МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Новосибирский государственный университет

Физический факультет
Кафедра Квантовой оптики

Л. В. Ильичёв

ЭЛЕМЕНТЫ КВАНТОВОЙ МЕТАФИЗИКИ

Часть 3
(ограничения на копирование и различение
квантовых состояний, "квантовая криптография"
и парадоксы причинных петель)

Учебное пособие

Новосибирск
2012

УДК 539.1.01
ББК (В)22,314
И 468

Ильичёв Л. В. Элементы квантовой метафизики: Учеб. пособие / Новосибирский государственный университет; Институт автоматики и электрометрии СО РАН. Новосибирск, 2011. Ч. 3: ограничения на копирование и различение квантовых состояний, "квантовая криптография" и парадоксы причинных петель. 87 с.

В настоящем учебном пособии представлен материал, основанный на курсе лекций, читаемых автором в Новосибирском государственном университете. Изложен современный взгляд на некоторые актуальные интерпретационные проблемы квантовой физики, слабо отражённые в отечественной литературе. Пособие является продолжением первых двух частей; включает в себя изложение физических причин и следствий ограничений на возможность копирования и различения квантовых состояний, их связь с причинной структурой пространства-времени; возможности использования гипотетических причинных петель в квантовой физике и приложений таких моделей к квантовой информатике.

Пособие рассчитано на студентов и аспирантов, обучающихся по специальностям, связанным с квантовой физикой. Оно может быть полезным и для молодых специалистов, работающих в этой области.

Учебное пособие подготовлено в рамках реализации Программы развития НИУ-НГУ на 2009-2018 гг.

Оглавление

Предисловие к Части 3

Третья часть "Элементов квантовой метафизики" является естественным продолжением первых двух частей. В центре внимания снова оказываются основы квантовой науки. И главным при любом рассмотрении интерпретационных проблем квантовой физики оказывается статус понятия состояния. Недостаток ясности в этом вопросе болезненно ощутим в настоящее время поскольку, несмотря на значительные усилия последних лет, направленные на синтез двух главных физических теорий – общей теории относительности и квантовой механики, результаты весьма скромны. Оказалось нарушенным поступательное движение теоретической мысли каждые четверть века, начиная с Фарадея (или даже с Лавуазье и Ломоносова), революционизирующее или, по крайней мере, существенно обогощающее наше понимание основ Мироздания. Последним таким прорывом можно считать объединение взаимодействий в рамках Стандартной модели. И этот последний успех относится к американскому периоду развития теоретической физики, начавшемуся после Второй мировой войны. С именами Фейнмана, Швингера и Дайсона связано создание квантовой электродинамики – чрезвычайно успешной и практичной теории, своеобразно воплощающей в себе американский подход к жизни. Отцы квантовой электродинамики были талантливыми физиками, но они не были метафизиками и философами как Эйнштейн, Бор и Гейзенберг. Дух квантовой электродинамики живёт в Стандартной модели и он же движет работами в теории струн, претендующей, но не доказавшей свои права на статус "окончательной

теории". Сомнения в возможности построить такую теорию и сомнения в правильности выбранного "струнного" направления всё чаще звучат в литературе вместе с ощущением необходимости вернуться (фигурально) в начало прошлого века для нового глубокого осмысления фундамента нашего миропонимания и прежде всего его квантового аспекта.

Существуют два основных подхода к понятию квантового состояния – *онтологический* и *эпистемологический* (или *реляционный*, как он назывался в Части 1 и Части 2). Согласно первому взгляду состояние ψ_S квантовой системы является реальностью, хоть и не "данной нам в непосредственном ощущении", но объективно существующей независимо от нас и нашего знания о системе. Мотивы, толкающие к принятию такого взгляда представляются довольно естественными: соотношение неопределенности лишило статуса привычного объективного существования классическое состояние как точки в фазовом пространстве системы, и мы испытываем (возможно неосознанный) дискомфорт, наблюдая пустоту пьедестала Реальности, и спешим воздвигнуть на него состояние той же системы в новом обличье волновой функции. Возможно крайней формой выражения онтологического парадигмы служит бытующее в английском языке и используемое в некоторых статьях выражение "the state ψ_S lives on the system" (Рис. 1, слева). От принявшего онтологическую концепцию требуется найти способ ужиться с парадоксом Эйнштейна-Подольского-Розена (см. Часть 1), встающего во всей своей значительности[1]. В противоположность этому эпистемологический взгляд сводит понятие состояния исключительно к особым образом оформленному нашему *зна-*

[1]Высказываются соображения, что авторы парадокса (по крайней мере Эйнштейн) руководствовались при написании своей работы неприятием онтологического взгляда на квантовое состояние.

нию о квантовой системе (Рис. 1, справа). Заметим, что в такой трактовке понятие квантового состояния приобретает черты реляционности, т.к. теперь при спецификации состояния требуется указать носителя знания о системе.

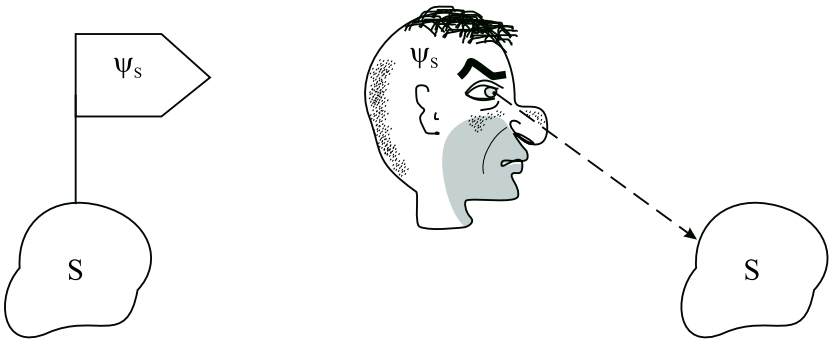

Рис. 1. Различие между онтологической (слева) и эпистомологической (справа) трактовками понятия квантового состояния.

В этом контексте интересно оценить взгляды Эверетта. Весьма примечательно, что центральным в подходе Эверетта является понятие *соотнесенных* квантовых состояний системы с одной стороны и памяти наблюдателя с другой. Здесь явно просматриваются мотивы реляционной (эпистемологической) концепции. С другой стороны, соотнесенные состояния возникают в рамках некоторой глобальной волновой функции Ψ. Взгляд Эверетта на статус глобальной волновой функции четко и недвусмысленно обозначен в его диссертации: "The state function Ψ is thought of as objectively characterizing the physical system, i.e., at all times an isolated system is thought of as possessing a state function, independently of our state of knowledge of it"[2]. Таким образом, глобальное

[2]Автор позволил себе отнести этот пассаж к глобальной волновой

состояние имеет по Эверетту онтологический характер. Налицо определенная непоследовательность и двойственность взглядов. Почему объекты квантового формализма, имеющие единую математическую природу, т.е. состояние Вселенной в целом и состояния ее подсистем, столь различны в плане своего отношения к Реальности? Разрешение противоречия простейшим образом, приписав глобальной волновой функции эпистемологический (реляционный) статус, потребует указания второго партнера реляции, что представляется затруднительным, т.к. его необходимо будет расположить вне Вселенной. Следует ли в свете этого отказаться от понятия глобальной волновой функции? Явится ли такой отказ фатальным для первоначальной оригинальной концепции Эверетта? Или, возможно, ошибочна наша интерпретация эвереттовской трактовки соотнесенных состояний как эпистемологических? Вопросы эти проще поставить, чем ответить на них.

