ФИЗИЧЕСКИЙ
ФАКУЛЬТЕТ
МГУ ИМЕНИ
М.В. ЛОМОНОСОВА

teach-in
ЛЕКЦИИ УЧЕНЫХ МГУ

ФИЗИЧЕСКИЕ ОСНОВЫ КВАНТОВОЙ ИНФОРМАЦИИ

КУЛИК
СЕРГЕЙ ПАВЛОВИЧ

ФИЗФАК МГУ

КОНСПЕКТ ПОДГОТОВЛЕН СТУДЕНТАМИ, НЕ ПРОХОДИЛ ПРОФ. РЕДАКТУРУ И МОЖЕТ СОДЕРЖАТЬ ОШИБКИ. СЛЕДИТЕ ЗА ОБНОВЛЕНИЯМИ НА VK.COM/TEACHINMSU.

ЕСЛИ ВЫ ОБНАРУЖИЛИ ОШИБКИ ИЛИ ОПЕЧАТКИ, ТО СООБЩИТЕ ОБ ЭТОМ, НАПИСАВ СООБЩЕСТВУ VK.COM/TEACHINMSU.

БЛАГОДАРИМ ЗА ПОДГОТОВКУ КОНСПЕКТА
СТУДЕНТА ФИЗИЧЕСКОГО ФАКУЛЬТЕТА МГУ
МЕЛЕЖЕНКО ДАНИЛА ЕВГЕНЬЕВИЧА

ОГЛАВЛЕНИЕ

Лекция 1. Квантовые технологии

Последние 10-20 лет ознаменованы колоссальным ростом разных технологий, на основе этих развивающихся технологий в эксперименте стало значительно легче работать. Вся квантовая механика двадцатого века подразумевает работу (и в теории, и в эксперименте) с ансамблем квантовых частиц, будь то фотоны, коллективные объекты-микрообъекты-нанообъекты. В настоящее время работа опустилась на уровень одиночных квантовых объектов.

Закон Мура

Начнем с утверждения о том, что у электрона (да и у любого микрообъекта) нет траектории. По соотношению неопределенности Гейзенберга, чем лучше известна одна из канонически сопряженных переменных, тем хуже можно измерить вторую. Так, при измерении координаты/уменьшении неопределенности в ней (а траектория – это одновременное знание координаты и импульса) и точно зная, где находится объект, вектор импульса становится совершенно неопределенным.

Аналогии очень помогают и будут часто использоваться в рамках курса, однако стоит помнить, что аналогия – это всегда некое ограничение, поэтому полностью уходить в аналогии не стоит. Аналогия канонически сопряженных переменных и соотношений неопределенности – прохождение света через щель (дифракция). Вместо плоской волны можно также мыслить в терминах фотонов, где фотон – волновой пакет огибающей Гаусса с частотой ω и энергией $\hbar\omega = \mathcal{E}$.

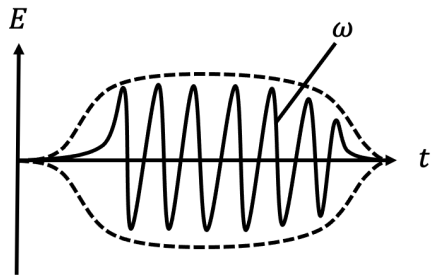

Рис.1.1. Фотон как волновой пакет.

При уменьшении потока фотонов любыми доступными способами в какой-то момент непрерывное распределение напряженности поля станет прерывным, так как свет, согласно некой интерпретации, состоит из отдельных частиц – фотонов. Еще одной аналогией может являться разлитая по столу жидкость, представляющая собой непрерывную пленку. Когда пленку сушат, она существенно уменьшается и превращается в капельки. Так, сушка – это ослабление, а капельки – это цуги.

Сразу же возникает вопрос о длине и времени излучения. Относительно времени оно определяется длиной когерентности излучения. Длина когерентности определяется исходным спектром излучения. Для того, чтобы понять пространственно-временные масштабы излучения необходимо пропустить пакет через интерферометр (заставить

интерферировать само с собой) – то, что разбивает пучок пополам, задерживает одну часть и сводит вместе.

Принцип измерения длины когерентности подразумевает такую задержку, чтобы потом, когда части встретятся, они уже перестали интерферировать, – это называется длиной когерентности. Также можно пропустить излучение через фильтр и сделать длину когерентности достаточно большой (например, 10 м), либо достаточно маленькой (в несколько см), это зависит от желаний экспериментатора. Главное – понимать пространственно-временные масштабы и чем они определяются. В данный момент мы рассматриваем продольную когерентность: то, что обуславливает интерференционные эффекты, если, поделив пополам, одну часть свернуть саму с собой, задержать и снова сбить. Поперечные масштабы подразумевают то же самое, но другой тип интерферона: интерферон Юнга (когда два отверстия совпадают, свет интерферирует сам с собой в одной точке. Если же их раздвинуть, то появляется радиус когерентности и то расстояние, на котором контраст осцилляции падает, называется радиусом поперечной когерентности).

Закон Мура заключается в том, что уменьшаются размеры интегральных схем, и в какой-то момент доходит до атомарного фотонного масштаба, что является проблемой. Это эмпирический закон, согласно которому число транзисторов в кристалле одной интегральной схемы (плотность упаковки) в течение первых 15 лет удваивалось каждый год.

Проблемы квантовой технологии

Первая проблема, которая стоит в квантовой технологии, связана с уменьшением масштабов, с которыми работают технологи (технологии позволяют работать все с меньшими масштабами, что приводит к тому, что мы упираемся в фотонный масштаб, а траектории для квантовых частиц нет, что не позволяет осуществлять наблюдение, так как сам процесс возмущает эту систему).

Вторая проблема – выделение энергии и рассеяния мощности: чем быстрее процессоры, те больше они греются. Существует целая наука о том, как их охлаждать/снимать тепло. Где находится термодинамический предел логической операции? Существует понятие бита – некой ячейки, хранящей два значения уровня энергии, и есть классические транзисторы, реализующие эти биты (устройства, при воздействии импульсом извне на которые состояние ячейки меняется на противоположное). За переброс бита отвечает такая термодинамическая величина как энтропия (как известно из термодинамики, энтропия связана с энергией). Тогда порог по выделению тепла, связанный с изменением состояния ячейки памяти, связан с переворотом на один бит, — это является неким термодинамическим порогом (все вычислительные процессы связаны с изменением состояния ячеек памяти).

Так, стоит понимать, что квантовость технологий ведет к уменьшению масштабов, что вынуждает упираться в масштаб порядка размера атома, где необходимо

учитывать соотношение неопределенности (наблюдение за системой уже меняет ее состояние).

Квантовые вычисления

Классические квантовые вычисления – это некое функциональное соотношение, когда соотношению y ставят в соответствие некий x или наоборот:

$$y \to F(x) \tag{1.1}$$

Есть понятие термодинамически обратимых операций (когда не происходит выделение тепла), а есть – логически обратимых (когда, например, из функции (1.1) можно посчитать обратную):

$$y \leftarrow F^{-1}(x) \tag{1.2}$$

Фундаментальных классических операций не так много. Самая известная битовая операций – инверсия. Таблица истинности:

0	1
1	0

Операция логически обратима. Одна из базовых операций – «управляемое нет» ($CNOT, XOR$):

a	b	$a \otimes b$	$a \otimes (a \otimes b)$
0	0	0	0
0	1	1	1
1	0	1	0
1	1	0	1

Так, есть контрольный бит, а есть бит-мишень (тот, что изменяется на выходе). Такая операция логически необратима. Для того, чтобы сделать ее обратимой, необходимо еще раз применить операцию $CNOT$ к результату (четвертый столбец). Так, получаем значения, схожие со значениями бита b, а значит операция обратима (если сохраняем в памяти значение одного из битов).

Рассмотрим еще одно свойство этой операции. Мы осуществляем ее со значениями $XOR(X, 0)$, где X -число с любым значением (0 или 1). Если a – любой, а $b = 0$ (первая и третья строчка таблицы истинности), то

$$XOR(X, 0) = (X, X) \tag{1.3}$$

Рассмотрим квантовый бит и обозначим это состояние двухуровневой системой:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \tag{1.4}$$

где $|0\rangle$ и $|1\rangle$ – вектора кет, а α и β – комплексные числа, связанные условиями нормировки. По условию игры, векторы ортогональны друг другу, волновая функция должна быть нормирована, а также

$$|\alpha|^2 + |\beta|^2 = 1 \tag{1.5}$$

Так, это есть произвольно представление квантового бита – кубита. Рассмотрим следующее состояние:

$$\frac{1}{\sqrt{2}}\{|0\rangle + |1\rangle\} \tag{1.6}$$

Применим к нему правило копирования:

$$(X, 0)\overset{XOR}{\rightarrow} = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle, |0\rangle) = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle) \tag{1.7}$$

Если условно обозначить $\frac{1}{\sqrt{2}}\{|0\rangle + |1\rangle\} = |D\rangle$ (диагональное состояние), то мы ждем, что по классике получится $(D, 0) = (D, D)$, но получается перепутанный класс состояний. Вкратце он подразумевает, что есть два кубита (контрольный и мишень); получается также двухкубитовое состояние, описываемое вектором

$$\frac{1}{\sqrt{2}}(|0_a\rangle|0_b\rangle + |1_a\rangle|1_b\rangle) \equiv |\psi_{ab}\rangle, \tag{1.8}$$

которое следует читать следующим образом: если значение одного кубита равно нулю, то значение второго обязательно будет равно нулю. Так, в квантовой механике суперпозиция всегда этимологически подразумевает под собой «или», т.е. «если…, то…, или если…, то…». Раз (1.8) заканчивается вектором – чистым состоянием (полностью определенное состояние), следовательно, мы знаем волновую функцию, подставляем в уравнение Шредингера, решаем и можем получить ответ в любой момент времени. Вычислить состояние подсистемы по правилам квантовой механики (например, состояние кубита a) можно следующим образом:

$$\rho_a = \frac{1}{2}[|0\rangle\langle 0| + |1\rangle\langle 1|] = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix}, \tag{1.9}$$

где $|0\rangle\langle 0|$ – диада (матричное представление оператора), ρ – оператор (матрица) плотности. Такая полная смесь означает, что нам неизвестно, в каком состоянии находятся кубиты. Так, мы получили перепутанное состояние, которое является максимально определенным (чистым) в двухкомпонентной системе и смешанным (совершенно неопределенным) для подсистем.

Парадокс «Демон Максвелла»

Есть некая ячейка (баллон), у которой есть некий поршень, позволяющий движение туда-обратно с минимальным трением. Баллон можно условно поделить

пополам – посередине есть отверстие, куда без трения то опускается, то вынимается перегородка: опустили – два баллона, подняли – один. В баллоне находится одна молекула; наблюдатель, опускающий и поднимающий перегородку, отмечает, что молекула оказывается в одной из частей и опускает перегородку. Так, в одной половине находится молекула, в другой – вакуум. Следующим шагом двигаем поршень по половине с вакуумом в направлении перегородки, в этот момент наблюдатель убирает перегородку. Молекула бесполезно бьется о стенки, но если бьется о поршень, то может его отодвинуть. Когда молекула бьется о стержень, то он отъезжает, совершает работу. Поршень отъехал, работа совершена, молекула летает по всему пространству баллона, мы вернулись в начальное состояние. В чем заключается парадокс? Можно бесконечно извлекать работу из вакуума, однако у наблюдателя после выполнения всех этапов остается бит информации, который следует стереть из памяти, чтобы не перегреться при миллионном повторении операции (так как при каждом выполнении будет выделяться $kT\ln 2$).

