можно записать следующие соотношения между классическими и квантовыми ресурсами каналов связи:

$1\ bit \le 1\ qubit$,

$1\ ebit \le 1\ qubit$,

$1\ qubit \le 1\ ebit + 2\ bits$,

$2\ bits \le 1\ ebit + 1\ qubit$.

Здесь знак ≤ означает, что ресурс в левой части неравенства может быть реализован из ресурса, стоящего в правой части, но не наоборот. Так первая строчка означает, что классический бит может быть передан посредством квантового бита, например, когда множество значений кубита ограничено лишь двумя ортогональными состояниями. Этот пример был рассмотрен в начале лекции. Вторая строчка означает, что пебит распределенного перепутывания можно создать посылая кубит, например, когда один наблюдатель приготавливает ЭПР-пару и посылает ее половинку (т.е. одну частицу) другому наблюдателю. Третья и четвертая строчки представляют более сложные проявления ресурсов, задействованных, например, в протоколах телепортации и плотной кодировки, соответственно. Так, третья строка говорит, что с помощью перепутанной пары (1 пебит) и 2 битов классической информации можно манипулировать кубитом (телепортировать его). Из четвертого неравенства следует, что 2 бита классической информации можно передать, имея перепутанную пару и посылая ее половинку, представленную кубитом (плотная кодировка). Последние два утверждения нужно воспринимать осторожно, поскольку, как неоднократно показывалось в предыдущих лекциях, половинка перепутанной пары не является в буквальном смысле кубитом – состояние каждой из частиц, составляющих максимально перепутанную пару – полностью смешанное: Напомню также, что пебиты относятся к непрямыми ресурсам, которые распределены симметрично между двумя удаленными пользователями, в то время как кубиты и биты относятся к прямым ресурсам. Их можно посылать в определенном направлении – от источника к приемнику.

Протокол плотной кодировки основан на следующем факте(см. Рис.2). Четыре взаимно ортогональных состояния Белла могут преобразовываться друг в друга путем выполнения операций над отдельными кубитами. Имея, скажем, состояние $\Phi^+ = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$, можно получить три оставшихся состояния Белла, выполняя операции $\{I, X, Y, Z\}$ только в канале Алисы (см.Лекцию 7) или Боба по отдельности.

Напоминание из Л7.

Основные квантовые операции над кубитами:

1. Тождественное преобразование.

$$I \equiv |0\rangle\langle 0| + |1\rangle\langle 1| \qquad \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad (14.1)$$

Действительно, $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} \to \begin{pmatrix} 0 \\ 1 \end{pmatrix}$,

$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} \to \begin{pmatrix} 1 \\ 0 \end{pmatrix}$.

2. Унилатеральный поворот Паули на π вокруг оси X (оптический эквивалент – пластинка $\delta = \pi/2, \chi = 45^0$. ЛЭ «НЕ»

$$X \equiv |0\rangle\langle 1| + |1\rangle\langle 0| \qquad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad (14.2)$$

Действительно, $\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}0\\ 1\end{pmatrix}\to\begin{pmatrix}1\\ 0\end{pmatrix}$,

$\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1\\ 0\end{pmatrix}\to\begin{pmatrix}0\\ 1\end{pmatrix}$.

3. Унилатеральный поворот Паули на π вокруг оси Z (оптический эквивалент – пластинка $\delta=\pi/2,\chi=0^0$. Зависимый от состояния фазовый сдвиг, отличающийся на π для $|0\rangle$ и $|1\rangle$. (Преобразует $|\Phi^+\rangle$ в $|\Phi^-\rangle$)

$$Z\equiv P(\pi) \qquad \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}, \qquad (14.3)$$

где $P(\theta)=\begin{pmatrix}1 & 0\\ 0 & e^{i\theta}\end{pmatrix}$ описывает действие фазовращателя.

Действительно, $\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}\begin{pmatrix}0\\ 1\end{pmatrix}\to\begin{pmatrix}0\\ -1\end{pmatrix}$,

$\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}\begin{pmatrix}1\\ 0\end{pmatrix}\to\begin{pmatrix}1\\ 0\end{pmatrix}$.

4. Унилатеральный поворот Паули на π вокруг оси Y

$$Y\equiv XZ \qquad \begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix} \qquad (14.4)$$

Действительно, $\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}\begin{pmatrix}0\\ 1\end{pmatrix}\to\begin{pmatrix}-1\\ 0\end{pmatrix}$,

$\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1\\ 0\end{pmatrix}\to\begin{pmatrix}0\\ 1\end{pmatrix}$.

5. Логическая операция Адамара. Оптический эквивалент – пластинка $\delta=\pi/2,\chi=22.5^0$

$$H\equiv\frac{1}{\sqrt{2}}\left[\left(|0\rangle+|1\rangle\right)\langle 0|+\left(|0\rangle-|1\rangle\right)\langle 1|\right] \qquad \begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} \qquad (14.5)$$

Поскольку существует только четыре возможности – по числу состояний Белла, то выбор операции, выполняемой Алисой, закодирован в двух битах классической информации. Причем, поскольку кодировка происходит на двухчастичных состояниях (Белла) *два бита классической информации кодируются двумя частицами*. После преобразования половинки ЭПР пары она посылает свой (преобразованный) кубит Бобу, а тот должен понять, какое из состояний Белла представлено этим кубитом. Для этого требуется произвести измерение состояния Белла (ИСБ).

Рассмотрим поэтапно работу протокола плотной кодировки.

1. Алиса (индекс “A”) и Боб (индекс “B”) получают распределенную между ними пару максимально перепутанных частиц в состоянии Белла $|\Phi^+\rangle$.

Замечание. Выбор исходного состояния Белла – произволен. В оригинальной версии Беннета и Визнера использовалось состояние $|\Psi^-\rangle$

2. Алиса выполняет одно из унитарных преобразований $\{I, X, Y, Z\}$ над своей частицей. Будем обозначать ее индексом "*Al*".
3. Алиса посылает преобразованную частицу Бобу.
4. Боб выполняет ИСБ. Результат – четыре числа – по числу состояний Белла.

Рассмотрим возможные исходы измерений Боба.

I. ИСБ дает $\left|\Phi^+\right\rangle_{Al,B} \to \left|0\right\rangle_{Al}\left|0\right\rangle_B + \left|1\right\rangle_{Al}\left|1\right\rangle_B$. Тогда, зная, что начальное состояние было $\left|\Phi^+\right\rangle_{A,B}$, Боб делает вывод, что Алиса выполнила тождественное преобразование над своей частицей, т.е. ничего с ней не сделала:

$\left|0\right\rangle_A \xrightarrow{I} \left|0\right\rangle_{Al}$, $\left|1\right\rangle_A \xrightarrow{I} \left|1\right\rangle_{Al}$

Пусть это соответствует передачи кода «0».

II. ИСБ дает $\left|\Psi^+\right\rangle_{Al,B} \to \left|0\right\rangle_{Al}\left|1\right\rangle_B + \left|1\right\rangle_{Al}\left|0\right\rangle_B$. Тогда, зная, что начальное состояние было $\left|\Phi^+\right\rangle_{A,B}$, Боб делает вывод, что Алиса выполнила операцию «NOT» или X: $\left|0\right\rangle_A \xrightarrow{X} \left|1\right\rangle_{Al}$, $\left|1\right\rangle_A \xrightarrow{X} \left|0\right\rangle_{Al}$.

Пусть это соответствует передачи кода «1».

III. ИСБ дает $\left|\Phi^-\right\rangle_{Al,B} \to \left|0\right\rangle_{Al}\left|0\right\rangle_B - \left|1\right\rangle_{Al}\left|1\right\rangle_B$. Тогда, зная, что начальное состояние было $\left|\Phi^+\right\rangle_{A,B}$, Боб делает вывод, что Алиса выполнила операцию Z: $\left|0\right\rangle_A \xrightarrow{Z} \left|0\right\rangle_{Al}$, $\left|1\right\rangle_A \xrightarrow{Z} \left|-1\right\rangle_{Al}$.

Пусть это соответствует передачи кода «2».

IV. ИСБ дает $\left|\Psi^-\right\rangle_{Al,B} \to \left|0\right\rangle_{Al}\left|1\right\rangle_B - \left|1\right\rangle_{Al}\left|0\right\rangle_B$. Тогда, зная, что начальное состояние было $\left|\Phi^+\right\rangle_{A,B}$, Боб делает вывод, что Алиса выполнила операцию Y: $\left|0\right\rangle_A \xrightarrow{Z} \left|-1\right\rangle_{Al}$, $\left|1\right\rangle_A \xrightarrow{Z} \left|0\right\rangle_{Al}$.

Пусть это соответствует передачи кода «3».

Протокол завершен. Боб получает информацию о четырех числах (2 бита классической информации), закодированных в состояниях Белла. При этом он принимает одну частицу, имеющую лишь два состояния $\left|0\right\rangle_{Al}, \left|1\right\rangle_{Al}$, т.е. 1 бит. Такая схема увеличивает информационную плотность канала передачи с одного до двух битов.

Казалось бы, что в рассмотренном протоколе нет прямого выигрыша в соотношении между используемым количеством ресурсов (две частицы) и количеством передаваемой информации (2 бит) – итого – 1 бит на частицу! Можно было просто закодировать каждый бит одной частицей и передать их непосредственно от Алисы к Бобу.

Однако, использование перепутанных состояний имеет одно преимущество. А именно, если перепутанное состояние распределено между пользователями (Алисой и Бобом) заранее, т.е. до отправки основного сообщения, то само сообщение может быть послано в виде одной частице позже – в удобное для передачи время.

Принято считать, что соответствующий эксперимент выполнен группой А.Цайлингера в 1996 г. В этом эксперименте использовалось поляризационно-

угловое перепутывание, которое получается при неколлинеарном частотно-вырожденном синхронизме типа II. Исходным являлось состояние $\left|\Psi^{+}\right\rangle_{A,B}$. Схема эксперимента (Рис.3) повторяет схему протокола (Рис.2). Однако анализ показывает, что в этом эксперименте имеется ряд «непонятных» моментов. Например, выполнение четырех операций $\{I, X, Y, Z\}$ - см. таблицу на Рис.4 - (кодирование двух битов классической информации) производится с помощью полу- и четвертьволновой пластинок, хотя из (7.1-7.4) следует, что это должны быть две полуволновых пластинки с соответствующими ориентациями. В частности, унитарное преобразование, которое «получено» в эксперименте, достигается действием обеих пластинок, выставленных под нулевым углом. Нетрудно показать, что действие пластинок сводится в этом случаю к преобразованию:

$$\delta = \frac{\pi}{2},\ \chi = 0 \to t = i;\ r = 0 \to D_{\lambda/2,0} = i\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

$$\delta = \frac{\pi}{4},\ \chi = 0 \to t = \frac{1}{\sqrt{2}}(1+i);\ r = 0 \to D_{\lambda/4,0} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1+i & 0 \\ 0 & 1-i \end{pmatrix},$$

$$D_{\lambda/4,0} \times D_{\lambda/2,0}\begin{pmatrix} a \\ b \end{pmatrix} \to \frac{i}{\sqrt{2}}\begin{pmatrix} a(1+i) \\ b(i-1) \end{pmatrix} \neq \begin{pmatrix} a \\ b \end{pmatrix}.$$

Кроме того, использовавшийся анализатор состояний Белла в принципе не позволяет измерить все четыре состояния Белла в силу линейности. В данном эксперименте различались лишь два состояния Белла: $\left|\Psi^{+}\right\rangle_{Al,B}$ и $\left|\Psi^{-}\right\rangle_{Al,B}$(более подробно об этом недостатке будет говориться при анализе схем по квантовой телепортации поляризационных состояний). Самый простой способ, позволяющий различить еще одно состояния Белла - в данном случае, это $\left|\Phi^{-}\right\rangle_{Al,B}$ - использовать дополнительный неполяризационный светоделитель вместо одного из четырех детекторов $D_{H..V'}$, что и было сделано в работе. Авторы наблюдали увеличение числа совпадений между детекторами $D_{H1}D_{H2}$, когда разность длин плеч в интерферометра Оу-Хонга-Манделя меньше длины когерентности бифотонного поля, которая определяется обратной шириной спектра (см.Лекцию 12). При этом, конечно, половина бифотонов все же попадает на каждый из детекторов D_{H1} или D_{H2}, поскольку состояния типа $\left|HH\right\rangle = \left|2,0\right\rangle$ и $\left|VV\right\rangle = \left|0,2\right\rangle$ нельзя однозначно зарегистрировать однофотонными детекторами.

Таким образом, в работе, в принципе, продемонстрирована возможность различения трех белловских состояний. Это дало возможность осуществить кодировку в тритах – когда информация определяется в терминах трех базисных состояний.

Напоминание из Лекции 2.

По Шеннону, информационная энтропия определяется как

$$H \equiv -\sum_i p_i \ln p_i = -\left\langle \ln p_i \right\rangle.,\qquad (14.6)$$

где p – функция распределения дискретной величины (у нас – вероятность найти двухчастичное состояние в одном из трех белловских состояний).

В квантовом случае (7.6) сводится к

$$H \equiv -\left\langle \ln p_i \right\rangle_\rho = -Sp\left(\rho \ln p_i\right). \qquad (14.7)$$

В (14.6) используется натуральный логарифм. Поэтому соответствующую энтропию (информацию) измеряют в «натах». Можно перейти к логарифму по другому, более удобному, основанию. Если M – любое число, то

$$M = 2^{\ln M} = 2^{\log_2 M} = 3^{\log_3 M} \to 2^{H_{bit}} = 3^{H_{trit}} \to$$

$$H_{bit} = \frac{H_{trit}}{\log_3 2} = \frac{H_{trit}}{0.631} = 1.58 H_{trit} \qquad (14.8)$$

В рассмотренном эксперименте, таким образом, удалось повысить информационную емкость канала в 1.58 раз по сравнению со случаем, когда сообщение кодируется в двоичной системе (информация измеряется в битах). Если бы удалось различить все четыре состояния Белла, то в соответствии с

$$H_{bit} = \frac{H_{quart}}{\log_4 2} = \frac{H_{trit}}{0.5} = 2H_{trit} \qquad (14.9)$$

емкость увеличилась в 2 раза, как и должно быть при плотной кодировке кубитов.

Замечание.

Измерить состояния Белла можно, например, применив к перепутанной паре операцию XOR, и измерив затем бит-мишень, что позволит отличить состояния $\Phi^{\pm} = \frac{1}{\sqrt{2}}\left(\left|00\right\rangle \pm \left|11\right\rangle\right)$ от состояний $\Psi^{\pm} = \frac{1}{\sqrt{2}}\left(\left|01\right\rangle \pm \left|10\right\rangle\right)$. Для определения знака в суперпозиции, Боб должен использовать преобразование Адамара над оставшимся кубитом, а затем, измерить его. Другим способом измерения состояний Белла в оптических процессах является применение преобразований частоты вверх (up-conversion). Этот метод также будет обсуждаться в лекции, посвященной телепортации.

ЛИТЕРАТУРА.

1. Ch.H.Bennet, S.J.Wiesner. Communication via One- and Two-Particle Operators on Einstein-Podolsky-Rosen States. Phys.Rev.Lett., 69, 2881 (1992).
2. K.Mattle, H.Weinfurter, P.Kwiat, and A.Zeilinger. Dense Coding in Experimental Quantum Communication. Phys.Rev.Lett., 76, 4656 (1996).
3. Ch.Bennet. Quantum Information and Computation. Physics Today, October 24 (1995).
4. A.Steane. Quantum Computing. ph\9708022.

ЛЕКЦИЯ 15. **КВАНТОВАЯ ТЕЛЕПОРТАЦИЯ КУБИТОВ.**

1. Копирование и передача квантовых состояний. Протокол квантовой телепортации. Требования, предъявляемые к нему: не нарушение теоремы о запрете клонирования; наличие неизвестного входного состояния; идентичность выходного состояния входному; отсутствие сверхсветовых сигналов; полное измерение оператора Белла.
2. Обзор некоторых экспериментальных результатов по квантовой телепортации. Эксперименты группы А.Цайлингера; группы Ф.де-Мартини; группы Дж.Кимбла.
3. Полное измерение состояний Белла. Эксперимент группы Я.Ши.
4. “No-Go” - теорема. Ее доказательство по Л.Вайдману. Телепортация при наличии взаимодействия между квантовыми системами. Операция “CNOT” как пример таких взаимодействий.
5. Телепортация состояний, описываемых непрерывными переменными (дополн.)

“ …телепортация - это мгновенная транспортировка кого-(чего) либо в пространстве посредством передовых технологий”
Teleportation is “.. apparently instanteneous transportation of persons etc., across space by advanced technological means”
The Oxford English Dictionary, 2nd edition (Clarendon Press, Oxford, 1989), vol.XVII, p.730)

*Будем различать два термина: **копирование** неизвестного квантового состояния и **передача** квантового состояния. Первый процесс запрещен соответствующе теоремой (см.Лекции 5 и 6). Во втором квантовое состояние уничтожается в одной пространственно-временной точке и появляется в другой точке. Тривиальной реализацией его служит передача состояния по каналу связи. Изощренной реализацией является квантовая телепортация.*

1. Протокол квантовой телепортации

Под протоколом мы будем понимать последовательность манипуляций, приводящих к решению данной задачи. Итак, протокол квантовой телепортации содержит четыре основных группы операций.

1. *Приготовление начального состояния частицы “1”. Это состояние представляет собой суперпозицию двух базисных (булевых) состояний*
$$\Psi_1 = \alpha\left|0_1\right\rangle + \beta\left|1_1\right\rangle, \qquad (15.1)$$
где комплексные амплитуды α *и* β *связаны условием нормировки* $\left|\alpha\right|^2 + \left|\beta\right|^2 = 1$.
2. *Приготовление состояния Белла двух частиц частиц “2” и “3”. В оригинальной работе использовалось синглетное состояние*
$$\left|\Psi_{23}\right\rangle = \frac{1}{\sqrt{2}}\left\{\left|0_2\right\rangle\left|1_3\right\rangle - \left|1_2\right\rangle\left|0_3\right\rangle\right\}. \qquad (15.2)$$
3. *Измерение состояний Белла двух частиц “1” и “2”. Другими словами совместное состояние двух частиц “1” и “2” проектируется в базис состояний Белла* $\left|\Psi_{12}^{(-)}\right\rangle, \left|\Psi_{12}^{(+)}\right\rangle, \left|\Phi_{12}^{(-)}\right\rangle, \left|\Phi_{12}^{(+)}\right\rangle$.

4. *Передача (сообщение) результата измерений (2 бита классической информации) по классическому каналу.*
5. *Выполнение трех унитарных преобразований над частицей "3" в соответствии с полученным сообщением*[1].

Традиционно принято считать, что третья группа операций выполняется участником протокола с именем Алиса, а четвертая - Бобом[2] (Рис.1) Всю схему квантовой телепортации можно представить в виде двух станций - станции Алисы и станции Боба. Первая имеет два входа и один выход. На первый вход поступает частица "1" в состоянии (1, а на другой - половина перепутанной пары - частица "2". Выход Алисы подключен к классическому каналу связи, по которому передается четыре возможных исхода измерения состояний Белла, т.е. 2 бита классической информации. Станция Боба также имеет два входа и один выход. На первый вход поступает информация, переданная Алисой по классическому каналу, а на второй - другая половинка перепутанной пары - частица "3". После выполнения Бобом трех унитарных преобразований частица "3" в скорректированном состоянии поступает на выход. При этом, как будет показано ниже, состояние частицы "3" на выходе станции Боба тождественно (является точной копией) неизвестного состояния частицы "1" - протокол КТ завершается.

Математически протокол КТ описывается предельно просто. Рассмотрим совместное состояние трех частиц до того как две из них попали к Алисе:

$$\left|\Psi_{123}\right\rangle = \left|\Psi_1\right\rangle \otimes \left|\Psi_{23}\right\rangle =$$
$$= \frac{\alpha}{\sqrt{2}}\left\{\left|0_1\right\rangle\left|0_2\right\rangle\left|1_3\right\rangle - \left|0_1\right\rangle\left|1_2\right\rangle\left|0_3\right\rangle\right\} + \frac{\beta}{\sqrt{2}}\left\{\left|1_1\right\rangle\left|0_2\right\rangle\left|1_3\right\rangle - \left|1_1\right\rangle\left|1_2\right\rangle\left|0_3\right\rangle\right\}. \qquad (15.3)$$

Прямые произведения состояний $\left|\times_1\right\rangle\left|\times_2\right\rangle$ теперь выразим в терминах четырех состояний Белла $\left|\Psi_{12}^{(-)}\right\rangle, \left|\Psi_{12}^{(+)}\right\rangle, \left|\Phi_{12}^{(-)}\right\rangle, \left|\Phi_{12}^{(+)}\right\rangle$:

$$\left|\Psi_{123}\right\rangle = \frac{1}{2}[\left|\Psi_{12}^{(-)}\right\rangle\left(-\alpha\left|0_3\right\rangle - \beta\left|1_3\right\rangle\right) + \left|\Psi_{12}^{(+)}\right\rangle\left(-\alpha\left|0_3\right\rangle + \beta\left|1_3\right\rangle\right) +$$
$$+ \left|\Phi_{12}^{(-)}\right\rangle\left(\alpha\left|1_3\right\rangle + \beta\left|0_3\right\rangle\right) + \left|\Phi_{12}^{(+)}\right\rangle\left(\alpha\left|1_3\right\rangle - \beta\left|0_3\right\rangle\right)]. \qquad (15.4)$$

Видно, что общее состояние трех частиц представляется суммой четырех слагаемых, каждое из которых факторизовано в отношении состояния Белла частиц "1" и "2" и состояния третьей частицы. Вероятность измерения того или иного состояния Белла из (4) равна $1/4$. Таким образом после измерения Алисы частица "3", находящаяся в станции Боба, окажется спроектированной на одно из четырех состояний, фигурирующих в (4). Эти состояния можно записать в виде:

$$-\left|\Psi_3\right\rangle \equiv -\begin{pmatrix}\alpha\\ \beta\end{pmatrix} = -I\begin{pmatrix}\alpha\\ \beta\end{pmatrix}, \quad -Z\left|\Psi_3\right\rangle = \begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix}\begin{pmatrix}-\alpha\\ \beta\end{pmatrix} = \begin{pmatrix}\alpha\\ \beta\end{pmatrix}, \qquad (15.5)$$

---

[1] Пятая группа операций - выполнение унитарных преобразований - считается тривиальной. В случае поляризационных состояний света, использованных в эти преобразования состоят в повороте двух или одной полуволновых пластин на разные углы.

[2] Иногда присутствует и третий участник - с именем Виктор, сверяющий конечное и исходное состояния, и без имени - "ассистент", помогающий Алисе приготовить ее состояние.

$$X\,|\Psi_3\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} \beta \\ \alpha \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}, \quad -Y\,|\Psi_3\rangle = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} -\beta \\ \alpha \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}.$$

Каждое из этих четырех возможных состояний частицы “3” связано линейным преобразованием с состоянием исходной частицы “1”. Поэтому, получив информацию от Алисы, какое именно состояние Белла в данный момент она измерила (с вероятностью 1/4), Боб должен выполнить это преобразование, получив в итоге исходное. Причем, в одном из четырех случаев, как видно из (5), Бобу вообще не нужно ничего делать со своей частицей. Мы рассмотрим эти преобразования при описании конкретного эксперимента. Таким образом, становится понятно, что в результате КТ происходит расщепление информации о состоянии частицы “1”. Одна часть этой информации - результат измерения Алисы совместного состояния частиц “1” и “2” - передается по классическому каналу связи. Попросту говоря это одно из четырех возможных закодированных сообщения, например, в цвете четырех ламп. Каждому состоянию Белла приписывается лампа определенного цвета, которые вспыхивают всякий раз, когда измеряется данное состояние. Боб, увидев вспышку определенного цвета (или получив эту информацию по телефону) выполняет соответствующее преобразование над своей частицей”3”, тем самым корректируя ее состояние. Подчеркнем, что эти преобразования являются унитарными, т.е. сохраняющими энергию - число частиц в протоколе КТ остается неизменным.

Другая часть информации - квантовая. Она заложена в полных корреляциях, существующих между частицами “2” и “3”, иными словами в состоянии Белла, которое используется во второй группе операция протокола (см. выше). Обратим внимание на некоторые особенности этого протокола.

- Сформулированное выше требование о запрете клонирования неизвестного состояния выполняется. Исходное состояние, записанное на частице “1” *уничтожается* в результате измерения совместного состояния Белла частиц “1” и “2”.
- Ни Алиса, ни Боб *ничего не знают* об исходном состоянии, поскольку владеют только частью полной информации - той, которая передается по классическому каналу.
- На выходе станции Боба создается, в принципе, *точная копия* исходного состояния. Причем состояние это по-прежнему неизвестное.
- Копирование происходит *не мгновенно*, а по крайней мере, спустя время, которое нужно затратить на передачу классического сообщения от Алисы к Бобу.

2. Обзор некоторых экспериментальных результатов по квантовой телепортации

Рассмотрим кратко три эксперимента, демонстрирующие эффект КТ.

1. В работе группы А.Цайлингера входным состоянием являлось поляризационное состояние одного из двух коррелированных фотонов, рождающихся в результате СПР. Две пары коррелированных фотонов возбуждалось при двукратном прохождении фемтосекундного лазерного импульса через нелинейный кристалл. Один фотон, таким образом оказывался дополнительным - его использовали как “триггер”, присутствие которого указывало на наличие второй пары. Пары

приготавливались в состоянии Белла $\left|\Psi_{23}^{(-)}\right\rangle$. Фотон из первой пары (после первого прохода лазерного импульса) смешивался на неполяризационном светоделителе с одним из фотонов другой пары. При точном совпадении оптических путей этих фотонов, в совпадениях отсчетов детекторов, стоящих в выходных модах светоделителя наблюдается эффект антикорреляции. В этом случае исчезают совпадения между детекторами. Ни исходное состояние телепортируемого фотона, ни состояние той половинки перепутанной пары, с которой он смешивается на светоделителе не имеют определенного поляризационного состояния. Следовательно, эффект антикорреляции будет иметь место в s случаях от общего числа испытаний. Именно такому числу исходов отвечают события, при которых поляризации фотона “1” и фотона “2” совпадают (обе - либо вертикальные, либо горизонтальные, в соответствующем базисе). В остальных случаях совпадения будут происходить, поскольку при ортогональных поляризациях эффекта антикорреляции нет. Поскольку состояние Белла фотонов “2” и “3” - синглетное, то каждый раз совпадение отсчетов двух детекторов, стоящих позади светоделителя (отсутствие эффекта антикорреляции) сопровождается копированием поляризации исходного фотона “1”. Действительно, всегда $\vec{e}_2 \perp \vec{e}_3$, в силу выбора состояния Белла. В то же время, при отсутствии эффекта антикорреляции $\vec{e}_1 \perp \vec{e}_2$, следовательно $\vec{e}_1 \square \vec{e}_3$. Ясно, что “чистота” копирования составляет лишь 25% - по вероятности измерения синглетного состоянния Белла с помощью светоделителя. В остальных случаях копирование не происходит - через станцию Боба пролетают “лишние” фотоны. Такой результат связан со спецификой использованного в этой работе измерения состояния Белла. Д.Н.Клышко предложил убрать такие фотоны введением затвора, срабатывающего только при поступлении импульса совпадения от станции Алисы. Таким образом полное копирование поляризационного состояния в обсуждаемой схеме возможно только при помощи неунитарной операции - поглощении “лишних” фотонов. В той же работе рассматривается способ увеличения благоприятных исходов копирования до 50%.

2. Другая работа была выполнена группой Де-Мартини из Рима. Суть ее сводится к предложенной С.Попеску идее двучастичной (вместо трехчастичной) телепортации. В целом два этих протокола совпадают, однако в варианте Попеску, входное состояние отсутствует. Вместо этого предлагается использовать какую-нибудь степень свободы одной из частиц перепутанной пары, которая не задействована в перепутывании. В эксперименте, сначала получаются фотоны, перепутанные по направлению распространения, т.е. по импульсам. Далее в протоколе появляется “ассистент”, помогающий Алисе закодировать состояние прямо в ее компоненте синглетной пары, вместо того, чтобы кодировать его в третьей частице. Конкретно, “ассистент” преобразует состояние с определенной поляризацией в суперпозицию $\Psi_2 = \alpha\left|H\right\rangle + \beta\left|V\right\rangle$. В такой двух-частичной схеме действия Алисы проще, чем в трех-частичной схеме. Это связано с тем, что заставить взаимодействовать разные степени свободы одной частицы проще, чем заставить взаимодействовать две разные частицы. В отличие от случая трех-частичного протокола, проектирование частицы “1” (т.е. бывшей частицы “2”) в базис состояний Белла не представляет серьезной проблемы и может быть выполнено со 100%-ой эффективностью. Для выполнения операция

проектирования необходимо перепутать поляризационные и импульсные свойства фотона “1”. Это делается с помощью светоделителей. Серьезным недостатком обсуждаемой схемы является то, что в ней отсутствует входное состояние - скорее такая схема годится для демонстрации, чем для сколько-нибудь реального использования. Так, что вряд ли такой протокол найдет применение в дальнейшем. Кроме того, в нем невозможно использовать в качестве входного состояния компоненту перепутанного состояния.

3. В третьем эксперименте была реализована схема КТ, предложенной Л.Вайдманом и разработанная, впоследствии, С.Брауштейном и Дж.Кимблом. Здесь используется перепутывание между координатой и импульсом. В этом варианте квантовой телепортации координата и импульс, определяющие *внешнее состояние* квантовой системы, передаются к другой - удаленной - квантовой системе. В схемах, обсуждаемых выше, передавалось *внутреннее состояние*, т.е. поляризация. Важное отличие между координатой и импульсом, с одной стороны и поляризации - с другой, заключается в том, что они имеют разные базисные представления. Для описания координаты и импульса требуется бесконечное число базисных состояний, т.к. любым двум различным координатам и импульсам отвечают два разных ортогональных собственных состояния. Действительно, собственные состояния координаты и собственные состояния импульса образуют бесконечномерное гильбертово пространство. В эксперименте реально были задействованы не координата *x* и импульс *p* частиц, а пучки света, которые характеризовались параметрами, удовлетворяющими таким же коммутационным соотношениям, как и $\hat{x}$ и $\hat{p}$. Аналогия основана на том факте, что одна (поперечная) мода квантованного поля излучения описывается так же, как и гармонический осциллятор (см. Лекцию 11). Оператор электрического поля можно переписать в терминах $\hat{X}$ и $\hat{P}$:

$$\hat{E}(t) = E_0\left(\hat{X}\cos(\omega t) + \hat{P}\sin(\omega t)\right). \qquad (15.6)$$

Собственные значения $\hat{X}$ и $\hat{P}$, называются квадратурными амплитудами поля и являются аналогами координаты и импульса. Хотя авторам этой работы и удалось выполнить измерения состояний Белла, все же качество копированного состояния оказалось довольно низким - около 58%, и то в предположении, что конечное состояние принадлежит определенному классу - классу когерентных состояний.

3. Полное измерение состояний Белла. Эксперимент группы Я.Ши.