В Части 3 рассмотриваются последствия для картины мира принятия онтологического взгляда на квантовое состояние. Сделаем это в контексте проблем копирования и различения квантовых состояний, возникающих в практике бурно развивающейся в настоящее время квантовой информатики и так называемой "квантовой криптографии". Действуя в рамках известной работы Дэвида Дойча (David Deutsch), мы воспользуемся мощным, хотя и экзотическим инструментом – замкнутой причинной петлей. Как известно, такие особенности в структуре пространства-времени допускаются общей теорией относительности (ОТО). Особенности квантовой эволюции в присутствие причинных

функции, хотя сам Эверетт явно это не указывает, на том основании, что Вселенная в целом представляет собой идеальную (и единственную) замкнутую систему.

петель представляют несомненный интерес, т.к. возникает возможность "столкнуть" две основные физические теории (ОТО и квантовую механику) и изучить разлетевшиеся "осколки". Это позволит лучше понять обе теории и их взаимоотношение.

Параграфы, отмеченные звёздочкой *, как и в Части 2, содержат материал, не входивший ранее в учебные тексты и лишь частично представленный в научной литературе.

1 "Сверхсветовой телеграф" Н.Герберта

В 1982 году в журнале Foundations of Physics была опубликована статья Ника Герберта с оригинальным названием *"FLASH – A Superluminal Communicator Based Upon a New Kind of Quantum Measurement"*. Помимо функции привлечения внимания к статье как к некоторому экстренному и необычному сообщению, слово FLASH явилось акронимом для First Laser-Amplified Superluminal Hookup. Год выхода статьи и статус журнала казалось бы не должны позволить появиться статье столь резко атакующей релятивизм и фундаментальный принцип **NS** (Non-Signalling) квантовой механики обсуждавшийся в Части 1. Ситуация здесь, однако, не столь проста, и целесообразно рассмотреть идею статьи. Дальнейшее изложение может показаться излишне педантичным, но это должно себя оправдать.

Исходные посылки Герберта достаточно стандартные: имеется фотонная пара в зацепленном состоянии

$$|\Psi\rangle_{AB} = \frac{1}{\sqrt{2}}\Big(|\lambda\rangle_A \otimes |\lambda^{\perp}\rangle_B - |\lambda^{\perp}\rangle_A \otimes |\lambda\rangle_B\Big), \qquad (1)$$

где λ и $\lambda^{\perp}$ обозначают две любые ортогональные поляризации, и запись состояния $|\Psi\rangle_{AB}$ инвариантна относительно выбора этой пары ортогональных поляризаций. Мы имеем таким образом аналог синглетного состояния двух частиц со спином 1/2 (в русскоязычной литературе это состояние известно как скалярный бифотон). Один фотон из этой пары поступает к Алисе, а второй – к Бобу. Перед Алисой стоит задача передать Бобу, находящемуся от неё на произвольно большом расстоянии, информационное сообщение, состоящее из 0 или 1 (т.е. один бит). Предполагается, что Алиса

и Боб неподвижны друг относительно друга и располагают синхронизованными часами. В заранее условленный момент времени начинается процедура передачи. Если содержание передаваемого бита есть 0, Алиса проводит измерение поляризации своего фотона в базисе $\{|V\rangle, |H\rangle\}$ (вертикальная и горизонтальная поляризации). При этом совместное состояние Алисы и фотонной пары претерпевает следующее изменение:

$$|A_0\rangle\langle A_0| \otimes |\Psi\rangle_{AB}\langle\Psi| \mapsto \hat{\varrho}_0, \tag{2}$$

где

$$\hat{\varrho}_0 = \frac{1}{2}|A_{0V}\rangle\langle A_{0V}| \otimes |H\rangle_B\langle H| + \frac{1}{2}|A_{0H}\rangle\langle A_{0H}| \otimes |V\rangle_B\langle V| -$$

$$\frac{1}{2}|A_{0V}\rangle\langle A_{0H}| \otimes |H\rangle_B\langle V| - \frac{1}{2}|A_{0H}\rangle\langle A_{0V}| \otimes |V\rangle_B\langle H|.$$

Здесь $|A_0\rangle$ – состояние Алисы, *намеревающейся* отправить сообщение 0; $|A_{0V}\rangle$ ($|A_{0H}\rangle$) – совместное состояние Алисы и её фотона, который при измерении оказался поляризованным вертикально (горизонтально). Если содержание бита, отправляемого Алисой, есть 1, она проводит измерение поляризации своего фотона в базисе $\{|R\rangle, |L\rangle\}$ правой (R) и левой (L) поляризаций. В этом случае вместо (2) имеем

$$|A_1\rangle\langle A_1| \otimes |\Psi\rangle_{AB}\langle\Psi| \mapsto \hat{\varrho}_1, \tag{3}$$

где

$$\hat{\varrho}_1 = \frac{1}{2}|A_{1R}\rangle\langle A_{1R}| \otimes |L\rangle_B\langle L| + \frac{1}{2}|A_{1L}\rangle\langle A_{1L}| \otimes |R\rangle_B\langle R| -$$

$$\frac{1}{2}|A_{1R}\rangle\langle A_{1L}| \otimes |L\rangle_B\langle R| - \frac{1}{2}|A_{1L}\rangle\langle A_{1R}| \otimes |R\rangle_B\langle L|.$$

Ранее в Части 1 и Части 2 неоднократно отмечался реляционный характер квантовых состояний. Оценим в этом контексте выражения (2) и (3). Они представляют собой состояния Алисы и фотонной пары по отношению к некоторому наблюдателю (назовём его Чарльзом), который знает содержание отправляемого сообщения, но не располагает информацией о результатах измерения поляризации фотона, проводимого Алисой. В реальности состояния $\hat{\varrho}_0$ и $\hat{\varrho}_1$ выглядят проще (это уточнение не является необходимым для дальнейшего, но его). Действительно, информация об исходах измерения поступает в окружение (Алиса может, например, рассказать о них коллегам по лаборатории). Мы абстрагируемся от элементов окружения, в которых записана эта информация, поэтому слагаемые в $\hat{\varrho}_0$ и $\hat{\varrho}_1$, недиагональные по исходам измерения и состояниям памяти Алисы исчезают при взятии следа следа по степеням свободы окружения (по состояниям памяти коллег), т.е.

$$\begin{aligned}\hat{\varrho}_0 &= \frac{1}{2}|A_{0V}\rangle\langle A_{0V}| \otimes |H\rangle_B\langle H| + \frac{1}{2}|A_{0H}\rangle\langle A_{0H}| \otimes |V\rangle_B\langle V| \quad (4)\\ \hat{\varrho}_1 &= \frac{1}{2}|A_{1R}\rangle\langle A_{1R}| \otimes |L\rangle_B\langle L| + \frac{1}{2}|A_{1L}\rangle\langle A_{1L}| \otimes |R\rangle_B\langle R|.\end{aligned}$$