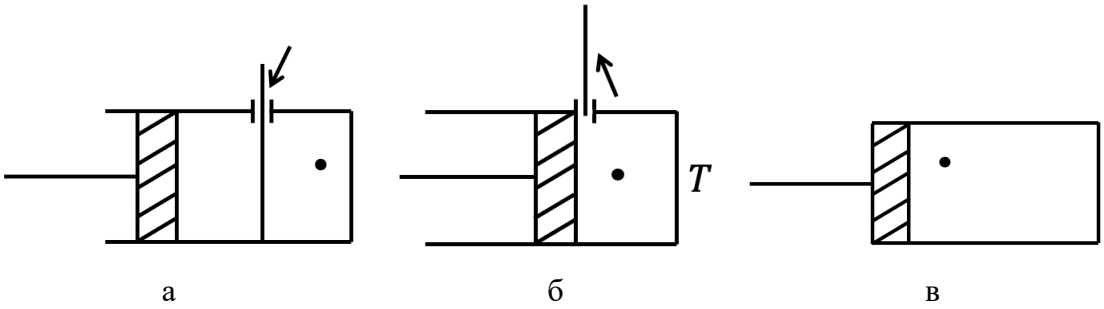

Рис.1.2. Поэтапное графическое изображение парадокса Максвелла.

Парадокс был разрешен в начале 60-х годов Чарльзом Беннетом, связавшим энтропию с информацией.

Лекция 2. Классическая информация

Разберем общие сведения для того, чтобы в дальнейшем оперировать ими в области квантовой механики. Есть регистр, набор из ячеек, в каждой из которых может быть либо 0, либо 1.

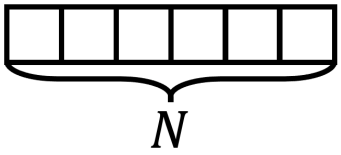

Рис. 2.1. Регистр из ячеек.

Такое информационное содержание ячейки называется битом. Тогда количество информации, которое можно записать в ячейках, равно

$$Q_n = 2^N \tag{2.1}$$

Сообщением называется набор символов, оказавшихся в регистре. Тогда вероятность того, что наугад выбранное сообщение совпадет с задуманным равно

$$P_N = \frac{1}{Q_N} \tag{2.2}$$

Информацией (информационное содержание) или энтропией называется число используемых в битах ячеек ($H, S \to N$).

$$H_{bit} = N = \log_2 Q_N = \log_2 \frac{1}{P_N} = -\log_2 P_N \tag{2.3}$$

Если рассматривать оцифрованную человеческую речь и записывать в виде 0 и 1, а затем подсчитать информационное содержание по этой формуле, оно окажется некорректным, так как одни символы в силу законов лингвистики встречаются чаще, а другие – реже. Оптимизируем выражение и запишем более строгое определение информационного содержания:

$$H_{bit} = -\sum_x p(x) \log p(x), \tag{2.4}$$

где x – случайная величина, $p(x)$ – функция распределения случайной величины. Так, допустим есть число M. Его всегда можно представить как

$$M \equiv 2^{\log_2 M} \equiv 3^{\log_3 M} = e^{\log_e M} = a^{\log_a M} \tag{2.5}$$

Глядя на определение информационного содержания очевидно, что показатель степени $\log_2 M = H_{bit}$, $\log_3 M = H_{trit}$. Вычислим отношение информационное содержания, выраженного в битах и тритах:

$$2^{H_{bit}} = 3^{H_{trit}} \tag{2.6}$$

$$H_{bit} = \log_2(3^{H_{bit}}) = H_{trit} \log_2 3 \tag{2.7}$$

$$\frac{H_{bit}}{H_{trit}} = \log_2 3 \tag{2.8}$$

Информация есть энтропия, а энтропия – это

$$H = \log \Delta\Gamma, \tag{2.9}$$

где $\Delta\Gamma$ – число микросостояний, в которых может находится система. Так, чем больше $\Delta\Gamma$, тем больше энтропия и наоборот. Рассмотрим банку, в которой находится термодинамическая температура – равновесный газ (поскольку температура стенок определена). Какое число микросостояний будет в такой системе? Много относительно единицы. Если при этом сфотографировать банку мгновенной камерой, то она увидит отдельные молекулы, а $H = 0$. Так, бытовое определение информации совершенное не соответствует его значению в физике и теории информации.

Чистое состояние – состояние, описываемое вектором. Вектор состояния один, он неповторимый и уникальный. Смешанное состояние можно представить как набор смешанных состояний, распределенных некоторым образом.

Условная вероятность

Представим, что есть два ящика: один назовем источником, другой – приемником. Традиционно источник называется Алисой, приемник – Бобом. Алиса посылает состояние Бобу, тот его измеряет и извлекает информацию. Для того, чтобы строго формализовать задачу, представим, что у Боба (его отправителя) есть некий мешок, в нем лежат состояния, которые необходимо послать. Так, он берет из мешка сообщения и посылает туда – там никто не знает, какое сообщение было послано. Задача заключается в том, чтобы взять сообщение, померить его/расшифровать и извлечь информацию. Ситуация идеальная и шум отсутствует. Необходимо понять, сколько информации из того, что получилось, отражает посланную информацию. На математическом языке это можно записать в виде условных вероятностей. Так, источник и приемник имеют следующие распределения: Алиса – $(p(x))$, Боб – $(p(y))$. Тогда

$$p(x,y) = p(y|x)\, p(x) \equiv p(x|y)\, p(y) \tag{2.10}$$

Раз есть вероятности и распределения, то можно посчитать энтропию:

$$S(y|x) \equiv \mathrm{def} - \sum_x p(x) \sum_y p(y|x) \log p(y|x) = -\sum_{x,y} p(y,x) \log \frac{p(y,x)}{p(x)} = \tag{2.11}$$

$$= -\sum_{x,y} p(y,x) \log p(x,y) + \sum_x \log p(x) \sum_y p(x,y) = S(x,y) - S(x)$$

Аналогичным образом,

$$S(x|y) = S(x,y) - S(y) \tag{2.12}$$

Взаимная информация

Вернемся к рассматриваемой задаче: есть два мешка (из одного берутся сообщения, отправляются по каналу связи) и приемная сторона. Задача любой теории информации (классической, квантовой) стоит в том, чтобы вычислить, как много из того, что посылалось, находится в том, что принимается. Так, вводится краеугольная в теории информации величина: взаимная информация $(I(x{:}\,y))$, а задача заключается в том,

чтобы эта величина была как можно больше, и случайное распределение, посылаемое нами, совпало с измеряемым.

$$I(x:y) = \sum_{x,y} p(x,y) \log \frac{p(x,y)}{p(x)p(y)} = \sum_{x,y} p(x,y) \log \frac{p(y|x)p(x)}{p(x)p(y)} = \tag{2.13}$$

$$= \sum_{x,y} p(x,y) \log p(y|x) - \sum_{x,y} p(x,y) \log p(y) = -S(y|x) - \sum_y \log p(y) \sum_x p(x,y) =$$

$$= -S(y|x) + S(y) = -S(x|y) + S(y),$$

где $\sum_x p(x,y) = p(y)$. Если есть независимые друг от друга случайные величины, то совместное распределение равно произведению, а взаимная информация равна нулю.

$$I(x,y) = \sum_{x,y} p(x,y) \log \frac{p(x,y)}{p(x)p(y)} = \tag{2.14}$$

$$= \sum_{x,y} p(x,y) \log p(x,y) - \sum_{x,y} p(x,y) \log p(x) - \sum_{x,y} p(x,y) \log p(y) =$$

$$= -S(x,y) + S(x) + S(y)$$

Так, $I(x:y)$ имеет три ответа: $= -S(y|x) + S(y)$; $-S(x|y) + S(y)$; $S(x) + S(y) - S(x,y)$.

Формула Шеннона

Вспомним рассматриваемую игру: через канал связи посылают некоторое множество $S(x)$ – некое информационное содержание, которое было в мешке. Тогда под $S(y)$ понимают то, что прилетело. Задача заключается в том, чтобы эти множества полностью совпадали друг с другом. Их совместное распределение подразумевает объединение двух множеств и равно $S(x,y)$.Вся заштрихованная область на рис. (2.2) называется совместной энтропией. Энтропия $(y|x)$ по формуле (2.12) – это область, заштрихованная горизонтально. Тогда вертикально заштрихованная область – это $S(x,y)$.

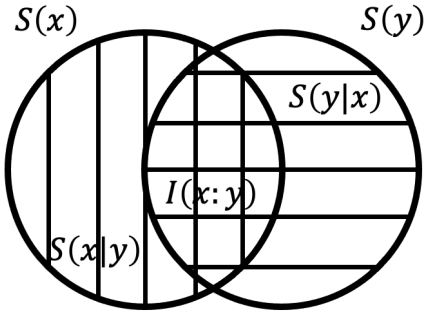

Рис. 2.2. Графическое изображение задачи.

Марковский процесс

Рассмотрим процесс передачи данных через некий доверенный узел ($x \to y \to z$). Так, данные идут не напрямую из x в z, а постепенно. Тогда

$$\mathrm{I}(z:x) \le I(x:y) \le S(x), \tag{2.15}$$

Значит информацию нельзя усилить. Для подобной тройной цепочки есть соотношение, связывающее совместное распределение и условные соответствующие:

$$p(x,y,z) = p(y|x)p(z|y)p(x) \tag{2.16}$$

Пример вычисления энтропии

Рассмотрим как работает информационное содержание (как на интуитивном, так и на строгом физико-математическом уровнях) на примере монетки: пусть 1 – орел, а 0 – решка. Монетка – бит информации, запишем информационное содержание при подбрасывании монетки (когда монетка лежит, энтропия равна нулю). Так как монетка честная,

$$"1" \to \frac{1}{2}, "0" \to \frac{1}{2} \tag{2.17}$$

$$H_{\text{монетка}} = -\sum p(x)\log_2 p(x) = 1 \tag{2.18}$$

Так, максимальное значение информации энтропии достигается на равновероятном распределении вероятности. Рассмотрим также пример с игральным кубиком и попробуем описать не бинарную систему в бинарной (шесть граней в битах):

$$p(1) = p(2) = \cdots = p(:::) = \frac{1}{6} \tag{2.19}$$

$$H = -\log\frac{1}{6} = 2{,}58 \tag{2.20}$$

Это является максимально возможной величиной, так как мы брали равномерное распределение (честный кубик). Возьмем нечестный кубик: пусть вероятность единицы будет равна

$$p(\cdot) = \frac{1}{2},\ p(:) = p(\cdots) = \cdots = p(:::) = \frac{1}{10} \tag{2.21}$$

Тогда энтропия (информационное содержание) равна $H = 2{,}16$. Если кость сделать максимально нечестной, и она будет постоянно оказываться на одной стороне, то ее энтропия будет равна нулю.

Канал с шумом

При рисовании множеств, одной из причин, по которому они не совпадают по умолчанию считалось искажение в канале связи. Введем модель и рассмотрим сам канал связи. Если говорить о бинарном канале (канале, через который передаются биты), то канал может также быть симметричным:

x		y		
0	→	1	p	$p(1\|0)$
1	→	0	p	$p(0\|1)$
0	→	0	$1-p$	$p(0\|0)$

$$1 \quad \rightarrow \quad 1 \quad 1-p \quad p(1|1)$$

Посчитаем условную энтропию:

$$S(x|y) = -\sum p(y) \log p(x|y) = \sum_y p(y) \sum_x p(x|y)\, p(y) \tag{2.22}$$

Будем считать, что вероятность того, что величина y случайно распределена равна $p(y) = \frac{1}{2}$. Тогда

$$S(x|y) = -\frac{1}{2}[p(0|0)\log p(0|0) + p(0|1)\log p(0|1) + p(1|0)\log p(1|0) + \tag{2.23}$$
$$+p(1|1)\log p(1|1)] = p\log p + (1-p)\log(1-p) = H(p)$$

$$H(x{:}\,y) = -S(x|y) + S(x) = S(x) - H(p) \tag{2.24}$$

Так, шум в канале связи, информационное содержание которого задается такими законами, уменьшает взаимную информацию. Увеличить взаимную информацию можно через увеличение $S(x)$. Максимальное значение достигается при равномерном распределении. Поэтому, задача заключается в максимизации взаимной информации, поэтому хорошо характеризовать канал некой величиной, не зависящей от модели шума. Такая величина называется емкостью канала связи (максимум величины I по всем возможным функциям). Для симметричного бинарного канала связи емкость канала равна

$$C = 1 - H(p) \tag{2.25}$$

и зажата между нулем и единицей. Шум в канале связи эту величину уменьшает. Есть также релаксационный канал, когда посылают единицу, а с некой вероятностью принимается ноль ($1 \rightarrow 0$). В то же время, если посылается ноль, то получается тот же ноль ($0 \rightarrow 0$).