Пусть, по прежнему, неизвестное квантовое состояние задается суперпозицией (1). Предположим, что состояние Белла, необходимое для выполнения протокола представляется в виде

$$\left|\Phi_{23}\right\rangle = \frac{1}{\sqrt{2}}\left\{\left|0_2 0_3\right\rangle - \left|1_2 1_3\right\rangle\right\}. \qquad (15.7)$$

Именно такое состояние реализуется при наложении двух пучков бифотонов типа I на выходе интерферометра Маха-Цандера, когда относительная фазовая задержка равна $\varphi = \pi$. Символами “0” и “1” закодированы две базисные поляризации, H и V,

соответственно. Следуя логике оригинальной работы Беннета и соавторов, перепишем совместное состояние трех частиц до измерения в станции Алисы:

$$\left|\Psi_{123}\right\rangle = \frac{\alpha}{\sqrt{2}}\left\{\left|0_1\right\rangle\left|0_2\right\rangle\left|0_3\right\rangle - \left|0_1\right\rangle\left|1_2\right\rangle\left|1_3\right\rangle\right\} + \frac{\beta}{\sqrt{2}}\left\{\left|1_1\right\rangle\left|0_2\right\rangle\left|0_3\right\rangle - \left|1_1\right\rangle\left|1_2\right\rangle\left|1_3\right\rangle\right\}. \quad (15.8)$$

Раскладывая (8) в базисе состояний Белла частиц “1” и “2”, перепишем его в виде:

$$\left|\Psi_{123}\right\rangle = \frac{1}{2}[\left|\Psi_{12}^{(-)}\right\rangle\left(-\alpha\left|1_3\right\rangle - \beta\left|0_3\right\rangle\right) + \left|\Psi_{12}^{(+)}\right\rangle\left(-\alpha\left|1_3\right\rangle + \beta\left|0_3\right\rangle\right) +$$

$$+\left|\Phi_{12}^{(-)}\right\rangle\left(\alpha\left|0_3\right\rangle + \beta\left|1_3\right\rangle\right) + \left|\Phi_{12}^{(+)}\right\rangle\left(\alpha\left|0_3\right\rangle - \beta\left|1_3\right\rangle\right)]. \quad (15.9)$$

$$\left|\Psi_{123}\right\rangle = \frac{1}{2}[\left|\Phi_{12}^{(+)}\right\rangle\left(\alpha\left|0_3\right\rangle - \beta\left|1_3\right\rangle\right) + \quad (15.10а)$$

$$+\left|\Phi_{12}^{(-)}\right\rangle\left(\alpha\left|0_3\right\rangle + \beta\left|1_3\right\rangle\right) + \quad (15.10б)$$

$$+\left|\Psi_{12}^{(+)}\right\rangle\left(-\alpha\left|1_3\right\rangle + \beta\left|0_3\right\rangle\right) + \quad (15.10в)$$

$$+\left|\Psi_{12}^{(-)}\right\rangle\left(-\alpha\left|1_3\right\rangle - \beta\left|0_3\right\rangle\right) + \quad (15.10г)$$

Функциональная схема эксперимента демонстрируется на рис.2. Не уточняя пока детали экспериментальной реализации, предположим, что пары фотонов “1” и “2” могут взаимодействовать друг с другом в четырех нелинейных кристаллах. Вспомним, что поляризационное состояние фотона “1” - не определено. В нем может быть представлена как вертикальная компонента (с вероятностью $\left|\alpha\right|^2$), так и горизонтальная (с вероятностью $\left|\beta\right|^2$). Не определено также и состояние фотона “2”, как компоненты перепутанного состояния (7). Поэтому четыре кристалла нужны для создания полной суперпозиции из четырех комбинаций двух независимых ортогональных поляризаций H и V: $\left|H_1H_2\right\rangle$, $\left|H_1V_2\right\rangle$, $\left|V_1H_2\right\rangle$ и $\left|V_1V_2\right\rangle$.

Математически измерение состояний Белла сводится к следующим процедурам.

Рассмотрим, например, процесс, при котором поляризации фотонов “1” и “2” одинаковы. Такой нелинейный процесс, когда во входных модах поля присутствует излучение одинаковой поляризации, а на выходе - излучение с ортогональной поляризацией представляет собой генерацию суммарной частоты с синхронизмом типа I. При этом оказываются задействованы первое и четвертое слагаемые в (8). В результате такого преобразования возникает фотон с суммарной частотой, который мы обозначим индексом “4”:

$\left|1_11_2\right\rangle \rightarrow \left|H_4\right\rangle$ - в первом кристалле (тип I) и (15.11)

$\left|0_10_2\right\rangle \rightarrow \left|V_4\right\rangle$ - во втором кристалле (тип I). (15.12)

Ясно, что для этого нужно использовать два одинаковых кристалла, ориентированных во взаимно ортогональных направлениях.

Подставляя (11) и (12) в состояние (8), получаем:

$$\left|\Psi_{43}\right\rangle = \alpha\left|V_40_3\right\rangle - \beta\left|H_41_3\right\rangle. \quad (15.13)$$

После первых двух кристаллов типа I в схеме присутствует излучение высокочастотное и низкочастотное излучение в обеих поляризациях. Их можно разделить, например. с помощью зеркала, пропускающего низкочастотную

компоненту и отражающего высокочастотную[3]. Попадая на поляризационный светоделитель, ориентированный в 45^0-ом базисе, состояние (13) распределяется между двумя пространственными модами:

$$\left|\Psi_{43}\right\rangle = \frac{1}{\sqrt{2}}\left\{\left|45^0\right\rangle_4\left(\alpha\left|0_3\right\rangle - \beta\left|1_3\right\rangle\right) + \left|135^0\right\rangle\left(\alpha\left|0_3\right\rangle + \beta\left|1_3\right\rangle\right)\right\}, \tag{15.14}$$

где использованы обычные связи между входными и выходными модами (поляризационного) светоделителя:

$$\left|45^0\right\rangle_4 = \frac{1}{\sqrt{2}}\left\{\left|V\right\rangle_4 + \left|H\right\rangle_4\right\} = \frac{1}{\sqrt{2}}\left\{\left|0_1 0_2\right\rangle + \left|1_1 1_2\right\rangle\right\} \equiv \left|\Phi_{12}^{(+)}\right\rangle \text{ и} \tag{15.15}$$

$$\left|135^0\right\rangle_4 = \frac{1}{\sqrt{2}}\left\{\left|V\right\rangle_4 - \left|H\right\rangle_4\right\} = \frac{1}{\sqrt{2}}\left\{\left|0_1 0_2\right\rangle - \left|1_1 1_2\right\rangle\right\} \equiv \left|\Phi_{12}^{(-)}\right\rangle. \tag{15.16}$$

Таким образом, если срабатывает детектор $D_4^I\left(45^0\right)$, это значит, что фотон “3” оказывается в состоянии

$$\left|\Psi_3\right\rangle = \alpha\left|0_3\right\rangle - \beta\left|1_3\right\rangle, \tag{15.17}$$

а если срабатывает детектор $D_4^{II}\left(135^0\right)$, то в состоянии:

$$\left|\Psi_3\right\rangle = \alpha\left|0_3\right\rangle + \beta\left|1_3\right\rangle. \tag{15.18}$$

Следовательно, с помощью двух кристаллов с синхронизмом типа I нам удалось распознать два состояния Белла $\left|\Phi_{12}^{(\pm)}\right\rangle$.

Аналогично рассматривается преобразование состояний при генерации излучения на суммарной частоте с синхронизмом типа II.

$$\left|0_1 1_2\right\rangle \to \left|V_4\right\rangle \text{ - в первом кристалле (тип II) и} \tag{15.19}$$

$$\left|1_1 0_2\right\rangle \to \left|H_4\right\rangle \text{ - во втором кристалле (тип II).} \tag{15.20}$$

Теперь мы будем рассматривать два других слагаемых в сумме (8), которые дают:

$$\left|\Psi_{43}\right\rangle = -\alpha\left|V_4 1_3\right\rangle + \beta\left|H_4 0_3\right\rangle. \tag{15.21}$$

Это состояние, в котором представлены обе поляризационных компоненты в обеих пространственных модах “1” и “4”.

После 45^0-ого поляризационного светоделителя, совместное двухмодовое состояние оказывается:

$$\left|\Psi_{43}\right\rangle = \frac{1}{\sqrt{2}}\left\{\left|45^0\right\rangle_4\left(-\alpha\left|1_3\right\rangle + \beta\left|0_3\right\rangle\right) + \left|135^0\right\rangle\left(-\alpha\left|1_3\right\rangle - \beta\left|0_3\right\rangle\right)\right\}, \tag{15.22}$$

где аналогично предыдущему случаю:

$$\left|45^0\right\rangle_4 = \frac{1}{\sqrt{2}}\left\{\left|V\right\rangle_4 + \left|H\right\rangle_4\right\} = \frac{1}{\sqrt{2}}\left\{\left|0_1 1_2\right\rangle + \left|1_1 0_2\right\rangle\right\} \equiv \left|\Psi_{12}^{(+)}\right\rangle \text{ и} \tag{15.23}$$

$$\left|135^0\right\rangle_4 = \frac{1}{\sqrt{2}}\left\{\left|V\right\rangle_4 - \left|H\right\rangle_4\right\} = \frac{1}{\sqrt{2}}\left\{\left|0_1 1_2\right\rangle - \left|1_1 0_2\right\rangle\right\} \equiv \left|\Psi_{12}^{(-)}\right\rangle. \tag{15.24}$$

Значит, если срабатывает детектор $D_4^{III}\left(45^0\right)$, то фотон “3” оказывается в состоянии

---

[3] Необходимо, чтобы коэффициенты отражения и пропускания не зависели от поляризации.

$$\left|\Psi_3\right\rangle = -\alpha\left|1_3\right\rangle + \beta\left|0_3\right\rangle, \tag{15.25}$$

а если срабатывает детектор $D_4^{IV}\left(135^0\right)$, то в состоянии:

$$\left|\Psi_3\right\rangle = -\alpha\left|1_3\right\rangle - \beta\left|0_3\right\rangle. \tag{15.26}$$

Таким образом, с помощью двух кристаллов с синхронизмом типа II нам удалось распознать два других состояния Белла $\left|\Psi_{12}^{(\pm)}\right\rangle$.

Протокол КТ завершен.

4. Доказательство “No-Go” теоремы.

Измерение состояний Белла проецирует состояния пары двухуровневых систем в ортогональный набор максимально перепутанных состояний (Белла).

Докажем, что ***невозможно выполнить полное измерение невырожденного оператора Белла (состояний Белла) без использования взаимодействий между квантовыми системами.***

Предположим, что над каждой из двух одно-частичной систем можно выполнять ***унитарные преобразования и локальные одночастичные измерения (LOLM)***.

Согласно постулату фон-Неймана, измерительная процедура состоит из двух частей: унитарная линейная эволюция и локальное детектирование.

У нас имеется четыре состояния Белла, которые являются собственными функциями оператора Белла:

$$\left|\Psi^-\right\rangle = \frac{1}{\sqrt{2}}\left(\left|\uparrow\right\rangle_L\left|\downarrow\right\rangle_R - \left|\downarrow\right\rangle_L\left|\uparrow\right\rangle_R\right), \tag{15.27}$$

$$\left|\Psi^+\right\rangle = \frac{1}{\sqrt{2}}\left(\left|\uparrow\right\rangle_L\left|\downarrow\right\rangle_R + \left|\downarrow\right\rangle_L\left|\uparrow\right\rangle_R\right), \tag{15.28}$$

$$\left|\Phi^-\right\rangle = \frac{1}{\sqrt{2}}\left(\left|\uparrow\right\rangle_L\left|\uparrow\right\rangle_R - \left|\downarrow\right\rangle_L\left|\downarrow\right\rangle_R\right), \tag{15.29}$$

$$\left|\Phi^-\right\rangle = \frac{1}{\sqrt{2}}\left(\left|\uparrow\right\rangle_L\left|\uparrow\right\rangle_R - \left|\downarrow\right\rangle_L\left|\downarrow\right\rangle_R\right). \tag{15.30}$$

Мы обозначили символами “L”, “R” левый и правый каналы, соответственно. В общем виде унитарные линейные преобразования, выполняемые над четырьмя состояниями в протоколе КТ имеют вид:

$$\left|\uparrow\right\rangle_L \to \sum_i a_i\left|i\right\rangle, \tag{15.31}$$

$$\left|\downarrow\right\rangle_L \to \sum_i b_i\left|i\right\rangle, \tag{15.32}$$

$$\left|\uparrow\right\rangle_R \to \sum_i c_i\left|i\right\rangle, \tag{15.33}$$

$$\left|\downarrow\right\rangle_R \to \sum_i d_i\left|i\right\rangle. \tag{15.34}$$

Здесь $\left|i\right\rangle$ - набор ортогональных одно-частичных (локальных) состояний. “Линейность” здесь означает, что эволюция частицы в одном канале не зависит от состояния частицы в другом канале. Тогда в результате линейной унитарной эволюции состояния Белла (27-30) приобретают следующий вид:

$$\left|\Psi^-\right\rangle \to \sum_{i,j} \alpha_{i,j} \left|i\right\rangle \left|j\right\rangle, \qquad \left|\Psi^+\right\rangle \to \sum_{i,j} \beta_{i,j} \left|i\right\rangle \left|j\right\rangle, \tag{15.35}$$

$$\left|\Phi^-\right\rangle \to \sum_{i,j} \gamma_{i,j} \left|i\right\rangle \left|j\right\rangle, \qquad \left|\Phi^+\right\rangle \to \sum_{i,j} \delta_{i,j} \left|i\right\rangle \left|j\right\rangle, \tag{15.36}$$

В правых частях преобразований (35,36) стоят суммы по всем различным парам $\{i, j\}$, причем порядок их следования несущественен.

Замечание. Состояния различимых частиц (фермионов) отвечают разным $\left|i\right\rangle$. Если же частицы неразличимы (бозоны), то запись $\left|i\right\rangle \left|j\right\rangle$ просто означает соответствующим образом симметризованные состояния:

$$\left|i\right\rangle \left|j\right\rangle \to \frac{1}{\sqrt{2}} \left(\left|i\right\rangle_1 \left|j\right\rangle_2 \pm \left|j\right\rangle_1 \left|i\right\rangle_2 \right) \tag{15.37}$$

Далее предположим, что у нас в распоряжении имеются лишь локальные детекторы, поэтому могут быть зарегистрированы только произведения состояний $\left|i\right\rangle \left|j\right\rangle$, но не их суперпозиции! Измерение невырожденного оператора Белла означает, что *существует, по крайней мере, один отличный от нуля коэффициент из набора* α_{ij}, β_{ij}, γ_{ij}, δ_{ij}, *а также, что если для определенных* i, j *он не равен нулю, то все остальные принимают нулевые значения*.

Учитывая соображения симметрии для неразличимых частиц, получаем, что для $i = j$ из (31-34, 35,36) возникают связи:

$$\begin{aligned} \alpha_{ii} &= a_i d_i - b_i c_i, \\ \beta_{ii} &= a_i d_i + b_i c_i, \\ \gamma_{ii} &= a_i c_i - b_i d_i, \\ \delta_{ii} &= a_i c_i + b_i d_i. \end{aligned} \tag{15.38}$$

Если же $i \neq j$, то

$$\begin{aligned} \alpha_{ij} &= a_i d_j + a_j d_i - \left(b_i c_j + b_j c_i\right), \\ \beta_{ij} &= a_i d_j + a_j d_i + b_i c_j + b_j c_i, \\ \gamma_{ij} &= a_i c_j + a_j c_i - \left(b_i d_j + b_j d_i\right), \\ \delta_{ij} &= a_i c_j + a_j c_i + b_i d_j + b_j d_i. \end{aligned} \tag{15.39}$$

Соотношения (38, 39) выписаны без учета фактора $1/\sqrt{2}$.

Способность измерения оператора Белла подразумевает, что для любого i по крайней мере три из коэффициентов α_{ii}, β_{ii}, γ_{ii}, δ_{ii} равны нулю. Из (38) следует, что четвертый коэффициент также должен быть равен нулю, и тогда мы получаем:

$$\alpha_{ii},\ \beta_{ii},\ \gamma_{ii},\ \delta_{ii} = 0 \tag{15.40}$$

Следовательно, из уравнений (38):

$$a_i d_i = b_i c_i = a_i c_i = b_i d_i = 0 \tag{15.41}$$

Но тогда, по крайней мере два из четырех коэффициентов равны нулю: либо $a_i = b_i = 0$, либо $c_i = d_i = 0$.

Теперь, предположим, что $\alpha_{ij} \neq 0$ (и, следовательно, $\beta_{ij} = \gamma_{ij} = \delta_{ij} = 0$) и, что $a_i = b_i = 0$.Тогда уравнения (39) приобретают вид:

$$\begin{aligned} \alpha_{ij} &= a_j d_i - b_j c_i \neq 0, \\ \beta_{ij} &= a_j d_i + b_j c_i = 0, \\ \gamma_{ij} &= a_j c_i - b_j d_i = 0, \\ \delta_{ij} &= a_j c_i + b_j d_i = 0. \end{aligned} \tag{15.42}$$

Эти уравнения не имеют решений. Нетрудно убедиться, что и во всех других случаях решений нет, что и доказывает исходное утверждение.

Однако, для бозонов можно измерить вырожденный оператор Белла, например, который различает лишь два состояния Белла. Когда мы рассматриваем вырожденный оператор Белла, утверждение, что по крайней мере три из четырех коэффициентов α_{ii}, β_{ii}, γ_{ii}, δ_{ii} равны нулю, уже неверно. Частные решения позволяют различить два из четырех состояний Белла. Такой алгоритм измерения (вырожденных) состояний Белла был реализован в экспериментах группы А.Цайлингера по плотной кодировке и квантовой телепортации (Рис.3). Светоделитель BS осуществляет преобразования, которые приводят к связям между входными $\left(|\uparrow\rangle \equiv |H\rangle,\ |\downarrow\rangle \equiv |V\rangle\right)$ и выходными $\left(|1\rangle \equiv |H\rangle_L,\ |2\rangle \equiv |V\rangle_L,\ |3\rangle \equiv |H\rangle_R, |4\rangle \equiv |V\rangle_R\right)$ одночастичными состояниями:

$$\begin{aligned} |\uparrow\rangle_L &\to \frac{1}{\sqrt{2}}\left(|1\rangle + |3\rangle\right), \\ |\downarrow\rangle_L &\to \frac{1}{\sqrt{2}}\left(|2\rangle + |4\rangle\right), \\ |\uparrow\rangle_R &\to \frac{1}{\sqrt{2}}\left(|1\rangle - |3\rangle\right), \\ |\downarrow\rangle_L &\to \frac{1}{\sqrt{2}}\left(|2\rangle + |4\rangle\right), \end{aligned} \tag{15.43}$$

Поляризационные светоделители PBS пропускают горизонтальную поляризацию и отражают вертикальную. В этой схеме каждый детектор D_i регистрирует состояние $|i\rangle$. На выходы $(2,3)$ и $(1,4)$ поступает состояние $|\Psi^-\rangle$, в то время как на выходы $(1,1)$, $(2,2)$, $(3,3)$ и $(4,4)$ поступают как состояние $|\Phi^-\rangle$, так и $|\Phi^+\rangle$, которые в такой схеме не различаются (см. лекцию 14).

Состояния Белла с помощью (43) преобразуются к виду:

$$\begin{aligned}
&\left|\Psi^-\right\rangle \to \frac{1}{\sqrt{2}}\left(|2\rangle|3\rangle - |1\rangle|4\rangle\right),\\
&\left|\Psi^+\right\rangle \to \frac{1}{\sqrt{2}}\left(|1\rangle|2\rangle - |3\rangle|4\rangle\right),\\
&\left|\Phi^-\right\rangle \to \frac{1}{2}\left(|1\rangle|1\rangle - |3\rangle|3\rangle - |2\rangle|2\rangle + |4\rangle|4\rangle\right),\\
&\left|\Phi^+\right\rangle \to \frac{1}{2}\left(|1\rangle|1\rangle - |3\rangle|3\rangle + |2\rangle|2\rangle - |4\rangle|4\rangle\right).
\end{aligned} \qquad (15.44)$$

Рассмотрим, например, первое преобразование в (44):

$$\left|\Psi^-\right\rangle = \frac{1}{\sqrt{2}}\left[|H\rangle_L |V\rangle_R - |V\rangle_L |H\rangle_R\right]^{in} \to$$

$$\frac{1}{\sqrt{2}}\left[\frac{1}{2}\{|1\rangle+|3\rangle\}\{|2\rangle-|4\rangle\} - \frac{1}{2}\{|2\rangle+|4\rangle\}\{|1\rangle-|3\rangle\}\right]^{out} =$$

$$\frac{1}{2\sqrt{2}}\left[|1\rangle|2\rangle - |1\rangle|4\rangle + |3\rangle|2\rangle - |3\rangle|4\rangle - |2\rangle|1\rangle + |2\rangle|3\rangle - |4\rangle|1\rangle + |4\rangle|3\rangle\right]^{out} =$$

$$\frac{1}{\sqrt{2}}\left[|2\rangle|3\rangle - |1\rangle|4\rangle\right]^{out}.$$

В последнем равенстве опять использовано свойство симметрии для неразличимых частиц:

$$|2\rangle|3\rangle = \frac{1}{\sqrt{2}}\left(|2\rangle_1|3\rangle_2 + |3\rangle_1|2\rangle_2\right).$$

Из (44) видно, что в этой схеме (Рис.3) лишь два состояния Белла могут быть однозначно измерены: $\left|\Psi^-\right\rangle$ - срабатывают детекторы *D₂ и D₃* либо *D₁ и D₄*; $\left|\Psi^+\right\rangle$ - детекторы *D₁ и D₂* либо *D₃ и D₄*. Два оставшиеся состояния Белла дают двойные отсчеты в каждом из четырех детекторов, но такие события невозможно зарегистрировать с помощью имеющихся счетчиков фотонов!

Телепортация при наличии взаимодействий между квантовыми системами.

При использовании взаимодействий, в принципе, можно добиться 100% качества (fidelity) передаваемого состояния. В этом случае можно осуществить полное измерение невырожденного оператора Белла, например, при использовании метода “перекрестных нелокальных измерений”.

Рассмотрим взаимодействие между частицами по следующей схеме:

$$\begin{aligned}
&|\uparrow\rangle^{in}|\uparrow\rangle^{in} \to |\uparrow\rangle^{out}|\downarrow\rangle^{out},\\
&|\uparrow\rangle^{in}|\downarrow\rangle^{in} \to |\uparrow\rangle^{out}|\uparrow\rangle^{out},\\
&|\downarrow\rangle^{in}|\uparrow\rangle^{in} \to |\downarrow\rangle^{out}|\uparrow\rangle^{out},\\
&|\downarrow\rangle^{in}|\downarrow\rangle^{in} \to |\downarrow\rangle^{out}|\downarrow\rangle^{out}.
\end{aligned} \qquad (15.45)$$

Такое взаимодействие называется “условным переворотом спина”. Видно, что преобразования осуществляют операцию CNOT на спинах: состояние первого спина не меняется. Спин второй частицы (после преобразования) зависит от спина первой - если первый спин направлен “вверх”, то второй переворачивается. Если первый спин направлен “вниз”, то второй остается без изменения.

Преобразования (19) переводят состояния Белла в прямые произведения:

$$\left|\Psi^-\right\rangle \equiv \frac{1}{\sqrt{2}}\left[\left|\uparrow\right\rangle^{in}\left|\uparrow\right\rangle^{in} - \left|\downarrow\right\rangle^{in}\left|\downarrow\right\rangle^{in}\right] \xrightarrow{(15.45\hat{a}\mathring{a}\eth\tilde{o}.)} \frac{1}{\sqrt{2}}\left(\left|\uparrow\right\rangle^{out}\left|\uparrow\right\rangle^{out} - \left|\downarrow\right\rangle^{out}\left|\uparrow\right\rangle^{out}\right) =$$

$$\frac{1}{\sqrt{2}}\left(\left|\uparrow\right\rangle^{out} - \left|\downarrow\right\rangle^{out}\right)\left|\uparrow\right\rangle^{out} = \frac{1}{\sqrt{2}}\left(\left|-45^0\right\rangle\right)\left|H\right\rangle. \qquad (15.46)$$

Аналогично,

$$\left|\Psi^+\right\rangle \to \frac{1}{\sqrt{2}}\left(\left|\uparrow\right\rangle + \left|\downarrow\right\rangle\right)\left|\uparrow\right\rangle = \left(\left|+45^0\right\rangle\right)\left|H\right\rangle, \qquad (15.47)$$

$$\left|\Phi^-\right\rangle \to \frac{1}{\sqrt{2}}\left(\left|\uparrow\right\rangle - \left|\downarrow\right\rangle\right)\left|\downarrow\right\rangle = \left(\left|-45^0\right\rangle\right)\left|V\right\rangle, \qquad (15.48)$$

$$\left|\Phi^+\right\rangle \to \frac{1}{\sqrt{2}}\left(\left|\uparrow\right\rangle + \left|\downarrow\right\rangle\right)\left|\downarrow\right\rangle = \left(\left|+45^0\right\rangle\right)\left|V\right\rangle, \qquad (15.49)$$

которые однозначно можно измерить (локальными) детекторами. Преобразования (45) - нелинейные, в том смысле, что состояние одной квантовой системы изменяется в зависимости от состояния другой системы.

В некоторых экспериментах по квантовой телепортации осуществлялись поляризационные преобразования. Состояния одного фотона (входного) переносилось на состояние выходного фотона. В группе А.Цайлингера теоретический предел “качества” телепортации составил 25%, поскольку различалось лишь одно состояние Белла $\left|\Psi^-\right\rangle$. При незначительной модификации установки можно повысить качество до 50%, но достигнуть 100%-ого результата невозможно, т.к. преобразования осуществлялись с помощью светоделителей и фазовых пластинок, т.е. линейных элементов. С.Попеску предложил некий прием, позволяющий преодолеть это препятствие, если использовать поляризационную и пространственную степени свободы одного и того же фотона. Такой эксперимент был выполнен в группе де-Мартини. Теоретический предел по полному измерению состояния Белла в этом случае составляет 100%. Однако такой метод работает только для передачи (телепортирования) поляризационного состояния, приготовленного на частице, уже являющейся компонентой (перепутанной) ЭПР-пары, образующей квантовый канал между двумя модами. Такой метод не годится для телепортации неизвестного состояния частицы, поступающей извне. Впервые эксперимент по полному измерению состояний Белла был выполнен в 2000 году в группе Я.Ши. Главный недостаток его связан с малой квадратичной восприимчивостью кристаллов, которые использовались для взаимодействий.

ЛИТЕРАТУРА:

1. C.Bennet, G.Brassard, C.Crepeau, R.Jozsa, A.Peres, and W.Wooters, Teleporting an Unknown Quantum State via Dual Classical and Einstein-Podolsky –Rosen Channels. Phys.Rev.Lett., **70**, 1895-1899 (1993).

2. N.Lutkenhaus, J.Calsamglia, and K.-A.Suominen. Bell measurements for teleportation. Phys.Rev.,A, 59, 3295 (1999).
3. L.Vaidman and N.Yordan. Methods for reliable teleportation.
4. D.Bouwmeester, J-W.Pan, K.Mattle, M.Eibl, H.Weinfurter, and A.Zeilinger, Experimental Quantum Teleportation. Nature, **390**, 575-579 (1998).
5. D.Boschi, S.Branca, F.De Martini, L.Hardy, and S.Popesku, Experimental realization of Teleporting an Unknown Pure Quantum State via Dual Classical and Einstein-Podolsky-Rosen Channels. Phys.Rev Lett., **80**, №6, 1121-1125 (1998).
6. A.Furasawa, J.L.Sorensen, S.L.Braunstein, C.A.Fuchs, H.J.Kimble, E.S.Polzik, Unconditional Quantum Teleportation. Science, **282**, 706-709 (1998).
7. Y.Kim, S.P.Kulik, Y.Shih, Quantum Teleportation with a Complete Bell State Measurement. Phys. Rev.Lett., **86**, № 7 1370-1373, 2001.

ЛЕКЦИЯ 16. **КЛАССИЧЕСКАЯ КРИПТОГРАФИЯ.**

1. Криптология, криптография и криптоанализ. Основные задачи криптографии. Понятия открытого текста, криптограммы, ключа и криптосистемы. Принцип Керкхгоффа. Приложения криптографии.
2. Вычислительно сложные задачи. Односторонние функции. Пример: электронная жеребьевка.
3. Понятия криптографического протокола и криптографического алгоритма. Корректность и полнота протокола.
4. Криптоанализ и основные виды атак. Подслушиватели (нарушители). Активный и пассивный, внутренний и внешний подслушиватели.
5. Стеганография и ее задачи.
6. Типы секретности сообщений (по Шеннону). Безусловно и условно стойкие шифры. Пример: код Вернама (одноразовый блокнот).
7. Распределение ключей. Генерация ключей, их хранение и уничтожение.
8. Одноключевые (симметричные) методы шифрования. Рассеивание и перемешивание. Понятие о криптосистемах DES и ГОСТ 28147-89, их достоинства и недостатки. Основные проблемы симметричных протоколов. Аутентификация секретного ключа. Атаки раздельных миров.
9. Двухключевые (асимметричные) методы шифрования. Механизм распределения ключей по открытому каналу по У.Диффи и М.Хеллману. Понятие о криптосистемах RSA и Эль-Гамаля. Электронная подпись.

Исторически ***криптография*** (наука о создании секретной информации) возникла из потребности передачи секретной информации. Вместе с ***криптоанализом*** (наука о взламывании секретной информации) криптография составляет часть науки ***криптологии***. Криптология в настоящее время является частью математики, кроме того, она имеет ряд важных приложений в информационных технологиях. Основой криптологии как науки послужила работа Шеннона “Теория связи в секретных системах” (1949г.).

Долгое время криптография была связана только с разработкой специальных методов преобразования информации для представления ее в форме, которая окажется недоступной для потенциального **подслушивателя**. С появлением компьютерных технологий обработки данных, задачи криптографии стали меняться. Вообще, считается что именно криптография стимулировала их развитие. В криптографии традиционно рассматривается некий злоумышленник (подслушиватель) *который осведомлен об используемых криптографических приемах, алгоритмах, протоколах, владеет современными вычислительными ресурсами и пытается скомпрометрировать их*. Под компрометацией понимается несанкционированное чтение (части) информации, формирование чужой подписи, изменение результатов голосования, модификации баз данных и проч. Все эти действия подслушивателя называются *криптографической атакой*. Специфика криптографии состоит в том, что она направлена на разработку приемов, обеспечивающим стойкость к любым атакам, хотя ясно, что на момент создания криптосистемы невозможно предусмотреть новые варианты атак. Отмечу и такую социально-этическую сторону криптографии как противоречие между желанием пользователей защитить свою информацию и передачу сообщений и желанием специальных государственных служб иметь возможность доступа к информации некоторых организаций и отдельных лиц с целью пресечения незаконной деятельности.

Классической задачей криптографии является обратимое преобразование некоторого исходного текста (т.н. ***открытый текст***) в кажущуюся случайной последовательность знаков, называемую ***криптограммой***. Количество знаков в открытом тексте и в криптограмме может отличаться. При этом криптограмма может содержать как новые (метод ***подстановки***), так и имеющиеся в открытом сообщении знаки (метод

перестановки). Главным требованием является то, что используя некоторые правила, можно однозначно и в полном объеме восстановить исходный текст.

Секретность алгоритма шифрования не может, в принципе, обеспечить безусловной стойкости, поскольку подслушиватель, по определению, обладает бесконечными вычислительными ресурсами. Поэтому в настоящее время используются т.н. открытые алгоритмы. Стойкость современных криптосистем основывается не на секретности алгоритма, а на секретности некоторой информации относительно малого размера, которая называется ***ключом***. Ключ используется для управлением процессом шифрования и должен быть легко сменяемым элементом криптосистемы. Он может быть заменен пользователями в любой момент времени. Сам алгоритм является долговременным элементом криптосистемы, его изменения требует вмешательства специалистов (разработчиков).

Под ***криптосистемой*** (***шифром***, ***кодом***) будем понимать набор процедур, которые управляются некоторой секретной информацией небольшого объема.

Существует правило, сформулированное в конце XIX века голландским криптографом Керкхоффом (***принцип Керкхгоффа***): *стойкость шифра (кода) должна быть обеспечена в том случае, когда подслушивателю известен весь механизм шифрования, за исключением секретного ключа, т.е. той информации, которая управляет процессами криптографических преобразований*. В более широком смысле - мы приходим к важному требованию - все долговременные элементы защиты должны предполагаться известными потенциальному подслушивателю. Таким образом, в криптологии всегда подслушиватель оказывается в более выгодном положении.

Основные приложения современной криптографии:

1. Защита от несанкционированного чтения или обеспечение конфиденциальности информации.
2. Защита от навязываемых ложных сообщений (как умышленных, так и непреднамеренных).
3. Идентификация законных пользователей
4. Контроль целостности информации.
5. Аутинтификация информации - установление санкционированным получателем того факта, что полученное сообщение послано санкционированным отправителем.
6. Электронная подпись
7. Системы тайного электронного голосования.
8. Электронная жеребьевка.
9. Защита от отказа факта приема сообщения.
10. Одновременное подписание контракта.
11. Защита документов от подделки.

Например, в пункте 2 утверждается способ защиты от навязывания ложного сообщения, который называется имитозащитой. ***Имитозащита*** - это способ формирования (в зависимости от секретного ключа) специальной дополнительной информации, называемой ***имитовставкой***, которая передается вместе с криптограммой. Для ее вычисления используется алгоритм, задающий зависимость имитовставки от каждого бита сообщения. Этот метод широко используется в квантовой криптографии. Чем больше длина имитовставки, тем больше вероятность обнаружить искажение криптограммы подслушивателем. Если используется алгоритм вычисления имитовставки с хорошими криптографическими свойствами, то вероятность того, что это не будет обнаружено законным пользователем составляет $P = 2^{-I}$, где I - длина имитовставки в битах.

Под ***вычислительно сложными задачами*** (***NP***) понимаются задачи, заведомо имеющие решение, но требующие для его нахождения выполнения чрезвычайно большого числа операций вычислителя. Другими словами - такого их числа, что

использование вычислительных устройств, вовлеченных в единый вычислительный процесс, не позволит найти решение с существенной вероятностью (например, 1 %) за обозримое время - десятилетия, столетия и т.д. Среднее число операций, которое необходимо для этого выполнить. Принимается за количественную меру сложности *NP* - задачи.