Легко заметить, что состояние поляризации фотона B, находящегося в распоряжении Боба, в первом случае есть

$$\frac{1}{2}|H\rangle_B\langle H| + \frac{1}{2}|V\rangle_B\langle V|, \quad (5)$$

а во втором –

$$\frac{1}{2}|R\rangle_B\langle R| + \frac{1}{2}|L\rangle_B\langle L|. \quad (6)$$

Но это есть две разные формы записи одного и того же оператора $\hat{1}/2$, описывающего состояние неполяризованного фо-

тона. Вывод Чарльза о возможности Алисы передать сообщение Бобу однозначно отрицательный. Срабатывает принцип **NS**. С точки зрения Алисы ситуация выглядит несколько иначе. В ходе своего измерения Алиса "приготавливает" для Боба его фотон в одном из четырёх состояний $|V\rangle_B$, $|H\rangle_B$, $|R\rangle_B$ и $|L\rangle_B$. Она может частично контролировать процесс приготовления – задать либо пару $\{|V\rangle_B, |H\rangle_B\}$, либо пару $\{|R\rangle_B, |L\rangle_B\}$. С её точки зрения это вполне достаточно для отправки сообщения. Проблема в том, что, хотя сообщение и *отправлено*, Боб не в состоянии его *расшифровать*. Это уже ясно с точки зрения Чарльза, для которого реальность представляется либо состоянием $\hat{\varrho}_0$, либо состоянием $\hat{\varrho}_1$. Для Боба (если ему известны только априорные вероятности p_0 и p_1 отправки 0 и 1) реальность задаётся состоянием

$$p_0\hat{\varrho}_0 + p_1\hat{\varrho}_1 \tag{7}$$

и перспективы расшифровки никак не могут быть выше. Состояние его фотона после момента измерения Алисы (о моменте он узнаёт по своим часам) такое же как и до этого момента:

$$\frac{p_0}{2}\Big(|H\rangle_B\langle H| + |V\rangle_B\langle V|\Big) + \frac{p_1}{2}\Big(|R\rangle_B\langle R| + |L\rangle_B\langle L|\Big) = \frac{1}{2}\hat{1}. \tag{8}$$

Всё сказанное является "стандартным" взглядом, исключающим использование зацепленных состояний для коммуникации и было, конечно, хорошо известно Герберту. Но он делает следующий нетривиальный ход в своих рассуждениях – предполагает наличие у Боба некоторого устройства, преобразующего любое из четырёх состояний $|V\rangle_B$, $|H\rangle_B$, $|R\rangle_B$

и $|L\rangle_B$ в состояния некоторой другой системы:

$$\begin{aligned} |V\rangle_B &\rightarrow |\psi_V\rangle, \ |H\rangle_B \rightarrow |\psi_H\rangle, \\ |R\rangle_B &\rightarrow |\psi_R\rangle, \ |L\rangle_B \rightarrow |\psi_L\rangle \end{aligned} \tag{9}$$

так, что четвёрка состояний $|\psi_V\rangle$, $|\psi_H\rangle$, $|\psi_R\rangle$ и $|\psi_L\rangle$ ортонормирована. Можно считать, что это есть множество собственных векторов некоторой наблюдаемой величины, отвечающие различным собственным значениям. Проведя измерение этой наблюдаемой, Боб может легко отличить состояние "неполяризованного" фотона (5) от состояние "неполяризованного" фотона (6). Это явится дешифровкой сообщения Алисы.

Вариантом осуществления преобразование (10), является копирование:

$$|V\rangle \mapsto |V\rangle^{\otimes n}. \tag{10}$$

Аналогично в случае остальных трёх состояний; символом $^{\otimes n}$ здесь обозначено n-кратное тензорное произведение. Состояния $|V\rangle^{\otimes n}$ и $|H\rangle^{\otimes n}$ автоматически оказываются ортогональными, также как $|R\rangle^{\otimes n}$ и $|L\rangle^{\otimes n}$. Для перекрёстных произведений состояний из этих пар, например для $|V\rangle^{\otimes n}$ и $|R\rangle^{\otimes n}$, имеем

$$|\langle V|^{\otimes n}|R\rangle^{\otimes n}| = |\langle V|R\rangle|^n = \frac{1}{\sqrt{2^n}}. \tag{11}$$

При $n \rightarrow \infty$ правая часть (11) стремится к 0 и состояния из "плоской" и "циркулярной" пар становятся ортогональными. В принципе нет необходимости неограниченно увеличивать число копий. Уже в случае $n = 2$ состояния

$$\frac{1}{2}|H\rangle\langle H| \otimes |H\rangle\langle H| + \frac{1}{2}|V\rangle\langle V| \otimes |V\rangle\langle V|$$

и

$$\frac{1}{2}|R\rangle\langle R| \otimes |R\rangle\langle R| + \frac{1}{2}|L\rangle\langle L| \otimes |L\rangle\langle L|, \tag{12}$$

заменяющие (5) и (6), не тождественны друг другу и могут быть различены, хотя и не с единичной вероятностью, как при $n \to \infty$.

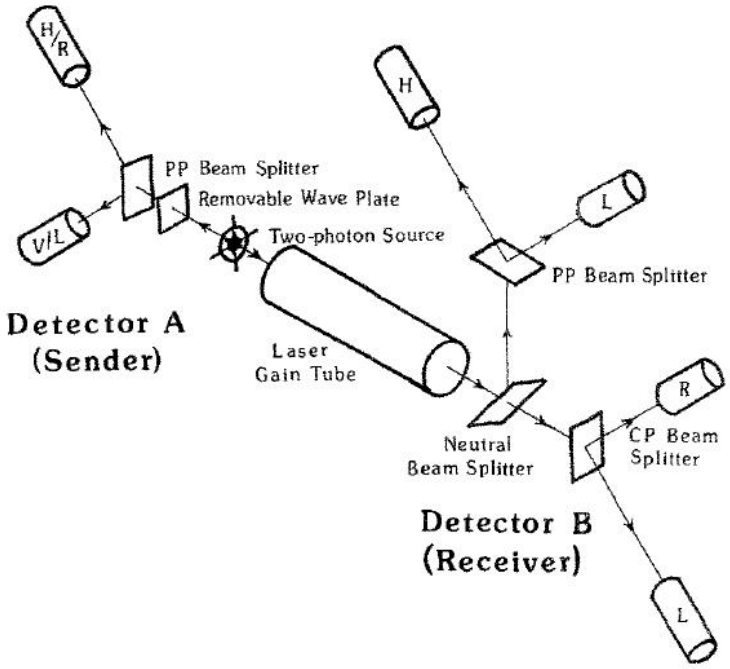

Рис. 2. Схема "сверхсветового телеграфа" из работы Н.Герберта. Пояснения в тексте.