Лекция 3. Квантовая энтропия

Энтропия Шеннона

Рассмотрим квантовые случаи, подобные игре из прошлой лекции, однако x заменим на A (Алиса), y заменим на B (Бен). Два мешка, один у приемника, другой – у передатчика. В мешке на передающей стороне есть квантовое состояние, в общем случае эти состояния описываются матрицами плотности ρ_x. Так, мы вытаскиваем состояние ρ_x с классической вероятностью p_x и посылаем в канал. В классической системе в мешках находятся биты, а здесь – вероятно, кубиты (квантовые биты), состояние необязательно чистое. Так, матрица плотности для мешка $X(A)$ равна

$$\rho = \sum_x \rho_x p_x \tag{3.1}$$

Энтропия фон Неймана

Ранее мы определили Шенноновскую энтропию как

$$H = -\sum_x p_x \log p_x \tag{3.2}$$

В случае с квантовыми состояниями, квантовая энтропия равна

$$S \equiv -\rho \log \rho = -\sum_x \lambda_x \log \lambda_x = 0 \tag{3.3}$$

$$0 \log 0 = 0 \tag{3.4}$$

Такая энтропия квантовых состояний также носит название энтропии фон Неймана. Если состояние чистое, энтропия фон Неймана равна

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{3.5}$$

$$\rho \equiv |\psi\rangle\langle\psi| = \begin{pmatrix} |\alpha|^2 & \alpha^*\beta \\ \alpha\beta^* & |\beta|^2 \end{pmatrix} \tag{3.6}$$

$$\lambda_{1,2} = 0; 1 \tag{3.7}$$

Если есть некая равновероятная смесь, то матрица плотности равна

$$\rho_{\text{см}} = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|) \tag{3.8}$$

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad |0\rangle\langle 0| = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \text{ и т. д.} \tag{3.9}$$

$$\rho_{\text{см}} = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix} \tag{3.10}$$

Так, неопределенность квантового состояния, которое количественно выражается энтропией, проявляет себя для смешанных состояний, а смесь подразумевает, что с некоторой вероятностью из мешка можно вытащить чистое состояние. Это, однако, не совсем правильно, так как одной матрице плотности можно сопоставить бесконечный набор таких состояний, которые с известными распределениями вытаскивают из мешка.

Так, если точно известно, какие в мешке есть распределения, можно получить матрицу плотности, а обратное неверно, и по предъявленной матрице плотности нельзя определить, что было в мешке.

Посчитаем энтропию фон Неймана некого состояния. Для этого возьмем состояние, описываемое следующим образом:

$$\rho = p|0\rangle\langle 0| + (1-p)[|D\rangle\langle D|] \tag{3.11}$$

Представим, что 0 – вертикальная поляризация, а 1 – горизонтальная.

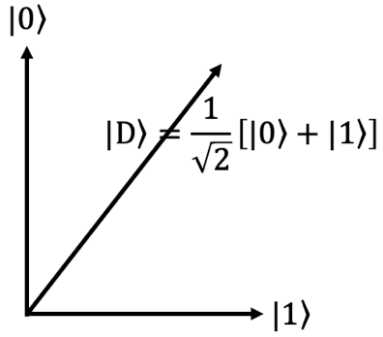

Рис. 3.1. Смешанное состояние по заданному базису.

Так, основным отличием квантового состояния от классического является факт существования таких неортогональных состояний (в классических состояниях есть хорошо определенные уровни: биты). Таким образом, в мешке есть состояние $|0\rangle$, выбираемое нами с вероятностью p, и состояние $|D\rangle$, выбираемое с вероятностью $(1-p)$.

$$|D\rangle = \frac{1}{\sqrt{2}}[|0\rangle + |1\rangle] \tag{3.12}$$

Дополним (3.11):

$$\rho = \frac{1-p}{2}\big[|0\rangle\langle 0| + [|0\rangle\langle 1|] + [|1\rangle\langle 0|] + [|1\rangle\langle 1|]\big], \tag{3.13}$$

где $|0\rangle = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$,$\langle 0| = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$, $\big[|0\rangle\langle 0| + [|0\rangle\langle 1|] + [|1\rangle\langle 0|] + [|1\rangle\langle 1|]\big] = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$. Тогда

$$\rho = \begin{pmatrix} \frac{1+p}{2} & -\frac{1-p}{2} \\ \frac{1-p}{2} & \frac{1-p}{2} \end{pmatrix} \tag{3.14}$$

Посчитаем собственные значения:

$$\left(\frac{1+p}{2} - \lambda\right)\left(\frac{1-p}{2} - \lambda\right) - \left(\frac{1-p}{2}\right)^2 = 0 \tag{3.15}$$

$$\lambda_{1,2} = \frac{1 \pm \sqrt{p^2 + (1-p)^2}}{2} \tag{3.16}$$

Возьмем равновероятное распределение:

$$p = \frac{1}{2} \to \lambda_1 = 0{,}864;\ \lambda_2 = 0{,}196 \tag{3.17}$$

Такой результат получается при вытаскивании из мешка неортогональных состояний. Если бы состояния были ортогональными, то $H = 1$. Представим, что через отверстие в стене поступает свет и точно известно, что с некоторой вероятностью могут быть следующие состояния: состояние, направленное вертикально вверх и состояние, направленное наискосок. Необходимо предложить способ, как достоверно их различить. Так, следует не мерять проекции на указанные направления, как можно было бы сделать в классическом подходе, а проецировать состояния на ортогональные и ставить поляризатор следующим образом:

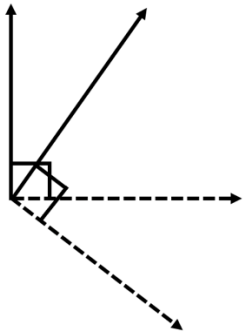

Рис. 3.2. Состояния и их проекции на ортогональные.

Если при постановке поляризатора первым образом произошел щелчок и детектор сработал, то мы точно знаем, что щелчок, находящийся на расстоянии прямого угла от сработавшего, точно не будет работать. Аналогично с другим набором «состояние-поляризатор», находящемся на расстоянии прямого угла, также могут быть случаи, когда щелчок не происходит. Так, можно достоверно различить состояния с некоторой вероятностью. Так, энтропия фон Неймана равна

$$S = -\sum \lambda_x \log \lambda_x = -\rho \log \rho \tag{3.18}$$

Условная энтропия фон Неймана

Введем совместную энтропию фон Неймана:

$$S(A,B) \equiv \rho^{AB} \log \rho^{AB} = -\sum \lambda_x^{AB} \log \lambda_x^{AB}, \tag{3.19}$$

где ρ^{AB} – матрица плотности совместного состояния. Ранее мы определяли, что классическая условная энтропия равна

$$H(y|x) = -\sum_x p(x) \sum_y p(y|x) \log p(y|x) = -\sum_{x,y} p(y,x) \log p(y|x) \tag{3.20}$$

Определим условную энтропию фон Неймана для квантового сценария:

$$\mathrm{def}\, S(A|B) \equiv S(A,B) - S(B) \tag{3.21}$$

Посчитаем конкретный пример для квантового случая: возьмем конкретное состояние, называемое запутанным или сцепленным:

$$|\psi^{AB}\rangle = \frac{1}{\sqrt{2}}[|0_A 0_B\rangle + |1_A 1_B\rangle], \tag{3.22}$$

где $|0_A 0_B\rangle \equiv |0_A\rangle \otimes |0_B\rangle$ и т.д. Так, если подсистема A находится в состоянии 0, то подсистема B находится в таком же состоянии, либо если подсистема A находится в состоянии 1, то подсистема B также находится в состоянии 1. Посчитаем матрицу плотности, она вводится для того, чтобы считать состояния подсистем. В курсе квантовой электроники мы рассматривали систему атом, который взаимодействовал с полем. Правило заключалось в том, что если предъявлена матрица плотности двух компонентов (например, сложной системы) ρ^{AB}, то состояние подсистемы, например, ρ_B вычисляется как

$$\rho_B = Tr_A \rho^{AB} \tag{3.23}$$

$$\rho(B) = \int p(A,B)dA \tag{3.24}$$

Проведем аналогичную операцию в нашем случае:

$$\rho = |\psi^{AB}\rangle\langle\psi^{AB}| = \tag{3.25}$$

$$= \frac{1}{2}[|0_A 0_B\rangle\langle 0_A 0_B| + |0_A 0_B\rangle\langle 1_A 1_B| + |1_A 1_B\rangle\langle 0_A 0_B| + |1_A 1_B\rangle\langle 1_A 1_B|]$$

$$\rho_B = Tr_A \rho^{AB} \tag{3.26}$$

$$\rho = \frac{1}{2}[|0_B\rangle\langle 0_B| + |1_B\rangle\langle 1_B|] = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix} \tag{3.27}$$

Так, нельзя путать состояния чистые и смешанные, перепутанные и факторизованные (этот случай будет рассмотрен на следующих лекциях), при этом перепутанное состояние чистое, а состояние его подсистем смешанное, но размерности этих состояний разные.

Перепутанное состояние

Вернемся к (3.21) и возьмем перепутанное состояние. Энтропия $S(A,B)$ равна нулю, а $S(B)$ – меньше нуля. Это условное математическое отличие от всех рассмотренных нами ранее случаев, так как никогда часть (рис. 2.2) не может быть отрицательна. Иногда неравенство

$$\mathrm{def}\, S(A|B) \equiv S(A,B) - S(B) < 0 \tag{3.28}$$

рассматривают как критерий перепутанности состояний.

Граница Холево

А. С. Холево определил границу, обозначаемую как χ. Рассмотрим все ту же игру: из мешка достают квантовые состояния ρ_x с соответствующими вероятностями p_x. Вероятности неизвестны, но в общем случае они неортогональны и смешаны. Состояния посылаются по каналу связи, на той стороне производится некое измерение,

оптимальное с точки зрения максимизации некой величины, нам уже известной. Задача игроков – максимизировать взаимную информацию. В классическом сценарии такая постановка задачи не совсем корректна, так как нет никаких препятствий на пути того, чтобы сделать область пересечения состояний максимально большой. Причина заключается в том, что состояния, посылаемые в канал, полностью различимы (ортогональны), а отделение сигнала от шума – техническая проблема. В квантовом случае ситуация принципиально другая: вопрос в этом случае ставится следующий – «укажите границу того, насколько хорошо можно принять информацию, посылаемую в канал». Эта граница есть величина взаимной информации.

$$H(A:B) \leq \chi = S(\rho) - \sum_x p(x) S(\rho_x), \tag{3.29}$$

где $\rho = \sum_x \rho_x p_x$. Отдельно доказывается то, что эта величина (граница Холево) превосходит по величине Шенноновскую энтропию:

$$H(A:B) \leq \chi = S(\rho) - \sum_x p(x) S(\rho_x) \leq H(p_x) \tag{3.30}$$

Следует также знать, что выражение существенно редуцируется при работе с чистыми состояниями. Возьмем пример, похожий на уже рассмотренные ранее: в мешке находится чистое состояние, при вытаскивании его с вероятностями получается смесь. Возможные классы состояний: $|0\rangle$ и $\cos\theta|0\rangle + \sin\theta|0\rangle$. Так, если $\theta = 0°$, то вытаскиваемое состояние совпадает с нулем, а если $\theta = 90°$, то вытаскиваем ортогональное состояние. Если же $\theta = 45°$, то вытаскиваем 0 и диагональное состояние. Посчитаем границу Холево:

$$S(\rho) = -\sum p_x S(\rho_x) \text{ для } 0 \tag{3.31}$$

Учтем, что $|0\rangle \to \frac{1}{2} = 1 - p$ и $\cos\theta|0\rangle + \sin\theta|0\rangle \to \frac{1}{2} = p$. Тогда матрица плотности такого состояния:

$$\rho = \begin{pmatrix} \frac{1+\cos^2\theta}{2} & \frac{\cos\theta\sin\theta}{2} \\ \frac{\cos\theta\sin\theta}{2} & \frac{\sin^2\theta}{2} \end{pmatrix} \tag{3.32}$$

Решим уравнение на собственные значения и получим следующий ответ:

$$\lambda_{1,2} = \frac{1 \pm \cos\theta}{2} \tag{3.33}$$

Найдем энтропию фон Неймана:

$$S(\rho) \overset{det}{=} -\left[\frac{1+\cos\theta}{2}\log\frac{1+\cos\theta}{2} + \frac{1-\cos\theta}{2}\log\frac{1-\cos\theta}{2}\right] \tag{3.34}$$

Если $\theta = 0; \pi$, то из мешка с равной вероятностью вытаскивается одно и то же состояние, информационная емкость такого процесса равна 0 и передать ничего нельзя. При $\theta = \frac{\pi}{2}$ из мешка достается ортогональное состояние (классический случай), два множества объединяются и область пересечения взаимной информации максимальна.