Рассмотрим другой пример - пункт 8 - электронная жеребьевка. Пусть удаленные пользователи *A* и *B* хотят сыграть по интернету партию в шахматы. Для этого они должны разыграть цвет фигур, т.е. обеспечить равную вероятность выбора белых фигур. Криптография предлагает реализовать это с помощью следующей схемы. В ней используется односторонняя функция $y = F(x)$ - т.е. функция, которая легко вычисляется в одну сторону и трудно вычисляется в другую. Считается, что пользователь, угадывающий результат опыта с двумя равновероятными событиями, получает право первого хода.

I. Пользователь *A* выбирает случайное число x_A, двоичное представление которого имеет , скажем, 90 разрядов; он вычисляет значение функции $y_A = F(x_A)$ и сообщает величину y_A пользователю *B*. (Пользователь В должен угадать, является ли число x_A четным или нечетным)

II. Поскольку используемая функция является однонаправленной, то *B* не может по значению y_A определить x_A. Поэтому он вынужден угадывать четность x_A. Предположим, *B* выбирает "x_A - четное число" и сообщает ответ пользователю А.

III. Пользователь А сообщает пользователю В число x_A.

IV. Пользователь В вычисляет значение $y = F(x_A)$ и если $y = y_A$, то В убеждается, что его партнер действительно предоставил для проверки первоначально выбранное число.

Понятие криптографического протокола.

В критографии широко используются два термина - алгоритм и протокол; интуитивно смысл их понятен.

Под ***алгоритмом*** мы будем понимать набор команд, действий, инструкций, вычислений, которые необходимо выполнить для того, чтобы из исходных данных получить некий результат. Понятие "алгоритм", в основном, используется в вычислительной математике и кибернетике. Алгоритм выполняется субъектом (*вычислителем*). В результате выполнения алгоритма могут возникать новые данные как результат преобразования исходных данных.

Под ***протоколом*** будем понимать совокупность действий (инструкций, команд, вычислений, алгоритмов), выполняемых в заданной последовательности двумя или более субъектами с целью достижения некоего результата. Участвующие в протоколах субъекты (*рабочая станция, программа ЭВМ, оператор, сервер, орган власти и т.д.*) действуют по предписанным алгоритмам. Таким образом, алгоритм служит внутренним элементом протокола. Понятие "протокол", в основном используется в системах связи (communications). Криптографические протоколы - это такие протоколы, которые используют криптографические преобразования данных. Для того, чтобы протокол приводил к желаемой цели, необходимо, чтобы выполнялись следующие требования:

- корректность протокола - совокупность действий, предусмотренных протоколом, должно обеспечить получение требуемого результата *при всех возможных ситуациях*;
- полнота и однозначность протокола - протокол должен конкретизировать действия каждого участника *для всех возможных ситуаций*;

- непротиворечивость - результаты, полученные различными участниками протокола, не должны быть противоречивыми;
- осведомленность и согласие участников протокола - каждый субъект должен заранее знать протокол и все шаги, которые он должен выполнить; все субъекты должны быть согласны выполнять свои функции.

Классификация основных типов подслушивателей и атак.

В современном криптоанализе рассматриваются следующие виды атак на засекречивающие системы:

1. Криптоанализ на основе шифротекста (криптограммы).
2. - на основе известного открытого текста и соответствующей ему криптограммы.
3. - на основе выбранного открытого текста.
4. - на основе выбранной криптограммы.
5. - на основе адаптированного открытого текста.
6. - на основе адаптированной криптограммы.
7. - на основе аппаратных ошибок.

Каждый криптографический алгоритм или протокол должен быть разработан с учетом наиболее полного перечня действий потенциального подслушивателя и с учетом всех возможных атак. Такие атаки состоят в выполнении нарушителем действий, с помощью которых подслушиватель пытается, в общем случае, *создать условия, при которых корректность использования алгоритмов и протоколов криптосистемы будет нарушена*. К таким действиям относятся попытки:

- прочитать криптограмму,
- взломать односторонние функции - т.е. вычислить значение аргумента по значению функции,
- выдать себя за другого субъекта,
- навязать ложные сообщения,
- расширить свои полномочия

Если такие действия возможны, то говорят, что криптосистема уязвима по отношению к такой-то атаке. По характеру действий можно выделить два типа подслушивателей:

I. ***Активный подслушиватель***. Он пытается навязать ложные сообщения, перехватить и модифицировать сообщения, получить доступ к базам данных, расширить свои полномочия, навязать ложный открытый ключ и проч.
II. ***Пассивный подслушиватель***. Он не предпринимает действий по дезорганизации криптографического протокола. Его целью является только перехват сообщений, передаваемых в рамках криптосистемы с целью ознакомления с их содержанием, вычисления распределяемых ключей и проч.

Существуют ***внутренние*** и ***внешние*** подслушиватели. Внутренним подслушивателем является лицо, имеющие некоторые легальные полномочия внутри криптосистемы. Соответственно, различают внутренние и внешние атаки. И внутренний и внешний подслушиватели могут быть активными и пассивными. Возможен и такой вид атак, когда внешние и внутренние подслушиватели объединяются. Это наиболее опасный вид атак. Сюда также следует отнести случай, когда подслушиватель (его уместно называть нарушителем) является разработчиком криптосистемы. Тогда он может использовать встроенные “потайные ходы” в алгоритмах формирования ключевых параметров и создания программных закладок.

Стеганографией называется техника скрытой передачи или скрытого хранения информации. Ее целью является сокрытие самого факта передачи сообщений) невидимые чернила, микрофотография, тайники, передача внутри видеокадров и проч.). *Принципиальное отличие криптографии от стеганографии состоит в том, что в ней не скрывается факт передачи сообщений, а скрывается только его содержание*.

Стеганографические методы могут обеспечить высокий уровень защиты информации только в том случае, если они будут дополнены предварительным криптографическим преобразованием сообщения.

Виды секретности сообщений (по К.Шеннону)

Шеннон рассматривал шифрование (кодирование) как отображение исходного сообщения в криптограмму - зашифрованное сообщение:

$$C = F_i\left(M\right), \qquad (16.1)$$

где C - криптограмма (от coding), F_i - отображение, M - исходное сообщение (от message), i = индекс, соответствующий конкретному используемому ключу. Для однозначного декодирования сообщения отображение F_i должно иметь единственное обратное отображение, такое, что

$$F_i F_i^{-1} = I\ , \qquad (16.2)$$

где I - тождественное отображение:

$$M = F_i^{-1}\left(C\right). \qquad (16.3)$$

Мы считаем, что источник ключей является статистическим процессом или устройством, которое задает отображения $F_1, F_2, ...F_{N_1}$ с вероятностями $p_1, p_2, ...p_{N_1}$. Число возможных сообщений N_2 конечно, а сообщения $M_1, M_2, ...M_{N_2}$ имеют априорные вероятности $q_1, q_2, ..q_{N_2}$.

Рассмотрим простейший шифр, в котором исходный алфавит сообщения совпадает с множеством знаков ключа и множеством знаков криптограммы. Пусть криптование выполняется путем замены знаков исходного сообщения на знаки криптограммы в зависимости от очередного значения символа ключа. Символ ключа выбирается среди случайной последовательности цифр от 0 до 39. Тогда сообщение, ключ и криптограмма представляются в виде последовательности знаков одного и того же алфавита:

$$M = \left(m_1 m_2 m_3 ... m_n\right),\ K = \left(k_1 k_2 k_3 ... k_n\right),\ C = \left(c_1 c_2 c_3 .. c_n\right)\ \ \left(N_2 = N_1\right)$$

Текущий шаг криптования выражается следующим образом:

$$c_i = f\ \left(m_i, k_i\right).$$

Например, будем использовать простой алфавит заглавных букв и некоторых знаков препинания:

А	Б	В	Г	Д	…	..	..	Э	Ю	Я		.	,	!	?	;
00	01	02	03	04				31	32	33	34	35	36	37	38	39

Допустим, мы хотим зашифровать сообщение “КОД ВЕРНАМА”. Запишем его в верхней строке таблицы. Ниже укажем соответствующие численные символы из верхней таблицы. В третью строку поместим случайную выборку из сорока знаков от 00 до 39. В последней строке разместим результат суммирования символов второй и третьей строки по модулю 40:

К	**О**	**Д**		**В**	**Е**	**Р**	**Н**	**А**	**М**	**А**
11	**15**	**05**	**34**	**03**	**06**	**17**	**14**	**01**	**13**	**01**
15	**04**	**13**	**28**	**11**	**09**	**38**	**30**	**02**	**24**	**05**
26	**19**	**18**	**22**	**14**	**15**	**15**	**04**	**03**	**37**	**06**

Например, четвертый символ “пробел” в сообщении имеет числовой код “34”. Соответствующее случайное число, выпавшее на этот символ, оказалось “28”. Тгда 34 + 28 = 62 = 40 + 22, следовательно, остаток при суммировании по модулю “40” равен 22. Таким образом, шифрование и дешифрование по рассмотренному алгоритму можно записать в виде:

$$M + k \left(\mathrm{mod}\, 40\right) = C . \qquad (16.4)$$

$$C - k \left(\mathrm{mod}\, 40\right) = M . \qquad (16.5)$$

Этот способ шифрования был изобретен в 1917г. Жильбером Вернамом. Клод Шеннон показал, что если ключ действительно случайный, если он имеет такую же длину, как и само сообщение и если он не используется дважды, то одноразовая передача сообщения абсолютно защищена. Примечательно, что результат не зависит от вычислительной мощности, доступной криптоаналитику. Шифры такого рода называются ***безусловно стойкими***. Другими словами, безусловно стойкими называются шифры, для которых криптоаналитик (даже если он обладает бесконечными вычислительными ресурсами) не может улучшить оценку исходного сообщения *M* на основе знания криптограммы *C* по сравнению с оценкой при неизвестной криптограмме. Ясно, что это возможно в случае, когда *M* и *C* являются статистически независимыми, т.е. когда выполняется условие:

$$P\left(M = M_i / C = C_i\right) = P\left(M = M_i\right) \qquad (16.6)$$

для всех возможных сообщений *M*. В нашем примере:

$$c_i = f\left(m_i, k_i\right) = \left(m_i + k_i\right) \mathrm{mod}\, L, \qquad (16.7)$$

где $L = 40$. Выбранный нами источник ключа обеспечивает равную вероятность выбора любого ключа длины $n \le L = 40$. В этом случае вероятность выбора данного ключа длины *n* составляет

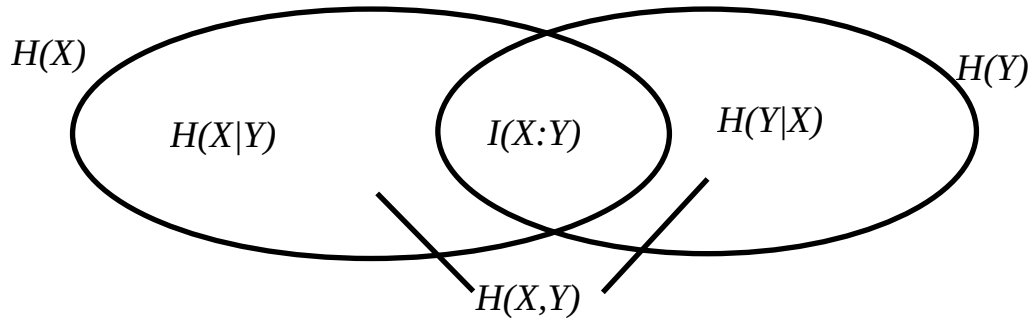
$$P\left(K = K_i\right) = L^{-n} . \qquad (16.8)$$

Отсюда следует, что для произвольных *M* и *C* выполняется условие

$$P\left(M = M_i / C = C_i\right) = L^{-n} . \qquad (16.9)$$

<u>Напоминание (из Лекции 3).</u> По определению взаимная информация *I(X:Y)* есть мера того сколько информации содержат *X* и *Y* друг о друге. Например, если *X* и *Y* - независимые величины, то *p(x,y) = p(x)p(y),* так что *I(X:Y)* = 0. Соотношения между основными мерами классической информации показаны на рисунке. *H(Y|X)* есть мера того, сколько информации, в среднем, оставалось бы в *Y* при условии, что мы бы знали *X*.
Тогда по Шеннону, криптосистема обладает абсолютной секретностью, если взаимная информация обращается в нуль:

$$I\left(M : C\right) \equiv H\left(C\right) - H\left(C \mid M\right) = 0, \quad M \equiv X \,,\; C \equiv Y$$



Условие (9) означает, что данной криптограмме длиной *n* с вероятностью L^{-n} может соответствовать любое исходное сообщение длины *n*. Мы доказали, что безусловно стойкие шифры существуют (если при шифровании нового сообщения брать новый ключ). Вообще, рассмотренный пример относится к криптосистемам, использующим равновероятный случайный ключ, имеющий длину, равную длине сообщения. Они называются ***одноразовыми блокнотами*** или *шифрами с лентой однократного использования*. На практике такие системы получили ограниченное применение, поскольку требуют передачи ключа большого объема. Для длинных ключей крайне усложняется процедура их управления (т.е. генерация, передача и хранение).

Другим недостатком кода Вернама является тот факт, что ключ должен использоваться лишь один раз. Если ключ используется повторно, то подслушиватель может записав разрозненные криптограммы восстановить как фрагменты открытого текста, так и сам ключ. Так, например, если Ева записала два сообщения, закриптованных одним ключом в двоичном коде, то она может сложить криптограммы и получить сумму двух открытых текстов:

$$s_1 \oplus s_2 = m_1 \oplus k \oplus m_2 \oplus k = m_1 \oplus m_2 \oplus k \oplus k \equiv m_1 \oplus m_2,$$

где использовано обстоятельство, что операция сложения по модулю два $\oplus$ (XOR) коммутативна.

Кроме того, чисто из физических соображений, известно, что классические состояния физических объектов могут быть измерены сколь угодно точно и без их возмущения. Поэтому в рамках классических физических представлений невозможно обеспечить секретное распределение ключа через открытый канал связи, т.к. нельзя гарантировать обнаружение попыток подслушивания (пассивного). Именно поэтому криптограммы с одноразовыми ключами не получили широкого применения.

Можно представить себе ситуацию, когда по криптограмме можно, в принципе, расшифровать исходное сообщение. Например, в случае, когда длина криптограммы превышает некую длину, для которой существует единственное решение обратной задачи (для шифра Вернама такая длина стремится к бесконечности). Если криптоаналитик имеет ограниченные вычислительные ресурсы, то такие задачи называют ***условно стойкими***.

Встречаются задачи, в которых для решения требуется настолько большие затраты, что вычисление становится экономически невыгодным или когда вычисление требует больше времени, чем время “ценности” сообщения. Тогда говорят, что решение является ***вычислительно нереализуемым***, а соответствующие шифры – ***вычислительно стойкими***[1]. Одним из элементов криптосистемы, на котором основывается ее стойкость является ключ.

Распределение ключей.

В понятие криптосистемы входит не только совокупность процедур шифрования и дешифрования, но и управление ключами. Управление ключами включает в себя:

- генерацию ключей;
- распределение ключей;
- хранение ключей;
- уничтожение ключей.

Сбой во время выполнения любой из этих процедур может привести к тому, что секретная информация (или ее часть) станет известна подслушивателю и ему даже не придется решать задачу криптоанализа.

Если подслушивателю становится известным ключ, то он получает все привилегии законного пользователя. Принципиальным при рассмотрении криптосистем является способ раскрытия ключа, основанный на криптоанализе. Под раскрытием ключа путем криптоанализа будем понимать определение ключа (включая его угадывание) [2]. Принципиально все криптосистемы подвержены атакам такого рода, они называются ***силовыми атаками*** и состоят в тотальном переборе по всему пространству ключей. Они

[1] Вообще под стойкостью криптосистем понимается сложность решения задачи криптоанализа в определенных условиях. К.Шеннон ввел понятие рабочей характеристики $W(n)$ шифра как среднее количество работы по нахождению ключа по известным n знакам криптограммы при использовании лучшего алгоритма крптоанализа. Количество работы может быть измерено, например, количеством операций, необходимых для вычисления ключа. Этот параметр связан с алгоритмом вычисления ключа.

[2] Остальные способы связаны с организационными и техническими мероприятиями.

являются наиболее слабыми; для их предотвращения требуется аккуратность в выборе длины ключа и процедур его генерации. В настоящее время безопасной считается длина ключа равная 80 битам (это число содержит около 10^{20} десятичных знаков).

Основным принципом ***генерации ключа*** является равновероятность выбора по всему ключевому пространству или множеству возможных ключей. При генерации ключей используются *электронные устройства, в которых протекает какой-нибудь случайный физический процесс*. Такие устройства называются датчиками шума. Например, число импульсов фотоэлектронов при засветке фотокатода ФЭУ светом с постоянной интенсивностью описывается распределением Пуассона – это один из широко используемых в криптографии шумовых процессов. Другим примером является случайный процесс прохождения (отражения) света через (от) светоделителя. Показания датчика замеряются через определенные интервалы времени и оцифровываются. Периодически механизм генерации ключей подвергается проверке, т.е. *тесту на случайность и равномерность шума*.

В криптографии используется несколько программных алгоритмов генерации псевдослучайных процессов. Один из них дается реккурентным соотношением:

$$g_i = (ag_i + b) \bmod M, \qquad (16.10)$$

где g_i - i-ый член порождаемой числовой последовательности; a, b, M и начальное порождающее число g_i- являются ключевыми параметрами.

Распределение ключей является одной из важнейших и дорогостоящих процедур. После того, как ключ установлен, то обмен сообщений предполагает наличие некоего канала, подверженному прослушиванию. Так, публичные объявления через средства массовой информации, служат примером полного пассивного прослушивания. Однако, чтобы определить ключ, два или несколько пользователей должны на каком-то этапе общения использовать очень надежный канал связи. Серьезные проблемы возникают, когда ключ приходится менять для увеличения стойкости криптосистемы. Обычно ключ меняется от сеанса к сеансу или после передачи определенного объема информации.

Для примера рассмотрим распределение ключей в ***одноключевых*** или симметричных протоколах. Здесь необходим защищенный канал связи, по которому секретный ключ доставляется к приемнику и передатчику. Таким каналом может служить доставка через доверенное лицо (как правило, используется три курьера), охраняемый канал связи, личная встреча абонентов и проч. Одна из схем двусторонней одноключевой связи показана на рис.1. Она содержит Источник ключа, Отправителя, Получателя, Защищенный канал связи, Открытый канал связи и (де)шифрующие устройства. Если криптографическая схема состоит из N пользователей, которые должны иметь возможность секретно общаться, то необходимо генерировать $N(N-1)/2$ ключей. Это число квадратично зависит от числа пользователей, поэтому такой метод трудно реализовать на практике при большом числе пользователей.

Хранение информации в зашифрованном виде предполагает хранение секретного ключа или нескольких секретных ключей, с помощью которых данные могут быть расшифрованы. Ключи должны храниться на защищенных от несанкционированного доступа носителях.

Ключ, на котором информация была зашифрована, подлежит гарантированному ***уничтожению***. Процедура уничтожения ключа должна производиться под контролем, поскольку старые ключи представляют такой же интерес как и действующие (используя старые шрифты и копии старых крптограмм можно восстановить секретную информацию).

ОДНОКЛЮЧЕВЫЕ (СИММЕТРИЧНЫЕ) МЕТОДЫ ШИФРОВАНИЯ.

Одним из методов криптования является замена символов исходного текста t на символы криптограммы c. Есть два способа: поточный и блочный. Поточный метод осуществлялся

в коде Вернама, когда t_i поочередно заменяются на c_i по определенному алгоритму. Результат зависит от секретного ключа.

К блочным методам относится, например, известная система DES (decryption - encryption - standard), принятая в 1977г. в США. В ней используется многократное чередование перемешивающих и рассеивающих преобразований, не управляемых ключом, а также простых преобразований, управляемых ключом.

Рассеиванием называется распространение влияния одного знака открытого текста на много символов криптограммы, что приводит к маскировке статистических свойств исходного сообщения - мощный фактор криптоанализа. Для предотвращения возможности вычисления ключа по частям также реализуют принцип распространения влияния одного знака ключа на большое число знаков криптограммы (***принцип рассеивания***).

Перемешивание - это шифрующее преобразование, которое нарушает взаимные связи статистических характеристик входного и выходного текста.

Алгоритм DES преобразует входную информацию блоками объемом 64 бит. Основные процедуры - подстановка и перестановка. Они реализуются разными блоками (S- и P-блоки). Например P-блоки реализуются с помощью переплетения проводников. Эти операции - нелинейные, именно они предопределяют криптографическое закрытие данных. Долгое время принципы выбора таблиц перестановок держались в секрете, хотя и алгоритм и сами таблицы были открыты. В настоящее время компания IBM опубликовала и сами критерии выбора S-блоков. Они выбираются так, чтобы изменение одного бита на входе приводит к изменению по крайней мере двух битов на выходе - т.н. принцип размножения ошибок. Общая схема алгоритма DES состоит в следующем. 64-битовый блок открытого текста после начальной перестановки делится на две части по 32 бит каждая. Левую и правую половины обозначим L и R, соответственно. Затем выполняются 16 раундов шифрующих операций вида:

$$L_i = R_{i-1}$$

$$R_i = L_{i-1} \oplus F\left(R_{i-1}, K_i\right).$$

Здесь K_i - 48-битовый подключ, вырабатываемый по простым процедурам из 56-битового секретного ключа и используемый на i-ом раунде. Сущность алгоритма заложена в преобразованиях, которые выполняются для получения значения функции $F\left(R_{i-1}, K_i\right)$. Все детали таких преобразований считаются известными, за исключением секретного ключа K_i .

Наиболее существенным недостатком системы DES является короткий секретный ключ, длина которого составляет 56 бит. Самым простым способом нелегального доступа к информации, зашифрованной с его помощью, считается перебор всех возможных ключей. Их число составляет $2^{56} \approx 10^{17}$. В настоящее время проведение такой атаки под силу организациям, имеющим очень мощные вычислительные средства.

Шифры, подобные криптосистеме DES, легко реализуются в виде электронных быстродействующих устройств, однако на уровне программной реализации применение процедур над отдельными битами и подблоками малого размера ведет к тому, что шифрующие программы обладают очень низкой скоростью шифрования.

В Российском стандарте шифрования (ГОСТ СССР 28147-89) задействуется 64-битовый шифр, использующий 256-битовый секретный ключ, представленный в виде восьми 32-битовых подключа Q_j, где j = 0, 1,...7. В этой системе функция $F\left(R, K\right)$ задается операцией суммирования по модулю 2^{32}, с помощью табличных подстановок, выполняемых над 4-битовыми подблоками и операцией циклического сдвига влево на 11 бит, выполняемой над 32-битовым подблоком. Таблицы подстановок служат дополнительным ключом и должны держаться в секрете. Этот долговременный ключ является общим для всех пользователей сети и поставляется в установленном порядке. Стойкость такой системы критически зависит от качества используемых таблиц

подстановок. При правильном выборе даже если таблицы станут известны подслушивателю, стандарт обеспечивает высокую стойкость. Однако, критерии выбора таблиц, в отличие от американских, до сих пор не опубликованы. Заметим, что требование секретности таблиц подстановок не согласуется с общепринятым принципом Керкхгоффа, поскольку данные элементы относятся скорее к алгоритму шифрования, а не к легко сменяемому секретному ключу. Вообще, секретность алгоритма шифрования существенно затрудняет определение открытого текста по криптограмме. Однако этот элемент повышения стойкости криптограммы на практике используется редко, поскольку крайне трудно обеспечить секретность элементов криптосистемы, которые используются долгое время и известны широкому кругу пользователей. Отсюда - в практических криптосистемах нужно обеспечить сменяемость алгоритма шифрования.

Для иллюстрации принципа Керкхгоффа рассмотрим вопрос о безусловной стойкости лучшей криптосистемы с секретным алгоритмом и с конечным временем шифрования. Как обычно, будем считать, что подслушиватель является представителя земного мира, обладает доступом к бесконечным вычислительным ресурсам (поскольку мы рассматриваем безусловную стойкость) и знает язык на котором написано исходное сообщение. Он хочет прочитать криптограмму, соответствующую исходному тексту с размером многократно превышающим размер ключа. Размер текста, который описывает любой алгоритм с конечным временем шифрования является конечным, следовательно, нападающий может опробовать все возможные алгоритмы путем перебора текстов. Действительно, для данного уровня развития технологии вычислений каждый *конечный текст* можно интерпретировать как алгоритм, написанный на языке машинных команд. При этом число вариантов интерпретации произвольной конечной последовательности битов является конечным, следовательно при наличии бесконечных вычислительных ресурсов путем проб можно определить как конечный секретный ключ, так и секретный алгоритм. Таким образом, с точки зрения безусловной стойкости секретность алгоритма является несущественным фактом. Только *разовый секретный ключ*, длина которого равна (или больше) длине сообщения, позволяет достигнуть безусловной стойкости, хотя это утверждение имеет, скорее теоретический смысл, чае практический. Все возможные атак в реальных условиях не могут быть предусмотрены замкнутой теоретической моделью. *Использование длинных ключей порождает проблему безопасного распределения ключей, что делает безусловно стойкие шифры практически менее надежными, чем условно стойкие криптосистемы с ключом размером 512, 256 и даже 128 бит*.

Основным недостатком Российского стандарта является низкая скорость при программной реализации (как и для DES), что связано с использованием большого числа операций над 4-битовыми подблоками. Кроме того, чтобы изменение одного входного бита оказало влияние на каждый выходной бит в случае Российской криптосистемы требуется выполнить 8 раундов, а в криптосистеме DES - только 5.

К достоинствам относят

- 256-битовый секретный ключ, что делает бессмысленными атаки, основанные на переборе секретного ключа не только в настоящее время, но и в далеком будущем, если говорить о классических компьютерах).
- простая аппаратная реализация, связанная с хорошим расписанием использования ключа
- 32 цикла шифрующих операций обеспечивают высокую стойкость.

Итак, существующие одноключевые криптографические протоколы обеспечивают хорошую защищенность при условии решения проблемы распределения ключа. Однако у этих систем существует *две принципиальные проблемы.*

1. распределение ключей по защищенному каналу;
2. ***аутентификация*** секретного ключа (или проблема первого общения). Под аутентификацией понимается процедура, позволяющая получателю удостоверится, что

секретный ключ принадлежит законному отправителю. Чтобы пояснить, о чем идет речь, представим себе, что Подслушиватель (Ева) перехватывает все сообщения, посылаемые Алисой и выдает себя как Алису для Боба, а для Алисы она представляется Бобом (***атака раздельных миров*** или с человеком посредине). Оказывается, что если у Алисы и Боба уже имеется секретный ключ (которым они обменялись, например, при встрече), то аутентификация вспомогательных ключей не представляет проблем. Однако, если секретный ключ не распределен, то теоретически аутентификация невозможна, хотя и существуют методы (классические) по ее оптимизации.

Что касается проблемы распределения ключа, то есть два способа ее решения. Первый - математический - достигается с помощью двухключевых протоколов или ***криптографии с открытым ключом***. Второй способ - физический - реализуется с помощью ***квантовой криптографии***. К сожалению, квантовое распределение ключа не дает метода аутентификации или борьбы с атаками раздельных миров.

Использование симметричных протоколов предполагает, что ***обе стороны доверяют друг другу***. Криптосистемы с открытым ключом позволяют реализовать протоколы взаимодействия сторон, которые ***не доверяют друг другу***. Ярким примером такого протокола является формирование электронной (или цифровой подписи).

ДВУХКЛЮЧЕВЫЕ (АСИММЕТРИЧНЫЕ) МЕТОДЫ ШИФРОВАНИЯ.

У.Диффи и М.Хеллман в 1976 году опубликовали работу, в которой утверждалось, что ***возможно построение практически стойких секретных систем, которые не требуют передачи секретного ключа***. Они ввели понятие ***односторонней функции с секретом***.

Под односторонней функцией с секретом понимается семейство обратимых функций f_z с параметром z, таких, что для какого-то z можно найти некие алгоритмы E_z и D_z, позволяющие просто вычислить значение $f_z(x)$ для всех x из области определения, а также $f_z^{-1}(y)$ для всех y их области значений, однако, практически для любых значений параметра z и практически для всех значений y из области значений f_z нахождение $f_z^{-1}(y)$ вычислительно неосуществимо даже при известном E_z (т.е. требуется знание D_z).

В качестве односторонней функции У.Диффи и М.Хеллман предложили функцию дискретного возведения в степень

$$f(x) = \alpha^x \pmod p,$$

где x - целое число, $1 \le x \le p-1$, а p – *к-битовое простое число*. Выбирается такое число $\alpha < p$, степени которого по модулю p представляют собой упорядоченное множество чисел $\{\alpha^1, \alpha^2, ..., \alpha^{p-1}\}$, которое является некоторой перестановкой чисел $\{1, 2, ..., p-1\}$. Такое число α называется первообразным корнем по модулю p. “***Секрет” - это тоже возведение в степень, но с другим показателем***!

Для очень больших модулей p (например, при $к$ = 1024 бит)для данного x легко вычислить значение этой функции. Такая процедура называется дискретным возведением в степень. Обратной к функции дискретного возведения в степень является функция $f^{-1}(y)$, которая ставит в соответствие заданному значению y такое значение x, для которого выполняется условие $\alpha^x = y \pmod p$. Задача нахождения такого x называется дискретным логарифмированием. Дискретные логарифмы сложно вычисляются, когда число $p-1$ содержит один большой простой множитель, например, когда оно представимо в виде $p-1 = 2p'$, где p' - простое число. Тогда трудоемкость дискретного логарифмирования равна примерно $\sqrt{p}$ умножений по модулю p.

Известные классические вычислительные алгоритмы, работающие по законам классической физики, имеют экспоненциальную сложность по размеру входных данных. Алгоритмов, имеющих полиномиальную сложность пока неизвестно, хотя и не доказано их отсутствие.

Замечание. П.Шор доказал, что квантовый алгоритм параллельного вычисления дает полиномиальную сложность для обращения дискретного логарифма

Механизм распределения секретных ключей по открытому каналу состоит в следующем.

1. Каждый абонент выбирает *случайный секретный ключ x* и *открытый ключ y*, соответствующий выбранному секретному ключу, в соответствии с формулой:

$$y = \alpha^x \pmod p. \qquad (16.11)$$

Для любого значения *x* легко вычислить *y*, однако при размере числа *p*, равном 512 бит и выше, вычислительно неосуществимо выполнение дискретного логарифмирования. Значит, невозможно определить число *x*, для которого значение $\alpha^x \pmod p$ равно заданному значению *y*.

2. Все абоненты размещают свои открытые ключи в общедоступном справочнике. Понятно, что это издание должно быть защищено от атак раздельных миров, когда подслушиватель подменяет открытые ключи или навязывает ложные сообщения. Если два абонента - Алиса и Боб хотят установить секретную связь, они делают следующие процедуры.

2.1. Алиса берет из справочника открытый ключ Боба и, используя свой секретный ключ, вычисляет ***общий секретный ключ***, пользуясь ***секретом*** - повторным возведением в степень с другим показателем.:

$$Z_{AB} = \left(y_B\right)^{x_A} = \left(\alpha^{x_B} \bmod p\right)^{x_A} = \alpha^{x_B x_A} \bmod p, \qquad (16.12)$$

где y_A и y_B - открытые ключи для Алисы (А) и Боба (В), а x_A, x_B - соответствующие секретные ключи. Общий секретный ключ Z_{AB} не нужно передавать по сети связи, поскольку Боб по известному из справочника открытому ключу Алисы аналогичным образом вычисляет его значение:

$$Z_{AB} = \left(y_A\right)^{x_B} = \left(\alpha^{x_A} \bmod p\right)^{x_B} = \alpha^{x_B x_A} \bmod p. \qquad (16.13)$$

3. Подслушивателю известны значения $y_B = \alpha^{x_B} \bmod p$ и $y_A = \alpha^{x_A} \bmod p$, но для того, чтобы вычислить Z_{AB} , он должен решить трудную задачу дискретного логарифмирования.
4. Общий секретный ключ может использоваться абонентами для шифрования вспомогательных (сеансовых) секретных ключей, а они, в свою очередь - для шифрования сообщений с использованием симметричных методов.

Итак, решение задачи дискретного логарифмирования существует, но оно вычислительно неосуществимо. Таким образом, стойкость метода Диффи-Хеллмана основана на сложности дискретного логарифмирования.

Наиболее популярные асимметричные схемы в настоящее время - это системы RSA (Ривест - Шамир - Адэльман) и Эль-Гамаля. Обе они используются для формирования электронной подписи, когда владелец секретного ключа может подписать документ, а его подпись может быть проверена любым желающим по открытому каналу. Цифровая подпись представляет собой некоторое число со специфической структурой, которое допускает проверку (с помощью открытого ключа) того факта, что оно было выработано для некоторого сообщения с использованием секретного ключа.

Заметим, что скорость шифрования двухключевым способом на несколько порядков ниже скорости, которой обладают одноключевые схемы.

Таким образом двухключевые системы являются, по-видимому, стойкими при классической реализации (по законам классической физики), но перестают быть таковыми в квантовой реализации.

ЛИТЕРАТУРА:

1.