В качестве устройства, копирующего поляризации фотонов, Герберт предложил использовать оптический квантовый усилитель. Процесс вынужденного испускания действительно порождает фотон с поляризацией, тождественной поляризации вынуждающего фотона. Цепной процесс вынужденных испусканий в усилителе осуществит по мнению Герберта

преобразование типа (10). На рис. 2 приведена оригинальная схема "ансибла"[3] из работы Герберта. Алиса, помещая или убирая пластинку $\lambda/4$ на пути фотона A, выбирает базис ($\{|V\rangle, |H\rangle\}$ или $\{|R\rangle, |L\rangle\}$), в котором измеряет поляризацию своего фотона. Попадание фотона B в квантовый усилитель, расположенный в лаборатории Боба, происходит после измерения в лаборатории Алисы, что обеспечивается часами, синхронизованными в их общей системе отсчёта. Родившиеся n фотонов попадают на 50%-й делитель пучка, нечувствительный к поляризации. Первая половина фотонов попадает на селектор в базисе $\{|V\rangle, |H\rangle\}$, а вторая половина – на селектор в базисе $\{|R\rangle, |L\rangle\}$. Если (для примера) все n фотонов имели поляризацию R, оба детектора в базисе плоских поляризаций обнаружат в среднем по $n/4$ фотонов, детектор R обнаружит $n/2$ фотонов, а детектор L – ноль фотонов. Это позволит Бобу идентифицировать сообщение Алисы как 1.

Герберт осознавал и отмечал мешающую роль спонтанных переходов в усилителе, но высказал убеждение, что этот эффект не явится принципиальным препятствием для осуществления сверхсветовой связи.

2 Ограничения на возможность копирования квантовых состояний (No-cloning Theorem)

Работа Герберта попала на рецензирование к Ашеру Пересу (см. Часть 2). Как он позже писал об этом, ошибоч-

[3]Фантастическое устройство для межзвёздной связи, созданное физиком из системы τ Кита в романе *The Dispossessed* Урсулы Ле Гуин. Ансибл фигурирует во всех её книгах из Хайнского цикла.

ность вывода о возможности сверхсветовой связи была для него очевидна. Более того, Перес выражал уверенность, что и автор работы в действительности не верит в нарушение принципов релятивистской физики. Однако Перес счёл правильным рекомендовать публикацию работы, рассматривая её как своего рода интеллектуальную провокацию, привлекающую внимание специалистов к не до конца понятным свойствам квантового мира. Расчёт оказался верным. В том же 1982 году вышли две независимые работы, в которых с разных позиций показана невозможность точного копирования *неизвестных*[4] квантовых состояний из *неортогонального* набора. Рассмотри сначала аргументы Вуттерса и Зурека. Они ввели термин *клонирование* квантового состояния – создание точной копии объекта при сохранении его в исходном и изначально неизвестном состоянии. Запрет на клонирование известен теперь в литературе как *No-cloning theorem*. Вуттерс и Зурек в своих рассуждениях опирались на линейность квантовомеханических преобразований. Устройство (копир или клонер) должно по замыслу действовать следующим образом:

$$|\psi\rangle \otimes |blank\rangle \otimes |env\rangle \rightarrow |\psi\rangle \otimes |\psi\rangle \otimes |env_{\psi}\rangle. \qquad (13)$$

Здесь $|\psi\rangle$ – состояние объекта, подлежащего клонированию; $|blank\rangle$ – некоторое стандартное состояние другой системы, которая должна превратиться в копию объекта; $|env\rangle$ – исходное состояние устройства и, возможно, некоторых иных систем, именуемых термином *окружение* (environment) и участвующих в процессе клонирования. В правой части (13) стоит резуклонирования: возниклаточная копия исходного объекта и изменилось в общем случае состояние окружения.

[4]Понятие *неизвестного* квантового состояния является достаточно тонким, и мы ещё вернёмся к его обсуждению.

Для иного исходного состояния $|\phi\rangle$ имеем аналогичный процесс:

$$|\phi\rangle \otimes |blank\rangle \otimes |env\rangle \rightarrow |\phi\rangle \otimes |\phi\rangle \otimes |env_\phi\rangle. \qquad (14)$$

Применительно к работе Герберта состояния $|\psi\rangle$ и $|\phi\rangle$ могут быть поляризационными состояниями фотона $|V\rangle$ и $|H\rangle$. По предположению устройство должно также успешно копировать и суперпозиции $|\chi\rangle = a|\psi\rangle + b|\phi\rangle$ ($|a|^2 + |b|^2 = 1$) этих состояний (у Герберта наряду с $|V\rangle$ и $|H\rangle$ надо также клонировать и состояния $|R\rangle = (|V\rangle + \imath|H\rangle)/\sqrt{2}$ и $|L\rangle = (|V\rangle - \imath|H\rangle)/\sqrt{2}$), т.е. мы должны иметь

$$(a|\psi\rangle + b|\phi\rangle) \otimes |blank\rangle \otimes |env\rangle \rightarrow \qquad (15)$$

$$(a|\psi\rangle + b|\phi\rangle) \otimes (a|\psi\rangle + b|\phi\rangle) \otimes |env_\chi\rangle.$$

Но если имеют место процессы (13) и (14), и если если эти процессы (как и все в квантовой механике) описываются линейными преобразованиями, то вместо (15) мы получим

$$(a|\psi\rangle + b|\phi\rangle) \otimes |blank\rangle \otimes |env\rangle \rightarrow \qquad (16)$$

$$a|\psi\rangle \otimes |\psi\rangle \otimes |env_\psi\rangle + b|\phi\rangle \otimes |\phi\rangle \otimes |env_\phi\rangle.$$

Правые части (15) и (16) никогда не совпадут, даже если состояние окружения преобразуется инвариантно, т.е. если $|env_\psi\rangle = |env_\phi\rangle$. Полученное противоречие ставит преграду квантовому клонированию. Заметим, что проблема возникла при совместном рассмотрении клонирования трёх состояний: $|\psi\rangle$, $|\phi\rangle$ и $a|\psi\rangle + b|\phi\rangle$. При $a \neq 0 \neq b$ и $|\psi\rangle \neq |\phi\rangle$ по крайней мере два состояния из этой тройки неортогональны.

Иной подход к проблеме клонирования квантовых состояний предложил Йен, исходя из унитарности процессов в замкнутой квантовой системе. Присоединяя к рассмотрению

достаточно большое окружение клонера (в пределе – всю хотя, как отмечалось в Части 2, при обсуждении согласованных историй, это весьма деликатный момент), можно считать процесс его работы унитарным. Обратимся вновь к выражениям (13) и (14). Теперь стрелки символизируют некоторое унитарное преобразование. Следовательно, скалярное произведение левых частей (13) и (14) должно совпадать со скалярным произведением правых:

$$\langle\phi|\psi\rangle = \langle\phi|\psi\rangle^2\langle env_\phi|env_\psi\rangle. \tag{17}$$

Все фигурирующие в этом выражении состояния можно считать нормированными. Рассмотрим наиболее интересный случай, когда состояния $|\psi\rangle$ и $|\phi\rangle$ не совпадают (т.е. $|\langle\phi|\psi\rangle| \neq 1$) и не ортогональны (т.е. $\langle\phi|\psi\rangle \neq 0$). В этой ситуации из (17) следует

$$1 = \langle\phi|\psi\rangle\langle env_\phi|env_\psi\rangle. \tag{18}$$

Поскольку $0 < |\langle\phi|\psi\rangle| < 1$ и $|\langle env_\phi|env_\psi\rangle| \leq 1$, равенство (18) не может быть выполнено. Мы снова пришли к противоречию, предполагая возможность клонирования неортогональных состояний.