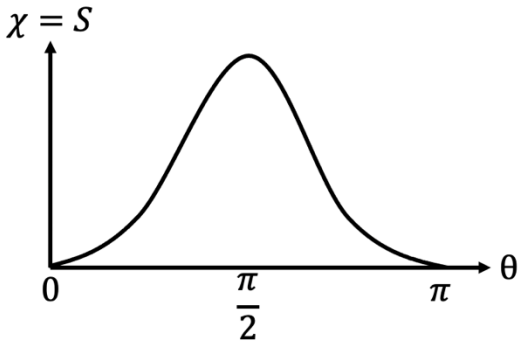

Рис. 3.3. График функции $S(p)$.

Во всех остальных случаях, когда $\theta \neq 0; \frac{\pi}{2}$, есть неортогональное состояние и максимум того, что можно извлечь из этого канала (из границы Холево) отмечено соответствующими точки на графике.

Заключение

На этой лекции говорилось о квантовой информации, мы обсудили существование энтропии фон Неймана (информация фон Неймана), которая характеризует, сколько информации находится в том или ином квантовом состоянии. Если состоянии чистое (описывается вектором состояния), то это информационное содержание или энтропия равно нулю. Если оно максимально смешанное, то и его информационная емкость также максимальна. Существует класс состояний, который называется двухкомпонентным или многокомпонентным: эти квантовые состояния составные, они могут быть смешанными или чистыми. На лекции мы рассмотрели особый класс таких состояний: чистых и максимально перепутанных, которые характеризуются тем, что их составное информационное содержание нулевое, а состояние их подсистем максимально смешанное и обладает информационной емкостью. Мы также обсудили аналогию с так называемыми Шенноновскими яйцами в классическом и квантовом случаях. Условная энтропия (условная информация) в классике всегда неотрицательна, в квантовом же случае условная информация может быть отрицательна. Помимо этого, мы остановились на границе Холево, описывающей, сколько информации можно извлечь даже при идеальных измерениях, когда в канал посылаются общие квантовые состояния (значит, неортогональные), и доказали, что максимум достигается в случае ортогональных состояний, что есть классический случай.

Лекция 4. Запрет клонирования квантовых состояний

Теорема о запрете клонирования квантовых состояний

В прошлый раз мы говорили о таком понятии, как взаимная и достижимая (как максимум величины) информация; обсуждали, что в случае классической коммуникации эта величина не является ничем особенным, так как нет причин, по которым нельзя достигнуть достижимой информации. Мы также говорили о квантовом диапазоне и о принципиальном ограничении, когда два пользователя (два мешка) обмениваются неортогональными состояниями, – тогда есть алгоритм, позволяющий вероятностно, но достоверно различить состояния (если есть отсчет, то мы знаем, что он точно не является отчетом, приходящим от другого состояния). Также всегда есть доля отчетов, которые нельзя идентифицировать: отсутствие отчета означает, что сигнал может быть связан с обоими состояниями.

На этой лекции мы в трех ипостасях рассмотрим теорему о запрете клонирования, лежащую в основе всех тех концепций. Есть некий ящик, выполняющий элементарные операции. На вход мы подаем некое состояние $|\psi\rangle$, а на выходе получаем $|\psi\rangle, |\psi\rangle$. Для того, чтобы рис. (4.1) был унитарным, следует иметь как два выхода, так и два входа.

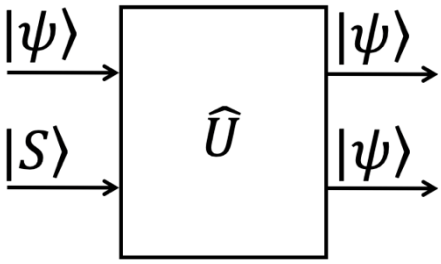

Рис. 4.1. Общая схема копирования.

Запишем операцию, изображенную на рис. (4.1):

$$\widehat{U}(|\psi\rangle \otimes |S\rangle) = |\psi\rangle|\psi\rangle \tag{4.1}$$

Поскольку листочек может быть любым, выражение также может быть записано иначе:

$$\widehat{U}(|\varphi\rangle \otimes |S\rangle) = |\varphi\rangle|\varphi\rangle \tag{4.2}$$

Для того, чтобы доказать теорему о невозможности клонирования произвольного квантового состояния, возьмем Эрмитово сопряжение от (4.2) и скалярно перемножим эти два выражения:

$$(\langle S| \otimes \langle\varphi|)U^{+}U(|\psi\rangle \otimes |S\rangle) = \langle\varphi|\langle\varphi||\psi\rangle|\psi\rangle, \tag{4.3}$$

где $U^{+}U = \hat{I}$, $\langle\varphi|\psi\rangle = (\langle\varphi|\psi\rangle)^2$. Тогда

$$x = x^2 \tag{4.4}$$

$$x = 0; 1 \tag{4.5}$$

Так, мы изобразили копирующую машину, работающую по определенному алгоритму, и на входе даем любые чистые состояния. Однако копирование будет происходить только в двух случаях: либо если состояние ортогонально, либо если состояния совпадают, поэтому в общем виде теорема о запрете клонирования звучит так: клонирование произвольных квантовых состояний невозможно.

Мы доказали теорему в общем случае, рассмотрим следующие два варианта. Представим ту же самую игру: есть посылающая и принимающая стороны, они обмениваются квантовыми состояниями по определенным протоколам, у них есть классический канал, по которому они сообщают некоторые состояния. Помимо этих двух сторон в играх всегда присутствует третье лицо: злоумышленник. Подслушиватель исходит из двух правил: изъять как можно больше информации и остаться как можно меньше замеченным. Это также справедливо в классике, однако в ней нет такой теоремы и нет механических фундаментальных запретов на то, чтобы он снял информацию и был замечен (понятие возмущения в классике отсутствует).

Вернемся к копированию в случае, когда есть подслушиватель. Есть универсальный копирующий аппарат, на вход поступает состояние $|\psi\rangle$ (то, которым обмениваются легитимные слушатели), копировальный аппарат находится в руках подслушивателя. Задача последнего заключается в том, чтобы $|\psi\rangle$ пролетело насквозь, а то, что останется у него $|F_\psi\rangle$ – некое состояние, искаженное по сравнению с тем, что он предъявляет/подсовывает в копировальную машину ($|F\rangle$) несло некий отпечаток копируемого состояния.

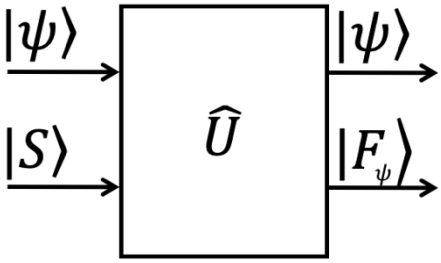

Рис. 4.2. Схема копирования в случае с подслушивателем.

Произведем те же операции:

$$\langle\varphi|\psi\rangle\langle F|F\rangle = \langle\varphi|\psi\rangle\langle F_\psi|F_\varphi\rangle \tag{4.6}$$

$$\langle F_\psi|F_\varphi\rangle = 1 \tag{4.7}$$

При таком сценарии подслушиватель хотел, чтобы реплика, применяемая на входе, несла максимальный отпечаток копируемого состояния, а получилось, что он ничего не снял и не добился успеха.

Разрешим устройству искажать входные состояния – это наиболее общая стратегия подслушивания. Для этого заменим $|\psi\rangle$ на выходе на $|\psi'\rangle$. Тогда

$$\langle\varphi|\psi\rangle = \langle\varphi'|\psi'\rangle\langle F_\psi|F_\varphi\rangle$$

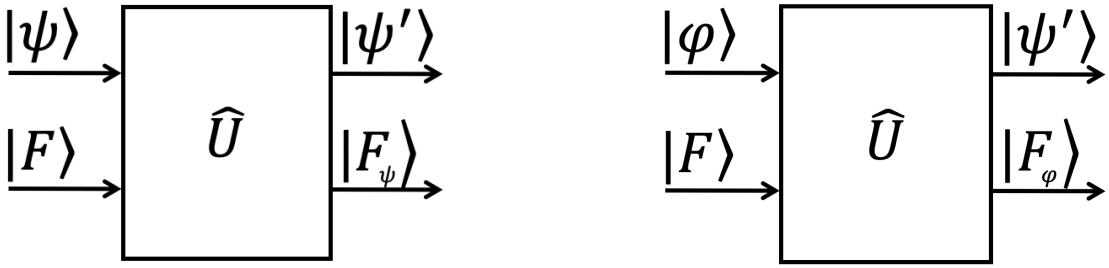

Рис. 4.3. Схема копирования в случае с подслушивателем.

Представим: универсальная копирующая машина, она не зависит от того, какое состояние подается на вход. Пусть на ход подали состояние $|\psi\rangle$, злоумышленник подсовывает следующий пустой ход: $|F\rangle$ (он может быть любым), так, должно быть два входа и два выхода (это будет унитарной операцией). Разрешим машине исказить входное состояние, а на втором выходе написать состояние $|F_\psi\rangle$ (то, что остается на руках у мошенника), который будет нести отпечаток настоящего исходного состояния.

Для второго состояния, произвольного $|\varphi\rangle$ напишем то же самое. Тогда злоумышленник подсовывает $|F\rangle$, а себе оставляет $|F_\varphi\rangle$. Возьмем Эрмитово сопряжение от этой операции:

$$(\langle\varphi|\langle F|)U^+U(|\psi\rangle|F\rangle) = \langle\varphi'|\langle F_\varphi|\psi'\rangle|F_\psi\rangle \tag{4.8}$$

$$\langle\varphi|\psi\rangle\langle F|F\rangle = \langle\varphi'|\psi'\rangle\langle F_\psi|F_\varphi\rangle, \tag{4.9}$$

где $\langle F|F\rangle = 1$, $\langle\varphi|\psi\rangle$ – некое комплексное число (скалярное произведение двух произвольных состояний), константа. Оно равно произведению двух чисел: первое – те искаженные состояния, что вылетают из клонера, второе – тоже искаженное состояние, которое хочет оставить себя подслушивать. Злоумышленнику важно, чтобы то, что остается у него, было маленьким (в идеале, равным нулю), чтобы достоверно различить, а сделать это можно только в случае с ортогональными состояниями. Поэтому злоумышленник хочет минимизировать $\langle F_\psi|F_\varphi\rangle$, а произведение этих двух чисел – константа. Тогда при минимизации $\langle F_\psi|F_\varphi\rangle$, $\langle\varphi'|\psi'\rangle$ автоматически растет и становится максимальной (их скалярное произведение становится равным единице, и они перестают отличаться). Таким образом, произвольные два состояния, улетающие в канал легитимному пользователю, перестают отличаться.

В этом и заключается квантовая криптография: если кто-то хочет несанкционированно подслушать, это возможно, но если анализировать то, что прилетает (например, открывать часть сообщений и сравнивать между собой), окажется, что при подслушивании, независимо от того, что посылается, прилетает одно и то же. Поэтому попытка взлома (подслушивания) всегда статистически становится известной.