ЛЕКЦИЯ 17. КВАНТОВАЯ КРИПТОГРАФИЯ

17.1. Проблема распределения ключа в классической криптографии и пути ее решения.

17.2. Физические основы квантового распределения ключа: теорема о запрете копирования и неразличимость неортогональных состояний. Общая схема протокола КРК.

17.3. Основные свойства поляризованных фотонов. Некоторые сведения из теории квантовых измерений. Сопряженные базисы. Три сопряженных базиса для поляризованных фотонов.

17.4. Протокол BB84. Сырой и просеянный ключ. Коррекция ошибок и усиление секретности - на примере протокола BB84. Подслушивание в протоколе BB84. Стратегия перехватчик-ретранслятор. Стратегия “задержанного выбора”. Активный подслушиватель и схема аутентификации Вегмана-Картера. Недостатки протокола BB84.

17.5. Протокол BB92. Его преимущества и недостатки по сравнению с BB84.

17.6. ЭПР протокол (протокол А.Экерта) - если есть время.

На предыдущей лекции были сформулированы две проблемы современной классической криптографии: распределение ключей и аутентификация. Вторая проблема, похоже, имеет разрешение (абсолютно защищенное) лишь при личной встрече владельцев ключа. Первая проблема – распределение ключа в классической криптографии решается с помощью криптографии с открытым ключом или двухключевых (асимметричных) протоколов. Такое ее решение назовем *математическим*, поскольку используется некий алгоритм, основанный на односторонних функциях с секретом, когда вычисление функции в одну сторону оказывается простым, а нахождение обратной функции занимает огромное количество вычислительных ресурсов. В частности, стойкость криптографических систем RSA и Эль-Гамаля основываются на том, что факторизация больших чисел требует экпоненциального по числу знаков факторизуемого числа N операций. Это значит, что при увеличении разряда числа на один (прибавление еще одной цифры к факторизуемому числу) умножает время, необходимое для факторизации на фиксированный множитель. При увеличении числа, задача быстро становится вычислительно не решаемой. Таким образом, в настоящий момент, защищенность двухключевых криптосистем основывается на медленности технического прогресса.

В одной из следующих лекций мы будем рассматривать алгоритм факторизации чисел, предложенный П.Шором. Этот алгоритм основан на параллельном методе вычислений, который можно осуществить в квантовом компьютере. Такой алгоритм позволяет принципиально изменить скорость факторизации – теперь она определяется полиномиальными по числу N временными затратами.

Другой путь решения проблемы распределения ключа основан на физических закономерностях. Он реализуется в квантовой криптографии. Основные аргументы в таком методе криптографии восходят к двум утверждениям:

- неизвестное квантовое состояние невозможно копировать;
- без возмущения невозможно извлечь информацию о неортогональных квантовых состояниях.

Последнее утверждение можно перефразировать: в общем случае любое измерение, выполняемое подслушивателем, приведет к изменению состояния носителя информации.

Далее будут рассмотрены основные протоколы квантовой криптографии. Строго говоря, речь будет идти не о новом типе криптографии в целом, а лишь о новом методе распределения ключа. Этот метод, вообще говоря, должен быть дополнен надлежащим протоколом аутентификации – абоненты должны идентифицировать друг друга до начала общения – об этом не следует забывать, говоря о преимуществах квантовой криптографии! На сегодняшний день единственный способ решения проблемы аутентификации состоит в обмене *коротким* секретным ключом при встрече абонентов. Квантовая криптография дает физический способ распределения ключа *большого размера*, который затем можно использовать в симметричных (одноключевых) протоколах. Поэтому, будучи до конца последовательным, следует говорить о квантовой криптографии как о *протоколе увеличения секретного ключа* (*Quantum Secret Growing protocol).*

Итак, общая схема квантового распределения ключа следующая.
Алиса посылает квантовое состояние, реализованное, например, в виде кванта света, Бобу. Подслушивание, как физический процесс, представляет собой серию экспериментов, выполняемых злоумышленником над перехваченными квантами. Поскольку акт подслушивания изменяет квантовое состояние носителя информации, то Алиса и Боб могут это установить с помощью определенных процедур уже по открытому каналу связи. Итак, протокол квантового распределения ключа должен включать в себя:

- установление синхронизации;
- по крайней мере двух пользователей – Алису и Боба;
- канал для обмена квантовыми состояниями или *квантовый канал связи*;
- открытый канал связи, который используется для проверки искажения посылаемых состояний.

Если после обмена сообщениями по открытому каналу пользователи убеждаются, что квантовые состояния не возмущены, то они включают хорошо известный протокол одноразового блокнота (код Вернама) используя распределенный секретный ключ. Если обнаруживается возмущение квантовых состояний, то сеанс связи либо прерывается, либо начинается заново.
Замечание. Открытый канал рассматривается как такой канал связи, который доступен любому желающему. Единственное ограничение, которые мы пока введем на открытый канал – чтобы подслушиватель был ***пассивным***. В случае активного подслушивателя пользователи могут осуществлять распределение ключа, но при условии, что изначально они владели некоторой секретной информацией, распределенной между ними и если подслушиватель не настолько активен, чтобы перехватывать всю посланную информацию (атака раздельных миров или с человеком посередине).

Идея, впервые высказанная Визнером, Беннетом и Брассардом [5] состоит в том, что пассивный подслушиватель не может достоверно различить неортогональные состояния (назовем их $|0\rangle, |1\rangle$), если он не знает базиса, в котором те были приготовлены. Предположим, что Ева настраивает свой измеряющий прибор в неком исходном состоянии $|m\rangle$. Ее цель – отличить состояния $|0\rangle, |1\rangle$ не возмущая их. Ее действия будут описываться следующими унитарными преобразованиями над входными состояниями (см. лекцию 6);

$$|0\rangle|m\rangle \to |0\rangle|m_0\rangle, \quad (17.1)$$

$$|1\rangle|m\rangle \to |1\rangle|m_1\rangle. \quad (17.2)$$

Унитарность сохраняет скалярное произведение, поэтому

$$\langle 0|1\rangle\langle m|m\rangle = \langle 0|1\rangle\langle m_0|m_1\rangle, \quad (17.3)$$

откуда следует, что

$$\langle m_0|m_1\rangle = 1. \quad (17.4)$$

Это означает, что конечное состояние измерительного прибора Евы одно и то же. Ева не возмутила квантовых состояний, но она и не получила никакой информации о них, в силу (17.4).

Мы рассматривали и более общее измерение, когда Ева возмущает исходные состояния:

$$|0\rangle \to |0'\rangle, \ |1\rangle \to |1'\rangle. \quad (17.5)$$

Тогда в результате действий подслушивателя:

$$|0\rangle|m\rangle \to |0'\rangle|m_0\rangle, \quad (17.6)$$

$$|1\rangle|m\rangle \to |1'\rangle|m_1\rangle. \quad (17.7)$$

И опять, в силу унитарности, получаем:

$$\langle 0|1\rangle = \langle 0'|1'\rangle\langle m_0|m_1\rangle. \quad (17.8)$$

Наилучшая ситуация с точки зрения Евы возникает, когда скалярное произведение $\langle m_0|m_1\rangle$ принимает минимальное значение. Это происходит при

$$\langle 0'|1'\rangle = 1, \quad (17.9)$$

(поскольку $\langle 0|1\rangle = const$). При этом она получает максимальную возможность различить два состояния своего прибора, но два исходно неортогональные состояния становятся неразличимыми (17.9).

Квантовое кодирование информации впервые было предложено в работах Стефана Визнера, а также Чарльза Беннета и Жиля Брассарда. С.Визнер рассматривал т.н. «квантовые деньги», т.е. деньги, которые в принципе невозможно подделать. Кроме того, он предложил способ распределения двух или трех сообщений, при котором чтение одного из них уничтожало бы информацию, содержащуюся в других. Ч.Беннет и Ж.Брассард предложили реалистичный протокол распределения ключа. Также они обсуждали криптографические схемы типа протокола жеребьевки.

ПРОТОКОЛ BB84 [5]

Этот протокол был предложен Ч.Беннетом и Ж.Брассаром в 1984 г. Для распределения ключа они рассматривали неортогональные состояния фотонов.

В оригинальной работе Ч.Беннет и Ж.Брассард рассматривали поляризационные состояния света в качестве квантовых систем, лежащих в основе протокола распределения ключа.

Основные свойства поляризованных фотонов.

Приготовить поляризованный свет можно, пропуская пучок света через какое-нибудь поляризационное устройство, например, призму Глана-Томсона. Ослабляя затем этот свет, можно в принципе, с некоторой вероятностью получить состояния типа смеси вакуумного и однофотонного фоковского:

$$\psi = |vac\rangle + |m,n\rangle, \qquad (17.10)$$

где $m+n=1$, а m и n представляют числа фотонов в двух ортогональных поляризационных модах. Хотя поляризация является непрерывно меняющейся величиной, принцип неопределенности запрещает извлечение более одного бита информации при измерении единичного фотона. Так, если свет, поляризованный вдоль оси α, направляется на поляризационный фильтр, ориентированный вдоль оси β, то отдельные фотоны проявляют дихотомность свойств и ведут себя вероятностным образом, поскольку могут быть либо пропущены с вероятностью $\cos^2(\alpha-\beta)$, либо поглощены с сопряженной вероятностью $\sin^2(\alpha-\beta)$. Детерминированность свойств отдельных фотонов, согласно такой интерпретации, возникает, лишь когда две оси параллельны (достоверное пропускание), либо скрещены (достоверное поглощение). Если же оси не перпендикулярны, так что некоторые фотоны пропускаются, то казалось бы, что можно извлечь дополнительную информацию об угле α, поместив поляроид в прошедший пучок под неким третьим углом. Однако это не так, поскольку прошедшие сквозь первый поляроид фотоны имеют определенную поляризацию β, т.е. они полностью утратили информацию о начальной поляризации α. Другой путь извлечения более одного бита информации из отдельного фотона состоит в приготовлении копий такого состояния и последующего их измерения. Однако такой путь запрещен no-cloning теоремой.

Напоминание из теории измерения (см.Лекцию 8)

Формально квантовая механика описывает внутреннее состояние системы с помощью вектора состояния ψ, имеющего единичную длину в линейном пространстве H, определенном на поле комплексных чисел (гильбертово пространство). В этом пространстве определено скалярное произведение векторов:

$$\langle\phi|\psi\rangle \equiv \sum_j \phi_j^* \psi_j\,, \qquad (17.11)$$

где символ «*» означает комплексное сопряжение. Каждое физическое измерение M, которое может быть выполнено над системой, соответствует разложению гильбертова пространства на ортогональные подпространства, причем на каждое подпространство приходится по одному результату измерений. Таким образом, число возможных исходов измерений ограничено размерностью d гильбертова пространства. Соответственно при наиболее полных измерениях гильбертово пространство раскладывается на d одномерных подпространств.

Пусть M_k является проекционным оператором в k-ое подпространство измерения M. Тогда тождественный оператор I есть просто сумма проекционных операторов:

$$I \equiv M_1 + M_2 + ... + M_k. \qquad (17.12)$$

Из определения вектора состояния известно, что если система, находящаяся в состоянии ψ, подвергается измерению M, ее поведение становится вероятностным: исход к-ого измерения описывается вероятностью $|M_k\psi|^2$, которая на векторном языке означает квадрат длины проекции вектора состояния в подпространство M_k. После измерения система переходит в новое состояние (постулат фон Неймана) $M_k\psi/|M_k\psi|$, которое является просто единичным вектором в направлении проекции старого вектора состояния в

подпространство M_k. Согласно этому постулату, измерение оставляет вектор состояния неизменным, (т.е. результат измерения является предопределенным, детерминированным) лишь, когда начальный вектор состояния лежал целиком в одном из ортогональных подпространств, характеризующих измерение.

Гильбертово пространство отдельного поляризованного фотона является двухмерным пространством (d = 2). Следовательно, поляризационное состояние фотона полностью может быть описано с помощью линейной комбинации, скажем, двух единичных векторов $r_1 = (1,0) \equiv |H\rangle$ и $r_2 = (0,1) \equiv |V\rangle$. Например, линейно поляризованный фотон под углом α к горизонтальному направлению, описывается вектором $\psi = (\cos\alpha, \sin\alpha)$. Измеряя такой фотон в вертикально-горизонтальном (лабораторном базисе) получим горизонтально поляризованный фотон с вероятностью $\cos^2\alpha$ и вертикально поляризованный фотон с вероятностью $\sin^2\alpha$. В этом смысле два вектора r_1 и r_2 представляют собой разложение двухмерного гильбертова пространства в два ортогональных одномерных пространства. Эти два вектора будем назвать *линейным прямоугольным базисом*.
Альтернативным базисом того же гильбертова пространства является т.н. диагональный базис, образованный векторами $d_1 = 1/\sqrt{2}\,(1,1) \equiv |+45^0\rangle$ и $d_2 = 1/\sqrt{2}\,(1,-1) \equiv |-45^0\rangle$.

Определение. Вообще, два (рассмотренных) базиса называются ***сопряженными (conjugated, mutually unbiased)***, если каждый вектор одного базиса имеет проекции одинаковой длины на все вектора другого базиса. Это означает, что система, приготовленная в некоем состоянии, представленном векторами одного базиса, будет вести себя совершенно случайным образом (потеряет всю запасенную информацию) будучи измеренной в сопряженном базисе. Математически это требование записывается как

$$\left|\langle \varphi_i | \psi_j \rangle\right|^2 = \frac{1}{2} \qquad (17.*)$$

Вообще же, в знаменателе выражения (*) должна стоять размерность гильбертова пространства.
Говоря о двухмерном гильбертовом пространстве, необходимо отметить, что существует третий базис, сопряженный линейному и диагональному – т.н. циркулярный базис, образованный право- и лево-циркулярно поляризациями: $c_1 = 1/\sqrt{2}\,(i,1) \equiv |R\rangle$, $c_2 = 1/\sqrt{2}\,(1,i) \equiv |L\rangle$. Однако для описание протокола распределения ключа нам потребуются лишь первые два базиса.

Описание протокола распределение ключа.
В традиционных протоколах с открытым ключом используются односторонние функции с секретом (повторное дискретное возведение в степень) без предварительного распределения секретной информации между пользователями. В квантовом протоколе квантовый канал используется для передачи некоторого массива случайных битов квантовых информации (кубитов), открытый канал – для обсуждения, см. табл.1.

- Вводится синхронизация между действиями Алисы и Боба, т.е. каждый из них знает наверняка, в какой момент времени посылается состояние;

- Алиса выбирает случайный массив битов (чередование 0 или 1 в моменты, оговоренные синхронизационным протоколом);
- Алиса выбирает случайную последовательность (поляризационных) базисов – чередование либо линейного, либо диагонального (L, D);
- Алиса посылает Бобу последовательность фотонов, кодируя поляризацию каждого фотона, исходя из массива битов и поляризационного базиса: каждый фотон имеет определенную поляризацию и описывается одним из четырех базисных векторов $r_{1,2}, d_{1,2}$. Будем полагать, что значение бита «0» отвечает за состояния $|H\rangle, |+45^0\rangle$, а «1» – за состояния $|V\rangle, |-45^0\rangle$;
- Боб принимает (измеряет) посланные Алисой фотоны в одном из двух базисов. Причем выбор базиса – случаен. Боб интерпретирует результаты своих измерений в бинарном представлении, т.е. пользуясь тем же правилом, что и Алиса: «0» $\rightarrow |H\rangle, |+45^0\rangle$ и «1» $\rightarrow |V\rangle, |-45^0\rangle$. Заметим, что как следует из теории измерений, Боб полностью теряет информацию о состоянии фотона, поляризованного в лабораторном базисе (*H*-*V*), измеряя его в диагональном базисе (+45-45) и наоборот. Следовательно, Боб получает достоверную информацию о состоянии фотонов только в половине всех случаев – когда выбранный им базис совпал с базисом Алисы, т.е. когда измерение дает детерминированный результат. Если подслушивания не было, то в оставшейся половине случаев Алиса и Боб имеют некоррелировынные результаты. Следовательно, в среднем, Боб получает массив битов с 25%-ым содержанием ошибок. Этот массив называется ***сырым ключом***. Кроме того, будем учитывать тот факт, что часть фотонов теряется при передаче. Практически, уровень технических ошибок в квантовых протоколах на сегодняшний день составляет несколько процентов (в отличие от уровня 10^{-9}, достижимого в современных оптотелекоммуникационных линиях связи). Этот уровень называется Quantum Bit Error Rate (QBER).
- Происходит обсуждение результатов измерений по открытому каналу связи, причем и Алиса и Боб предполагают, что их могут подслушать, но не перехватить или изменить результаты. Сперва, они определяют, какие из фотонов были зарегистрированы Бобом. Затем, определяют, в каких случаях Боб угадал базис. Боб сообщает базис, в котором производилось измерение, но не сообщает сам результат. При этом теряется 50% информации – когда Боб неверно угадал базис. ***Если сообщение не подслушивалось, то Алиса и Боб делают вывод, что биты, закодированные этими фотонами, переданы правильно***. Заметим, что по открытому каналу информация о случайной последовательности битов, посылаемых Алисой, не передается – вывод делается только на основе теории квантовых измерений! Каждый из переданных таким образом фотонов в правильном базисе несет один бит информации, а именно был ли он поляризован вертикально или горизонтально в лабораторном базисе или под углами плюс-минус 45 град. - в диагональном базисе. В итоге у Боба остается более короткий массив битов, который называется ***просеянным ключом***.

Затем, Алиса и Боб проверяют, были ли попытки подслушивания во время распределения ключа. Для этого они сравнивают некоторые биты, которые, как они считают, были распределены правильно, по открытому каналу связи. Позиции битов по шкале синхронизационного протокола, должны выбираться

случайно, скажем, сравнивая каждый третий бит. В этом случае обнаружение подслушивания имеет высокую вероятность и состоит в том, что Алиса и Боб имеют разные биты. Если сравнение не обнаруживает разницы, то Алиса и Боб делают вывод, что распределение ключа произошло с высокой степенью надежности (все же имеется вероятность не обнаружить подслушивания, но при этом, у подслушивателя окажется мало информации).

Последний шаг протокола квантовой криптографии состоит в том, чтобы используя классические алгоритмы, ***исправить ошибки*** и уменьшить информацию, доступную Еве. Последняя процедура называется ***усилением секретности*** (privacy amplification). Простейшая *процедура коррекции ошибок* состоит в следующем. Алиса случайно выбирает пары битов и производит над ними операцию XOR. Боб выполняет такую же операцию над соответствующими своими битами. Если результат совпадает, они сохраняют первый из двух битов и уничтожают второй – поскольку сама процедура происходит по открытому каналу и результат доступен Еве. Если результаты отличаются – оба бита выкидываются (на практике используется более сложный алгоритм). После этой процедуры Алиса и Боб имеют одинаковые копии ключа, но у Евы все же может остаться некоторая информация о нем. Возникает необходимость в ее уменьшении – вступает в силу *протоколы усиления секретности*. Эти классические протоколы работают следующим образом. Алиса опять выбирает случайно пары битов и вычисляет их сумму по модулю 2 (XOR). Но в отличие от процедуры коррекции ошибок, она не сообщает это значение. Она лишь оглашает какие биты были выбраны, например, 103 и 539. Затем Алиса и Боб заменяют два бита на результат операции XOR. Таким образом Алиса и Боб укорачивают их ключи. Если Еве доступна лишь часть информации о двух битах, то ее информация о результате выполнения операции XOR будет еще меньше. Рассмотрим, например, случай, когда Еве известен только первый бит и ничего не известно про второй. Тогда она вообще ничего не знает про результат операции XOR. Если же Ева знает значения каждого из битов с вероятностью, скажем, 60%, то вероятность того, что она угадает значение операции XOR будет только $0.6^2 + 0.4^2 = 52\%$ (сумма вероятностей того, что оба бита угатаны неправильно и правильно, соответственно). Такую процедуру можно повторить несколько раз. Подчеркнем, что на этих этапах (выполнения протоколов коррекции ошибок и усиления секретности) работают исключительно классические протоколы, использующие открытые каналы связи. Итак, если вероятность ошибок не превосходит некоторой критической величины (в нерелятивистских схемах предел, по-видимому, составляет < 11% [11-13]что определяется потерями в оптическом волокне), то далее возможна коррекция ошибок в нераскрытой части при помощи классических кодов и дальнейшее сжатие ключа (privacy amplification) для получение результирующего секретного ключа.

- Включается абсолютно стойкий протокол одноразового блокнота через открытый канал связи.
- Весь протокол повторяется каждый раз при необходимости посылки очередного сообщения.

Заметим, что на практике для передачи квантовых битов и обмена классическими сообщениями можно использовать один и тот же канал связи.

Замечание. Потери оптического волокна в окнах телеком составляют примерно: 1.55 мкм 0.2 дБ/км ($0.2=10\lg I_2/I_1$, $I_2/I_1=1.047$); 1.31 мкм 0.35 дБ/км;

0.8 мкм 2 дБ/км.

Подслушивание в протоколе BB84

Из-за того, что по квантовому каналу передается случайная смесь двух базисов, любая попытка подслушивания приводит к риску изменения поляризационного состояния фотона. Это приведет к различию в значениях битов Алисы и Боба, если измерения проводились в совпадающих базисах. Например, в некотором смысле, оптимальная стратегия подслушивания состоит в том, что Ева перехватывает все фотоны в квантовом канале, производит свои измерения только в одном из двух базисов (или вообще, только в одном) и ретранслирует исходы (т.н. ***стратегия перехватчик-ретранслятор***). Затем она пересылает Бобу (ретранслирует) другой кубит в состоянии, соответствующем результату ее измерения. Это не противоречит теореме о запрете копирования. В половине всех случаев Ева правильно угадает базис и, следовательно, Алиса-Боб не распознают ее присутствие. Однако, в другой половине случаев Ева неверно угадывает базис, поэтому она перешлет Бобу правильный кубит лишь в с вероятностью 50% (mutially unbiased bases). Этот кубит будет обнаружен Алисой-Бобом, в половине от этого числа случаев, т.к. они получат некоррелированные результаты (выявляется в протоколе коррекции ошибок). В итоге при использовании этой стратегии, Ева получает 50% информации - в случае угадывания базиса - в то время как Алиса-Боб получают 25% ошибочных битов в просеянном ключе, т.е. после выкидывания исходов в неправильных базисах. Этот случай подслушивания легко регистрируется. В другом варианте этой стратегии подслушивания Ева применяет ее только к каждому десятому биту. В этом случае она получает доступ к 5 процентам информации, в то время как Алиса и Боб обнаруживают 2.5%. Заметим, что рассмотренный случай ***активного подслушивателя в квантовом канале*** не взламывает протокола.

- Вообще, анализируя ситуацию на этапе, когда Алиса и Боб имеют просеянный ключ и учитывая возможное присутствие Евы, можно сказать, что существует некоторая корреляция между классической информацией, доступной легитимным пользователям (Алисе и Бобу) и подслушивателем – Евой. Такая ситуация типична для классических криптографических протоколов. Чтобы анализировать ее количественно, вводится функция распределения $P(\alpha,\beta,\varepsilon)$, где все участники протокола – Алиса Боб и Ева описываются случайными параметрами α,β,ε, соответственно. Предположим, что такое совместное распределение вероятностей $P(\alpha,\beta,\varepsilon)$ (классическое) существует. При этом Алиса и Боб обладают лишь маргинальным распределением $P(\alpha,\beta)$. Задача состоит в том, чтобы ограничить доступную Еве информацию. Для данного распределения $P(\alpha,\beta,\varepsilon)$ пока неизвестен критерий, дающий секретный ключ, распределенный между Алисой и Бобом или $S(\alpha,\beta\square\varepsilon)$ - условная энтропия. Однако существует некая граничная мера даваемая разностью между взаимной шенноновской информацией Алисы и Боба $I(\alpha,\beta)$ и взаимной информацией Евы $I(\alpha,\varepsilon);I(\beta,\varepsilon)$:

$$S(\alpha,\beta\square\varepsilon)\geq\max\left\{I(\alpha,\beta)-I(\alpha,\varepsilon),I(\alpha,\beta)-I(\beta,\varepsilon)\right\}. \qquad (17.13)$$

Эта оценка показывает, что ***установление секретного ключа возможно, если Боб обладает большей информацией, чем Ева***!
В приведенной только что аргументации есть слабое звено – мы предполагали, что Ева выполняет атаку до того, как Алиса и Боб включили процедуру коррекции ошибок. Формально это означает, что совместное распределение $P(\alpha,\beta,\varepsilon)$ существует. Однако Ева может дождаться окончания протокола коррекции ошибок и только затем провести атаку. Такой вид атак называется «***стратегией задержанного выбора***»
Для нейтрализации ***активного подслушивателя в открытом канале*** можно воспользоваться схемой аутентификации Вегмана-Картера. В этой схеме Алиса и Боб должны изначально иметь небольшой секретный ключ, установленный, например, при личной встрече. С помощью такого ключа устанавливается нечто вроде «контрольной суммы» или метки, зависящей от каждого бита сообщения. Подслушиватель, который не знает ключа, имеет низкую вероятность сгенерировать правильную метку. Таким образом, метка устанавливает легитимность сообщения, а ее изменение указывает на попытку подслушивания.

Рассмотренный протокол BB84 является типичным и иллюстрирует основные принципы квантового распределения ключа. На его примере мы также рассмотрели некоторые протоколы коррекции ошибок, усиления секретности и стратегии подслушивателя. Рассмотрим некоторые другие протоколы квантовой криптографии.
Замечание. К очевидным недостаткам квантового распределения ключа следует отнести чисто практическую сложность их реализации. Квантовые состояния очень хрупки и подвержены сильному влиянию окружения, кроме того, они не могут быть усилены (простыми способами). Говоря о криптографических приложениях, пока не ясно как осуществить цифровую подпись или ability to settle disputes before judge.

ÏÐÎÒÎÊÎË Â92 [7]

Рассуждения, приведенные выше, основывались на том факте, что любое измерение неортогональных состояний, которое не возмущает их, в то же время не дает о них никакой информации (т.е. информации, позволяющей различить их). В 1992 году Ч.Беннет и Ж.Брассард предложили протокол распределения ключа, основанный на передаче только *двух неортогональных состояний* квантовой системы вместо четырех.
Рассмотрим два неортогональных состояния $|u_0\rangle$ и $|u_1\rangle$, таких, что $\langle u_0|u_1\rangle \neq 0$. Пусть $P_1 = 1-|u_0\rangle\langle u_0|$ и $P_0 = 1-|u_1\rangle\langle u_1|$ - два проектора в подпространства ортогональные состояниям $|u_0\rangle$ и $|u_1\rangle$, соответственно. Заметим, что эти два оператора не коммутируют и что их индексы переставлены по отношению к соответствующим состояниям. Нетрудно убедиться, что оператор P_0 уничтожает состояние $|u_1\rangle$:

$$P_0|u_1\rangle = (1-|u_1\rangle\langle u_1|)|u_1\rangle = |u_1\rangle - |u_1\rangle \equiv 0, \qquad (17.14)$$

но дает ненулевой результат при действии на $|u_0\rangle$:

$$P_0|u_0\rangle = (1-|u_1\rangle\langle u_1|)|u_0\rangle = |u_0\rangle - |u_1\rangle\langle u_1|u_0\rangle;\ \to W = 1-|\langle u_0|u_1\rangle|^2 > 0. \qquad (17.15)$$

В последнем соотношении фигурирует величина $W = \left(P_0 \left|u_0\right\rangle\right)^* P_0 \left|u_0\right\rangle$ - вероятность ненулевого исхода. Аналогичные соотношения справедливы и для оператораP_1.

Распределение ключей происходит следующим образом.

1. Устанавливается синхронизация моментов посылки состояний.
2. Алиса приготавливает и посылает Бобу случайную бинарную последовательность квантовых состояний $\left|u_0\right\rangle$ и $\left|u_1\right\rangle$, где, например, $\left|u_0\right\rangle \to 0$, а $\left|u_1\right\rangle \to 1$.
3. Боб, независимо от Алисы, случайным образом решает, какой из двух операторов P_0 или P_1 применить к полученной последовательности состояний.
4. Затем Боб по открытому каналу сообщает Алисе номера синхронизационной шкалы, для которых он получил положительный результат. При этом он не сообщает, какой из двух операторов он использовал. Остальные события игнорируются
5. Если подслушивания не было, то оставленные события, составляющие приблизительно, $\left(1-\left|\left\langle u_0 \middle| u_1\right\rangle\right|^2\right)\Big/2$ -ую часть от общего числа испытаний, должны быть коррелированы. Заметим, что для поляризационного кодирования состояний “0º”и “45º”эта величина равна 1/2. Таким образом, если Алиса посылала $\left|u_0\right\rangle$, а Боб измерял P_0, если Алиса посылала $\left|u_1\right\rangle$, то Боб измерял P_1.
6. Перед тем, как Алиса и Боб установят секретный ключ, они должны провести процедуру коррекции ошибок и усиления секретности, действуя, например, так же как и в протоколе BB84. Жертвуя некоторыми битами, они убеждаются в идентичности некоторого их числа. Протокол иллюстрируется в таблице 2.

Итак, наше базовое предположение о невозможности извлечения однозначной информации об неортогональных состояниях без их возмущения, позволило ввести более простой, по сравнению с BB84, протокол. Однако, на практике, реализация такого протокола не нашла широкого применения. Дело в том, что все-таки существуют способы различимости двух неортогональных состояний, ценой некоторых потерь. Идея и соответствующие демонстрационные эксперименты основаны на том, что измерение, выполняемое в базисе, ортогональном, например, состоянию $\left|u_0\right\rangle$, однозначно выделяет такое состояние, в том смысле, что только состояние $\left|\updownarrow\right\rangle$ не пройдет через поляроид, ориентированный горизонтально. Другое же состояние $\left|\square\right\rangle$ пройдет через горизонтальный поляроид с 50%-ми потерями.

ЭПР-ПРОТОКОЛ [6]

В 1991 году А.Экерт предложил протокол основанный на перепутанных состояниях. Впоследствии оказалось, что этот протокол является разновидностью BB84, однако в обзорах по квантовым способам распределения ключа, как правило, он фигурирует отдельно. Примечательно также, что казалось бы, абсолютно умозрительные рассуждения, приведшие Эйнштейна, Подольского и Розена к их известному парадоксу, а также идеи, высказанные Дж.Беллом, все-таки нашли свое практическое воплощение. Сам А.Экерт, формулируя суть протокола, отмечал, что здесь «распределение ключа зависит

от полноты квантовой механики». Под полнотой понимается тот факт, что квантовое описание обеспечивает максимально возможную информацию о рассматриваемой системе. Экспериментальная реализация рассматриваемого протокола, во всяком случае в принципиальном смысле, мало отличается от установок по наблюдению нарушения неравенств Белла. Можно сказать, что при распределении ключа вводится квантовый канал, где сам ключ существует без какого-либо «элемента реальности», связанного с этим ключом. В этом смысле он защищен полнотой квантовой механики.

Канал состоит из источника перепутанных фотонов, находящихся в синглетном состоянии. Частицы разлетаются вдоль оси *z* в направлениях к легитимным пользователям – Алисе и Бобу. Каждый из них получает по одной частице или половинке перепутанной пары. Затем Алиса и Боб выполняют измерение над свой частицей, ориентируя поляризационные призмы вдоль трех направлений: для Алисы – a_i, для Боба – b_j (*i, j = 1, 2, 3*). Конкретно, измеряя углы от вертикальной оси[1]:

$$\phi_1^a = 0,\ \phi_2^a = \frac{\pi}{4},\ \phi_3^a = \frac{\pi}{2}; \tag{17.16}$$

$$\phi_1^b = \frac{\pi}{4},\ \phi_2^b = \frac{\pi}{2},\ \phi_3^b = \frac{3\pi}{4}. \tag{17.17}$$

Алиса и Боб выбирают ориентацию призм случайно и независимо друг от друга для каждой пары перепутанных частиц. Каждое измерение дает результат либо +1, либо –1, т.е. срабатывает один из двух детекторов, установленных в выходных модах поляризационной призмы Алисы и Боба. Параметризованный таким образом сигнал представляет один (для одной частицы) бит информации.

Далее измеряется корреляция между парами детекторов Алисы и Боба, чтобы сформировать величину:

$$E\left(a_i, b_j\right) = P_{++}\left(a_i, b_j\right) + P_{--}\left(a_i, b_j\right) - P_{+-}\left(a_i, b_j\right) - P_{-+}\left(a_i, b_j\right), \tag{17.18}$$

где аргументы в корреляционных функциях *P* означают выбранное направление. Например, $P_{-+}\left(a_i, b_j\right)$ означает вероятность того, что при данных установках поляризационных призм a_i, b_j Алиса получила результат «-1», а Боб «+1». Можно показать, что величина *E* принимает значения

$$E\left(\phi_i^a, \phi_j^b\right) = -\cos\left(\phi_i^a - \phi_j^b\right). \tag{17.19}$$

Для двух пар одинаковых ориентаций анализаторов (поляризационных призм) $\left(\phi_1^a, \phi_1^b\right); \left(\phi_3^a, \phi_3^b\right)$ квантово-механические предсказания дают полную антикорреляцию результатов, полученных Алисой и Бобом:

$$E\left(a_1, b_1\right) = E\left(a_3, b_3\right) = -1.$$

Следуя Клаузеру, Хорну, Шимони и Хольту можно ввести наблюдаемую величину - наблюдаемую Белла, составленную из корреляционных коэффициентов (17.18):

$$S = E\left(a_1, b_3\right) + E\left(a_1, b_2\right) + E\left(a_2, b_3\right) - E\left(a_2, b_2\right), \tag{17.20}$$

которая равна

$$S = -2\sqrt{2}. \tag{17.21}$$

После того, как перепутанные частицы поступили к Алисе и Бобу, те могут объявить по открытому каналу связи ориентации анализаторов, которые были

[1] Эти наборы значений углов не являются единственными.