Заметим, что проблемы клонирования неизвестного состояния из фиксированного ортонормированного набора состояний $\{|\psi_1\rangle, ..., |\psi_n\rangle\}$ не существует. Действительно, этот набор можно расширить до ортонормированного базиса пространства состояний системы (напомню, что речь идёт только о системах с конечномерным пространством). Этот базис можно считать набором собственных векторов оператора некоторой наблюдаемой величины с невырожденным набором собственных значений. Измеряя эту наблюдаемую в состоянии, предложенным для копирования, мы однозначно идентифицируем его. После этого нет принципиальной про-

блемы в приготовлении любого числа систем той же природы в данном уже известном нам состоянии. Поэтому ещё раз отметим, что запрет на клонирование касается неизвестного элемента из набора (возможно, известного) неортогональных состояний.

Полезно оценить проблему клонирования в контексте эпистемологической (реляционной) трактовки понятия квантового состояния. Выше использовался термин "неизвестное состояние". При этом оно предполагалось чистым, т.е. представимым вектором в гильбертовом пространстве системы и дающее максимально полное её описание. Как совмещаются эти обстоятельства? Представим себе Алису, которая приготавливает систему в (чистом) состоянии из некоторого фиксированного набора (в простейшем случае из двух) неортогональных векторов. Это состояние есть представитель знания Алисы о системе. Боб может знать о составе набора, но для него является тайной выбор Алисы. При этом Боб должен приготовить ещё одну систему, знание Алисы о которой окажется точно таким же, как и её знание о первой системе, с которой она работала сама. Получая в распоряжение эту систему, Боб каким-то способом должен сделать заключение о действительном содержании знания Алисы о системе, отличив его от всех остальных возможных альтернативных содержаний, для последующего воспроизводства его в копии. Таким образом, Боб должен приготовить не элемент физической реальности, объективно существующий и потенциально равно доступный к восприятию любым наблюдателем, а некоторый своего рода "элемент субъективной реальности", который способна оценить только Алиса. С этой точки зрения обнаруженные ограничения на возможность Бобу осуществить такую операцию копирования уже не кажется столь удивительным.

3 Секретный обмен ключом (квантовая криптография)

Запрет на клонирования квантовых состояний делает невозможным "сверхсветовой телеграф", но в утешение даёт в руки криптографам уникальный способ гарантировать секретность связи. Часто этот способ называют "квантовой криптографией", что не совсем правильно, т.к. процедура шифровки сообщений остаётся прежней, а квантовые технологии позволяют обнаружить нарушение тайны переписки.

В 1917 году, отвечая на потребности разведывательных служб воюющей Европы, Верном изобрёл так называемый "одноразовый блокнот" – способ шифровки сообщений. К исходному нешифрованному тексту, записанному по каким-нибудь стандартным правилам в виде последовательности нулей и единиц (битов), применяется ключ – случайная последовательность битов той же длины. Если на n-ом месте ключа стоит 0, соответствующий символ сообщения не изменяется, а если стоит 1, символ в сообщении инвертируется, т.е. 0 заменяется на 1, а 1 на 0. Это есть ни что иное как побитовое сложение по $mod\,2$. Зашифрованное сообщение отправляется по открытому (несекретному) каналу связи, например, по радио. Дешифровка происходит таким же образом, т.к. очевидно, что двойное побитовое сложение оставляет сообщение неизменным. Для успеха всей процедуры отправитель (Алиса) и получатель (Боб) должны обладать ключом.

Естествен вопрос: где после шифровки находится информация, содержащаяся в исходном сообщении? В теории кодирования доказывается, что в шифрованном сообщении этой информации нет – оно также как и ключ представляет собой случайную последовательность битов. Нет этой инфор-

мации, естественно, и в ключе, т.к. он вообще мог появится до составления сообщения. Информация содержится исключительно в корреляциях между шифрованным сообщением и ключом. По этой причине перехват шифрованного сообщения совершенно бесполезен для третьей стороны, Евы[5], если она не обладает ключом. "Одноразовый блокнот" оказывается абсолютно надёжным при условии *секретности ключа*[6]. В классическом случае Алисе и Бобу остаётся надеяться, что секретный канал, по которому передавался ключ, остался действительно секретным. Использование в этом канале квантовых технологий позволяет им хоть и не предотвратить подслушивание, но всегда его обнаружить. Поэтому Алиса и Боб могут обрести полное спокойствие за секретность ключа, если факт подслушивания обнаружен не был. Рассмотрим несколько так называемых протоколов (последовательностей операций) секретного обмена ключом.

Протокол BB84. В идее Беннета и Брассара, опубликованной в 1984 году, как и в других протоколах квантовой криптографии, ключ возникает естественным путём в некотором смысле одновременно у Алисы и Боба. Пусть активная роль принадлежит Алисе. Пользуясь генератором случайных чисел, она создаёт две последовательности нулей и единиц одинаковой длины. Символы первой последовательности будут передаваться Бобу путём шифровки их двумя способами. Эти способы будем нумеровать числами 0 и 1. В способе "0"символ 0 шифруется фотоном вертикальной поляризации,

[5]Её называют так от созвучия английского произношения имени Eve и начала слова eavesdropper (подслушивающий).

[6]Если один и тот же ключ используется для кодировки двух и более сообщений, у Евы появляется шанс дешифровки.

а символ 1 – фотоном горизонтальной поляризации:

$$\begin{aligned} 0 &\mapsto |V\rangle, \\ 1 &\mapsto |H\rangle. \end{aligned} \tag{19}$$

В способе "1" символы 0 и 1 шифруются, соответственно, диагональной (D) и антидиагональной ($\overline{D}$) поляризациями:

$$\begin{aligned} 0 &\mapsto |D\rangle = \frac{1}{\sqrt{2}}(|V\rangle + |H\rangle), \\ 1 &\mapsto |\overline{D}\rangle = \frac{1}{\sqrt{2}}(|V\rangle - |H\rangle)\rangle. \end{aligned} \tag{20}$$

В принципе, мы могли бы с тем же успехом использовать в способе "1"правую и левую циркулярные поляризации.