Помимо того, что системы квантовой криптографии позволяют обнаружить момент подслушивания, также существует способ, позволяющий исправлять эти ошибки.

Таким образом, в отличие от частных (ортогональных и одинаковых), произвольные квантовые состояния копировать нельзя.

Фотон

Мы часто оперируем понятием фотона, остановимся на нем поподробнее. Совершенно правильно определяют, что оператор рождения действует на вакуум и получается единица, что и называется фотоном.

$$a^{+}|0\rangle = |1\rangle \tag{4.10}$$

Но это совершенно не продвигает на пути поставленной задачи и не создает никаких образов. Мы также знаем, что энергия фотона равна

$$\hbar\omega = \mathcal{E}_{|1\rangle}, \tag{4.11}$$

что также не позволяет сформировать образ. Рассмотрим концепцию пакетов, близкую к тому, что называется корпускулами, но являющуюся компромиссным вариантом между записанным ранее выражением и нашим мышлением. Важно понимать, что как любой образ-интерпретация, эта идея имеет множество вопросов, однако может быть достаточно удобна в понимании и применении.

Будем понимать под фотоном некую огибающую и набивку (рис. 4.4), где последняя и есть частота ω. Важно также понимать, что мы рассматриваем только временной язык (продольные, временные, частотные моды).

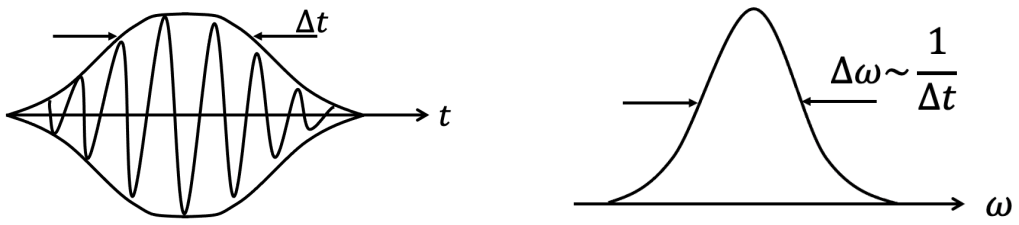

Рис. 4.4. Концепция фотона как пакета и графическое изображение его центральной частоты.

Возьмем излучение непрерывного лазера мощностью 1 Вт и оценим:

$$1\ \text{Вт} = \frac{\mathcal{E}}{\text{с}*\text{см}^2} = \frac{N\hbar\omega}{\text{с}*\text{см}^2} \tag{4.12}$$

Найдем, сколько фотонов непрерывного излучения в одном вате:

$$\omega = \frac{2\pi}{T} = -\frac{2\pi\ \text{с}}{\lambda} = 3 * 10^{15} \tag{4.13}$$

$$N = \frac{10^7\ \text{эрг}}{\hbar\omega} = \frac{10^7}{10^{-27}*3*10^{15}} = \frac{10^{34}*10^{-15}}{3} \sim 3 * 10^{18}\ \text{шт} \tag{4.14}$$

ФИЗИЧЕСКИЙ ФАКУЛЬТЕТ МГУ ИМЕНИ М.В. ЛОМОНОСОВА
teach-in
ЛЕКЦИИ УЧЕНЫХ МГУ

Возникает вопрос, что есть Δt для фотона. Введем понятие продольной моды, иными словами, продольную длину когерентности. Для того, чтобы определить длину когерентности представим отверстие в стене и летящий пучок с некоторым числом фотонов (электромагнитная волна). Для того, чтобы измерить длину, необходимо раздвоить пучок, поставить интерферометр Маха-Цендера или Рождественского и поменять одно из плеч в длине. При этом через детектор осуществляется наблюдение.

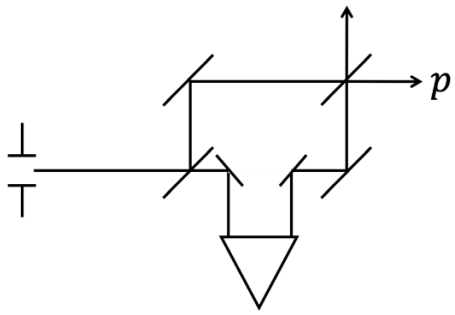

Рис. 4.5. Определение длины когерентности.

При изменении длины плеча, интенсивность меняется следующим образом (рис. 4.5), а видность (размах колебаний) определяется как

$$1\ \text{Вт} = \frac{I_{max} - I_{min}}{I_{max} + I_{min}} \tag{4.15}$$

Размах падает на какой-то длине (длине когерентности) l, можно рассчитать задержку по времени:

$$l_{\text{ког}} = \underline{c} * \tau_{\text{ког}}, \tag{4.16}$$

где $\underline{c}$ – длина в секунду, $\tau_{\text{ког}}$ – секунда. Объем когерентности складывается из двух факторов: продольная когерентность и поперечная. Для измерения продольной нужно взять интерферометр, подвинуть одно из плеч и смотреть, как падает видность интерференции. Как только она падает в два раза – необходимо ее зафиксировать и пересчитать во времени – так получаем длину цуга. На временном языке, считается, что в таком объеме (на такой длине) (рис. 4.4) цуг спадает, и та порция энергии, которая отвечает одному фотону, локализована в таком цуге по временной координате.

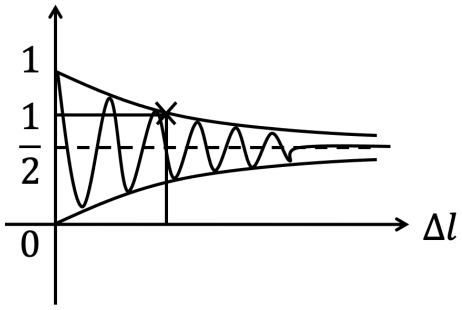

Рис. 4.5. Интенсивность при изменении длины плеча.

Поперечная когерентность идеологически измеряется таким же образом, только переменная, которую мы меняем при наблюдении за видностью, расположена поперек. Представим плоскую волну и два отверстия размером a, из которых в дальнюю зону идут исходящие излучения. Есть область их пересечения, что является полным аналогом светоделителя – в этой области два поля могут интерферировать, а могут не интерферировать. Эксперимент сводится к разведению отверстий далеко двух от друга и наблюдению огибающей в области пересечения. Размер ее основного пика и осцилляций определяется масштабом одного отверстия. При открытии второго отверстия, синус дополнится квадратом косинуса, чей период будет определяться расстоянием между отверстиями.

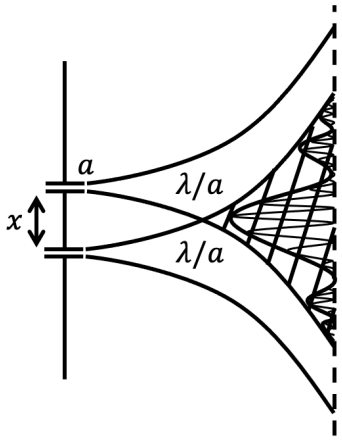

Рис. 4.6. Интерферометр Юнга.

В какой-то момент при сильном раздвижении отверстий, глубина модуляции упадет, и он и перестанут интерферировать.

Также интересен вопрос о том, будет ли солнечный свет (и любой бесконечный спектр) интерферировать сам с собой. Проделаем в шторе отверстие. На пути расходящегося пучка света поставим вырожденный интерферометр Маха-Цендера и фиксируем показания детектора. В прямом свете при нулевой задержке детектор покажет E_1. Так, искусство техники заключается в том, чтобы удержать это все стабильным.

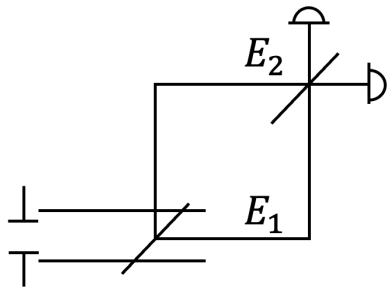

Рис. 4.7. Интерферометр Маха-Цендера.

Следует помнить, что, как и любая модель, эта интерпретация фотона как волнового пакета ограничена.

Лекция 5. Перепутанные состояния

Перепутанные состояния

Впервые этот термин (сцепленные, запутанные состояния) в русскоязычной литературе появился в журнале «Успехи химии» в 1936 году. В физику термин был введен Эрвином Шредингером в 1935 году (статья «Современное состояние квантовой механики»). Такие состояния являются ресурсом квантовой теории информации, на нем много что построено в дальнейшем.

Представим некое двумерное множество (доску). Все, что слева от этой черты, будет иметь индекс «1», справа – «2». Нижние квадранты отмечены символом $|0\rangle$, верхние – $|1\rangle$. Представим, что на пересечении линий находится некий источник, излучающий частицы парами, импульс сохраняется в пространстве.

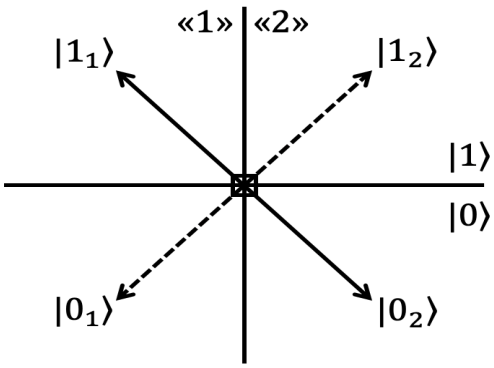

Рис. 5.1. Перепутанные состояния на примере двумерного множества.

Помня, что суперпозиции в квантовой механике имеют вербальное значение союза «или», запишем две группы возможностей:

$$C_1|1_1\rangle|0_2\rangle + C_2|0_1\rangle|1_2\rangle \approx |\psi_{12}\rangle \tag{5.1}$$

Такое совместное состояние двухчастичной квантовой системы (одно из возможных) называется перепутанным, так как

$$|\psi_{12}\rangle \neq |\psi_1\rangle \otimes |\psi_2\rangle \tag{5.2}$$

Так, если состояние совместной системы двух частей не сводится к прямому произведению состояний подсистем, то оно называется перепутанным. Для того, чтобы ввести такое состояние необходимы минимум две подсистемы, также должен быть некий параметр, принимающий по крайней мере два значения. Немаловажно отметить фигурирование жестких корреляций (корреляция – это синхронность флуктуаций), – в классике примером будет являться корреляции типа «да-нет»: так, столб случайно появляется справа и обязательно появляется слева, а может и не появиться.