выбраны случайным образом при каждом измерении. Затем, результаты измерений разделяются на две группы. К первой группе относятся результаты, полученные при разных ориентациях анализаторов, т.е., приводящие к (21). Ко второй – при одинаковых. Не учитываются те результаты, когда частица Алисы или Боба по каким-то причинам не была зарегистрирована вообще. Затем Алиса и Боб сообщают результат, который они получили только для первой группы измерений. Это позволяет им установить то значение S, которое для невозмущенных состояний частиц должно оказаться равным (21). В свою очередь последнее утверждение дает основание легитимным пользователям считать, что результаты, относящиеся ко второй группе измерений, антикоррелированы и могут быть преобразованы в секретный набор битов – *сырой ключ*.

Подслушиватель не может воспользоваться информацией, перехватывая перепутанные частицы, поскольку самой информации там нет. Считается, что она появляется в результате измерений, выполняемых Алисой. По Экерту измерение Алисы приготавливает состояние частицы Боба, хотя более последовательно было бы утверждать, что эта информация закодирована в корреляционных функциях P и величине E.

ËÈÒÅÐÀÒÓÐÀ

[1] W. Diffie and M.E. Hellman, IEEE Trans. Inf. Theory IT-22, 644 (1977).

[2] R. Rivest, A. Shamir, and L. Adleman, *"On Digital Signatures and Public-Key Cryptosystems"*, MIT Laboratory for Computer Science, Technical Report, MIT/LCS/TR-212 (January 1979).

[3] P.W. Shor, *Proceedings of the 35th Annual Symposium on the Foundations of Computer Science* (IEEE Computer Society, Los Alamos, CA, 1994) p. 124.

[4] C.H. Bennett, G. Brassard, and A.K. Ekert, *"Quantum cryptography"*, Scientific American, October 1992, p. 50.

[5] S. Wiesner, SIGACT News **15**, 78 (1983); original manuscript written circa 1970. C.H. Bennett and G. Brassard, in "Proc. IEEE Int. Conference on Computers, Systems and Signal Processing", IEEE, New York (1984). C.H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography," J. Cryptology **5**, 3 (1992).

[6] A.K. Ekert, Phys. Rev. Lett. **67**, 661 (1991); A.K. Ekert, J.G. Rarity, P.R. Tapster, and G.M. Palma, Phys. Rev. Lett. **69**, 1293 (1992).

[7] C.H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).

[8] A. Muller, J. Breguet, and N. Gisin, Europhys. Lett. **23**, 383 (1993).

[9] P.R. Tapster, J.G. Rarity and P.C.M. Owens, Phys. Rev. Lett. **73**, 1923 (1994).

[10] P D. Townsend, J.G. Rarity, and P.R. Tapster, Electron. Lett. **29**, 1291 (1993).

[11] D.Mayers, A.Yao, Unconditional Security in Quantum Cryptography, quant-ph/9802025.

[12] E.Biham, M.Boyer, P.O.Boykin, T.Mor, V.Roychowdhury, A Proof of the Security of Quantum Key Distribution, quant-ph/9912053.

[13] P.W.Shor, J.Preskill, Simple Proof of Security of the BB84 Quantum Key Distribution Protocol, quant-ph/0003004.

ЛЕКЦИЯ 18. КВАНТОВАЯ КРИПТОГРАФИЯ (ПРОДОЛЖЕНИЕ).

1. Как приготовить квантовые состояния. Ослабленные лазерные импульсы. Оценка однофотонного состояния при ослаблении импульса когерентного поля. Двухфотонные импульсы.
2. Способы кодирования квантовых состояний.

2.1. Кодирование поляризации. Оптические волокна, сохраняющие поляризацию.

2.2. Фазовая кодировка. Фарадеевское зеркало. Ротатор. Циркулятор. Система “Plug&Play”.

2.3. Кодирование по частоте.

3. Протокол А.Экерта (ЭПР- протокол)
4. Подслушивание в квантовой криптографии. Суть проблемы. Безусловная и практическая стойкость.

4.1. Индивидуальные (некогерентные) атаки. Стратегия передатчик-ретранслятор. Стратегия «промежуточного базиса». Симметричные индивидуальные атаки. Оценка максимальной взаимной информации Алиса и Боба, Алисы и Евы при односторонних сообщениях. Критерий стойкости для протокола BB84.

4.2. Когерентные атаки. Коллективные атаки.

4.3. Атаки класса «Троянский конь».

4.4. Атаки с помощью светоделителя.

Как приготовить квантовые состояния в криптографии.

Прежде, чем перейти к обсуждению различных видов криптографических атак, рассмотрим проблемы, связанные с генерацией квантовых состояний, используемых при квантовом распределении ключа. В рассмотренных трех протоколах использовались одно- и двухфотонные фоковские состояния света. Такие состояния, практически очень трудно получить экспериментально, хотя в последнее время появились сообщения о их генерации в квантовых точках (т.н. *фотонные пушки*, когда система испускает только один фотон и не может испустить два – антигруппировка фотонов). На сегодняшний день практическим источником однофотонных состояний служат ослабленные лазерные импульсы или коррелированные пары фотонов. Число единичных фотонов, либо пар фотонов в импульсе распределено по закону Пуассона. Поэтому имеется некая вероятность того, что в импульсе находится более одного фотона (или более одной пары фотонов). Эти избыточные фотоны могут, в принципе, быть использованы подслушивателем для извлечения информации о передаваемом ключе. Под импульсом будем понимать то фиксированное время, в течение которого должен прийти фотон (пара фотонов).

1. Ослабленные лазерные импульсы.

Наиболее простое решение проблемы приготовления однофотонных фоковских состояний – это ослабление лазерных импульсов, поле которых находится в когерентном состоянии со средним числом фотонов N. Вероятность найти n фотонов в таком когерентном состоянии описывается распределением Пуассона:

$$P(n,N)=\frac{N^n}{n!}e^{-N} \qquad (18.1)$$

Соответственно, вероятность того, что в (когерентном) не пустом (т.е. с $n\neq 0$) импульсе содержится более одного фотона, равна

$$P(n>1\,|\,n>0,N)=\frac{1-P(0,N)-P(1,N)}{1-P(0,N)}=\frac{1-\left[N^{0}e^{-N}/0!\right]-N^{1}e^{-N}/1!}{\left[N^{0}e^{-N}/0!\right]}= \qquad (18.2)$$

$$\frac{1-e^{-N}(1+N)}{1-e^{-N}}\approx N/2$$

Эта вероятность может быть сделана произвольно малой при уменьшении N. Однако в этом случае большинство импульсов окажется пустым! Действительно, при малых N

$$P(n=0)=\frac{N^0}{0!}e^{-N}=e^{-N}\to 1-N\,. \qquad (18.3)$$

Наличие пустых импульсов уменьшает скорость передачи битов, поскольку такие импульсы следует отбросить в протоколе, они не несут информации. Уменьшение скорости обмена битами может быть компенсировано увеличением частоты повторения импульсов. В настоящее время в телекоммуникационных схемах используется частота порядка ГГц. Однако на практике возникает другая серьезная проблема – темновые отсчеты детекторов. Сейчас используются индий-галиевые полупроводниковые детекторы на длинах волн телекоммуникационной связи (ИК-диапазон), которые обладают высоким темновым шумом. Поэтому детекторы стробируются – включаются чуть раньше прихода несущего информацию импульса, а выключаются чуть позже. Ясно, что увеличение частоты повторения импульсов приводит к увеличению доли темновых импульсов, поэтому нужен некий оптимум. Практически – это уровень в несколько МГц. Используется уровень приблизительно N = 0.1. Из (2) следует, что 5% непустых импульсов содержит больше одного фотона – эти события определяют уровень ошибок.

Генерация двухфотонных импульсов в процессе СПР.

В другом способе получения псевдо-однофотонных состояний состоит в использовании пар фотонов, генерируемых при СПР. Один фотон при этом рассматривается как триггер для другого – т.н. генератор известного числа фотонов. Второй детектор активизируется только после того, как первый детектор регистрирует фотон, поэтому, по определению, N = 1. Хотя в процессе СПР пары излучаются в случайные моменты времени, синхронизационная шкала теперь задается (например, сигнальными) фотонами, давшими отсчет в первом детекторе. В типичных нелинейных кристаллах при мощности накачки 1 мВт удается получить около миллиона пар в секунду в одной пространственно-частотной моде (имеется в виду одномодовый световод сечением несколько микрометров). Соответственно, при использовании временного окна около 1 нсек условная вероятность зарегистрировать второй фотон из другой пары оказывается $10^6\times10^{-9}\approx10^{-3}=0.1\%$. Окно выбрано из соображений временного разрешения детектора. Оказывается, что такой способ генерации однофотонных состояний выгоднее описанного выше (при ослаблении лазерных импульсов), поскольку чтобы получить такое же среднее число ослабленных фотонов нужно использовать более высокую частоту повторения импульсов.

Говоря о практических реализациях КК, следует выделить <u>три основных способа кодирования.</u>

1. ***Кодирование по поляризации***. Этот способ используется, в основном при передаче сообщений через открытое пространство, поскольку для передачи по волокну, необходимо использовать т.н. поляризационно-сохраняющие волокна (polarization-montaining fiber). Эти типы волокон не обеспечивают стабильного сохранения произвольного поляризационного состояния кубита из-за возникающих температурных и фазовых флуктуаций двупреломления. А именно, свет, поляризованный вдоль одной из главной оси такого волокна, останется поляризованный в этом направлении и на выходе. Однако, например, линейно поляризованный свет под углом 45 градусов к главной оси окажется поляризованным произвольно, из-за флуктуаций относительной фазы между двумя собственными волнами, распространяющимися вдоль волокна. В этом смысле поляризационно-сохраняющее волокно похоже по своему действию на обычное одномодовое волокно. Оно сохраняет степень поляризации (конечно, имеется в виду случай, когда длина когерентности света намного превышает эффективную длину волокна)

$$L_{eff} = LD = L\left(\frac{1}{u_{fast}} - \frac{1}{u_{slow}}\right), \qquad (18.4)$$

т.е. линейно поляризованный свет на входе в обычное волокно станет в общем случае поляризованным эллиптически на выходе, а положение точки, изображающей состояние поляризации на сфере Пуанкаре, будет флуктуировать. Состояние поляризации на выходе можно сделать любым, пространственно конфигурируя участки волокна. Наиболее часто встречается метод скручивания куски волокна в петли. Число витков в петле устанавливает оптическую разность хода δ, а ориентация петли в пространстве – углу поворота пластинки. Следовательно, две-три петли (пластинки $\lambda/4, \lambda/2, \lambda/4$) могут сформировать любое чистое поляризационное состояние на выходе волокна, но это состояние подвержено сильным флуктуациям.

2. ***Кодирование по фазе***. Такой способ впервые был предложен Беннетом в его работе, описывающей протокол B92. Именно такой способ в настоящее время нашел практическое воплощение. Он основан на использовании двухплечевого интерферометра Маха-Цандера. Интерферометр выполнен на оптическом волокне и включает в себя два симмметричных смесителя (аналог светоделителя). В одном из плеч помещается фазовый модулятор. Разность длин плеч должна быть меньше длины когерентности. Учитывая сдвиг фаз на 90 град. при отражении от светоделителя, набеги фаз в фазовых модуляторах Алисы и Боба, а также фиксированный набег фаз из-за разницы длин плеч, можно вычислить интенсивность в выходной моде «0» станции Боба (см. Рис. 1):

$$I_0 = \overline{I}\cos^2\left(\frac{\phi_A - \phi_B + k\Delta L}{2}\right), \qquad (18.5)$$

где $k = \frac{2\pi}{\lambda}$ – волновое число, а $\overline{I}$ - средняя интенсивность источника света. Если аргумент косинуса равен $\pi/2 + \pi n$, n – целое, то в этой моде наблюдается деструктивная интерференция – весь свет направляется в моду «1». Если же аргумент косинуса равен πn, то весь свет направляется в моду «0». При промежуточных фазовых сдвигах свет регистрируется в обеих модах. Устройство в целом работает как оптический переключатель, причем важно поддерживать разность хода постоянной для наблюдения стабильной интерференции. На вход интерферометра подаются однофотонные состояния, полученные в одном из описанных выше методов. При реализации протокола BB84 Алиса кодирует фазу четырьмя способами – прикладывая сдвиг фаз $\phi_A = (0, \pi/2, \pi, 3\pi/2)$. Соответственно, она кодирует состояние «0» фазами $(0, \pi/2)$, «1» – фазами $(\pi, 3\pi/2)$. Со своей стороны, Боб осуществляет выбор базиса, вводя фазовую задержку 0, либо $\pi/2$. Кроме того, он отождествляет детектор, стоящий в моде «0» с значением бита «0», а моду «1» с битом «1». Если разность фаз равна 0 или π, то Алиса и боб использовали совместные базисы, следовательно, они получают детерминированные результаты. В этих случаях Алиса может предсказать результат Боба (значение бита или выходную моду светоделителя Боба) в зависимости от фазового сдвига, который она приложила. Если же разность фаз равна $\pi/2$ либо $3\pi/2$,то базисы несовместны, следовательно, фотон в станции Боба может с равной вероятностью попасть в любую моду. Полностью протокол BB84 при фазовой кодировке приводится в таблце1. На практике, удобнее использовать другую схему – два разбалансированных интерферометра Маха-Цандера. Это вызвано, прежде всего, тем, что необходимо поддерживать разность плеч постоянной, что трудно выполнимо на больших расстояниях. Схема показана на Рис.2. Нетрудно заметить, что временная функция распределения отсчетов в станции Боба будет содержать три пика. Первый соответствует тому, что и у Алисы и у Боба фотоны пошли через короткое плечо. Третий пик отвечает случаю, когда фотоны «выбрали» длинные пути. И, наконец,

центральный пик соответствует ситуации, когда фотон Алисы пошел по короткому пути, а фотон Боба – по длинному, либо наоборот. Эти две последние ситуации неразличимы. Физически это значит, что разность длин плеч интерферометра Алисы должна быть такой же, как и у Боба, с точностью до длины когерентности света (реально – это несколько миллиметров). Такая схема гораздо более стабильна, здесь, как бы обе «половинки» фотона распространяются по одному и тому же пути. Однако остается проблема температурной стабилизации обоих интерферометров. ***Эта проблема является общей для обоих рассмотренных методов – поляризационного и фазового кодирования. Для ее решения необходима схема активной компенсации флуктуаций разности длин оптических плеч.***

Простое решение проблемы состоит в том, чтобы иногда запускать в систему относительно интенсивные лазерные импульсы с N>>1, чтобы производить коррекцию фазовых или поляризационных искажений. Такие импульсы можно чередовать со слабыми, квантовыми.

Другой подход предусматривает пассивную компенсацию поляризационных флуктуаций в волокне. Такая схема включает в себя т.н. фарадеевское зеркало. Это зеркало состоит из 45-градусного ротатора Фарадея и обычного 180-градусного зеркала. Ротатор Фарадея поворачивает поляризацию на сфере Пуанкаре на 90 градусов вокруг полярной оси (соединяющей южный и северный полюса). Специфика такого преобразования состоит в том, что направление вращения не зависит от направления распространения света. Значит, проходя через ротатор в прямом, а затем, в обратном направлении, поляризационное преобразование описывается одним и тем же оператором. Соответствующее поляризационное преобразование описывается матрицей

$$R=\begin{pmatrix}\cos\delta & \sin\delta\\ -\sin\delta & \cos\delta\end{pmatrix}=\left\{\delta=\frac{\pi}{4}\right\}=\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ -1 & 1\end{pmatrix}, \qquad (18.6)$$

Отражение от обычного зеркала наглядно представляется отражением относительно экваториальной плоскости, как будто бы северный и южный полюс меняются местами:

$$M\begin{pmatrix}\alpha\\ \beta\end{pmatrix}\to\begin{pmatrix}\alpha^*\\ \beta^*\end{pmatrix}. \qquad (18.7)$$

Следовательно, общий эффект, вызванный фарадеевским зеркалом, состоит в преобразовании исходного состояния в ортогональное:

$$RMR\psi^{in}=RMR\begin{pmatrix}\alpha\\ \beta\end{pmatrix}=RM\begin{pmatrix}\alpha+\beta\\ \beta-\alpha\end{pmatrix}\to R\begin{pmatrix}\alpha^*+\beta^*\\ \beta^*-\alpha^*\end{pmatrix}\to$$
$$\begin{pmatrix}\alpha^*+\beta^*+\beta^*-\alpha^*\\ -\alpha^*-\beta^*+\beta^*-\alpha^*\end{pmatrix}\to\begin{pmatrix}\beta^*\\ -\alpha^*\end{pmatrix}=\psi^{out}. \qquad (18.8)$$

Нетрудно убедиться, что конечное состояние ортогонально начальному, т.е.

$$\left\langle\psi^{out}\middle|\psi^{in}\right\rangle=0. \qquad (18.9)$$

Ясно, что произвольное поляризационное преобразование, совершаемое волокном, на конце которого установлено фарадеевское зеркало, сводится к тому, что свет, прошедший по пути: волокно - фарадеевское зеркало – то же волокно, окажется в ортогональном состоянии (Рис.3):

$$\left[U^{-1}RMRU\right]\psi=\left[RMR\right]\psi\to\psi_{\perp}. \qquad (18.10)$$

Криптографическая система, основанная на кодированном по фазе протоколе BB84 и использующая двойное прохождение света через одно и то же волокно, снабженная фарадеевским зеркалом, получила название “Plug&Play”, поскольку в ней автоматически корректируются фазовые искажения, возникающие при распространении поляризованного света через волокно. Такая схема была реализована в университете Женевы в 1997 году. С ее помощью было продемонстрировано квантовое распределение ключа на расстоянии 23

км. Такая схема лежит в основе единственного, на сегодняшний день, коммерческого криптографического устройства, поэтому ее работа заслуживает детального анализа.
Основные этапы работы схемы состоят в следующем (рис.4).

Общая идея.

В станции Боба находится лазерный диод, излучающий световые импульсы во втором окне telecom 1300нм[1]. Импульс может пройти либо по короткому плечу интерферометра Боба, либо по длинному. Если он идет по короткому пути, то, пройдя поляризационный светоделитель, оказывается поляризованным вертикально, затем его поляризация портится в длинном волокне, попадает в интерферометр Алисы, его часть отражается от фарадеевского зеркала, опять попадает в волокно, на выходе которого поляризация после автокоррекции становится горизонтальной, попадает в длинное плечо интерферометра Боба. Если исходный импульс попал в длинное плечо интерферометра Боба, то в конечном итоге он окажется в коротком плече станции Боба. Таким образом на светоделителе С1 в станции Боба возникает суперпозиция двух импульсов.
Более детальная работа всей схемы описана ниже.

Сначала рассмотрим принцип действия ***циркулятора*** (Рис.5). Циркулятор представляет собой двухплечевой интерферометр Маха-Цандера, в каждое из плеч которого помещен 45-градусный ротатор Фарадея, причем, в верхнем плече он осуществляет преобразование $H \xrightarrow{R} -45^0$, а в нижнем - $V \xrightarrow{R} +45^0$. Выходной поляризационный светоделитель ориентирован в диагональном базисе, поэтому он смешивает поляризации +45 и –45 град. без потерь, следовательно свет оказывается лишь в одной выходной моде с поляризацией +45 град. Если же теперь подать, скажем вертикально поляризованный свет в ту же выходную моду, которая теперь рассматривается как входная, то свет, разделившись на делителе, окажется поляризованным –45 град. в верхнем плече и +45 град. в нижнем. Но теперь, проходя через соответствующие фарадеевские ротаторы, его поляризация повернется в ту же сторону (на сфере Пуанкаре) и в верхнем плече он станет поляризованным горизонтально, а в нижнем – вертикально. После смешения на светоделителе весь свет выйдет в верхнюю выходную моду с вертикальной поляризацией.

Итак, короткий и достаточно интенсивный лазерный импульс подается в систему через циркулятор. Далее он разделяется на светоделителе. Обозначим ту половину импульсов, которая попадает в короткое плечо через P_1, а те импульсы, которые оказываются в длинном плече через P_2. Часть P_1 попадает на поляризационный светоделитель, после которого импульс становится поляризованным горизонтально. Затем P_1 попадает в волокно. Вторая половина импульсов P_2 идет через длинное плечо и, отразившись от поляризационного светоделителя становится поляризованной вертикально. Фазовый модулятор, находящийся в длинном плече, при этом выключен, т.е. фазового сдвига в P_2 не происходит. Задержка между P_1 и P_2 составляет около 200нсек. Оба импульса направляются через волокно к станции Алисы. P_1 проходит через светоделитель. Часть света поступает на детектор, который обеспечивает сигнал синхронизации. Этот детектор также важен при рассмотрении атак типа «троянского коня». Другая часть поступает на ослабитель и линию задержки – она выполнена в виде витка световода. Наконец, импульс попадает на фазовый модулятор, а затем – на фарадеевское зеркало. Часть импульсов P_2 проделывает тот же путь. Алиса включает свой фазовый модулятор на короткое время и вводит сдвиг фаз только в импульс P_1. Происходит кодирование бита так, как это необходимо в оригинальном протоколе BB84. Ослабитель подобран так, что когда импульс покидает станцию Алисы, в нем не содержится более одного фотона. Пройдя обратный путь по волокну до поляризационного светоделителя, поляризация импульса в точности ортогональна той, которая была изначально на входе в волокно (благодаря действию фарадеевского зеркала).

[1] Стандартные длины волн telecom составляют 900, 1300 и 1550 нм.

Следовательно, теперь P_1 отражается, а не проходит через PBS. Теперь этот импульс проходит через длинное плечо интерферометра. В это время Боб включает фазовращатель и вводит фазовую задержку, согласно оригинальному протоколу. Соответственно, импульс P_2 теперь поступает в короткое плечо. Оба импульса суммарно проходят один и тот же путь, значит они перекрываются на светоделителе BS1 и интерферируют, как и должно быть по протоколу. Счетчики фотонов, помещенные в выходные моды BS1 регистрируют отсчеты. Заметим, что фазовой модуляции подвержены только импульсы P_1.

При тестировании схема давала довольно низкий уровень QBER – около 1.4%. Та линия задержки, которая находится у Алисы, необходима, чтобы разделить во времени слабые «однофотонные» состояния и сильные отраженные лазерные импульсы, возникающие на любых неоднородностях оптической части установки. Заметим, что в принципе, такие импульсы могут дать Еве информацию об устройстве станции Алисы, в частности, о значении фазовых задержек, т.е. значениях бита!

Кодирование по частоте.

Применяется и другой способ кодировки – с помощью «частотно-фазовой» модуляции. Имеется в виду, что кубиты кодируются не по несущей частоте, а по относительной фазе между сателлитами относительно центральной частоты спектра.

Источник излучает короткие импульсы квазимонохроматического света с частотой ω_S. Первый фазовый модулятор PM_A модулирует фазу пучка с частотой $\Omega << \omega_S$ и малой глубиной модуляции. Сам фазовый модулятор накачивается радиочастотным генератором $РЧГ_A$, фаза которого Φ_A может управляться. Пучок ослабляется настолько, чтобы в сателлитах содержалось меньше одного фотона на импульс, в то время как центральная частота спектра представлялась классическим сигналом, содержащим много фотонов. После прохождения через волокно, пучок попадал на второй фазовый модулятор, где осуществлялось повторное частотно-фазовое кодирование PM_B. Этот фазовый модулятор накачивался вторым генератором с такой же частотой Ω и фазой Φ_B. Генераторы должны быть синхронизованы. В итоге, после прохождения через второй модулятор в спектре света содержится центральная частота ω_S, сателлиты, введенные Алисой, а также сателлиты, введенные Бобом. Все эти пики с частотами $\omega_S \pm \Omega$ взаимно когерентны, поэтому пучки интерферируют. Боб может считать информацию, проанализировав интерференционную картину, предварительно подавив с помощью интерференционных фильтров излучение на центральной частоте. Такая схема была использована группой из Безансона (Годбегюр) для реализации протокола B92. Значение бита «0» у Алисы кодировалось фазовым сдвигом 0, «1» – фазовым сдвигом π $\left(\Phi_A \to 0, \pi\right)$. Боб случайно выбирал сдвиг фаз $\Phi_B \to 0, \pi$. Ясно, что если $\left|\Phi_A - \Phi_B\right| = 0$, то интерференция конструктивная, т.е. соответствующий детектор имеет ненулевую вероятность зарегистрировать фотон. Если же $\left|\Phi_A - \Phi_B\right| = \pi$, то эта вероятность обращается в нуль!

ЭПР-ПРОТОКОЛ

В 1991 году А.Экерт предложил протокол, основанный на перепутанных состояниях. Впоследствии оказалось, что этот протокол является разновидностью BB84, однако в обзорах по квантовым способам распределения ключа, как правило, он фигурирует отдельно. Примечательно также, что казалось бы, абсолютно умозрительные рассуждения, приведшие Эйнштейна, Подольского и Розена к их известному парадоксу, а также идеи, высказанные Дж.Беллом, все-таки нашли свое практическое воплощение. Сам А.Экерт, формулируя суть протокола, отмечал, что здесь «распределение ключа зависит от полноты квантовой механики». Под полнотой понимается тот факт, что квантовое

описание обеспечивает максимально возможную информацию о рассматриваемой системе. Экспериментальная реализация рассматриваемого протокола, во всяком случае, в принципиальном смысле, мало отличается от установок по наблюдению нарушения неравенств Белла. Можно сказать, что при распределении ключа вводится квантовый канал, где сам ключ существует без какого-либо «элемента реальности», связанного с этим ключом. В этом смысле он защищен полнотой квантовой механики.

Канал состоит из источника перепутанных фотонов, находящихся в синглетном состоянии (Рис.6). Частицы разлетаются вдоль оси *z* в направлениях к легитимным пользователям – Алисе и Бобу. Каждый из них получает по одной частице или половинке перепутанной пары. Затем Алиса и Боб выполняют измерение над свой частицей, ориентируя поляризационные призмы вдоль трех направлений: для Алисы – a_i, для Боба – b_j ($i, j = 1, 2, 3$). Конкретно, измеряя углы от вертикальной оси[2]:

$$\phi_1^a = 0,\ \phi_2^a = \frac{\pi}{4},\ \phi_3^a = \frac{\pi}{2}; \qquad (18.11)$$

$$\phi_1^b = \frac{\pi}{4},\ \phi_2^b = \frac{\pi}{2},\ \phi_3^b = \frac{3\pi}{4}. \qquad (18.12)$$

Алиса и Боб выбирают ориентацию призм случайно и независимо друг от друга для каждой пары перепутанных частиц. Каждое измерение дает результат либо +1, либо –1, т.е. срабатывает один из двух детекторов, установленных в выходных модах поляризационной призмы Алисы и Боба. Параметризованный таким образом сигнал представляет один (для одной частицы) бит информации.

Далее измеряется корреляция между парами детекторов Алисы и Боба, чтобы сформировать величину:

$$E\left(a_i, b_j\right) = P_{++}\left(a_i, b_j\right) + P_{--}\left(a_i, b_j\right) - P_{+-}\left(a_i, b_j\right) - P_{-+}\left(a_i, b_j\right), \qquad (18.13)$$

где аргументы в корреляционных функциях *P* означают выбранное направление. Например, $P_{-+}\left(a_i, b_j\right)$ означает вероятность того, что при данных установках поляризационных призм a_i, b_j Алиса получила результат «-1», а Боб «+1». Можно показать, что величина *E* принимает значения

$$E\left(\phi_i^a, \phi_j^b\right) = -\cos\left(\phi_i^a - \phi_j^b\right). \qquad (18.14)$$

Для двух пар одинаковых ориентаций анализаторов (поляризационных призм) $\left(\phi_2^a, \phi_1^b\right); \left(\phi_3^a, \phi_2^b\right)$ квантово-механические предсказания дают полную антикорреляцию результатов, полученных Алисой и Бобом:

$$E\left(a_2, b_1\right) = E\left(a_3, b_2\right) = -1.$$

Следуя Клаузеру, Хорну, Шимони и Хольту можно ввести наблюдаемую величину - наблюдаемую Белла, составленную из корреляционных коэффициентов (13):

$$S = E\left(a_1, b_1\right) + E\left(a_1, b_3\right) - E\left(a_3, b_1\right) - E\left(a_3, b_3\right), \qquad (18.15)$$

которая равна

$$S = -2\sqrt{2}. \qquad (18.16)$$

После того, как перепутанные частицы поступили к Алисе и Бобу, те могут объявить по открытому каналу связи ориентации анализаторов, которые были выбраны случайным образом при каждом измерении. Затем, результаты измерений разделяются на две группы. К первой группе относятся результаты, полученные при разных ориентациях анализаторов, т.е., приводящие к (16). Ко второй – при одинаковых. Не учитываются те результаты, когда частица Алисы или Боба по каким-то причинам не была зарегистрирована вообще. Затем Алиса и Боб сообщают результат, который они получили только для первой группы измерений. Это позволяет им установить то значение *S*, которое для невозмущенных состояний частиц должно оказаться равным (16). В свою очередь

[2] Приведенные значения углов не являются единственными.

последнее утверждение дает основание легитимным пользователям считать, что результаты, относящиеся ко второй группе измерений, антикоррелированы и могут быть преобразованы в секретный набор битов – *сырой ключ*.

Подслушиватель не может воспользоваться информацией, перехватывая перепутанные частицы, поскольку самой информации там нет. Считается, что она появляется в результате измерений, выполняемых Алисой. По Экерту измерение Алисы приготавливает состояние частицы Боба, хотя более последовательно было бы утверждать, что эта информация закодирована в корреляционных функциях P и величине E.

ПОДСЛУШИВАНИЕ В КВАНТОВОЙ КРИПТОГРАФИИ.

Суть проблемы

Мы рассмотрели наиболее распространенные протоколы квантового распределения ключа. В идеальном случае на этапе получения просеянного ключа, когда Алиса послала Бобу последовательность кубитов, после того как Алиса и Боб обменялись информацией о базисах, эти просеянные ключи идентичны для обоих участников. Однако в реальности возможно появление некоторых ошибок в просеянном ключе, поэтому Алиса и Боб должны использовать протоколы классической теории информации для устранения таких ошибок. Такими протоколами являются протокол коррекции ошибок и усиления секретности. Первый необходим для установления идентичных ключей, а второй - для обеспечения секретности ключа. Целью действий Алисы и Боба является поиск такого протокола, который либо обеспечивает секретный ключ, либо сигнализирует об ошибке и останавливает весь процесс распределения. Полный анализ всех возможных стратегий подслушивателя на сегодняшний день невозможен. Общая концепция такого анализа содержит два направления – безусловное и практическое доказательство секретности квантовой криптосистемы. Термин «безусловное доказательство» означает, что секретность обеспечивается по отношению к целому классу атак, при условии, что Ева использует не только лучшие из имеющихся сегодня технологий, но и прогнозируемые технологии завтрашнего дня. Другими словами, должны быть доказаны соответствующие математические теоремы, выраженные в общих абстрактных терминах. С другой стороны, «практические доказательства» восходят к конкретным программным обеспечениям и технологиям. Они основываются на реализации общих физических принципов.

Итак, мы должны предположить, что Ева обладает совершенной технологией. Единственным ограничением для ее действий выступают законы квантовой механики, но не сегодняшний уровень развития технологии. Так, Ева не может клонировать кубиты. Но ей разрешается выполнять любые унитарные преобразования над одним или несколькими кубитами или даже использовать вспомогательные системы, в том числе и квантовые. Более того, после осуществления таких взаимодействий Ева может сохранять свою вспомогательную систему невозмущенной, в полной изоляции от окружения, в течении любого времени! И только после всех обсуждений по открытому каналу, которые, конечно, доступны ей, она может выполнить измерение над своей системой по своему выбору, будучи ограниченной при этом лишь законами квантовой механики. Будем также полагать, что все ошибки, возникающие в криптосистеме, связаны с наличием Евы. Также будем считать, что Алиса и Боб полностью изолированы от Евы, т.е. «Ева не может подглядеть через плечо» о том, что делает, например, Алиса.

Индивидуальные (некогерентные) атаки.