Зашифрованную таким образом первую последовательность битов Алиса отправляет Бобу в виде последовательности фотонов. Боб знаком с протоколом, но не знает, естественно, ни первой, ни второй последовательности Алисы. Он генерирует случайным образом свою последовательность битов. Она будет служить ему указанием базиса, в котором следует измерять поляризации каждого пришедшего фотона (0 соответствует базису $\{|V\rangle, |H\rangle\}$, а 1 – базису $\{|D\rangle, |\overline{D}\rangle\}$). Рассмотрим следующую таблицу как пример реализации протокола:

0	0	1	0	1	1	0	1	0	1	0	0
0	1	0	0	1	1	0	1	1	0	1	0
$\oplus$	$\otimes$	$\oplus$	$\oplus$	$\otimes$	$\otimes$	$\oplus$	$\otimes$	$\otimes$	$\oplus$	$\otimes$	$\oplus$
1	1	0	1	0	0	1	0	1	0	0	1
$\otimes$	$\otimes$	$\oplus$	$\otimes$	$\oplus$	$\oplus$	$\otimes$	$\oplus$	$\otimes$	$\oplus$	$\oplus$	$\otimes$
1	0	1	0	0	1	1	0	0	1	0	1
	0	1						0	1		

Первая и вторая строки представляют, соответственно, первую и вторую последовательности Алисы. Четвёртая строка является последовательностью Боба типов измерения, а шестая содержит результаты этих измерений. В третьей строке продублированы вторая последовательность Алисы, а в пятой – последовательность Боба с помощью символов $\oplus$ и $\otimes$, отвечающих использованию вертикально-горизонтального или диагонально-антидиагонального базисов. Иногда случайно для шифровки и дешифровки одного и того же n-ого бита Алиса и Боб используют одинаковые базисы. Такие случаи отмечены в седьмой строке и выявляются при общении по открытому каналу. При этом Алиса диктует Бобу содержание второй последовательности, а он, сравнивая его со своей последовательностью, отмечает и указывает Алисе совпавшие биты. Естественно, что при этом в открытый канал не поступает информация ни о содержании сообщения (первая последовательность Алисы), ни о результатах измерения Боба. Те случаи, когда базисы не совпали, отбрасываются, т.к. Боб дешифровал соответствующие биты не тем способом, каким зашифровала их Алиса и поэтому результат дешифровки никак не коррелирует с исходным символом. Зато при совпадении базисов бит оказывается дешифрован Бобом абсолютно точно. Получившаяся последовательность, в среднем в два раза более короткая, единая для Алисы и Боба при условии, что не было вмешательства Евы. С целью убедиться в этом Алиса и Боб жертвуют некоторой частью этой новой последовательности и сравнивают эту часть, общаясь по открытому каналу. Если обнаруживается полная корреляция, они могут спокойно использовать оставшуюся часть в качестве ключа. Нарушение корреляции будет свидетельствовать о вмешательстве Евы. Действительно, Ева может делать только то же самое, что делал Бобт.е. вы-

бирать случайным образом один из двух базисов, проводить измерение и фиксировать результат. При этом она должна отправить фотон далее Бобу. Это фотон отправляется уже не в том состоянии, в котором его приготовила Алиса, а в том, в котором его обнаружила Ева. В среднем в половине тех случаев, когда Алиса и Боб использовали одинаковые базисы, Ева использовала другой. В этих ситуациях результат измерения Боба уже никак не будет коррелировать с содержанием сообщения Алисы. Обнаружение достаточно большой доли дискорреляций (близкой, как легко понять, к 25%) при проверке сигнализирует Алисе и Бобу о возможном факте подслушивания. Значит сгенерировать секретный ключ им не удалось и следует отложить попытку до лучших времён.

Очевидна роль теоремы о запрете клонирования. Если бы у Евы было устройство, способное, как в идее Герберта, клонировать любое состояние из набора $\{|V\rangle, |H\rangle, |D\rangle, |\overline{D}\rangle\}$ она могла бы полностью скрыть своё участие в информационном обмене, всегда приготавливая для Боба именно то состояние, в котором фотон был отправлен Алисой, предварительно узнав это состояние.

Протокол B92. Беннет (рис. 3) в 1992 году предложил протокол секретной генерации ключа с использованием Алисой для шифровки всего двух состояний. А именно, пусть Алиса шифрует свою (теперь уже единственную) последовательность битов следующим образом:

$$\begin{aligned} 0 &\mapsto |V\rangle, \\ 1 &\mapsto |\overline{D}\rangle. \end{aligned} \tag{21}$$

Заметим, что при отправки 0 Алиса пользуется элементом из базиса $\oplus$, а при отправке 1 – из базиса $\otimes$. Боб также как и в протоколе BB84 выбирает случайным образом базис

Рис. 3. Чарльз Беннет.

$\oplus$ или базис $\otimes$, руководствуясь 0 или 1 в своей случайной последовательности. Результаты измерения Боб записывает несколько иначе: в случае базиса $\oplus$ и регистрации фотона в состоянии $|V\rangle$ ($|H\rangle$) он записывает 0 (1), а в случае измерения в базисе $\otimes$ и регистрации фотона в состоянии $|D\rangle$ ($|\overline{D}\rangle$) он записывает 1 (0). Заметим теперь, что в тех случаях, когда в результатах Боба появляется единица можно утверждать, что базисы шифровки и дешифровки *не совпадали*. Боб сообщает номера этих битов Алисе, удаляет все остальные биты из своей исходной последовательности и инвертирует оставшуюся последовательность. Теперь она совпадает с соответствующей подпоследовательностью Алисы. Также как и в протоколе BB84 Алиса и Боб раскрывают и сравнивают часть последовательности для проверки секретности. Ева не сможет скрыть своё вмешательство, если у неё нет устройства, распознающего неортогональные состояния $|V\rangle$

и $|\overline{D}\rangle$. А такое устройство запрещено.

Протокол E91. Данный протокол генерации секретного ключа (автор Артур Экерт, рис. 4) основан на свойствах зацепленных состояний и использует процедуру проверки неравенства Белла (см. Часть 1). Отличие от традиционной схемы проверки состоит в расширении числа направлений, вдоль которых измеряются проекции спинов частиц (мы для простоты будем говорить о зацепленной паре частиц с половинным спином). Алиса и Боб, получая фрагменты синглетной

Рис. 4. Артур Экерт.

пары, случайным образом выбирают одно из трёх направлений $\boldsymbol{\alpha}_1$, $\boldsymbol{\alpha}_2$, $\boldsymbol{\alpha}_3$ (у Алисы) и $\boldsymbol{\beta}_1$, $\boldsymbol{\beta}_2$, $\boldsymbol{\beta}_3$ (у Боба), лежащим в одной плоскости. Их взаимное расположение показано на рис. 5. Углы между векторами кратны $\pi/4$. При этом

$$\boldsymbol{\beta}_1 = \boldsymbol{\alpha}_2 \ \text{ и } \ \boldsymbol{\beta}_2 = \boldsymbol{\alpha}_3. \tag{22}$$

Следовательно, результаты измерения проекций спинов

вдоль этих направлениях строго антикоррелируют (различаются знаками).

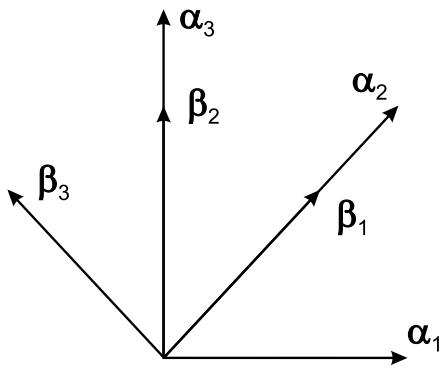

Рис. 5. Схема направлений измерений проекций спинов в протоколе E91.