Запишем две пары состояний Белла, обособленно стоящих в этой науке:

$$|\psi_{12}^{\pm}\rangle = \frac{1}{\sqrt{2}}[|0_1\rangle|1_2\rangle \pm |1_1\rangle|0_2\rangle], \tag{5.3}$$

где $(-) = e^{i\pi}$.

$$|\phi_{12}^{\pm}\rangle = \frac{1}{\sqrt{2}}[|0_1\rangle|0_2\rangle \pm |1_1\rangle|1_2\rangle] \tag{5.4}$$

Эти состояния ортогональны ($\langle\phi^+|\psi^-\rangle = 0$). Так, с вероятностью $\frac{1}{2}$ реализуется либо одна пара чисел, либо другая, но какая – непонятно. Состояние чистое. Посчитаем состояние подсистемы. В классике, если есть распределение некой совместной двухкомпонентной системы, то посчитать состояние подсистемы достаточно легко:

$$P_1(x) = \int dy\, P_{12}(x,y) \tag{5.5}$$

$$P_2(y) = \int dx\, P_{12}(x,y) \tag{5.6}$$

В квантовом случае, волновую функцию при вектор-состоянии отдельно для частицы 1 и отдельно для частицы 2 записать невозможно. В этом случае состояние описывают с помощью матрицы плотности:

$$\rho_{12} \equiv |\psi_{12}\rangle\otimes\langle\psi_{12}| \tag{5.7}$$

$$\rho_1 = Sp_2\rho_{12} \tag{5.8}$$

$$\rho_2 = Sp_1\rho_{12} \tag{5.9}$$

Дополним (5.7):

$$\rho_{12} = \frac{1}{\sqrt{2}}[|0_1 1_2\rangle\langle 1_2 0_1| + |0_1 1_2\rangle\langle 0_2 1_1| + |1_1 0_2\rangle\langle 1_2 0_1| + |1_1 0_2\rangle\langle 0_2 1_1|] \tag{5.10}$$

Найдем состояние подсистем:

$$\rho_1 = Sp_2\rho_{12} = \frac{1}{2}[|0_1\rangle\langle 0_1| + |1_1\rangle\langle 1_1|] \tag{5.11}$$

$$\rho_2 = Sp_1\rho_{12} = \frac{1}{2}[|0_2\rangle\langle 0_2| + |1_2\rangle\langle 1_2|] \tag{5.12}$$

Свойство таких максимально перепутанных чистых состояний заключается в том, что состояния подсистем полностью смешанные, что невозможно придумать в классике. Запишем некоторое выделенное трехчастичное состояние (GHZ или ГХЦ) и посмотрим, выполняются ли для него такие свойства.

$$|\psi_{123}\rangle \equiv \frac{1}{\sqrt{2}}[|0_1 0_2 0_3\rangle + |1_1 1_2 1_3\rangle] \tag{5.13}$$

Перед интерпретацией определения проговорим, что есть состояния Белла (двухкомпонентные чистые перепутанные): так, если каким-то образом становится известно, что состояние первой частицы равно нулю, то однозначно состояние второй частицы равно единице, и наоборот (сильные/жесткие корреляции и синхронность флуктуаций). В случае с (5.13), если каким-то образом померили, что состояние первой частицы – ноль, то состояние всех остальных также равно нулю; если же у второй частицы состояние один, то и у остальных один. Повернем голову на 45°, т.е. поменяем

базис (очевидно, что, если мы поворачиваем голову, само состояние (суть) не меняется). Перепишем состояния:

$$|0_i\rangle \equiv \frac{1}{\sqrt{2}}[|A\rangle + |D\rangle],\ i = 1,2,3 \tag{514}$$

При этом состояния остаются ортогональными.

$$|1_i\rangle \equiv \frac{1}{\sqrt{2}}[|A_i\rangle - |D\rangle] \tag{5.15}$$

Обратные преобразования:

$$A_i = \frac{1}{\sqrt{2}}[|0_i\rangle - |1_i\rangle] \tag{5.16}$$

$$D_i = \frac{1}{\sqrt{2}}[|0_i\rangle + |1_i\rangle] \tag{5.17}$$

Тогда в этом базисе $|\psi_{123}\rangle$ равен

$$|\psi_{123}\rangle = [|D_1D_2A_3\rangle + |D_1A_2D_3\rangle + |A_1D_2D_3\rangle + |A_1A_2A_3\rangle] \tag{5.18}$$

Интерпретируем состояние: допустим, каким-то образом измерили состояние третьей частицы, и оно оказалось равным A, тогда две другие частицы будут равны $|D_1D_2\rangle + |A_1A_2\rangle$, что подразумевает смешанное состояние. Так, узнав состояние, в котором находится первая частица, мы ничего не можем сказать о состоянии подсистем. Получается, если в описании двухкомпонентных систем присутствует полная ясность, то с трех компонентов и выше: чем больше – тем непонятнее.

Эффект спонтанного параметрического рассеяния света

Представим кристалл, у которого $\chi^{(2)} \neq 0$, получающий пары фотонов.

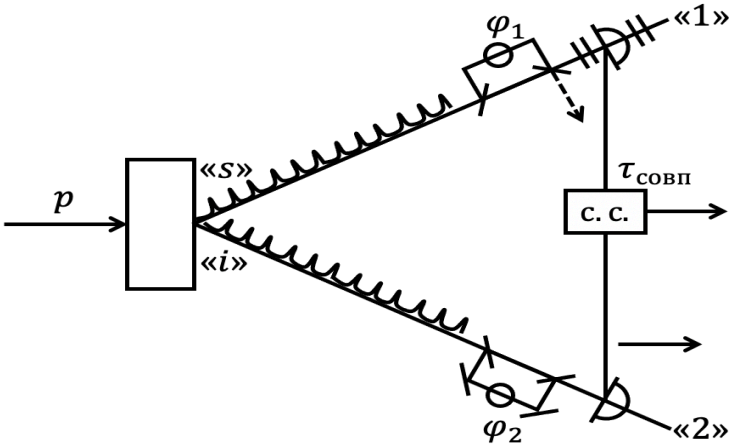

Рис. 5.2. Графическое изображение эффекта спонтанного параметрического рассеяния света.

Известно, что с некоторой вероятностью фотон накачки может распасться на пару фотонов, они будут иметь некие свойства:

$$\hbar\omega_p = \hbar\omega_S + \hbar\omega_i \tag{5.19}$$

$$\hbar\vec{k}_p = \hbar\vec{k}_S + \hbar\vec{k}_i \tag{5.20}$$

У этого процесса спектр накачки формируется свойствами кристалла. Волновая функция (вектор состояния) выглядит следующим образом:

$$|\psi\rangle_{12} = |1_1\rangle\otimes|1_2\rangle \tag{5.21}$$

Поставим невырожденный интерферометр Маха-Цендера и начинаем двигать плечи. В какой-то момент (интерференция первого порядка по интенсивности и второго порядка по полю) видность исчезнет. Расположим в каждом из каналов (плеч) фазовую задержку, чтобы определить длину когерентности. Перепишем состояние (5.21) после интерферометров

$$\rightarrow \left(|S_1\rangle + e^{i\psi_1}|L_1\rangle\right)\otimes\left(|S_2\rangle + e^{i\psi_2}|L_2\rangle\right) \tag{5.22}$$

Как из этого состояния сделать перепутанное? Будем регистрировать только те события, что происходят одновременно. Поставим детекторы – у них есть счетчики и схемы совпадения (в пределах окошка τ). Пусть τ:

$$\tau_{\text{совп}} \ll \tau_{\text{з(задержки)}} \ll \tau_{\text{ког}} \tag{5.23}$$

$$|\psi\rangle_{12} = |S_1\rangle|S_1\rangle + e^{i(\varphi_1+\varphi_2)}|L_1L_2\rangle, \tag{5.24}$$

что является состоянием Белла. Такой тип состояний также называется перепутанным по координатам энергия-время. Так, есть два детектора, щелкающие всегда, а есть счетчик, который щелкает только на совпадающие. Пусть число щелчков прорежено, тогда найдем число совпадений:

$$\mathrm{N}_{\text{совп}} \sim |\langle\psi|'\psi'\rangle|^2 \sim \cos^2(\varphi_1 + \varphi_2) \tag{5.25}$$

Так, из двух шумов может получиться интерференционный эффект – он будет проявляться в том, что число совпадений зависит от $\cos^2(\varphi_1 + \varphi_2)$. Как следствие этого, можно зафиксировать аргумент равным $\frac{\pi}{2}$ или, например, 1, тогда совпадений не будет. Если после этого синхронно крутить фазы, то с точки зрения шума меняться ничего не будет и совпадений импульсов никогда не будет. Также, атрибутом двухфотонной интерференции является сумма фаз (атрибут «неклассичности»).

Поляризационные перепутанные состояния

Рассмотрим другой способ получения максимально перепутанных состояний на основе рассматриваемого эффекта. Поскольку процесс (рис. 5.2) происходит в анизотропном кристалле, излучение на выходе всегда поляризовано. Один из режимов (синхронизм типа 1 в нелинейной оптике) заключается в том, что поляризация фотонов одинакова (она может быть обыкновенной или необыкновенной). Пусть все фотоны поляризованы горизонтально. Возьмем точно такой же кристалл, повернем на 90° и поставим с прежним. Обычно для таких синхронизмов типа 1, если излучение в двух

модах поляризовано горизонтально, то накачка будет поляризована вертикально: p^V. Это справедливо для первого кристалла: если его повернуть на 90° - синхронизма не будет. Для того, чтобы он был, необходимо поменять поляризацию в накачке. Тогда

$$|\psi\rangle_{12} = \frac{1}{\sqrt{2}}\left(|H_1H_2\rangle + e^{i\varphi}|V_1V_2\rangle\right) \tag{5.26}$$

Большое количество парадоксов и эффектов, которые будут рассматриваться в дальнейшем, по большей мере основываются на этих двух типах экспериментально подготавливаемых перепутанных состояний.

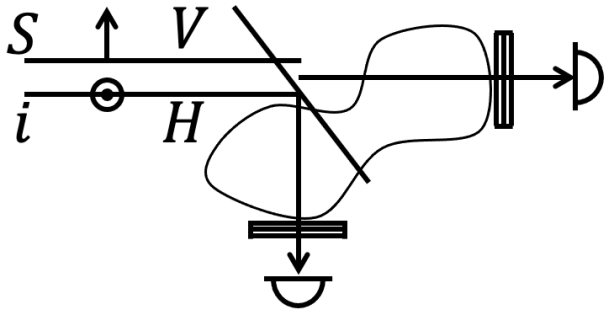

Рис. 5.3. Частновыраженный коллинеарный режим.

Фотоны (сигнальный и холостой) можно заставить распространяться в одном пучке одного цвета в одну сторону – это так называемый частотновырожденный коллинеарный режим, - далее устанавливается светоделитель.

Так как неизвестно, какой фотон какой, – каждый может отразиться либо пройти. В этом случае (единственное отличие фотонов – по поляризации) возможны следующие пары событий:

$$|V\rangle \otimes |H\rangle \tag{5.27}$$

$$|HV\rangle + e^{i\varphi}|VH\rangle \tag{5.28}$$

Лекция 6. Перепутанные состояния (продолжение)

Перепутанные состояния

Заново выпишем базис в пространстве размерности четыре для двухкомпонентных двухкубитовых состояний (состояния Белла):

$$|\psi_{12}^{\pm}\rangle = \frac{1}{\sqrt{2}}\{|0_1\rangle|1_2\rangle \pm |1_1\rangle|0_2\rangle\}, \tag{6.1}$$

$$|\phi_{12}^{\pm}\rangle = \frac{1}{\sqrt{2}}\{|0_1\rangle|0_2\rangle \pm |1_1\rangle|1_2\rangle\} \tag{6.2}$$

Важно помнить, что состояния двухкомпонентных систем чистые, а состояния подсистем для максимально перепутанных состояний – полностью смешанные. Например, используя формализм матрицы плотности:

$$\rho_1 = Sp_2\rho_{12} = \frac{1}{2}[|0_1\rangle\langle 0_1| + |1_1\rangle\langle 1_1] \to \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix}, \tag{6.3}$$

где $\rho_{12} = |\psi_{12}^{\pm}\rangle\langle\psi_{12}^{\pm}|$. Любое чистое состояние двух кубитов можно разложить по (6.1), (6.2), также как и любое состояние кубита можно разложить в базисе $|0\rangle, |1\rangle$ или в любом другом. Введем термин степени перепутывания. Возьмем для примера состояние типа

$$\psi = \mathcal{E}^2|0_1 1_2\rangle + (1 - \mathcal{E}^2)|1_1 0_2\rangle, \tag{6.4}$$

где число $\mathcal{E}^2$ – степень перепутывания. Она отображает, насколько перекошены амплитуды в суперпозиции (максимально перепутаны, когда они одинаковы). Мы рассмотрели простейшие случаи двухкубитного перепутывания.

Приведем экспериментально достижимый операциональный пример на основе спонтанного параметрического рассеяния света и обсудим его в контексте перепутывания и других степеней свобод: представим кристалл.