Этом классе атак предполагает, что Ева создает некие вспомогательные частицы (пробы), осуществляет взаимодействие проб с каждым кубитом, посылаемым от Алисы к Бобу и затем измеряет пробы одну за другой. Важно, что при этом наиболее реалистичном классе атак считается, что Ева ждет только окончания процедуры сравнения базисов и не дожидается окончания процедур коррекции ошибок и усиления секретности.

Индивидуальные атаки имеют важную особенность – они полностью могут быть рассмотрены классически! Это значит, что Алиса, Боб и Ева обладают некой классической информацией в виде случайных величин $\alpha, \beta, \varepsilon$, соответственно и что самое важное – законы квантовой механики позволяют рассматривать совместное распределение вероятностей $P(\alpha, \beta, \varepsilon)$. Такая задача многократно обсуждалась в классической криптографии, поэтому многие результаты могут быть заимствованы оттуда непосредственно.

Один из типов индивидуальных атак мы рассматривали на прошлой лекции. Это т.н. ***стратегия «перехватчик-ретранслятор»***, когда Ева перехватывает все кубиты Алисы и измеряет их в одном из двух базисов. Считается, что Ева знает, в каких базисах следует производить измерения, но не знает какой базис конкретно был выбран для кодировки конкретного бита. В этом случае взаимная информация Алисы и Евы(т.е. число битов, которое можно сохранить записывая α , зная ε):

$$I(\alpha, \varepsilon) = H_{a\ priori} - H_{a\ posteriori} = 1 - \sum_r P(r) H(i \mid r). \qquad (18.17)$$

Здесь второе слагаемое (сумма) – апостериорная или условная энтропия – есть просто усреднение по всем возможным результатам r, которые может получить Ева. Условная энтропия, фигурирующая в этой сумме, вычисляется по стандартному правилу:

$$H(i \mid r) = -\sum_i P(i \mid r) \log\left(P(i \mid r)\right), \qquad (18.18)$$

а условная вероятность дается формулой

$$P(i \mid r) = \frac{P(r \mid i) P(i)}{P(r)} \equiv \frac{P(r \mid i) P(i)}{\sum_i P(r \mid i) P(i)}. \qquad (18.19)$$

При данной стратегии Ева получает один из четырех возможных результатов:
$r \in \{\updownarrow, \leftrightarrow, \square, \square\}$. После того, как базис становится известным (возьмем, для примера, H-V-базис), исход Алисы становится детерминированным и принимает два значения $i \in \{\updownarrow, \leftrightarrow\}$.В этом случае из (17-19) получаем:

$$P(i \mid r) \to P(i = \updownarrow \mid r = \updownarrow) = 1; \quad P(i = \updownarrow \mid r = \square) = \frac{1}{2},$$

следовательно, $P(r) = \frac{1}{2}$.

Отсюда находим взаимную информацию:

$$I(\alpha, \varepsilon) = 1 - \frac{1}{2} h(1) - \frac{1}{2} h\left(\frac{1}{2}\right) = 1 - \frac{1}{2} = \frac{1}{2} = 50\%,$$

где мы воспользовались определением шенноновской энтропии:

$$h(p) = p \log_2(p) + (1-p) \log_2(1-p).$$

Другая ***стратегия*** этого типа заключается в том, что Ева использует для измерения ***промежуточный базис***, в котором все кубиты, закодированные Алисой имеют вероятность быть зарегистрированы. Например, это базис, повернутый на 22.5^0 (или базис Брейдбарта). В этом случае вероятность того, что Ева правильно измеряет значение кубита одинакова для всех реализаций и равна $p = \cos^2(\pi/8) = 0.854$. Тогда значение QBER оказывается

$QBER = 2p(1-p) \approx 25\%$,

а взаимная информация Алисы и Евы:

$I(\alpha,\varepsilon)=1-H(p)\approx 40\%$,

Последняя оценка показывает, что эта стратегия, хоть и проще в реализации (используется лишь один базис), но дает меньше преимуществ Еве, по сравнению с «перехватчиком-ретранслятором».

Симметричные индивидуальные атаки.

Эта стратегия предполагает следующую последовательность в действиях Евы. Ева последовательно перехватывает все кубиты, посылаемые Алисой один за другим. Затем она приготавливает вспомогательные квантовые состояния, называемые пробами и осуществляет взаимодействие проба-кубит. Ева имеет возможность приготовить свою пробу в произвольном состоянии. Кроме того, считается, что Ева может осуществить любой тип взаимодействия, но само взаимодействие не должно зависеть от состояния кубита Алисы. Взаимодействие должно описываться унитарным оператором. После взаимодействия пробы с кубитом, кубит направляется к Бобу. Считается, что с точки зрения Боба не важно, находится ли кубит в начальном состоянии (т.е. до взаимодействия), либо в измененном – принимается, что гильбертово пространство кубита остается тем же!

Предположим, что H_{Eve} -гильбертово пространство пробы Евы, а $C^2\otimes H_{Eve}$ - гильбертово пространство системы проба-кубит. Пусть $|\vec{m}\rangle,|0\rangle$ - начальные состояния кубита и пробы, соответственно, а U – унитарный оператор взаимодействия. Тогда состояние кубита, полученного Бобом (после взаимодействия) вычисляется, как обычно, с помощью следа по «лишним» переменным, т.е. по степеням свободы состояния Евы:

$$\rho_{Bob}(\vec{m})=Tr_{H_{Eve}}\left(U|\vec{m},0\rangle\langle\vec{m},0|U^{\dagger}\right). \qquad (18.20)$$

Мы ограничимся при рассмотрении этого вида атак протоколом BB84. В этом случае состояние Боба связано с начальным состоянием кубита, посылаемого Алисой $|\vec{m}\rangle$, соотношением:

$$\rho_{Bob}(\vec{m})=\frac{I+\eta\vec{m}\vec{\sigma}}{2}. \qquad (18.21)$$

Здесь введен коэффициент сжатия $\eta\in[0,1]$. Соотношение (21) просто показывает, что из-за попытки подслушивания (взаимодействие кубита с пробой) чистота состояния, получаемого Бобом, уменьшается. Это соответствует уменьшению диаметра сферы Блоха (Пуанкаре) (Рис.7) без изменения радиального положения изображающей точки (в протоколе BB84 четыре точки располагаются на экваторе). Атаки такого типа называются симметричными. Не вдаваясь в детали вычислений, сформулируем основные результаты воздействия на BB84 этого класса атак.

1. можно показать, что $\eta=F-D$, где F – качество (fidelity) – вероятность того, что при подслушивании Боб получит правильный результат:

$F=\langle\updownarrow|\rho_{Bob}(\vec{m})|\updownarrow\rangle$,

а D – это QBER. Напомню, что определяется как отношение числа неправильных битов к общему числу посланных битов:

$$QBER=\frac{N_{wrong}}{N_{right}+N_{wrong}}=\frac{R_{error}}{R_{sifted}+R_{error}}\approx\frac{R_{error}}{R_{sifted}}. \qquad (18.22)$$

2. Качество F зависит от двух действительных параметров x и y:

$$F=\frac{1+\cos x}{2-\cos y+\cos x} \qquad (18.23)$$

Интересно отметить, что в протоколе шести состояний (6-state protocol) число действительных параметров уменьшается до одного. Его смысл сводится к отношению

качества «копий» исходного кубита, находящихся у Боба и Евы. Случай, когда эти копии одинаковы, соответствует оптимальному подслушиванию.

3. Как только Алиса, Боб и Ева выполнили измерения над своими квантовыми системами, они получили наборы случайных классических переменных $\alpha, \beta, \varepsilon$. Оказывается, что секретный ключ, распределенный между Алисой и Бобом, возможен при проведении лишь процедур коррекции ошибок и усиления секретности тогда и только тогда, когда взаимная шенноновская информация $I(\alpha,\beta) > I(\alpha,\varepsilon) \equiv I(\beta,\varepsilon)$. Последнее равенство взаимных информаций выполняется в при симметричных атаках.
4. Интересно сравнить максимальную информацию, доступную Еве (т.н. взаимную информацию между Бобом и Евой или, что тоже самое, между Алисой и Евой) и информацию доступную Бобу (т.е. взаимную информацию между Алисой и Бобом).

Оказывается, что

$$I^{\max}(\alpha,\varepsilon) = 1 - h\left(\frac{1+\sin(x)}{2}\right) \xrightarrow[D\to 0]{} 2.9D. \qquad (18.24)$$

Ассимптотика берется при малых уровнях QBER (т.е. D).

Информация Боба:

$$I(\alpha,\beta) = 1 - h(D) = 1 + D\log_2(D) + (1-D)\log_2(1-D). \qquad (18.25)$$

Можно построить зависимости обеих информаций от уровня QBER. Кривая (24) возрастает, кривая (25) – убывает. Эти две кривые пересекаются в точке D_0:

$$I(\alpha,\beta) = I^{\max}(\alpha,\varepsilon) \Leftrightarrow D = D_0 \equiv \frac{1-\frac{1}{\sqrt{2}}}{2} \approx 15\%. \qquad (18.26)$$

Следовательно, критерием стойкости протокола BB84 по отношению к индивидуальных когерентных атак, является условие:

$$D < D_0 \approx 15\%. \qquad (18.27)$$

Другими словами, при уровнях QBER превышающих D_0 никакие процедуры коррекции ошибок и усиления секретности не обеспечат Алисе и Бобу секретности ключа – при индивидуальных атаках.

Когерентные атаки

При этом классе атак Ева может любым унитарным образом перепутать пробу любой размерности, находящейся в любом состоянии со всей последовательностью кубитов сразу (такие атаки еще называются ***совместными***). Затем, она удерживает эту пробу до конца открытого обсуждения и производит наиболее общее измерение.

Коллективные атаки – это подкласс когерентных атак, в котором каждый кубит Алисы (фотон) *i* индивидуально перепутывается с отдельной пробой P_i. Т.е. здесь Ева получает пробы в таких же состояниях, как и при некогерентных атаках. Однако после окончания открытого обсуждения Ева может провести общее измерение на всех пробах сразу, т.е. все пробы рассматриваются как единая большая квантовая система. Важно, что при коллективных атаках перед общим измерением все пробы P_i не перепутаны и независимы друг от друга. На сегодняшний день нет общего доказанного утверждения какой из классов перечисленных атак является наиболее эффективным.

При когерентных (совместных и коллективных) атаках обычно предполагается, что Ева производит свое измерение после полного завершения открытого сеанса связи между Алисой и Бобом. Этот сеанс включает в себя не только обсуждение базисов, но и выполнение протоколов коррекции ошибок и усиления секретности. Однако при более реалистичных индивидуальных атаках считается, что Ева ждет только окончания процедуры сравнения базисов.

Атаки класса «Троянский конь»

До сих пор рассматривались стратегии подслушивания, при которых Ева стремилась извлечь максимальную информацию из кубитов, пересылаемых от Алисы к Бобу. Однако Ева может использовать совершенно другую стратегию. Она сама испускает сигналы, которые поступают на станции Алисы и Боба через квантовый канал. Например, она может послать лазерные импульсы в волокно, которое соединяет станции А и Б и проанализировать отраженный свет. В принципе, таким образом можно проанализировать каки когда стрелял настоящий лазер, когда открывался счетчик фотонов, как настроены фазовые модуляторы или светоделители и проч. Поэтому, любые неоднородности в оптических трактах передатчика и приемника должны быть сведены к минимуму. С технической точки зрения нет сомнений, что атаки типа «троянского коня» могут быть предотвращены. Но, с другой стороны, довольно очевидно, что не существует физических принципов, запрещающих Еве выполнить такую атаку.

ЛИТЕРАТУРА

1. C.A.Fuchs, N.Gisin, R.B.Griffiths, C.-S.Niu, and A.Peres. “Optimal Eavesdropping in Quantum Cryptography. I”. Phys.Rev.A. 56, 1163-1172 (1997).
2. N.Gisin. Quantum Cryptography. Quant-ph/0101098.

ЛЕКЦИЯ 19. КВАНТОВЫЕ АЛГОРИТМЫ

19.1 В чем проблема?

19.2 Компьютерное моделирование физических процессов. Дискретизация. Ограничение, накладываемое на классический компьютер. Полиномиальный класс задач P.

19.3 Моделирование времени. Алгоритм клеточного автомата.

19.4 Моделирование вероятности. Экспоненциальный рост объема вычислительного устройства. Класс задач NP.

19.5 Элементарные логические операции над кубитами. Унитарность. Формализм операторов рождения и уничтожения.

19.6 Моделирование квантовых эффектов. Квантовый компьютер и построение его гамильтониана. Эволюция состояния К.К. Программный счетчик (курсор)

19.7 Недостатки компьютера и необратимые потери энергии.

19.8 Квантовый регистр. Случай N кубитов.

Говоря о квантовых алгоритмах, как о наборе вычислительных процедур, основанных на законах квантовой механики, в первую очередь хотелось бы остановиться на принципиальном вопросе об обоснованности таких вычислений вообще. Впервые, по-видимому это было сделано Ричардом Фейнманом в начале 80-ых годов. Вопрос, который он ставил звучал приблизительно так: как построить гамильтониан физической системы, которую можно рассматривать в качестве компьютера?

Прежде чем ответить на этот вопрос, рассмотрим сами предпосылки обращения к квантовой механике как к теории, способной дать новые вычислительные алгоритмы.

О каком же компьютере идет речь, когда говорят о моделировании законов физики? В науке о вычислениях обычно не рассматривается вопрос о конкретном вычислительном устройстве - речь идет об универсальном компьютере. Поэтому вопрос перефразируется так - могут ли законы физики быть смоделированы при помощи универсального компьютера? Будем считать, что элементы такого компьютера локально соединены между собой, но пусть это не будет бесконечно большое число соединений.

Какого рода физические законы мы хотим моделировать на этом компьютере? Прежде всего - законы в классическом приближении, когда работают локальные дифференциальные уравнения. Но реальный мир - это квантовый мир, поэтому хотелось бы симулировать квантовую физику. Что же за симуляции мы будем рассматривать? Это, конечно, аппроксимационное моделирование, в котором строятся численные алгоритмы решения дифференциальных уравнений. Затем компьютер производит вычисления на основе этих алгоритмов и мы получаем примерное представление о том как работает физика. Это законный подход, но речь пойдет о другом. Хочется говорить о том, насколько возможно *точное* моделирование, т.е. так как это происходит на самом деле в природе. ***Если существование такой возможности было бы доказано и такой тип компьютера стал бы реальностью, то оказалось бы, что все, что происходит в ограниченном объеме пространства и времени точно бы анализировалось за ограниченное число логических операций***. Очевидно, что существующие физические теории не позволяют сделать это. В противном случае мы бы работали

с бесконечно малыми элементами пространства, бесконечно большими длинами волн, суммировались бесконечные ряды и т.д., т.е. если бы такое предположение было бы верным, то законы физики не работали.

Но теперь мы имеем представление о том, как модифицировать законы физики. Например, мы должны изменить наше представление о том, что пространство непрерывно и представлять его как решетку, т.е. ввести дискретизацию. Дискретизация означает, что элемент пространства можно описать конечным числом, а время описывается прерывистыми скачками… Посмотрим каким бы был в этом случае физический мир и как бы представлялась задача о его моделировании. Во-первых, возникла бы проблема того, что скорость света слегка зависела бы от направления; кроме того появились бы другие элементы анизотропии, которые можно было бы зарегистрировать экспериментально. Эта анизотропия могла бы быть очень малой. Конечно, физическое знание всегда неполно и всегда можно сказать, что можно построить модель, выводы которой лежат вне области, доступной на сегодняшний день. Можно предположить, что такая анизотропия будет обнаружена в будущем. С точки зрения физики было бы очень красиво, если можно ***предсказать новый результат***, *совместимый с существующими теориями и известными фактами и не находящий пока объяснения*, но похоже, таких примеров в настоящее время нет (ситуация в физике в конце XIX начале XX века была не такой - имелись экспериментальные результаты, несовместимые с физическими теориями). Поэтому возражений против анизотропии, в принципе, нет. Вопрос только в величине такой анизотропии.

Другой важный момент заключается в том, что законы природы обратимы, а правила компьютерных вычислений - нет. Однако это утверждение может быть оспорено - компьютерные вычисления могут быть сделаны обратимыми и соответствующие методы очень пригодятся нам в дальнейшем. Это то самое место на котором изменяются взаимоотношения между физикой и вычислениями: появляются новые возможности для вычислений. Более того, возможно, что эти новые вычислительные возможности позволят нам понять что-то о физике.

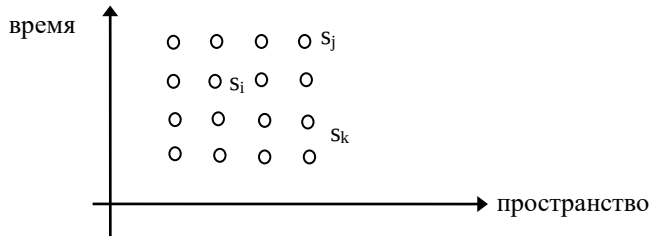
Таким образом, правила моделирования, которые мы хотим построить, состоят в том, что число вычислительных элементов, необходимых для моделирования большой физической системы, пропорционально пространственно-временному объему физической системы. Т.е. если мы хотим объяснить что-то физически, мы можем сделать это точно и нам нужен компьютер определенного размера. Если удвоив объем пространства и времени нам потребуется компьютер экспоненциально большего размера, это будет рассматриваться как нарушение правил - ***тем самым мы устанавливаем правила игры.***

<u>Моделирование времени.</u>

Для этого потребуется ввести дискретизацию времени. Известно, что при физических измерениях не может быть достигнута бесконечная точность, поэтому потребуем дискретизацию в масштабах 10^{-27}сек. При необходимости эта величина может быть сделана еще меньше!

Один из способов моделирования времени состоит в том, что компьютер переходит от состояния к состоянию, например, в модели клеточных автоматов.

Такое требование не противоречит нашей интуиции о ходе времени - мы переходим от одного состояния к другому. В этом смысле время невозможно моделировать вообще (как в модели клеточного автомата[1]) - его можно лишь имитировать (есть очевидная разница между имитацией и моделированием - полет шмеля может имитировать каждый, но далеко не каждый знает как построить модель, описывающую этот процесс). Тогда возникает следующий вопрос - можно ли время моделировать, а не имитировать? Представим себе мир с пространственно-временной точки зрения, т.е. когда представляющие точки распределены в пространстве и времени (заглядывая вперед во времени). Тогда мы могли бы сказать, что компьютер работает по правилу: состояние s_i в пространственно-временной точке дается функцией $s_i = F_i\left(s_j, ...s_k, ..\right)$, определенной в некоторых соседних с i точках.



Видно, что если эта функция устроена так, что ее значение в точке *i* зависит от значения в нескольких точках, находящихся позади во времени (т.е. в более ранние моменты), то мы просто должны переопределить описание клеточного автомата. Это так, поскольку вы вычисляете какое-то значение в т. *i* на основе значений в предыдущих точках, а тех - опять в предыдущих точках, значит можно вычислить все следующие значения двигаясь в определенном порядке. Но можно представить себе более сложную модель компьютера, работающего с более общим классом функций - обобщенных связей между пространственно-временными точками. Если *F* зависит от всех точек как в прошлом, так и в будущем, что будет в этом случае? Как в этом случае можно представить действие физических законов?

Как устроены современные теории. Замечено, что во многих физических теориях соответствующие математические уравнения сильно упрощаются, если, скажем, частицам, разрешается двигаться назад во времени (электрон - позитрон) или вообще существуют связи, соединяющие прошлое и будущее объектов. Можно ли в этом случае построить компьютер, работающий по такому алгоритму? Предположим, что мы знаем такую функцию F_i и эта функция зависит, в том числе, от переменных, расположенных в будущие моменты времени. Как тогда упорядочить данные, чтобы они автоматически удовлетворяли упомянутым выше уравнениям? Может статься, что это вообще невозможно. В случае клеточного автомата это возможно, поскольку из данного ряда можно получить следующий ряд, и затем опять следующий ряд и т.д. - т.е. мы указали способ как это сделать
Тогда,

[1] Согласно модели клеточного автомата пространство разбивается на набор клеток; есть правило изменения величины, записанной в каждой клетке; состояния в каждой клетке меняются одновременно при каждом следующем шаге.

Классическая физика удовлетворяет принципу причинности. Можно, в терминах информации в прошлом, если задействовать координату и импульс или два значения координаты в разные моменты времени (нужно обладать двумя кусочками информации в каждой точке) вычислить будущее, хотя бы в принципе. Поэтому классическая физика локальна, причинна и обратима и поэтому, с очевидностью, вполне пригодна для компьютерного моделирования. Здесь нет никаких проблем.

Моделирование вероятности

Говоря о квантовой механике, мы признаем, что здесь имеем дело лишь возможностью предсказывать вероятности.

Один из способов получить компьютер, моделирующий вероятностные теории - описание чего-то, что происходит с определенной вероятностью, - это рассчитать эту вероятность и интерпретировать полученное число для представления реальности. Например, предположим, что частица имеет вероятность $P(x, t)$ находиться в точке x во время t. Типичный случай - когда вероятность удовлетворяет дифференциальному уравнению, скажем уравнению диффузии:

$$\frac{\partial P(x,t)}{\partial t} = -\nabla^2 P(x,t).$$

Теперь можно дискретизировать время и координату, а, возможно, и саму вероятность и решать это дифференциальное уравнение как мы решаем обычные уравнения теории поля, создавая для этого алгоритм, работающий в дискретной модели. Во первых, здесь появляется проблема с дискретизацией вероятности. Если мы собираемся ограничиться κ цифрами (разрядами), это означает, что когда вероятность какого-нибудь события становится меньше чем $2^{-\kappa}$, то мы говорим, что этого никогда не произойдет. На практике, так оно и есть. Если вероятность события меньше, чем 10^{-20}, мы говорим, что оно никогда не произойдет или не будет происходить слишком часто. Но на самом деле здесь имеется определенная трудность. Если мы рассматриваем много частиц, скажем, R в системе, то мы должны описывать вероятность при условии, что частицы находятся в точках $x_1, x_2 ..., x_R$ в момент t. Так описывается вероятность для системы. Поэтому нам нужно κ-разрядное число для каждой конфигурации системы, для каждой из R "конфигураций" величины x. Поэтому, если у нас есть N пространственных точек (в смысле клеточного автомата), нам необходимо описать N^R конфигураций. На самом деле мы считаем, что в каждой точке пространства имеется информация типа электрического поля и проч., поэтому R окажется такого же порядка что и N если количество информации, выраженное в битах, совпадает с числом точек в пространстве. Следовательно, мы получаем порядка N^N конфигураций, которое необходимо описать, для того чтобы получить вероятность. Значит эта величина окажется гораздо большей, чем размер нашего компьютера, который порядка N.

Подчеркнем, что если описание изолированной части природной системы, состоящей из N переменных, требует введения обобщенной функции N переменных и если компьютер моделирует такую систему либо производя вычисления, либо просто записывая эту функцию, то при удвоении размера системы ($N \to 2N$) *потребуется экспоненциальный рост размера моделирующего компьютера.*

Поэтому, согласно правилам, введенным выше, невозможно, моделировать вычисление вероятностей.

Существует ли другая возможность? Мы не можем ожидать вычисления вероятности некой конфигурации для вероятностной теории. Но другой способ моделирования вероятностных процессов в природе состоит в построении компьютера самого по себе описывающегося вероятностным образом! В таком компьютере выход не является однозначной функцией входа. Тогда можно попробовать моделировать природу так: компьютер начинает работу с определенного состояния - начального состояния, если угодно, и приходит к конечному состоянию ***с той же вероятностью***, что и реальный процесс, который начинается с соответствующего начального состояния и приходит к конечному состоянию. Как мы узнаем чему равна вероятность? Мы видим, что природа непредсказуема. Тогда как мы хотим собираемся предсказать результат с помощью компьютера? Мы не можем, это непредсказуемо, если процесс вероятностный. Но что мы действительно можем сделать в вероятностной системе - это повторить эксперимент в природе много раз. Повторяя один и тот же эксперимент в компьютере много раз (что не займет больше времени, чем это занимает в таком же природном процессе) мы получим частоту повторения конечного состояния пропорциональную количеству испытаний с приблизительно таким же исходом (плюс - минус корень из числа испытаний n), как это случается в природе. Другими словами, можно представить машину, которая моделирует природную систему и в которой происходит в точности то же самое, что и в природе. Но если бы мы повторяли определенный эксперимент достаточное число раз, чтобы определить природную вероятность, то мы также можем проделать соответствующий эксперимент и на компьютере и получим соответствующую вероятность с соответствующей точностью (где точность определяется статистикой).

Теперь давайте подумаем о характеристиках локального вероятностного компьютера, который может моделировать природу (под природой будем понимать квантовые системы). Одна из характеристик - это то, как какая-то величина ведет себя в локальной области в пренебрежении тем, что происходит в других областях. Например, предположим, что имеются переменные в системе, которые описывают весь мир (x_A, x_B), причем, переменные x_A - это те, которыми интересуемся мы - вокруг нас, а x_B - остальные переменные вселенной. Если нас интересует вероятность того, что что-то произойдет “вокруг нас”, т.е. в т. x_A , мы должны проинтегрировать общую вероятность по “лишним” переменным. Если мы уже вычислили эту вероятность, то нам осталось выполнить интегрирование:

$$P(x_A) = \int P(x_A, x_B)\, dx_B ,$$

что само по себе довольно трудно. Однако если мы симитировали вероятность, это становится очень просто: нам ничего не нужно делать для вычисления интеграла - мы просто отбросим все значения вероятности от переменной x_B, просто глядя на нужную нам область x_A. Следовательно такая величина будет иметь природные характеристики: если она локальна, то можно обнаружить, что происходит в данной области, не посредством интегрирования или какой-нибудь другой процедуры, а просто отбрасывая все, что происходит в других местах, что вообще не является операцией.

Итак, мы подошли к вопросу о том, как моделировать с помощью компьютера квантово-механические эффекты. Квантовая механика описывает эффекты посредством дифференциальных уравнений относительно волновой функции ψ. Если у нас имеется одна частица, ψ является функцией x и t и такое дифференциальное уравнение можно смоделировать как то вероятностное уравнения, которое было выписано выше. Так можно моделировать уравнение Шредингера для одной частицы. Но полное описание квантовой механики дается волновой функцией $\psi(x_1, x_2, ...x_R, t)$, которая является амплитудой вероятности найти частицы в точках $(x_1, x_2, ...x_R)$ и поэтому не может быть смоделирована на обычном компьютере, как имеющая слишком много переменных. В этом обычном компьютере число элементов пропорционально R или N. Такая же проблема возникает и с вероятностным описанием в классической физике. Как же можно моделировать квантовую механику? Есть два способа это сделать. Можно отказаться от правила, по которому работает компьютер. Мы говорим: давайте сделаем компьютер из квантово-механических элементов, которые удовлетворяют законам квантовой механики. Другой путь такой - пусть компьютер будет логическим универсальным автоматом.

Прежде всего заметим, что законы квантовой физики обратимы во времени, поэтому мы должны рассматривать квантовые вычислительные устройства, подчиняющиеся законам обратимости. Напомним, что одним из выводов науки о вычислениях (computer science) является факт, что универсальное вычислительное устройство может быть сделано на основе соответствующей сложной сети элементарных логических элементов. В классическом компьютере проводники, соединяющие ЛЭ должны быть идеальными, и переносить токи, вызывающие падения напряжения на сопротивлениях, которые соответствуют двум уровням “1” и “0”.

Напоминание о классических вычислениях

Эти элементарные логические элементы могут быть лишь элементами “NOT” и “AND”. На самом деле достаточно лишь одного элемента “NAND = NOT AND”, который при наличии на одном входе единицы выполняет операцию NOT над значением другого входа. Эти элементы показаны на рис. 1. Поскольку в классическом компьютере проводники играют существенную роль, мы можем рассматривать и два других элементарных ЛЭ, которые называются “FAN OUT” (размножитель, веер, копировальное устройство и проч. - Рис. 1в) - когда один провод раздваивается и “EXCHANGE” (Рис. 1г)- когда проводники перекрещиваются. А вообще, операции NOT и AND реализуются с помощью транзисторов (Рис. 1д, е).

Что определяет минимум свободной энергии, которая затрачивается при работе идеального компьютера, собранного на основе этих элементарных ЛЭ? Например, при работе элемента AND его выходной сигнал принимает два логических значения, соответствующих двум уровням напряжения или тока. При его переключении энтропия меняется на величину $\Delta S = \ln 2$. При постоянной температуре такое изменение энтропии приводит к выделению тепла $\Delta Q = kT \ln 2$.

Долгое время эта величина считалась пределом энергозатрат, приходящихся на один бит. Вообще же, проблема выделения тепла в современной вычислительной технике играет важную роль. Оказывается, что современные транзисторные схемы выделяют тепла порядка $10^{10} KT$. В основном, это происходит из-за того, что логические уровни обеспечиваются падением напряжения на резисторах! Энергетически было бы значительно выгоднее, если бы энергия запасалась бы в реактивных элементах, таких как конденсаторах или катушках, - ее можно ,было бы преобразовывать. Но современная технология, ориентированная на кремниевые чипы, пока не в состоянии решить эту проблему.
Даже в природной копирующей машине - молекуле ДНК затрачивается порядка $100кT$ при воспроизводства одного бита информации - величина все еще на порядок превышающая предельный уровень $KTln2$! В квантовых системах биты записываются не на системах, состоящих из 10^{11} атомов, как в классических транзисторах, а на одном атоме - кубите.

Ч.Беннет впервые показал, что если элементарные ЛЭ будут сделаны обратимыми, то названный предел окажется преодолимым, а затраты свободной энергии окажутся независимыми от уровня сложности всего устройства или числа шагов, которое необходимо выполнить для решения той или иной задачи.

В классических вычислениях известны три обратимых ЛЭ. Это “NOT” - однобитовый ЛЭ (Рис.2а), Управляемое НЕ или CNOT - двухбитовый ЛЭ (Рис.2.б) - операция сложения по модулю два. Как известно, сам по себе CNOT не является обратимым. Однако, если сохранить значение контрольного бита a, то CNOT становится обратимым.

Заметим, что ЛЭ “FAN OUT” можно получить из CNOT”. Если $b = 0$, то значение, записанное на контрольном входе а копируется на выход b' (Рис.2.в). Операция EXCHANGE также реализуема на CNOT (Рис.2г).

Для построения универсального классического компьютера необходим трехбитовый элемент или ЛЭ Тоффоли. Он называется CCNOT. Значение бита мишени c меняется на противоположное, если оба контрольных бита a и b установлены в 1 (Рис.3). Если сохранять значение контрольных битов, то ЛЭ Тоффоли является обратимым.

Любой логический элемент может быть построен на основе комбинаций трех перечисленных основных ЛЭ. Но оказывается, чтобы добиться обратимости любого ЛЭ, необходимо в его устройство, кроме той функции, которую он выполняет, добавлять нечто еще. Этот добавок называется “garbage” или отход. Более того, существуют простые соображения, которые показывают, что размер “мусорного ящика” должен совпадать с размером входных данных (в битах). Рассмотрим некое обратимое логическое устройство, преобразующее n входных битов в n выходных. Пусть решение задачи, которое осуществляет это логическое устройство требует присутствие на выходе k битов информации, при наличии на входе m битов. Оказывается, что при этом необходимо иметь (на входе) пустой регистр, состоящий из k нулей! Тогда, рассматривая задачу как преобразование n входных битов в n выходных, мы видим, что размер “мусорного ящика” совпадает с размером входных данных m , а его содержимое - входные данные - это цена, которую нужно платить за обратимость.

Квантовый компьютер

Итак мы хотим узнать как, в принципе, может быть устроен компьютер, работающий по законам квантовой механики. *Более строгая формулировка*: как выглядит гамильтониан для системы, состоящей из взаимодействующих частей, причем система в целом должна вести себя как универсальный компьютер. Заметим, что большая система неизбежно взаимодействует с окружением и поэтому трудно будет поддерживать обратимость. Поэтому мы хотим построить небольшую систему, максимально упростив ее устройство. *Наш гамильтониан будет описывать только внутренние взаимодействия в системе, но не будет затрагивать такие операции, требующие обмена с окружением*, как приготовление начального состояния и чтение выходного состояния.