После проведения достаточно большой серии измерений над фрагментами последовательности синглетных пар Алиса и Боб, используя открытый канал, выясняют направления своих измерений для каждого члена последовательности и делят их на две группы. В первой группе ориентации различны, а во второй совпадают, т.е. относятся к случаям (22). После этого объявляются результаты измерения из первой группы и на их основе подсчитывается величина Белла (все обозначения взяты из третьего параграфа Части 1)

$$\langle \hat{S}_{Bell} \rangle = \frac{1}{2}\Big(\langle \hat{\mathcal{A}}(\boldsymbol{\alpha}_3)\hat{\mathcal{B}}(\boldsymbol{\beta}_1)\rangle + \tag{23}$$

$$\langle \hat{\mathcal{A}}(\boldsymbol{\alpha}_3)\hat{\mathcal{B}}(\boldsymbol{\beta}_3)\rangle + \langle \hat{\mathcal{A}}(\boldsymbol{\alpha}_1)\hat{\mathcal{B}}(\boldsymbol{\beta}_1)\rangle - \langle \hat{\mathcal{A}}(\boldsymbol{\alpha}_1)\hat{\mathcal{B}}(\boldsymbol{\beta}_3)\rangle \Big).$$

Здесь $\hat{\mathcal{A}}(\boldsymbol{\alpha}_i)$ ($\hat{\mathcal{B}}(\boldsymbol{\beta}_i)$) – оператор удвоенной проекции спина частицы Алисы (Боба) вдоль указанного направления. Если

частицы не подвергались воздействию со стороны Евы и отсутствуют какие-либо технические помехи, усреднение $\langle ... \rangle$ в последнем выражении осуществляется по синглетному состоянию и даёт

$$\langle \hat{S}_{Bell} \rangle = -\sqrt{2}. \tag{24}$$

В этом случае строго антикоррелирующие результаты измерений из второй группы используются Алисой и Бобом в качестве ключа.

Посмотрим, что произойдёт при вмешательстве Евы. Она может перехватывать частицы и проводить над ними любые измерения, прежде чем направить их к Алисе и Бобу. Пусть $\mathbf{n}_A$ и $\mathbf{n}_B$ – направления, вдоль которых Ева проводит измерения проекций спинов частиц, предназначенных, соответственно, Алисе и Бобу. При этом, изменив, если необходимо, $\mathbf{n}_A$ и (или) $\mathbf{n}_B$ на противоположные, считаем, что это направления, вдоль которых проекции спинов положительны. Любой тактике Евы соответствует некоторое распределение вероятностей $p(\mathbf{n}_A, \mathbf{n}_B)$. Теперь Алиса и Боб при вычислении любого из четырёх слагаемых правой части (23) получат

$$\langle \hat{\mathcal{A}}(\boldsymbol{\alpha}_i)\hat{\mathcal{B}}(\boldsymbol{\beta}_j) \rangle' = \tag{25}$$

$$\int (\boldsymbol{\alpha}_i \cdot \mathbf{n}_A)(\boldsymbol{\beta}_j \cdot \mathbf{n}_B) p(\mathbf{n}_A, \mathbf{n}_B)\, d^2\mathbf{n}_A\, d^2\mathbf{n}_B.$$

Естественно, что для Евы есть смысл выбирать направления $\mathbf{n}_A$ и $\mathbf{n}_B$ в тоже плоскости, в которой лежат $\boldsymbol{\alpha}_i$ и $\boldsymbol{\beta}_j$. Нетрудно проверить, что величина $\langle \hat{S}_{Bell} \rangle'$, построенная из слагаемых вида (25), окажется равной

$$\langle \hat{S}_{Bell} \rangle' = \frac{\sqrt{2}}{2} \int (\mathbf{n}_B \cdot \mathbf{n}_B) p(\mathbf{n}_A, \mathbf{n}_B)\, d^2\mathbf{n}_A\, d^2\mathbf{n}_B, \tag{26}$$

что немедленно даёт

$$-\frac{\sqrt{2}}{2} \leq \langle \hat{S}_{Bell} \rangle' \leq \frac{\sqrt{2}}{2}. \tag{27}$$

Таким образом, вмешательство Евы должно не только в два раза уменьшить модуль величины $\langle \hat{S}_{Bell} \rangle$, но может также поменять её знак. Обнаружение величины Белла в интервале (27) является сигналом Алисе и Бобу о возможном подслушивании.

4 Различение квантовых состояний

Из сказанного выше следует тесная связь между проблемой клонирования неизвестного квантового состояния, выбранного из неортогонального набора, и идентификацией такого состояния. До сих пор необходимость идентификации возникала в контексте своего рода игры против партнёра, старающегося скрыть свой выбор. Аналогичная проблема появляется также при передаче классической информации по квантовому каналу связи. Неидеальность канала, шум, которому подвержено передаваемое сообщение, создаёт естественную проблему восстановления сообщения, как проблему идентификации неортогональных и в общем случае смешанных квантовых состояний. Рассмотрим этот вопрос подробнее.

Работа неидеального квантового канала связи описывается в терминах квантовой операции. Информация, предназначеннадля отправки, записывается в виде состояния $\hat{\varrho}_{in}$ на входе в канал (см. рис.). Выходное состояние $\hat{\varrho}_{out}$ связано с входным соотношением

$$\hat{\varrho}_{out} = \sum_{\lambda} \hat{\mathcal{E}}^{(\lambda)} \, \hat{\varrho}_{in} \, \hat{\mathcal{E}}^{(\lambda)\dagger}, \tag{28}$$

где выражение в правой части есть действие некоторой квантовой операции на входное состояние. Это понятие достаточно подробно обсуждается во втором параграфе Части 2. Набор операторов $\{\hat{\mathcal{E}}^{(\lambda)}\}$ определяет свойства канала. Эти операторы подчиняются соотношению

$$\sum_{\lambda} \hat{\mathcal{E}}^{(\lambda)\dagger}\hat{\mathcal{E}}^{(\lambda)} = \hat{1}_{\mathcal{H}_{in}}, \tag{29}$$

отвечающему единичной вероятности срабатывания канала; $\mathcal{H}_{in}$ – гильбертово пространство входных состояний.