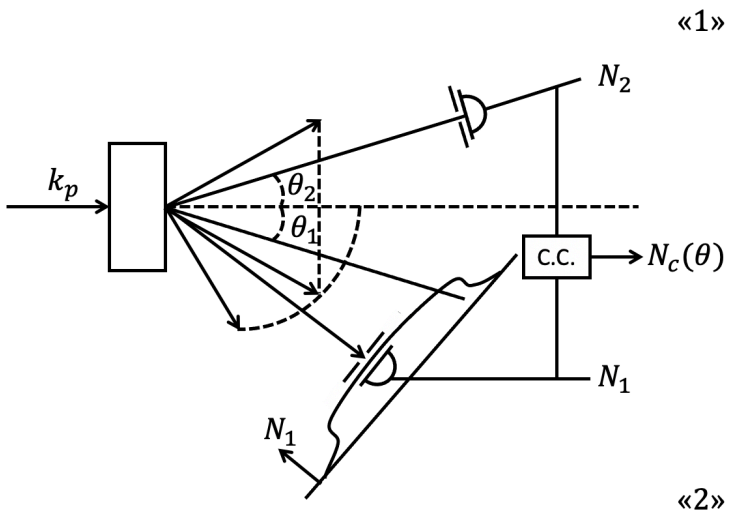

Рис. 6.1. Спонтанное параметрическое рассеяние света.

Обычное спонтанное параметрическое рассеяние подразумевает излучающиеся из кристалла пары фотонов, для которого выполняется следующее условие:

$$\overrightarrow{k_1} + \overrightarrow{k_2} = k_p \tag{6.5}$$

где сохраняются энергия и поперечный импульс (продольный импульс сохраняется до толщины кристалла).

$$\omega_1 + \omega_2 = \omega_p \tag{6.6}$$

(6.5) и (6.6) – векторные и скалярные условия на направление разлетов. Они всегда летят в противоположном направлении так, чтобы сумма поперечных импульсов была равна нулю. Существенная часть для предыдущего и последующего изложений заключается в том, что пара фотонов может излучиться в любом направлении. Так, если говорить в терминах одного из них (например, возьмем нижнюю полуплоскость – условно холостой фотон), одночастичное состояние может полететь в очень широкий диапазон углов. Для того, чтобы охарактеризовать угловой спектр, возьмем счетный детектор, поставим перед ним небольшое отверстие и будем водить детектор по выделенному квадранту. Так, будем наблюдать некое распределение интенсивности.

Перейдем к наблюдению за парной корреляцией. Для этого поставим второй детектор в оставшемся квадранте с таким-же отверстием для того, чтобы выделить соответствующий вектор k в дальней зоне, и фиксируем его. Устанавливается схема совпадений. Так, есть два детектора: один прибит гвоздями и регистрирует фотоны, приходящие с определенным k. Второй детектор перемещается и сканирует по всему угловому пространству. Счетчик первого детектора регистрирует интенсивность, пропорциональную среднему числу фотонов; интенсивность, регистрируемая вторым счетчиком, нам уже известна, – есть совпадение. Нас интересует зависимость числа совпадений (степень корреляции) от первого угла. Так как (6.5) дает жесткие корреляции, это будет очень узкое распределение.

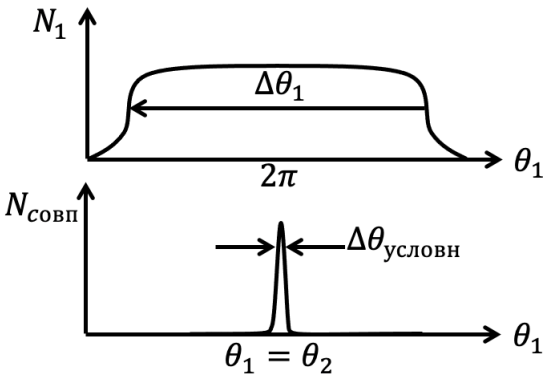

Рис. 6.2. Парная корреляция.

Михаил Владимирович Федоров посчитал, что перепутывания можно охарактеризовать операционально и померять. Так, параметр Федорова выглядит следующим образом:

$$\mathcal{K} \sim \frac{\Delta\theta_1}{\Delta\theta_{\text{усл}}} \tag{6.7}$$

Понятие моды Шмидта на языке угловых распределений – это некое пространственное распределение поля, которое внутри полностью когерентно. Параметр перепутывания (параметр Федорова) почти равен числу Шмидта. По теореме Шмидта, любое состояние двухчастичной системы можно разложить:

$$|\psi_{12}\rangle = \sum_i c_i |\alpha_i\rangle |p_1\rangle \tag{6.8}$$

При этом также есть число Шмидта, характеризующее степень перепутывания:

$$K \equiv \frac{1}{\sum_i c_i^4} \geq 1 \tag{6.9}$$

Очевидно, что состояние Белла попадает под это определение. Так, число Шмидта для подсистемы $|\psi_{12}^{\pm}\rangle$ равно двум, что помимо степени перепутывания также является размерностью подпространства каждой подсистемы. Вспоминая общий пример: интерпретируем состояние Белла в терминах безусловной ширины к условной:$\left(\frac{2}{1} = 2\right)$. Также важно помнить о том, что чем больше распределено состояние подсистемы, тем выше степень перепутывания.

Принято считать, что аналога перепутыванию в классике нет, однако это не так. Представим сильно выпившего охотника с ружьем, который идет и постоянно стреляет из него во все стороны. Очевидно, что речь идет о двухкомпонентной системе.

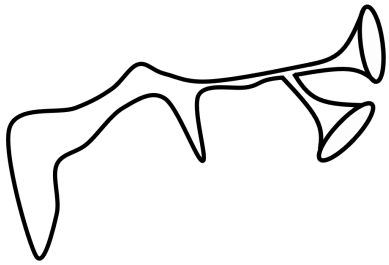

Рис. 6.3. Ружье в аналогии «пьяный охотник».

Тогда распределение дробинок, вылетающих только из одного ствола, по углу выглядит следующим образом:

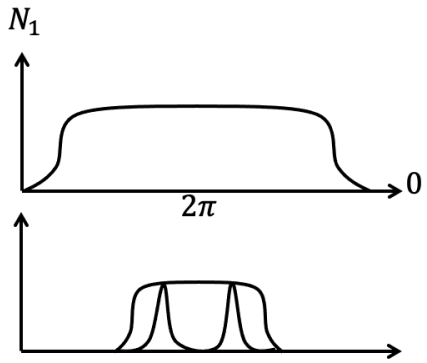

Рис. 6.4. Распределение дробинок, вылетающих из одного и другого ружей, в аналогии «пьяный охотник».

Ствола два, поэтому если мы фиксируем, что охотник в данный момент времени куда-то стреляет и мы зафиксировали положение одного ствола, то, сканируя другим, в корреляции будет далеко не все. Однако, отношение распределений будет показывать степень корреляции. В глобальном смысле, это полная аналогия.

В теории квантовой информации есть мера, характеризующая количество перепутываний. Часто можно услышать мнение (довольно справедливое), что величину перепутывания можно измерить числом состояний Белла, которые там находятся. Рассмотрим состояние Вернера:

$$\rho_W = F|\psi^-\rangle\langle\psi^-| + (1-F)(|\psi^+\rangle\langle\psi^+| + |\phi^-\rangle\langle\phi^-| + |\phi^+\rangle\langle\phi^+|), \qquad (6.10)$$

где F – число синглетов. В теории квантовой информации есть термин, который в некотором смысле аналогичен термину кубита: $ebit$.

Рассмотрим меры, относящиеся к чистым перепутанным состояниям. Составим произвольное состояние двух кубитов:

$$|\psi_{12}\rangle = c_1|0_1\rangle|0_2\rangle + c_2|0_1\rangle|1_2\rangle + c_3|1_1\rangle|0_2\rangle + c_4|1_1\rangle|1_2\rangle \qquad (6.11)$$

Условие нормировки:

$$\sum_{i=1}^{4}|c_1|^2 = 1 \qquad (6.12)$$

Для того, чтобы понять, является состояние перепутанным или нет, следует помнить, что если чистое двухкомпонентное состояние максимально перепутано, то состояния подсистем максимально смешанные. А значит, если построить матрицу плотности, посчитать ее редуцированный след и найти условия, при которых она будет смешанной, это и будет являться условием максимальной перепутанности:

$$\rho_{12} \equiv |\psi_{12}\rangle\langle\psi_{12}| \qquad (6.13)$$

$$\rho_{12} \to \rho_1 = Sp_2\rho_{12} \qquad (6.14)$$

Тогда меры перепутывания:

$$0 \le \mathrm{C} = 2|c_1c_4 - c_2c_3| \le 1 \qquad (6.15)$$

Возьмем ϕ^-:

$$c_1 = \frac{1}{\sqrt{2}} = \cdots; c_2 = -\frac{1}{\sqrt{2}} \tag{6.16}$$

Смешанные перепутанные состояния

Допустим есть чистое перепутанное состояние и разлетающиеся подсистемы (смесь кубитов), на них могут независимо действовать разные шумы, чем можно испортить чистоту состояния.

Довольно важный класс операций, которые можно производить над перепутанными состояниями, – локальные операции и классические коммуникации. Если локально (унитарно) с сохранением энергии поворачивать кубит (и даже согласовывать операции), то такие операции не меняют степень перепутывания. Так, физически можно понять, как из чистого состояния получить смешанные. Для того, чтобы характеризовать количество перепутываний в смешанном состояния, используют термин $entanglement\ of\ formation$. Его можно последовательно вводить для нескольких типов состояний:

1. Чистые состояния: энтропия подсистемы: $E(\rho_1)$). Для максимально перепутанного состояния, состояния подсистем максимально смешанные, а значит, обладают максимальной энтропией. Если состояния не перепутанные, то состояние подсистемы чистое (они факторизуются), а значит энтропия равна нулю.

2. Ансамбль чистых состояний (набор двухкомпонентных состояний $|\psi_{12}^i\rangle$ и классическое число распределения вероятностей этих чистых состояний p_i). Тогда перепутыванием создания ансамбля называется среднее entanglement of formation по ансамблю:

$$\mathcal{E} = \sum_i p_i^{E(\psi_i)} \tag{6.17}$$

   Вспомним, что, если есть матрица плотности, (ее всегда можно составить из ансамбля), но в обратную сторону (каким ансамблем эта матрица плотности образована) сказать ничего нельзя, так как существует бесконечное количество ансамблей. Поэтому для смешанного состояния эта величина (6.17) будет являться минимальной из всех возможных ансамблей, которые образует это состояние.

Лекция 7. Парадокс Эйнштейна- Подольского-Розена

Парадокс Эйнштейна-Подольского-Розена (ЭПР)

В первую очередь, рассмотрим две цитаты из статьи «Можно ли считать, что квантово-механическое описание физической реальности является полным?» 1936 года:

1. «какой бы смысл ни вкладывался в термин «полный» (речь идет о том, что такое полное описание физической теории), от всякой полной теории нужно, как нам кажется, требовать следующее: каждый элемент физической реальности должен иметь отражение физической теории»
2. «если мы можем без какого бы то ни было возмущения системы можем предсказать с достоверностью, т.е. с вероятностью равной единице, значение некоторой физической величины, то существует элемент физической реальности, соответствующий этой физической величине. Нам кажется, что этот критерий, хотя он далеко не исчерпывает всех возможных способов распознавания физической реальности, по крайней мере дает нам один из тех способов коль скоро выполняется формулирование в нем условия. Этот критерий рассматривается не как необходимое, а только как достаточное условие реальности».