Насколько маленьким должен быть такой компьютер? Т.е. насколько маленьким может быть носитель числа? Естественно, что число будет представляться битом. Будем записывать бит на двухуровневой системе. Фейнман назвал ее “атомом”. Мы называем ее кубитом. Тогда *n*-битовое число представляется состоянием регистра или набором *n* двухуровневых систем. В зависимости от того, в каком из двух состояний $|0\rangle,|1\rangle$ находится кубит, меняется и значение всего числа или регистра, на котором оно записано. Соответственно, число может быть прочитано, определяя или измеряя состояние составляющих регистр кубитов. Рассмотрим, например, устройство квантового ЛЭ CCNOT. Пусть *G* представляет некую операцию, производимую над тремя атомами *a, b* и *c*. Эта операция преобразует начальное состояние атомов *a, b* и *c* в конечное состояние a',b',c'. Таким образом, связь между конечным и начальным состояниями и осуществляется функцией, которую мы хотим построить. Заметим, что мы не производим перемещение кубитов из одной точки в другую. Мы просто изменяем их. В классическом компьютере это происходит по-другому. Между начальным и конечным состояниями имеются реальные проводники, по которым текут токи. В нашем случае все обстоит гораздо проще. С начала мы имеем три кубита (атома) в некоем состоянии, а в результате операции *G* это состояние меняется и кубиты принимают значения a',b',c'. Математически эта операция выражается в том, что выход $|a'\rangle,|b'\rangle,|c'\rangle$ есть результат действия *G* на вход $|a\rangle,|b\rangle,|c\rangle$. Известно, что в квантовой механике операторы, изменяющие состояния, должны быть линейными. Поэтому мы полагаем, что *G* - это линейный оператор. Он представляется матрицей, причем почти все матричные элементы $G_{a',b',c',a,b,c}$ равны нулю (см. таблицу истинности для ЛЭ Тоффоли). Ясно, что такая операция будет обратимой, поскольку обеспечивается условием $G^*G = I$. Таким образом, *G* - эрмитова матрица (кроме того, она еще и действительная матрица $G^* = G$, но это только в данном конкретном случае CCNOT).

Теперь давайте запишем некую эффективную матрицу $A_{a,b...c}$, отвечающую данному оператору *G*, которая будет иметь индексы, соответствующие тем элементарным ЛЭ из которых состоит тот ЛЭ, который мы хоти построить.

Например, мы хотим записать матрицу, соответствующую NOT. Матрица A_a имеет вид

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Это 2x2 матрица может быть реализована множеством способов (мы рассматривали фазовую пластинку в пол-длины волны). Рассмотрим здесь метод, развитый Фейнманом - метод операторов рождения и уничтожения. Будем использовать нестандартные обозначения, чтобы не путать операторы с использованными уже буквами.

Матрица, соответствующая оператору $\underline{a}$:

4

уничтожает 1, записанный на атоме a и преобразует его в 0. Соответственно, $\underline{a}$ - это оператор, преобразующий состояние $|1\rangle$ в состояние $|0\rangle$. Однако, если исходное состояние атома было $|0\rangle$, оператор $\underline{a}$ дает число 0, т.е. действуя на состояние, он не изменяет его, а просто дает “пустое состояние” - число 0.

Действительно

$$\begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix}\begin{pmatrix}1\\ 0\end{pmatrix}=\begin{pmatrix}0\\ 0\end{pmatrix}\equiv 0, \qquad \begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix}|1\rangle=\begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix}\begin{pmatrix}0\\ 1\end{pmatrix}=\begin{pmatrix}1\\ 0\end{pmatrix}\equiv|0\rangle$$

Сопряженный оператор дается матрицей

$$\underline{a}^{*}=\begin{pmatrix}0 & 0\\ 1 & 0\end{pmatrix}.$$

Этот оператор, действуя на состояние “0” дает состояние “1”: $|0\rangle\rightarrow|1\rangle$. Действуя же на состояние $|1\rangle$, поскольку более “высоких” состояний нет, он дает численный нуль.

Обращаю внимание, что эти обозначения не являются стандартными для операторов рождения (a) и уничтожения ($a^{\dagger}$).

Любой оператор, представимый матрицей 2x2, может быть представлен в терминах этих операторов $\underline{a}$ и $\underline{a}^{*}$. Например, произведение $\underline{a}^{*}\underline{a}\equiv N_a$ дается матрицей

$$\underline{a}^{*}\underline{a}=\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}$$

Этот оператор дает 1 для состояния $|1\rangle$ и 0 - для состояния $|0\rangle$. Т.е. оператор N дает число, которое представляет состояние атома. Произведение операторов $\underline{a}\underline{a}^{*}\equiv 1-N_a$ представляется матрицей

$$\begin{pmatrix}0 & 0\\ 0 & 1\end{pmatrix}$$

и дает о для состояния $|1\rangle$, для состояния $|0\rangle$ дает 1.

Имеется также диагональная матрица

$$I=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix},$$

с помощью которой можно записать известное выражение

$$\underline{a}\underline{a}^{*}+\underline{a}^{*}\underline{a}=I.$$

Используя формализм операторов рождения и уничтожения, можно записать матрицу для NOT: $A_a=\underline{a}+\underline{a}^{*}$. Естественно, что эта матрица обратима (унитарна): $A_a^{*}A_a=I$.

Аналогично можно записать выражение для матрицы, описывающей действие оператора CNOT:

$\underline{aa}^* \left(b + \underline{b}^* \right) + \underline{aa}^*$.

Первое слагаемое в этом выражении $\underline{aa}^*$ выделяет условие, при котором на входе а записана единица*:* a = 1; тогда мы хотим, чтобы ко входу b применялось преобразование NOT. Второе слагаемое выделяет условие, при котором на входе а находится 0; при этом ко входу b применяется тождественное преобразование I.

Следующий вопрос, неизбежно появляется при рассмотрении результата действия нескольких элементарных ЛЭ. Что из себя представляет матрица логического устройства, состоящего из набора элементарных ЛЭ, т.е. как весь объект в целом действует на входное состояние? Т.е. мы хотим представить результат в виде:

$\left| \psi_{out} \right\rangle = M \left| \psi_{in} \right\rangle$.

Можно показать, что в этом случае матрица M будет являться произведением матриц, описывающих действие всех последовательных элементарных ЛЭ:

$M = A_{a,b} A_{c,d} A_{bc,d} ..$

Такая матрица будет унитарной, поскольку все составляющие ее матрицы унитарны. Поэтому вся операция в целом будет обратима.

Таким образом общая задача формулируется так. Пусть A_1, A_2, A_3,….$A_к$ - последовательность необходимых элементарных операций в некотором логическом устройстве, которое действует на n атомов. Мы хотим построить матрицу M размером $2^n \times 2^n$, которая будет отвечать всей операции в целом. Каким образом можно построить такое физическое устройство, если мы знаем как работают простейшие элементы?

Вообще в квантовой механике временная эволюция состояния (выходного состояния) дается формулой:

$e^{iHt} \psi_{in}$,

где ψ_{in} - это входное состояние системы, описывающейся гамильтонианом H. Построить гамильтониан, который дает $M = e^{iHt}$, при том, что M - это произведение некоммутирующих матриц, представляется очень трудной задачей. Однако, заметим, что для фиксированного момента времени, если разложить экспоненту $e^{iHt} = 1 + iHt - H^2 t^2 / 2 + ...$, то видно, что оператор H действует на состояние бесконечное число раз - однократно, двукратно, трехкратно, поэтому, четвертое и т.д. - в целом, общее состояние представляется суперпозицией всех таких возможностей. Отсюда следует, что задача нахождения гамильтониана этих композиционных матриц может быть решена следующим образом.

Добавим к n атомам, находящимся в нашем регистре, совершенно новый набор $к + 1$ атомов, которые будут отвечать за “положения программного счетчика”. Обозначим как q_i и q^*_i операторы рождения и уничтожения для точки программы i когда i меняется от 0 до $к$. Физически это можно реализовать с помощью электрона, двигающегося от одного свободного места к другому. Если

положение *i* уже занято электроном, то назовем это состояние $|1\rangle$, если положение свободно, то это состояние $|0\rangle$. Наш гамильтониан принимает вид:

$$H = \sum_{i=0}^{k-1} q_{i+1}^{*} q_i A_{i+1} + c.c. =$$

$$q_1^{*} q_0 A_1 + q_2^{*} q_1 A_2 + q_3^{*} q_2 A_3 + q_1^{*} q_0 A_1 + \ldots + q_0^{*} q_1 A_1^{*} +$$

$$q_1^{*} q_2 A_2^{*} + q_2^{*} q_3 A_3^{*} \ldots$$

Здесь операция *A* применяется к регистру *n* атомов, а операторы *q* действуют на программный счетчик.

Первое, на что можно обратить внимание, это что если все программные места свободны, т.е. все программные атомы находятся в состоянии $|0\rangle$, ничего не происходит, т.к. каждый член в гамильтониане начинается с оператора уничтожения и, поэтому, дает 0.

Во-вторых, заметим, что если какое-то одно программное место занято (состояние $|1\rangle$), а остальные нет, то при действии гамильтониана ситуация не изменится - всегда какое-то (другое) состояние будет занято, а все другие свободны. (На самом деле число программных мест, которые находятся в состоянии $|1\rangle$ - это сохраняющееся число.) Мы будем полагать, что при работе нашего компьютера либо все программные места свободны, либо какое-то одно занято. Два или более программных мест не может мыть занято во время штатной работы.

Пусть в начальный момент место 0 занято, т.е. находится в состоянии $|1\rangle$ (и, поэтому, все остальные находятся в состояниях $|0\rangle$). Если в итоге, в некоторый момент времени t место к окажется в состоянии $|1\rangle$ (поэтому все другие - в состояниях $|0\rangle$), то мы делаем вывод, что на *n*-регистр подействовала матрица *M*, которая равна $A_к \ldots A_2 A_1$, как мы и хотели. Это получается следующим образом. Предположим, что регистр начинает работу в каком-нибудь начальном состоянии ψ_{in} и, что “место 0” программного счетчика занято. Тогда единственный член в полном гамильтониане, который будет действовать первым, (т.к. гамильтониан работает в последовательные моменты времени) - это первый член $q_1^{*} q_0 A_1$. Оператор q_0 изменит состояние “места 0” на “свободно”, в то время как q_1^{*} изменит “место 1” на “занято” Таким образом, член $q_1^{*} q_0$ просто передвигает занятое место из положения 0 в положение 1. Но все это умножается на матрицу A_1, которая действует только на регистр *n* атомов, и, поэтому умножает начальное состояние регистра *n* атомов на A_1.

Далее, гамильтониан действует во второй раз. Тогда первый член не даст ничего, поскольку q_0 дает 0 на “месте 0” (из-за того, что это место свободно). Теперь работает второй член (прости господи) $q_2^{*} q_1 A_2$, который опять передвинет занятое место - будем его называть курсором. Курсор передвинется из положения 1 в положение 2, а на регистр действует матрица A_2 - т.е. в целом мы получили матрицу $A_2 A_1$, подействовавшую на регистр.

Таким образом, поскольку гамильтониан (первая строчка) действует в последовательные моменты времени, курсор будет передвигаться от 0 до *к*, а последовательное действие матриц A_i на регистр как раз и даст общую матрицу *M*. Заметим однако, что гамильтониан должен быть эрмитовым, поэтому должна оставаться операция комплексного сопряжения всех операторов. Предположим, что для данного состояния, мы получили позицию курсора в "положении 2", следовательно, мы имеем матрицу A_2A_1, подействовавшую на регистр. Теперь q_2 , который передвинет занятое положение на следующую позицию, не обязательно возникает из первой строчки - он может прийти из второй, т.е. из члена $q_1^* q_2 A_2^*$, который передвинет курсор назад из положения 2 в положение 1! Когда это происходит, на регистр действует оператор A_2*, поэтому полный оператор, действующий на регистр, в этом случае оказывается $A_2^* A_2 A_1$.Но $A_2^* A_2 = 1$, откуда весь оператор вырождается в значение A_1. Поэтому ясно, что когда курсор вернулся в "положение 1" полный результат оказывается таким, как будто бы на регистр подействовал только оператор A_1! Тогда по мере продвижения курсора разными членами в гамильтониане вперед и назад, операция *A* накапливается, либо вновь редуцируется.

На некотором этапе, например, когда курсор находится в положении *j*, матрицы от A_i до A_j подействовали поочередно на регистр. Совершенно неважно каким путем курсор пришел в "положение *j*"- из "положения 0" до "*j*" или пройдя дальше и вернувшись назад, или возвращаясь назад, а потом вперед и т.д. - важно, что он оказался в "положении *j*". Поэтому, верным оказывается утверждение, что если курсор оказался в положении *к*, мы имеем общий результат для регистра *n* атомов, состоящий в том, что матрица *M* подействовала на начальное состояние - как мы и хотели.

Как мог бы работать такой компьютер? Начнем с того, что поместим входные данные (биты) во входной регистр, а курсор 0 в "положение 0" (т.е. "положение 0" занято). Затем, проверим положение *к*, например, с помощью рассеяния электронов, свободно оно или занято (имеет ли курсор). В момент, когда мы обнаружили курсор в положении *к*, уберем курсор так, что он не сможет вернуться в программную строку. Тогда мы знаем, что регистр содержит выходные данные. Мы можем измерить их в удобное для нас время. Конечно существуют некие внешние параметры, задействованные в процедуре измерения и определяющие её, которые не являются частями компьютера. При этом мы говорим, что компьютер вступает во взаимодействие с внешним миром и при загрузке данных, и при чтении результата.

С математической точки зрения продвижение курсора вверх и вниз по программной строке в точности отвечает действию матрицы *A* в гамильтониане. Другими словами, работа компьютера представляет собой распространение неких волн, например, возникающих при распространении сильно ограниченных (одномерных) электронных пучков или спиновых волн - они хорошо изучены. Эти волны распространяются вперед и назад по программной строке, из них можно сформировать пакеты и проч.

Недостатки компьютера и необратимые потери энергии.

Вообще имеется много неидеальностей такого устройства, но главная из них заключается в том, что коэффициенты связи оказываются неодинаковыми вдоль программной строки. Строка настолько длинная, что при реальном вычислении небольшие нерегулярности будут вызывать малые вероятности рассеяния и волны не будут распространяться строго по “баллистическим траекториям”, при этом беспорядочно двигаясь вперед и назад.
Например, если система построена на подложке из обычных физических атомов, то тепловые колебания этих атомов изменят коэффициенты связи, что приведет к сбоям.

Рассмотрим простой пример. Рассмотрим регистр, построенный из трех классических битов. Такой 3-х битовый регистр может хранить одно из восьми различных чисел - от нуля до семи, т.е. находиться в одном из восьми состояний: 000, 001, 011,...111. Но квантовый регистр, составленный из трех кубитов, может одновременно хранить до восьми чисел. Поскольку регистр представляет собой суперпозицию. Примечательно, что восемь различных чисел могут физически присутствовать в одном регистре одновременно На самом деле, это не более удивительно, чем одновременное присутствие состояний $|0\rangle$ и $|1\rangle$ в одном кубите:

$$|\ \rangle = (\alpha_1|0\rangle + \beta_1|1\rangle)\otimes(\alpha_2|0\rangle + \beta_2|1\rangle)\otimes(\alpha_2|0\rangle + \beta_2|1\rangle) =$$
$$\alpha_1\alpha_2\alpha_3|0\rangle|0\rangle|0\rangle + \alpha_1\alpha_2\beta_3|0\rangle|0\rangle|1\rangle + \alpha_1\beta_2\beta_3|0\rangle|1\rangle|1\rangle + \alpha_1\beta_2\alpha_3|0\rangle|1\rangle|0\rangle +$$
$$+\beta_1\alpha_2\alpha_3|1\rangle|0\rangle|0\rangle + \beta_1\beta_2\alpha_3|1\rangle|1\rangle|0\rangle + \beta_1\alpha_2\beta_3|1\rangle|0\rangle|1\rangle + \beta_1\beta_2\beta_3|1\rangle|1\rangle|1\rangle$$

Каждое из восьми состояний имеет соответствующую вероятность быть обнаруженным, например, состояние $|1\rangle|1\rangle|0\rangle$ имеет вероятность $\beta_1\beta_2\alpha_3$.

В этом примере было использован один из фундаментальных принципов квантовой механики, который состоит в том, что совместное пространство квантовых состояний двух систем является тензорным произведением пространств отдельных состояний. Поэтому пространство квантового состояния n кубитов - это пространство C^{2^n}. Базисные вектора этого пространства можно параметризовать бинарными строками длиной n. В дальнейшем широко будет использоваться тензорное разложение такого пространства на n копий размерностью $\boldsymbol{C^2}$. Здесь базисное состояние V_b, отвечающее бинарной строке $b_1b_2..b_n$, представляется как

$$V_{b_1b_2..b_n} = V_{b_1}\otimes V_{b_2}\otimes ...\otimes V_{b_n}$$

При добавлении кубитов к регистру его емкость по отношению к хранению квантовой информации растет экспоненциально: четыре кубита могут хранить 16 различных чисел одновременно, и т.д. В общем случае N кубитов хранят 2^N чисел. Так регистр из 250 кубитов - совместное состояние 250 двухуровневых атомов хранит одновременно больше чисел, чем количество атомов во вселенной. Заметим, что это заниженная оценка количества квантовой информации, поскольку элементы суперпозиции присутствуют в непрерывно изменяемой пропорции, которая определяется взаимными фазами тех или иных состояний.

Например, если кубиты - это атомы, то подействовав на них подобранными по длительности и интенсивности лазерными импульсами (модель Цолера-Цирака), можно повлиять на соответствующие состояния освещаемых атомов (кубитов). Тогда начальная суперпозиция закодированных чисел превратиться в другую

суперпозицию. В процессе такой эволюции каждое число в суперпозиции подвергается воздействию, так что получается, что производится большой объем параллельных вычислений В этом состоит ***принцип параллелизма***, введенный Д.Дойчем. Следовательно квантовый компьютер за один шаг вычислений может провести одну операцию, например, над 2^N различными (входными) числами. А результатом будет - представляться соответствующей суперпозицией на выходе. Для выполнения аналогичной задачи классический компьютер должен повторить вычисления 2^N раз или использовать 2^N параллельно работающих процессоров.

ЛИТЕРАТУРА

1. Simulating physics with computers, Internat. J. Theoret. Phys. 21, 467-488 (1982).
2. Quantum mechanical computers, Found.Phys. 16, 507-531(1986).

ЛЕКЦИЯ 20. КВАНТОВЫЕ АЛГОРИТМЫ (продолжение)

20.1. Примеры ЛЭ и соответствующих матриц, используемых для квантовых вычислений.

20.2. Квантовое преобразование Фурье.

20.3. Квантовые алгоритмы:

- 20.3.1. Алгоритм Саймона или задача “Оракула”;
- 20.3.2. Алгоритм разложения на простые множители или алгоритм Шора; дискретное логарифмирование.
- 20.3.3. Алгоритм поиска в базе данных или “алгоритм Гровера”

Подчеркнем еще раз, что для того, чтобы использовать физическую систему для выполнения вычислений, мы должны уметь изменять состояние этой системы. Законы квантовой механики разрешают единственный тип преобразований – унитарные преобразования векторов состояний. Унитарная матрица – это такая матрица, у которой транспонированная и сопряженная матрица равна обратной матрице. Мы требуем, чтобы преобразования состояний были представлены с помощью унитарных матриц и, таким образом, суммирование вероятностей получения каждого возможного исхода должно давать единицу.

Напоминание. Матрица называется эрмитовой, если $A^{\dagger} = A \to A^{*}_{mn} = A_{nm}$

Матрица называется унитарной, если $A^{\dagger}A = AA^{\dagger} = I$

Также мы требуем локальности преобразований. Это означает, что унитарные преобразования выполняются над фиксированным числом *n* битов. Физически это оправдано тем, что мы знаем, как построить ЛЭ, действующие на два бита, а *n*-битовые преобразования всегда можно выполнить с помощью двухбитовых.

Рассмотрим систему, состоящую из *n* компонент, каждая из которых имеет два состояния (кубит). В классической физике полное описание состояния такой системы требует только *n* битов. В квантовой механике, полное описание состояния такой системы требует знания $2^n - 1$ комплексных чисел, поскольку это состояние описывается суперпозицией всех базисных состояний (в примере, рассмотренном на предыдущей лекции n = 3, есть 8 амплитуд базисных состояний плюс условие нормировки плюс общая фаза, итого 7 комплексных чисел). Точнее говоря, состояние квантовой системы представляется точкой в 2^n - мерном векторном пространстве. Для каждого из 2^n возможных положений классических компонент существует базисное состояние такого векторного пространства, которое представляется в виде, например, $\left|0111...0001\right\rangle$. Такая запись означает, что первый бит равен 0, второй - 1 и т.д. Запись в виде *кет-вектора* $\left|S\right\rangle$ свидетельствует о том, что состояние S - чистое. Смешанные состояния в этой лекции мы не рассматриваем. Гильбертово пространство, связываемое с такой системой - это комплексное векторное пространство, имеющее эти 2^n векторов в качестве базисных.. Состояние этой системы в любой момент времени описывается вектором единичной длины в этом векторном пространстве. Итак, суперпозицию состояний будем описывать в виде:

$$\sum_{i=0}^{2^n-1} a_i \left|S_i\right\rangle, \qquad (20.0)$$

где a_i - комплексные амплитуды, удовлетворяющие условию нормировки $\sum_i |a_i|^2 = 1,$ а каждый вектор $|S_i\rangle$ - базисный вектор гильбертова пространства.

Если на каком-то вычислительном шаге машина производит измерение (в каком-то из этих базисов), то вероятность обнаружить систему в этом базисе $|S_i\rangle$ есть просто $|a_i|^2$. Однако измерение состояния в машине проектирует полное состояние на наблюдаемый базисный вектор (пример с поляризацией фотонов). Следовательно, "подсматривание" за состоянием машины во время вычисления, приведет к разрушению состояния и остановке вычисления.

Действие квантовых логических элементов должны представляться в виде таблиц истинности: каждому входному вектору ставится в соответствие выходной вектор. Например,

$$|00\rangle \to |00\rangle,$$
$$|01\rangle \to |01\rangle,$$
$$|10\rangle \to \frac{1}{\sqrt{2}}\left(|10\rangle + |11\rangle\right), \qquad (20.1)$$
$$|11\rangle \to \frac{1}{\sqrt{2}}\left(|10\rangle - |11\rangle\right).$$

Не все таблицы истинности отвечают физически реализуемым квантовым ЛЭ, поскольку многие таблицы не представляют собой унитарных преобразований. Преобразование (20.1) можно записать в виде матрицы. В ней строки соответствуют входным базисным векторам, а столбцы – выходным базисным векторам.

Элемент (*i, j*) матрицы дает значение коэффициента *j*-ого базисного ***выходного*** вектора, когда *i*-ый базисный вектор является ***входным*** для ЛЭ. Таблица истинности для примера, приведенного выше есть:

	$\|00\rangle$	$\|01\rangle$	$\|10\rangle$	$\|11\rangle$
$\|00\rangle$	1	0	0	0
$\|01\rangle$	0	1	0	0
$\|10\rangle$	0	0	$\frac{1}{\sqrt{2}}$	$\frac{1}{\sqrt{2}}$
$\|11\rangle$	0	0	$\frac{1}{\sqrt{2}}$	$-\frac{1}{\sqrt{2}}$

(20.2)

Соответственно, входной регистр, т.е. вектор, образованный суперпозицией базисных векторов $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ представляется в виде столбца

$$\begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \end{pmatrix}. \qquad (20.3)$$

Квантовый ЛЭ является "правильным" только если матрица, которой он представлен, унитарна, т.е. обратная к ней матрица равна эрмитово-сопряженной (транспонирование + комплексное сопряжение).

Рассмотрим следующий пример. Пусть входное состояние представлено суперпозицией:

$$\frac{1}{\sqrt{2}}\left[|10\rangle - |11\rangle\right] = \frac{1}{\sqrt{2}}\begin{pmatrix}0\\0\\1\\-1\end{pmatrix}. \qquad (20.4)$$

Подействуем на это состояние матрицей (2):

$$\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1/\sqrt{2}&1/\sqrt{2}\\0&0&1/\sqrt{2}&1/\sqrt{2}\end{pmatrix}\begin{pmatrix}0\\0\\1/\sqrt{2}\\-1/\sqrt{2}\end{pmatrix} = \begin{pmatrix}0\\0\\1/2-1/2\\1/2+1/2\end{pmatrix} = \begin{pmatrix}0\\0\\0\\1\end{pmatrix} = |11\rangle. \qquad (20.5)$$

Этот пример наглядно демонстрирует проявление эффекта интерференции при квантовых вычислениях. Независимо от того, стартовали ли мы с состояния $|10\rangle$ или $|11\rangle$, у нас всегда есть шанс получить состояние $|10\rangle$ на выходе нашего ЛЭ (см. (20.1)). Однако, когда мы стартуем с суперпозиции этих двух состояний (20.4), амплитуда вероятности получить на выходе состояние $|10\rangle$ обращается в нуль. Аналогичные рассуждения можно провести и для случая другого входного состояния, когда вместо знака "-" стоит "+":

$$\frac{1}{\sqrt{2}}\left[|10\rangle + |11\rangle\right] = \frac{1}{\sqrt{2}}\begin{pmatrix}0\\0\\1\\1\end{pmatrix} \qquad . \qquad (20.6)$$

В этом случае, на выходе нашего ЛЭ (20.3) исчезает амплитуда состояния $|11\rangle$!

По правилам квантовой механики если мы используем двухкубитовый ЛЭ к регистру, состоящему из большого числа битов (кубитов) - в этом случае рассматриваемая цепь должна иметь больше двух проводников- мы должны подействовать матрицей на соответствующие кубиты и оставить остальные кубиты без изменения. Эта процедура отвечает умножению состояния всего регистра на тензорное произведение матрицы ЛЭ и состояния двух выделенных кубитов и единичной матрицы, действующей на оставшиеся кубиты.
Напомним, что квантовый ЛЭ рассматривается как набор логических "проводников", соединяющих вход и выход.

<u>Квантовое преобразование Фурье.</u>

<u>Напоминание.</u> Для дискретного сигнала, представляющего собой решетчатую функцию, и, как правило, определенного на конечном промежутке времени (времени измерения) преобразование Фурье принимает вид так называемого дискретного преобразования Фурье (ДПФ):

$$X(k) = \frac{1}{N}\sum_{n=0}^{N-1} X(nT)\exp\left\{-\frac{i2nk}{N}\right\} = \frac{1}{N}\sum_{n=0}^{N-1} X(nT)W^{nk}\ . \qquad (20.*)$$

Обратное преобразование имеет вид:

$$X(nT) = \sum_{k=0}^{N-1} X(k)\exp\left\{\frac{i2nk}{N}\right\} = \sum_{n=0}^{N-1} X(k)W^{-nk}\ . \qquad (20.**)$$

Здесь: T – период дискретизации,
n – номер отсчета дискретизированного сигнала, n = 0, 1, 2,…, N-1;

k – номер гармоники сигнала, k = 0, 1, 2,…, N-1, частота гармоник равна $k/T_{изм}$, где $T_{изм}$– период измерения;
W – вспомогательная функция.
Недостатком данного алгоритма является большой объем повторяющихся вычислений W^{nk} при различных комбинациях n и k. Устранение этих избыточных операций приводит к так называемому алгоритму быстрого преобразования Фурье, который обычно и используется. Быстрое Преобразование Фурье (БПФ) - способ вычислить преобразование последовательности A за время $O(n\ logn)$, вместо обычного $O(n^2)$ в случае, если n - степень 2. (*конец напоминания)*.

Поскольку квантовые вычисления имеют дело с унитарными преобразованиями, полезно рассмотреть некоторые из основных преобразований. Рассмотрим пример, в котором вводится техника для осуществления квантовым компьютером дискретного преобразования Фурье за полиномиальное время. Это преобразование будет представлено матрицей, строки и столбцы которой будут обозначать индексы состояний. Такие состояния соответствуют бинарному представлению целых чисел в компьютере. В частности, строки и столбцы будут обозначаться индексами, начиная с “0”, до некоторого числа, которое будет оговорено.

Это преобразование работает следующим образом. Рассмотрим число a, которое удовлетворяет двойному неравенству
$0 \le a \le q$ для некоторого q, где число q представлено некоторым числом битов, которое растет полиномиально. Мы хотим выполнить преобразование, которое переводит состояние $|a\rangle$ (это одно из базисных состояний, которыми может быть представлен вектор в q-мерном пространстве: $|a\rangle = V_a \equiv V_{a_0 a_1 a_2 \ldots a_{l-1}} \equiv V_{a_0} \otimes V_{a_1} \otimes V_{a_2} \otimes \ldots \otimes V_{a_{l-1}} = |a_0 a_1 \ldots a_{l-1}\rangle$) - в суперпозицию состояний

$$\frac{1}{\sqrt{q}} \sum_{c=0}^{q-1} |c\rangle \exp\left(2\pi i ac/q\right). \qquad (20.7)$$

Другими словами, мы хотим применить к состоянию $|a\rangle$ матрицу, элементы (a,c) которой упорядочены по правилу $\frac{1}{\sqrt{q}} \exp\left(2\pi i ac/q\right)$. Такое преобразование Фурье лежит в основе нескольких квантовых алгоритмов. Будем обозначать соответствующую матрицу как A_q. В нашем примере мы ограничимся случаем, когда q является числом, пропорциональным степени двойки. Итак, пусть $q = 2^l$, а целое число a представим двоичной последовательностью $|a_{l-1}, a_{l-2}, \ldots a_1, a_0\rangle$. Оказывается, что для квантового преобразования Фурье A_q нам необходимо только два типа ЛЭ. Это однобитовые логические элементы $R_j \equiv \frac{1}{\sqrt{2}} H$, которые действуют на j-ый бит в квантовом компьютере:

$$R_j = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix},\quad \begin{array}{c|cc} & |0\rangle & |1\rangle \\ |0\rangle & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ |1\rangle & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{array}, \qquad (20.8)$$

и двухбитовые ЛЭ S_{jk}, которые действуют на биты, находящихся в регистре в положениях j и k, $j < k$.:

$$\begin{array}{c|cccc} |j,k\rangle & |00\rangle & |01\rangle & |10\rangle & |11\rangle \\ |00\rangle & 1 & 0 & 0 & 0 \\ |01\rangle & 0 & 1 & 0 & 0 \\ |10\rangle & 0 & 0 & 1 & 0 \\ |11\rangle & 0 & 0 & 0 & e^{i\theta_{k-j}} \end{array}, \qquad (20.9)$$

где $\theta_{k-j} = \pi/(2)^{k-j}$.

Например, пусть регистр представлен бинарной строкой $|01110101\rangle$, т.е. биты пронумированы по индексу l: $|7,6,5,4,3,2,1,0\rangle$. ЛЭ (20.9) действует на пару кубитов из регистра так, что если значения кубитов для индексов j и k, $j < k$ отличаются, либо оба равны нулю, то ничего не происходит, а если кубиты оказываются в состоянии “1”, то значения кубитов не меняются, но добавляется фазовый множитель $\exp\{i\theta_{k-j}\}$. Например, пусть $k = 6$, $j = 2$ (оба кубита имеют значение “1”). Получаем фазовый сдвиг $\exp\{i\theta_{6-2}\} = e^{\frac{i\pi}{2^4}} = e^{\frac{i\pi}{16}}$. Таким образом, действие матриц $S_{j,k}$ при действии их на регистр, сводится к $\sum_{0\le j<k<l} \frac{\pi}{2^{k-j}} a_j b_k$ - т.е. только при $a = b = 1$, добавляется фаза $\exp\left\{i\frac{\pi}{2^{k-j}}\right\}$.

Чтобы выполнить преобразование Фурье, достаточно подействовать на входной регистр набором матриц:

$$R_{l-1}S_{l-2,l-1}R_{l-2}S_{l-3,l-1}S_{l-3,l-2}R_{l-3}...R_1S_{0,l-1}S_{0,l-2}...S_{0,2}S_{0,1}R_0. \qquad (20.10)$$

Другими словами, запись (20.10) означает, что ЛЭ R_j действуют в обратном порядке от R_{l-1} до R_0, а между R_{j+1} и R_j применяются ЛЭ $S_{j,k}$, где $k > j$. Например, для 3-х битов ($l = 0, 1, 2,3$) матрица будет иметь вид:

$$A_q = R_2S_{1,2}R_1S_{0,2}S_{0,1}R_0. \qquad (20.11)$$

Для того, чтобы выполнить преобразование Фурье A_q при $q = 2^l$, нам необходимо l ЛЭ R_j и $1+2+3+...(l-1)$ элементов $S_{j,k}$. Сумма арифметической прогрессии, которую образуют число ЛЭ $S_{j,k}$ равна $S_l = \frac{(a_1+a_n)}{2}n = \frac{1+l-1}{2}(l-1) = l(l-1)/2$. Тогда полное число ЛЭ, реализующих квантовое преобразование Фурье равно $l + \frac{l(l-1)}{2} = \frac{l(l+1)}{2}$. Для трех кубитов

нужно 6 ЛЭ. ***Заметим, что при экспоненциальном росте числа q, количество ЛЭ растет полиномиально с увеличением l.*** Здесь l - число кубитов, необходимых для представления q. Т.е. при добавлении одного двоичного разряда в представлении числа, само число вырастает в 2 раза (экспоненциально), а число ЛЭ - в $\frac{(l+1)(l+2)}{l(l+1)}=\frac{l+2}{l}$ раз. Например, для рассмотренного случая l = 3 (q = 8), при увеличении до l + 1 = 4 (q = 16), получаем $\frac{l+2}{l}=\frac{5}{3}=1.67$ - в такое число раз увеличится число ЛЭ. Если же исходное число кубитов велико, скажем, l = 100 ($2^{100} = 10^{30}$, поскольку $1024 = 2^{10} \approx 10^3$), то $\frac{l+2}{l}=\frac{102}{100}=1.02$ - разница впечатляет!

Применение указанной последовательности преобразований (матриц) (20.10) дает состояние на выходе:

$$\frac{1}{\sqrt{q}}\sum_b \exp\left(2\pi iac/q\right)\left|b\right\rangle, \qquad (20.12)$$

где b представляет собой состояние, в котором все биты переставлены, по отношению к c, т.е. бинарное число, полученное при чтении битов числа c справа налево. Таким образом, для получения настоящего квантового преобразования Фурье, нам нужно либо выполнить еще одно преобразование, переставляющее биты в состоянии $\left|b\right\rangle$ для получения $\left|c\right\rangle$, либо просто читать биты в обратном порядке.

Как же работает такое преобразование Фурье?

Рассмотрим преобразование, переводящее состояние $\left|a\right\rangle=\left|a_{l-1}....a_0\right\rangle$ в состояние $\left|b\right\rangle=\left|b_{l-1}....b_0\right\rangle$. Прежде всего, заметим, что матрица R действует l раз (0, 1, 2,...l-1, т.е. всего l раз). Значит множители $1/\sqrt{2}$ в матрицах R перемножаются, что дает общий множитель $\left(1/\sqrt{2}\right)^l=\frac{1}{2^{\frac{l}{2}}}=\frac{1}{\sqrt{q}}$. Поэтому, остается только понять, как получаются фазовые множители $\exp\left\{2\pi iac/q\right\}$ в выражении (20.7). Прежде всего, заметим, что матрицы $S_{j,k}$ не изменяют значения кубитов, они лишь меняют относительные фазы. Поэтому имеется лишь один способ переключить значение j-ого бита из a_j в b_j - с помощью матриц R_j. Их действие добавляет фазу π, если оба бита a_j и b_j находятся в состоянии 1 (имеют значение 1) и не меняет значение бита в других случаях $a=o, b=0$; $a=0, b=1$; $a=1, b=0$. Далее, действие матрицы $S_{j,k}$ сводится к добавлению $\pi/2^{k-j}$ к соответствующей фазе, когда оба значения битов a_j и b_j равны 1, в противном случае, амплитуды не меняются. Тогда на пути преобразования от $\left|a\right\rangle$ к $\left|b\right\rangle$ происходит изменение фазы

$$\sum_{0\le j<l}\pi a_j b_j+\sum_{0\le j<k<l}\frac{\pi}{2^{k-j}}a_j b_k. \qquad (20.13)$$

Поскольку в первой сумме в (20.13) стоит повторяющийся индекс j, то можно формально учесть это просто оставив только вторую сумму, но потребовав, чтобы индекс j мог бы принимать значение k. Т.о. выражение (20.13) можно преобразовать к виду:

$$\sum_{0\le j\le k<l} \frac{\pi}{2^{k-j}} a_j b_k. \qquad (20.14)$$

Разница с предыдущим заключается только в индексе суммирования.
Поскольку состояние *c* представляет собой “реверсированное” состояние *b*, это выражение можно переписать как

$$\sum_{0\le j\le k<l} \frac{\pi}{2^{k-j}} a_j c_{l-1-k}, \qquad (20.15)$$

где мы просто поменяли порядок изменения индекса *κ*: теперь биты в *c* нумеруются в обратном направлении.
Сделаем замену $l-k-1\to p$ в сумме (20.15). Тогда $k=l-p-1$ и

$$\sum_{0\le j\le k<l} \frac{\pi}{2^{k-j}} a_j c_{l-1-k}, \xrightarrow[l-k-1=p]{} \sum_{0\le k\le l-p-1<l} \frac{\pi}{2^{l-p-1-j}} a_j c_p = \left(Пусть\ p\equiv k\right) \qquad (20.16)$$
$$= \sum_{0\le j+k<l} 2\pi \frac{2^j 2^k}{2^l} a_j c_k.$$

Учтем, что при суммировании добавление фазы 2π не влияет на общую фазу. Тогда, в итоге при суммировании по всем *j* и *k*, меньшим, чем *l*, получаем искомую фазу:

$$\sum_{j,k=0}^{l-1} 2\pi \frac{2^j 2^k}{2^l} a_j c_k = \frac{2\pi}{2^l} \sum_{j=0}^{l-1} 2^j a_j \sum_{k=0}^{l-1} 2^k c_k, \qquad (20.17)$$

где последнее равенство следует из свойства дистрибутивности умножения. Теперь получается, что $q=2^l$, $a=\sum_{j=0}^{l-1} 2^j a_j$ - двоичное представление числа *a* и аналогично для *c*, поэтому выражение (20.17) равно $2\pi ac/q$, что играет роль фазы в комплексной амплитуде перехода $|a\rangle\to|c\rangle$ преобразования (20.7).

Имеется, однако, большая проблема. Преобразование Фурье, которое было рассмотрено - это некая унитарная операция, описываемая матрицей размером LxL. Поэтому нельзя изначально предполагать, что ее можно осуществить за poly (logL) число элементарных операций. Можно показать, что любую унитарную операцию размером LxL можно выполнить на квантовом компьютере за $O\left(L^2\right)$ шагов. Однако классическому компьютеру требуется такое же количество шагов для выполнения операции умножения матрицы размером LxL на L - мерный столбец. В нашем случае Фурье преобразования A_q эта граница не может считаться удовлетворительной. Так для больших значений *j - k* при выполнении преобразования, выполняемого ЛЭ $S_{j,k}$ (20.9), происходит домножение на число, имеющее очень малый фазовый множитель. Так в рассмотренном примере, этот фактор составляет $e^{\frac{i\pi}{16}}$, когда мы брали кубиты, номера которых отличались на 4. Если же оперировать с длинными числами, двоичное представление которых имеет много разрядов, показатель экспоненты резко уменьшается (для кубитов, отличающихся на 8 позиций, он составит $e^{\frac{i\pi}{2^8}}=\exp\{i\pi/256\}$! Такое преобразование очень трудно *точно* реализовать физически и поэтому при выполнении квантовых вычислений появились бы факторы нарушающие такие вычисления. К счастью, было показано (Д.Коппершит, 1994), что результат можно интерпретировать как

приблизительное преобразование Фурье, в котором игнорируются эти малые множители. Такое приблизительное преобразование весьма близко к точному и сильно уменьшает число ЛЭ, реализующих матрицы $S_{j,k}$. В целом, это позволяет выполнить квантовое преобразование Фурье не за $O\left(L^2\right)$, а за $O\left(L\log L\right)$ шагов. Эти свойства вытекают из классической теории быстрого преобразования Фурье, где показано, как уменьшить число в $O\left(L^2\right)$ шагов, нужных для матричного умножения, до $O\left(L\log L\right)$ шагов. Если применить тот же прием в квантовом случае, то модно показать, что число шагов сводится к $O\left(\left(\log L\right)^2\right)$. Этот факт позволяет использовать рассмотренное квантовое преобразование Фурье в алгоритме факторизации.

Алгоритмы факторизации числа на простые множители и дискретного логарифмирования были предложены Питером Шором. Сами по себе эти квантовые алгоритмы, действительно приводящие к выходу из *NP*-класса сложности не являются прорывом в области вычислительной техники, в том смысле, что эти методы, не являются основными в решении вычислительных задач. Единственная причина, по которой они интересны - то, что такие методы (односторонние функции) используются при распределении ключа. Заметим, однако, что к настоящему времени найден классический алгоритм, позволяющий определить является ли данное число простым или нет за полиномиальное время.

Перечислим известные к настоящему времени квантовые алгоритмы.

1. Алгоритм Саймона или задача “Оракула”, 1997г.. (экспоненциальное время при классических вычислениях и квадратичное время при квантовых). Он также известен под названием “алгоритм Дойча” (1985) и, наверное, является первым квантовым алгоритмом. Этот алгоритм решает задачу определения типа функции, глядя только на результат ее действия.
2. Алгоритм разложения на простые множители или алгоритм Шора 1993г. Для факторизации L - битового числа N лучший классический алгоритм[1] асимптотически дает время $O\left(\exp\left(cL^{1/3}\log^{2/3}L\right)\right)$. Квантовый метод дает асимптотически $O\left(L^2\log L\log\log L\right)$ шагов. Заметим, что функция $\log\left(\log L\right)$ растет чрезвычайно медленно, поэтому можно считать, что квантовый метод дает $O\left(L^2\log L\right)$. Ключевая идея этого алгоритма - определение периода некой последовательности с помощью фурье-преобразования. Период этой последовательности экспоненциально зависит от L, поэтому такой метод непрактичен для обычных классических вычислений.
3. Алгоритм поиска в базе данных . Известен также под названием “алгоритм Гровера” 1997г. Имеется список из N наименований. Классический алгоритм дает порядка $N/2$ обращений к базе данных для отыскания нужного наименования. Квантовый требует порядка $O\left(\sqrt{N}\right)$ обращений. Например,

[1] С поправкой на статью, вышедшую в 2002 г, где предлагается классический полиномиальный алгоритм, требующий времени порядка $O\left(\left(\log L\right)^{12}\right)$.

если N = 10^4, классический метод дает ответ примерно за 5000 обращений, а квантовый - за 100. Если же $N = 10^6$, то в классике поиск потребует $5x10^5$. А квантовый метод всего 1000!

ЛИТЕРАТУРА

1. P.Shor. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on Quantum Computer. Quant-ph/9508027.
2. P.Shor. Introduction to Quantum Algorithms. Quant-ph/000503.

ЛЕКЦИЯ 21. ХОЛОДНЫЕ ИОНЫ В ЛОВУШКАХ.

21.1. Основные положения, лежащие в основе метода П.Цоллера и Дж.Цирака:
кубит, представлен двухуровневым ионом;
уровни - долгоживущие; к каждому иону имеется доступ в виде сфокусированного излучения;
ионы локализованы в ловушке - их движение ограничено;
кулоновское отталкивание обуславливает коллективное движение ионов;
имеются вспомогательные уровни и лазеры для чтения данных.

21.2. Формула Раби для переходов в классическом поле. Модель Джейнса-Каммингса и предел Лэмба-Дике.

21.3. Схема уровней в модели квантовых вычислений Цирака и Цоллера. Доступ посредством оптических и рамановских переходов.

21.4. Модельный гамильтониан и мода центра масс. Случай точного резонанса. Воздействие $\pi/2$-, π-, и 2π-импульсов.

21.5. Реализация ЛЭ CNOT.

21.6. Чтение состояния регистра ионов.

В этой лекции мы рассмотрим метод квантовых вычислений, предложенный Цираком и Цоллером.

1. Будем считать, что кубит - это двухуровневый ион. Эти уровни должны быть долгоживущими, что даст возможность пренебречь процессами спонтанного излучения - одним из основных факторов, приводящих к декогернции.
2. Предположим, что к каждому иону имеется доступ при помощи сфокусированного лазерного излучения (Рис.1.).
3. Ионы находятся в линейной ловушке (Пауля), что ограничивает их поступательное движение (Рис.2.).
4. Благодаря кулоновскому взаимодействию (отталкиванию), направленному вдоль оси ловушки, возникает коллективное движение ионов. Это приводит к тому, что отдельные ионы могут взаимодействовать между собой посредством “колебательной шины данных”.
5. Чтение конечного состояния такого регистра ионов осуществляется с помощью других лазеров.

Будем считать, что ионы в ловушке имеют по крайней мере один долгоживущий (узкий) уровень. Такой уровень может оказаться в микроволновом диапазоне (например, благодаря переходу в сверхтонкой структуре), либо в оптическом диапазоне (переходы в метастабильное возбужденное состояние). Например, используются ионы бериллия $^9Be^+$ с переходом в УФ диапазоне на длине волны 313нм (переход $^2S_{1/2} \to {}^2P_3$).

Итак, предположим, что ионы, благодаря конфигурации ловушки, двигаются в гармоническом потенциале с частотами

$$\omega_z \ll \omega_x, \omega_y \qquad (21.1)$$

Это соотношение означает, что ионы локализованы вдоль оси z и их поперечным движением можно пренебречь.

Схема уровней, показанная на рис.2 является типичной для редкоземельных ионов.

Далее будем предполагать, что ионы охлаждены до температур порядка 10^{-6} К, поэтому колебательные движения вдоль оси z происходят так, что все они находятся в основном состоянии, т.е. в состоянии равновесия. В этом случае

движение ионов описывается в терминах нормальных мод, т.е. сводится к движению несвязанных осцилляторов. Осцилляторы могут быть проквантованы стандартным способом. Низшее возбужденное состояние колебаний является возбужденным состоянием движения центра масс *N* ионов (ЦМ).
Коллективные колебания ЦМ служат своеобразной шиной данных, которая обуславливает взаимодействие ионов.
Физическое требование, которому должна удовлетворять система, состоит в достижении предела Лэмба-Дике. Это означает, что каждый ион локализован в области много меньшей, чем длина волны используемого излучения. Типичные значения расстояний между ионами составляют единицы - десятки микрометров.

Задача о квантовых вычислениях на любой физической системы сводится к возможности построения одно- и двухкубитовых ЛЭ. Однокубитовые ЛЭ в системе “ион (атом) + поле” создать достаточно просто. Для этого существует техника переходов Раби, которая позволяет управлять внутренним состоянием кубита. Однокубитовые переходы и, следовательно, ЛЭ связаны только с вращением вектора состояния отдельного иона (вектора Блоха) без изменения его перемещения

Напоминание.
Вероятность перехода в двухуровневой системе под действием классического поля с частотой ω дается формулой Раби:

$$W_{12} = \frac{|\Omega|^2}{|\Omega|^2 + \Delta^2} \sin^2\left(\frac{\sqrt{|\Omega|^2 + \Delta^2}}{2} t \right), \qquad (21.0)$$

где $\Omega = \frac{\langle e|d|g\rangle \cdot E}{\hbar}$ - частота Раби, а $\Delta = \omega_{21} - \omega$ -расстройка между частотой поля и боровской частотой (частотой перехода $\omega_{21} = \frac{E_2 - E_1}{\hbar}$). Этот результат получается по теории возмущений при условиях, когда амплитуды состояний малы, т.е. $\Omega \ll \Delta$. (*конец напоминания*)

Обозначим атомные уровни, которые мы будем использовать для проведения вычислений, как $|g\rangle, |e\rangle$. Также введем вспомогательный уровень $|e'\rangle$. Структура уровней ионов показана на рис.3. В оригинальной работе частоты переходов ω и ω' вырождены. Эти переходы возбуждаются излучением с разной поляризацией. Но удобнее рассматривать невырожденный режим, поскольку экспериментальные методы частотной селекции развиты лучше, чем поляризационный контроль. Также мы будем считать, что лазерное поле непосредственно находится в резонансе с соответствующими парами уровней (для простоты), хотя часто эти переходы дипольно запрещены и используется техника рамановского возбуждения на разностной частоте.

На рис.3 второй символ, обозначающий состояние, относится к колебательному движению центра масс (внешняя степень свободы), а первый - к внутренней степени свободы иона. Так, символы $|0\rangle, |1\rangle$ обозначают основное и возбужденные состояния колебаний ЦМ, которые не будут использоваться при вычислениях, но являются вспомогательными.
Вообще, связь между ЦМ иона и его внутренней энергией возникает из электро-дипольного взаимодействия:

$$dE(r,t) = d\{E(0,t) + r\,\mathrm{grad}\,E(0,t) + ...\}, \quad (21.2)$$

$$Z = \sqrt{\frac{\hbar}{2m\omega_z}}\left(A + A^{\dagger}\right). \quad (21.3)$$

Здесь A - оператор уничтожения фонона для моды ЦМ, а E - напряженность поля.

Если лазер настроен на частоту ω, то в резонансе оказывается пара уровней $|g,p\rangle$ и $|e,p\rangle$. Таким образом, осцилляции ЦМ при такой настройке не возникают. Гамильтониан, описывающий такое взаимодействие поля и вещества имеет вид:

$$H = E|e\rangle\langle e| + \frac{1}{2}\Omega e^{i\phi}|e\rangle\langle g| + \frac{1}{2}\Omega e^{-i\phi}|g\rangle\langle e|, \quad (21.4а)$$

где E - энергия перехода, а электромагнитное поле рассматривается классически, Ω - частота Раби.

Если лазер настроен на частоту $\omega - \omega_z$, то в резонансе оказывается пара уровней $|g,1\rangle$ и $|e,0\rangle$. В этом случае гамильтониан, описывающий взаимодействие имеет вид:

$$H = E|e\rangle\langle e| + \frac{\eta\Omega}{2\sqrt{N}}\left(e^{i\phi}|e\rangle\langle g|A + e^{-i\phi}|g\rangle\langle e|A^{\dagger}\right), \quad (21.4б)$$

где N - число ионов, находящихся в ловушке, A - оператор уничтожения фонона в моде ЦМ, η - параметр Лэмба-Дике, который равен

$$\eta = \sqrt{\frac{\hbar k^2 \cos^2\theta}{2M\omega_z}} = \sqrt{\frac{\left(\textit{энергия отдачи иона}\right)^2}{\textit{энергия фонона ЦМ}}} \quad (21.5в)$$

Если же лазер настроен на частоту $\omega' - \omega_z$, то в резонансе оказывается пара уровней $|g,1\rangle$ и $|e',0\rangle$

Прежде, чем двигаться дальше, нам нужно подробнее остановиться на модели взаимодействия поля с веществом.

<u>Модель Джейнса-Каммингса.</u>

Мы рассматриваем двухуровневую систему, которую будем представлять атомом, имеющего основное $|g\rangle$ и возбужденное $|e\rangle$ состояния. Атом взаимодействует с одной модой электромагнитного поля, например, в резонаторе. Гамильтониан системы имеет вид:

$$H_0 = E|e\rangle\langle e| + \omega a^{\dagger}a, \quad (21.5)$$

$$H_1 = \frac{1}{2}\Omega|e\rangle\langle g|ae^{i\phi} + \frac{1}{2}\Omega|g\rangle\langle e|a^{\dagger}e^{-i\phi}. \quad (21.6)$$

Три члена в (5, 6) символично отражены на схемах переходов, показанных на рис.4. Будем полагать $\hbar \equiv 1$. Мы ввели т.н. мгновенную частоту Раби:

$$\Omega e^{i\phi} = -2\langle e|d|g\rangle E. \quad (21.7)$$

Здесь d - оператор дипольного момента атома, а E - амплитуда электрического поля. ϕ - фаза поля в центре атома. Заметим, что частота Раби - действительная величина. В модели предполагается, что частотная расстройка

$$\Delta = E - \omega \quad (21.8)$$

мала, т.е.

$$|\Delta| \ll \omega, \tag{21.9}$$

а разность энергий для всех других атомных уровней удовлетворяет условию

$$|\Delta| \gg E'. \tag{21.10}$$

В общем же будем считать, что частота Раби

$$|\Omega| \ll \omega. \tag{21.11}$$

Заметим, что в модели также используется приближение вращающейся волны, когда удерживаются только медленно меняющиеся члены при взаимодействии.
Рассмотрим оператор

$$S = a^{\dagger}a + |e\rangle\langle e|, \tag{21.12}$$

который коммутирует с гамильтонианом. Это означает, что гильбертово пространство состояний разделяется на два ортогональных подпространства.
Подпространство с собственным значением оператора S: s = 0, представляет основное состояние атома и отсутствие фотонов: $|g,0\rangle$.

$$H|g,0\rangle = 0. \tag{21.13}$$

Это состояние будем рассматривать как основное состояние системы.

Подпространство с $s \geq 1$ охватывает состояния $|g,s\rangle$ и $|e,s-1\rangle$. Отсюда, задача о решении уравнения Шредингера сводится к двумерной задаче.
В представлении взаимодействия

$$|\Psi_I\rangle = e^{iH_0}|\Psi\rangle, \tag{21.14}$$

$$O_I = e^{iH_0 t} O e^{-iH_0 t}. \tag{21.15}$$

Тогда, возмущенная часть гамильтониана

$$H_1 \to H_I = \frac{1}{2}\left(\Omega|e\rangle\langle g|ae^{i\phi}e^{i\Delta t} + \Omega|g\rangle\langle e|a^{\dagger}e^{-i\phi}e^{-i\Delta t}\right), \tag{21.16}$$

а волновая функция удовлетворяет уравнению

$$i\frac{\partial \Psi_I}{\partial t} = H_I \Psi_I. \tag{21.17}$$

Для $s \geq 1$, положим

$$|\Psi_I\rangle = |\psi_s\rangle = c_{gs}|g,s\rangle + c_{es}|e,s-1\rangle. \tag{21.18}$$

Из уравнения (17) можно найти коэффициенты c_{gs} и c_{es}.
Вкратце, рассмотрим решения.
Случай точного резонанса, $\Delta = 0$:

$$E_{s\pm} = s\omega \pm \frac{1}{2}\sqrt{s}\Omega. \tag{21.19}$$

Для $s \geq 1$ собственные функции имеют вид перепутанных состояний атома и электромагнитного поля:

$$|\Psi_{s\pm}\rangle = \sqrt{\frac{1}{2}}\left(|g,s\rangle \pm e^{-i\phi}|e,s-1\rangle\right). \tag{21.20}$$

Другими словами, состояние системы описывается суперпозицией двух возможностей: атом в основном состоянии плюс фотон; атом в возбужденном состоянии, фотонов нет.

Матрица унитарного преобразования e^{-iHt} для подпространства $s \geq 1$ имеет вид:

$$V_s(\Omega t,\phi)=\begin{array}{c} \\ |g,s\rangle \\ |e,s-1\rangle \end{array}\begin{array}{c} \begin{array}{cc} |g,s\rangle & |e,s-1\rangle \end{array} \\ \begin{pmatrix} \cos\frac{\sqrt{s}}{2}\Omega t & ie^{-i\phi}\sin\frac{\sqrt{s}}{2}\Omega t \\ ie^{i\phi}\sin\frac{\sqrt{s}}{2}\Omega t & \cos\frac{\sqrt{s}}{2}\Omega t \end{pmatrix} \end{array} \tag{21.21}$$

Рассмотрим случай одного фотона s =1. Для $\Omega t=\pi,$ из (21) получаем:

$$V_s(\pi,\phi)=\begin{pmatrix} 0 & ie^{-i\phi} \\ ie^{i\phi} & 0 \end{pmatrix}. \tag{21.22а}$$

Если фаза лазера равна $\phi=\pi/2,$ то получаем преобразование

$$V_s(\pi,\pi/2)=\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \tag{21.22б}$$

т.е. $|g,1\rangle\to-|e,0\rangle$ и $|e,0\rangle\to|g,1\rangle.$

или, другими словами, состояние атома меняется на противоположное. Такой импульс поля называется π - *импульсом*.

Если время взаимодействия равно $\Omega t=2\pi$, то матрица (21) становится

$$V_s(2\pi,\phi)=-\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \tag{21.22в}$$

для любых значений фазы ϕ *поля!*

Пусть теперь время взаимодействия атома и поля равно $\Omega t=\pi/2.$ Матрица (21) принимает вид:

$$V_1(\pi/2,\phi)=\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & ie^{-i\phi} \\ ie^{i\phi} & 1 \end{pmatrix}. \tag{21.23}$$

Если в начальный момент состояние системы было $|e,0\rangle$, т.е. представляло собой факторизованное состояние поля и вещества, то после взаимодействия состояние принимает вид перепутанного:

$$|e,0\rangle\to\frac{1}{\sqrt{2}}\left(|e,0\rangle+ie^{-i\phi}|g,1\rangle\right). \tag{21.24}$$

Такое воздействие называется $\pi/2$ - *импульсом*.

Важным, для дальнейшего рассмотрения, является случай преобразования

$$V_1(\pi/2,\pi/2)=\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}=R \tag{21.25}$$

Это частный случай $\pi/2$ - *импульса*, когда фаза электромагнитного поля в центре атома равна $\phi=\pi/2.$

Такое преобразование $V_s(\theta,\phi)$ может быть реализовано несколькими способами и в различных системах. Однако в этой лекции мы ограничимся лишь случаем ионов в ловушке, на каждый из которых сфокусировано управляющее лазерное излучение. Заметим, лишь, что для системы, состоящей из атомов в резонаторе, импульсы поля прикладываются при пролете атома через микроволновой резонатор. В методе ядерного магнитного резонанса, прикладываются аналогичные импульсы магнитного поля.

Теперь мы можем приступить к моделированию ЛЭ CNOT, реализованному на основе любой пары ионов, имеющихся в ловушке.

Напомним, что этот двухкубитовый обратимый ЛЭ выполняет функцию:

$$CNOT\left|x_{control}, x_{target}\right\rangle = \left|x_{control}, x_{target} \oplus x_{control}\right\rangle. \qquad (21.26)$$

Возьмем $g_1 = 0_{control}$; $e_1 = 1_{control}$; $g_2 = 0_{target}$; $e_2 = 1_{target}$. Запись (26), как обычно, означает, что состояние контрольного кубита сохраняется. А состояние кубита-мишени становится результатом сложения по модулю "2" значений контрольного кубита и кубита мишени.

Тогда искомая операция будет выражаться следующим набором преобразований:

$$CNOT = R_2\left(CSF\right)_{12} R_2^{-1}, \qquad (21.27)$$

где оператор R_2 - это введенный выше оператор R для иона 2:

$$R = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix},$$

а т.н. оператор "control sign flip" действует на ионы 1 и 2 по правилу:

$$\begin{aligned} &\left|g_1, g_2, 0\right\rangle \to \left|g_1, g_2, 0\right\rangle, \\ &\left|g_1, e_2, 0\right\rangle \to \left|g_1, e_2, 0\right\rangle, \\ &\left|e_1, g_2, 0\right\rangle \to \left|e_1, g_2, 0\right\rangle, \\ &\left|e_1, e_2, 0\right\rangle \to -\left|e_1, e_2, 0\right\rangle. \end{aligned} \qquad (21.28)$$

Здесь слева выписаны все возможные комбинации состояний двух двухуровневых ионов 1 и 2, находящихся в основном колебательном состоянии моды ЦМ $\left|0\right\rangle$.

Рассмотрим, каким образом можно осуществить эти операции в рамках нашей системы.

Оператор R. Для выполнения этой операции мы подаем $\pi/2$ - *импульс* на ион 2 с помощью соответствующим образом сфазированного и настроенного по частоте лазера. Напомним, что в модели Джейнса-Каммингса этот оператор задается выражением (25).

Оператор CSF. Он задается действием операторов

$$CSF_{12} = U_1\left(\pi, 0\right) W_2\left(2\pi, 0\right) U_1\left(\pi, 0\right). \qquad (21.29)$$

Здесь $U_1\left(\pi, 0\right)$ - это π- импульс, подаваемый на первый ион, с фазой $\phi = 0$, когда частота лазера настроена на переход $\omega_a = \omega - \omega_z$ (такая операция оставляет состояние иона 2 без изменения!) и приводит к следующим преобразованиям:

$$\begin{aligned} &(1)\left|g_1, p_2, 0\right\rangle \to \left|g_1, p_2, 0\right\rangle, \\ &(2)\left|g_1, p_2, 1\right\rangle \to \left|e_1, p_2, 0\right\rangle, \\ &(3)\left|e_1, p_2, 0\right\rangle \to -\left|g_1, p_2, 1\right\rangle, \\ &(4)\left|e_1, p_2, 1\right\rangle \to \left|e_1, p_2, 1\right\rangle. \end{aligned} \qquad (21.30)$$

По-прежнему, символ p обозначает любое состояние (второго) иона.

Оператор $W_2(2\pi,0)$ описывает действие 2π- импульса с фазой $\phi=0$, когда частота лазера настроена на переход $\omega'-\omega_z$. При этом все состояния остаются без изменения, за исключением (см. 22в):

$$(1)\left|p_1,g_2,1\right\rangle\to-\left|p_1,g_2,1\right\rangle,$$
$$(2)\left|p_1,e_2',0\right\rangle\to-\left|p_1,e_2',0\right\rangle. \qquad (21.31)$$

С учетом правил действия операторов (30, 31) получаем необходимые преобразования:

$$\left|g_1,g_2,0\right\rangle\xrightarrow{30(1)}\left|g_1,g_2,0\right\rangle\xrightarrow{31(unchanged)}\left|g_1,g_2,0\right\rangle\xrightarrow{30(1)}\left|g_1,g_2,0\right\rangle,$$

$$\left|g_1,e_2,0\right\rangle\xrightarrow{30(1)}\left|g_1,e_2,0\right\rangle\xrightarrow{31(unchanged)}\left|g_1,e_2,0\right\rangle\xrightarrow{30(1)}\left|g_1,e_2,0\right\rangle,$$

$$\left|e_1,g_2,0\right\rangle\xrightarrow{30(3)}-\left|g_1,g_2,1\right\rangle\xrightarrow{31(1)}\left|g_1,g_2,1\right\rangle\xrightarrow{30(2)}\left|e_1,g_2,0\right\rangle,$$

$$\left|e_1,e_2,0\right\rangle\xrightarrow{30(3)}-\left|g_1,e_2,1\right\rangle\xrightarrow{31(unchanged)}-\left|g_1,e_2,1\right\rangle\xrightarrow{30(2)}-\left|e_1,e_2,0\right\rangle.$$

Мы получили в итоге результат, совпадающий с (28). *Заметим, что конечным результатом эволюции будет перемена знака, но лишь в том случае, если оба иона находятся в возбужденном (внутреннем) состоянии* $\left|e\right\rangle$. *И до, и после логической операции CNOT мода ЦМ находится в вакуумном (невозбужденном) состоянии* $\left|0\right\rangle$.

Операция чтения данных.

Наиболее распространенным методом регистрации внутреннего состояния ионов осуществляется в т.н. методе “размещения” электронов.

Эта процедура может быть выполнена при использовании какого-нибудь другого уровня и лазера, настроенного на частоту перехода между этим уровнем и основным состоянием $\left|g\right\rangle$. Если такой переход разрешен, то процесс будет сопровождаться резонансной флуоресценцией или рассеянием в случае, когда система находится в состоянии $\left|g\right\rangle$ и не будет, когда система находится в состоянии $\left|e\right\rangle$. Представим себе, что основное состояние $\left|g\right\rangle$ на некоторое время связывается с возбужденным $\left|e\right\rangle$, например, при действии $\pi/2$ - импульса. Тогда ион оказывается в состоянии суперпозиции $\alpha\left|g\right\rangle+\beta\left|e\right\rangle$. Если затем осуществить переход между двумя состояниями $\left|g\right\rangle$ и $\left|p\right\rangle$ (дипольно-разрешенный переход с малым временем жизни), то состояние $\left|p\right\rangle$ возбудиться, а затем распадатся с испусканием фотона (спонтанное испускание). Это произойдет только, если система находилась в состоянии $\left|g\right\rangle$! Таким образом, регистрация фотонов, испущенных в процессе такого распада и является косвенным признаком того, что система находилась в состоянии $\left|g\right\rangle$. Измерение таких фотонов будет происходить с вероятностью $\left|\alpha\right|^2$, поскольку это и есть вероятность найти систему в состоянии $\left|g\right\rangle$. Даже если эффективность детектирования фотона при единичном распаде $\left|p\right\rangle$ очень мала (в эксперименте

она составляет десятые доли процентов), то можно повторить возбуждение много раз и увеличить число “рассеянных” фотонов - тем самым будет однозначно зарегистрировано, что система находилась в состоянии $|g\rangle$. Если же система размещается в метастабильном состоянии $|e\rangle$, то фотоны излучаться не будут. После усреднения по многим экспериментам, количество испытаний, в которых наблюдались фотоны, окажется пропорциональным $|\alpha|^2$

Заметим, что реализация всего протокола вычислений на системе ионов в ловушке (мы рассмотрели лишь ЛЭ CNOT) крайне трудна. Лишь отдельные ее компоненты были продемонстрированы, а именно, колебательное движение ЦМ системы, состоящей из семи ионов (Инсбруг).
Заметим также, что для выделения двух сверх-узких уровней, работающих в качестве кубитов возможно несколькими путями. Доступ к этим уровням возможен непосредственно с помощью лазера, если переход лежит в оптическом диапазоне (резонансное возбуждение) или с помощью двух лазеров и т.н. ***рамановского перехода***, когда в резонансе оказывается разностная частота (Рис. 5).

ЛИТЕРАТУРА

1. J.Cirac and P.Zoller. Quantum Computations with Cold Trapped Ions. Phys.Rev.Lett. 74, 4091 (1995).
2. П.В.Елютин. Теоретические основы квантовой радиофизики. Изд-во МГУ, 1982.
3. Д.Боумейстер, А.Экерт, А.Цайлингер. Физика квантовой информации. Москва, “Постмаркет”, 2002. - 376 с.
4. M.Rubin and / Lectures on Quantum Computations. UMBS, 1999 (unpublished).

ФИЗИЧЕСКИЙ
ФАКУЛЬТЕТ
МГУ ИМЕНИ
М.В. ЛОМОНОСОВА