В течение лекции и дальше будем работать со следующим состоянием Белла:

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}\{|0_1 1_2\rangle - |1_1 0_2\rangle\} \tag{7.1}$$

Состояние примечательно тем, что оно неизменно в любом базисе. Представление Шредингера:

$$|\psi\rangle = \frac{1}{\sqrt{2}}\{|B_x\rangle|C_y\rangle - |C_x\rangle|B_y\rangle\} \tag{7.2}$$

Для того, чтобы доказать инвариантность, следует записать его выражение в другом базисе. Используем оператор поворота:

$$\widehat{D} = \begin{pmatrix} t & r \\ -r^* & t^* \end{pmatrix} \tag{7.3}$$

$$|t|^2 + |r|^2 = 1 \tag{7.4}$$

$$t = \cos\delta + \mathrm{i}\sin\delta\cos 2\chi \tag{7.5}$$

$$r = \mathrm{i}\sin\delta\sin 2\chi \tag{7.6}$$

Так, если речь идет об фазовых пластинках толщины d и углом, отсчитываемым от вертикали χ, то

$$\delta = \frac{(n_o - n_e)d\pi}{\lambda} \tag{7.7}$$

Преобразование, примененное к состояниям (7.2), будет давать следующие преобразования:

$$D\begin{pmatrix}B_1\\B_2\end{pmatrix}=\begin{pmatrix}B_x\\B_y\end{pmatrix} \tag{7.8}$$

$$D\begin{pmatrix}C_1\\C_2\end{pmatrix}=\begin{pmatrix}C_x\\C_y\end{pmatrix} \tag{7.9}$$

$$B_x = tB_1 + rB_2 \tag{7.10}$$

$$B_y = -r^*B_1 + t^*B_2 \tag{7.11}$$

$$C_x = tC_1 + rC_2 \tag{7.12}$$

$$C_y = r^*C_1 + t^*C_2 \tag{7.13}$$

Так, с помощью оператора $\widehat{D}$ осуществляется переход от состояний в базисе xy к состояниям в базисе 1,2. Подставим в (7.2):

$$|\psi\rangle = \frac{1}{\sqrt{2}}[(tB_1 + rB_2)(-r^*C_1 + t^*C_2) - (tC_1 + rC_2)(-r^*B_1 + t^*B_2)] = \tag{7.14}$$

$$= \frac{1}{\sqrt{2}}[-tr^*B_1C_1 + tt^*B_1C_2 - rr^*B_2C_1 + rt^*B_2B_2 + tr^*C_1B_2 - tt^*C_1B_2 + rr^*C_2B_2 - rt^*c_2B_2] = \frac{1}{\sqrt{2}}[(|t|^2 + |r|^2)B_1C_2 - (|r|^2 + |t|^2)B_2C_1],$$

где $(|t|^2 + |r|^2) = 1, (|r|^2 + |t|^2) = 1$, что и требовалось доказать. Такое свойство называется инвариантностью синглетного состояния Белла к смене базисов. Остальные три состояния Белла не обладают этим свойством, они инвариантны только по отношению к частным преобразованиям.

Далее мы будем говорить о парадоксе Эйнштейна-Подольского-Розена в варианте Бома, довольно упростившего описание. Будем держать в уме, что синглетное состояние Белла инвариантно к тому, как на него смотреть. Для парадокса к рассмотрению предлагается конкретная физическая реализация: представим источник, испускающий какие-то частицы со спином ½.

$$|\psi\rangle = \frac{1}{\sqrt{2}}\{|\uparrow_1\downarrow_2\rangle - |\downarrow_1\uparrow_2\rangle\} \tag{7.15}$$

Поставим магнит, ориентированный вдоль оси Z, допустим, щелкнул детектор, регистрирующий спин вверх первой частицы. Тогда исходя из (7.15), вторая частица будет иметь спин вниз на ось Z. Важно понимать, что частицы разлетелись очень далеко, и мы на них никак не воздействуем, поэтому вероятно, что и до измерения первой частицы, спин второй был направлен вниз.

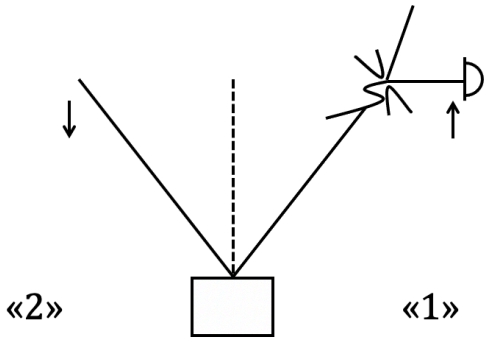

Рис. 7.1. Магнит, ориентированный вдоль оси Z.

Представим следующую ситуацию: наблюдатель, устанавливающий магниты и замеряющий результаты, свободен в выборе и ориентирует магниты вдоль направления X. Тогда

$$|\psi\rangle \equiv \frac{1}{\sqrt{2}}[|\rightarrow_1\leftarrow_2\rangle - |\leftarrow_1\rightarrow_2\rangle] \tag{7.16}$$

Состояния инвариантны. Проведем те же самые рассуждения с ориентацией магнитов вдоль направления X. В момент измерения мы знаем, что спин одной частицы повернут так (→) (тогда спин другой повернут ←), на частицы никак не воздействуем. Так, так как мы предполагаем, что этому (←) соответствует элемент физической реальности, то спин имел такую проекцию и до измерения первой частицы. Поскольку мы можем произвольно ориентировать магниты (в том числе, после того как вылетели частицы), то можно постулировать, что у частицы спин имеет определенное направление и вдоль направления Z, и вдоль направления X, что противоречит основам квантовой механики (так как мы знаем, что проекции компонента спина не коммутируют, значит, не существуют одновременно). Это парадокс, значит очевидно, что он имеет решение.

Неравенство Белла

Неравенство Белла также иногда называют парадоксом. Мы выведем неравенства, которые можно интерпретировать и проверять в физических экспериментах с двух позиций: с позиции квантовой теории результат будет один, с позиции классической теории – другим. Мы сформулируем парадокс для двух наблюдателей, но также существует неравенство Клышко-Мермина на случай N наблюдателей. Так, для N наблюдателей соотношение между разницей предсказаний классической теории и квантовой формулируется в виде $2^{(N-1)/2}$. Представим источник перепутанных состояний – для определенности будем использовать состояние $|\psi^-\rangle$. Пусть есть два наблюдателя (A и B), каждого есть ручка, принимающая два хорошо-различимых значения (± 1), наблюдатели действуют совершенно независимо.

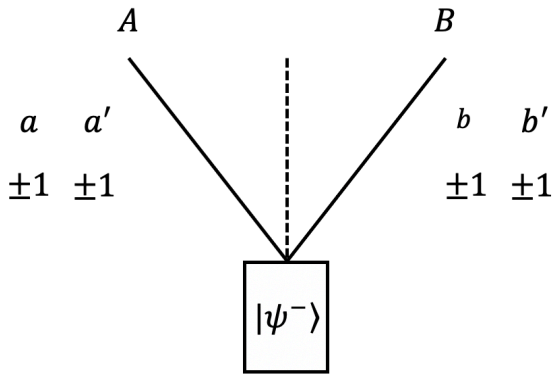

Рис. 7.2. Источник перепутанных состояний ($|\psi^-\rangle$).

Если рассуждать с точки зрения зеленой и красной ламп, в каждый момент времени, независимо от того, какую ручку выбрал каждый из наблюдателей, есть четыре возможных комбинации:

$$+ \quad +$$
$$+ \quad -$$
$$- \quad +$$
$$- \quad -$$

Предположим, что такая ситуация описывается некой функцией распределения:

$$P(A, A', B, B') \geq 0 \tag{7.17}$$

$$\sum_{a,a',b,b'} P(A, A', B, B') = 1 \tag{7.18}$$

Тогда маргинальное распределение вероятности:

$$P(A', B, B') = P(1, A', B, B') + P(-1, A', B, B') \tag{7.19}$$

Построим наблюдаемую Белла:

$$\langle S \rangle = \frac{1}{2}[\langle AB \rangle + \langle A'B \rangle + \langle AB' \rangle - \langle A'B' \rangle] \tag{7.20}$$

Мы проводим много независимых экспериментов: каждый раз фиксируем цвета лампочек. В неравенстве Белла в варианте Хорна-Шамони-Хольта утверждается, что$|\langle S \rangle| \leq 1$. Докажем это:

$$S = \frac{1}{2}(ab + a'^b + ab' - a'b') \equiv \frac{1}{2}[a(b + b') + a'(b - b')] \tag{7.21}$$

Рассмотрим две ситуации:

$$b = b' \tag{7.22}$$

$$|S| = 1 \tag{7.23}$$

В случае второй ситуации:

$$b = -b' \tag{7.24}$$

$$|S| = 1 \tag{7.25}$$

Учитывая (7.18):

$$|\langle S\rangle| = |\sum P(A, A', B, B')\, S| \leq \sum |P * S| = \sum P|S| = \sum P = 1 \tag{7.26}$$

Так, доказательство строилось на предположениях, что существует $\exists P$, что $p \geq 0$ и $|S| = 1$, так как мы считали, что результат измерения наблюдателя A не влияет на результат измерения наблюдателя B. Будь это не так, запись (7.21) выглядела бы следующим образом:

$$S' \overset{?}{=} \frac{1}{2}\left[a(b)b(a) + a'(b)b(a') + a(b')b'^{(a)} - a'(b')b'(a')\right] \tag{7.27}$$

$$S = 0, \pm 1, \pm 2 \tag{7.28}$$

Докажем неравенство Белла в квантовом случае: будем усреднять по функции

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}[|0_1 1_2\rangle - |1_1 0_2\rangle] \tag{7.29}$$

Представим следующие операторы:

$$a = \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{7.30}$$

$$a' = \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{7.31}$$

$$b = \frac{1}{\sqrt{2}}(-\sigma_z - \sigma_x) = \frac{1}{\sqrt{2}}\begin{pmatrix} -1 & -1 \\ -1 & 1 \end{pmatrix} \tag{7.32}$$

$$b' = \frac{1}{\sqrt{2}}(\sigma_z - \sigma_x) = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix} \tag{7.33}$$

$$\langle S\rangle = \frac{1}{2}[\langle ab\rangle \ldots] = \frac{1}{\sqrt{2}} \tag{7.34}$$

Частично рассмотрим, как это получается:

$$\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \otimes \begin{pmatrix} -1 & -1 \\ -1 & 1 \end{pmatrix} \rangle = \langle \psi^- | \begin{pmatrix} 0 & 0 & -1 & -1 \\ 0 & 0 & -1 & 1 \\ -1 & -1 & 0 & 0 \\ -1 & 1 & 0 & 0 \end{pmatrix} | \psi^- \rangle \tag{7.35}$$

Левая часть (7.29):

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \tag{7.36}$$

$$|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{7.37}$$

$$|01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \tag{7.38}$$

Правая часть:

$$\begin{pmatrix}0\\1\end{pmatrix}\otimes\begin{pmatrix}1\\0\end{pmatrix}=\begin{pmatrix}0\\0\\1\\0\end{pmatrix} \tag{7.39}$$

Складываем части:

$$|\psi^-\rangle=\frac{1}{\sqrt{2}}\begin{pmatrix}0\\1\\1\\0\end{pmatrix} \tag{7.40}$$

$$\ldots\otimes\begin{pmatrix}0 & 1 & 1 & 0\end{pmatrix}\begin{pmatrix}0 & 0 & -1 & -1\\0 & 0 & -1 & 1\\-1 & -1 & 0 & 0\\-1 & 1 & 0 & 0\end{pmatrix}\begin{pmatrix}0\\1\\1\\0\end{pmatrix}=\cdots=\frac{1}{\sqrt{2}} \tag{7.41}$$

$$\langle S\rangle=\frac{1}{2}\left[\frac{1}{\sqrt{2}}+\frac{1}{\sqrt{2}}+\frac{1}{\sqrt{2}}+\frac{1}{\sqrt{2}}\right]=\frac{1}{2}\frac{4}{\sqrt{2}}=\sqrt{2} \tag{7.42}$$

Так, в классике $\langle S\rangle=1$, а в квантовом случае – $\sqrt{2}$. Проанализируем, что не так в классике. Мы сформулировали три условия (локальный реализм), при которых и получили такой результат, значит, следует отказаться от одного из них. С точки зрения формальной логики, противоречию было придумано следующего объяснение: так, есть утверждения:

1) все короткие анекдоты хорошие

2) этот рассказ длинный

3) вывод: он плохой

Проведем аналогию:

1) классические локальные теории ведут к некоторому неравенству ($|\langle S\rangle|\leq 1$)

2) квантовые теории нарушают это неравенство ($|\langle S\rangle|=\sqrt{2}>1$)

3) вывод: квантовая теория не локальна

Так, следует отказаться от предположения, что в квантовой механике априорно существует функция распределения для состояний.

ФИЗИЧЕСКИЙ
ФАКУЛЬТЕТ
МГУ ИМЕНИ
М.В. ЛОМОНОСОВА

teach-in
ЛЕКЦИИ УЧЕНЫХ МГУ