Предположим, что для записи сообщения служит некоторый набор $\{|i\rangle\}_{i=0}^{N-1}$ из N ортонормированных состояний. Они кодируют буквы алфавита и другие символы используемого языка. На выходе канала буква "i"оказывается представленной состоянием

$$\hat{\varrho}_i = \sum_{\lambda} \hat{\mathcal{E}}^{(\lambda)} |i\rangle\langle i| \hat{\mathcal{E}}^{(\lambda)\dagger}. \tag{30}$$

Появляется проблема идентификации состояния (30) из набора $\{\hat{\varrho}_i\}_{i=0}^{N-1}$ всех возможных таких состояний. В общем случае они не являются набором чистых ортогональных состояний. Декодировка на рис. состоит в как можно более точной идентификации состояний, что требует некоторой процедуры измерения. Предположим, что это измерение может оказаться обобщённым. В данное понятие вкладывается следующее. Обобщённое измерение представляет собой некоторую квантовую операцию, применительно к $\hat{\varrho}_{out}$:

$$\hat{\varrho}_{out} \mapsto \sum_{i=0}^{N-1} \hat{\mathcal{E}}_i \, \hat{\varrho}_{out} \, \hat{\mathcal{E}}_i^{\dagger}, \tag{31}$$

результат которой в виде классической информации – символа "i" – представляет интерес. Регистрация данного результата позволяет трактовать (идентифицировать) $\hat{\varrho}_{out}$ как $\hat{\varrho}_i$. Вероятность $Prob_i$ получения результата i есть

$$Prob_i = Tr_{\mathcal{H}_{out}}\left(\hat{\pi}_i\hat{\varrho}_{out}\right), \tag{32}$$

где

$$\hat{\pi}_i \doteq \hat{\mathcal{E}}_i^{\dagger}\hat{\mathcal{E}}_i. \tag{33}$$

Набор положительных эрмитовых операторов $\{\hat{\pi}_i\}_{i=0}^{N-1}$ представляет собой разложение единичного оператора в пространстве $\mathcal{H}_{out}$ состояний на выходе квантового канала:

$$\sum_{i=0}^{N-1}\hat{\pi}_i = \hat{1}_{\mathcal{H}_{out}}. \tag{34}$$

Физический смысл этого равенства состоит в единичной вероятности срабатывания декодера, т.е. получения исхода обобщённого измерения. Обобщённым оно называется потому, что разложение единицы, даваемое системой ортогональных проекторов при обычном измерении, называемом также измерением фон Неймана (см. выражение (5) в Части 2), есть частный вариант соотношения (34). Операторы (33) не обладают в общем случае условием ортогональности: $\hat{\pi}_i\hat{\pi}_j \neq \delta_{i,j}\hat{\pi}_i$.

Оптимальная декодировка должна минимизировать вероятность ошибки идентификации. Пусть известны априорные вероятности $\{p_i\}_{i=0}^{N-1}$ ($\sum_i p_i = 1$) появления букв в тексте сообщения, т.е. вероятности появления состояния $\hat{\varrho}_i$ на выходе информационного канала. Вероятность ошибки идентификации зависит от используемого обобщённого измерения $\{\hat{\pi}_i\}_{i=0}^{N-1}$ и включает в себя усреднение по вероятностям

$\{p_i\}_{i=0}^{N-1}$:

$$P_{err}[\{\hat{\pi}_i\}] = \sum_{\substack{i,j \\ i\neq j}} p_i Tr_{\mathcal{H}_{out}} \left(\hat{\pi}_j \hat{\varrho}_i \right). \tag{35}$$

Здесь

$$\sum_{\substack{j \\ i\neq j}} Tr_{\mathcal{H}_{out}} \left(\hat{\pi}_j \hat{\varrho}_i \right) = 1 - Tr_{\mathcal{H}_{out}} \left(\hat{\pi}_i \hat{\varrho}_i \right)$$

есть вероятность неправильной идентификации состояния $\hat{\varrho}_i$. Минимум вероятность ошибки (35) по всем возможным обобщённым измерениям

$$P_{err} \doteq min_{\{\hat{\pi}_i\}_{i=0}^{N-1}} P_{err}[\{\hat{\pi}_i\}] \tag{36}$$

реализуется некоторым "идеальным" обобщённым измерением[7].

Рассмотрим подробно случай $N = 2$, когда текста осуществляется с помощью состояний $|0\rangle$ и $|1\rangle$. Их можно считать состояниями кубита, т.е. реализовать при $dim\mathcal{H}_{in} = 2$. Здесь возможно точное аналитическое нахождение оптимального измерения. Обобщённое измерение представлено в этой ситуации парой положительных эрмитовых операторов $\hat{\pi}_0$ и $\hat{\pi}_1$ с условием (34):

$$\hat{\pi}_0 + \hat{\pi}_1 = \hat{1}_{\mathcal{H}_{out}}. \tag{37}$$

[7]Такое измерение действительно существует. Поскольку мы считаем размерности всех гильбертовых пространств конечными, пространство всех обобщённых измерений можно представить в виде *компактного* топологического пространства. Вероятность $P_{err}[\{\hat{\pi}_i\}]$ является непрерывной функцией на этом пространстве и, согласно известной теоремы функционального анализа, достигает в нём своих верхней и нижней граней.

Это обобщённое измерение должно идентифицировать состояние из пары $\hat{\varrho}_0$ и $\hat{\varrho}_1$ с априорными вероятностями p_0 и p_1. Вероятность ошибки с учётом (37) может быть записана в виде

$$P_{err}[\{\hat{\pi}_i\}] = p_0 + Tr_{\mathcal{H}_{out}}\left[\hat{\pi}_0(p_1\hat{\varrho}_1 - p_0\hat{\varrho}_0)\right]. \tag{38}$$

Требуется найти положительный эрмитов оператор $\hat{\pi}$

$$0 \leq \hat{\pi} \leq \hat{1}_{\mathcal{H}_{out}}, \tag{39}$$

минимизирующий число $Tr_{\mathcal{H}_{out}}(\hat{\pi}\,\hat{\Gamma})$, где $\hat{\Gamma} = p_1\hat{\varrho}_1 - p_0\hat{\varrho}_0$. При этом минимальная вероятность ошибки (36)

$$P_{err} = p_0 + min_{0\leq\hat{\pi}\leq\hat{1}} Tr_{\mathcal{H}_{out}}(\hat{\pi}\,\hat{\Gamma}). \tag{40}$$

Эрмитов оператор $\hat{\Gamma}$ имеет диагональное представление

$$\hat{\Gamma} = \sum_k \gamma_k |\psi_k\rangle\langle\psi_k|. \tag{41}$$

Здесь $|\psi_k\rangle$ – ортонормированный базис собственных векторов, а γ_k – соответствующие собственные значения. Имеем

$$Tr_{\mathcal{H}_{out}}(\hat{\pi}\,\hat{\Gamma}) = \sum_k \gamma_k \langle\psi_k|\hat{\pi}|\psi_k\rangle. \tag{42}$$

Поскольку из (39) следует

$$0 \leq \langle\psi_k|\hat{\pi}|\psi_k\rangle \leq 1, \tag{43}$$

мы имеем

$$Tr_{\mathcal{H}_{out}}(\hat{\pi}\,\hat{\Gamma}) \geq \sum_{\substack{k \\ \gamma_k<0}} \gamma_k. \tag{44}$$

Целесообразно искать оператор $\hat{\pi}$, подчинив его условиям

$$\langle\psi_k|\hat{\pi}|\psi_k\rangle = \begin{cases} 0, & \text{если } \gamma_k < 0, \\ 1, & \text{если } \gamma_k \geq 0. \end{cases} \tag{45}$$

Исходя из этих соотношений, можно показать, что оператор $\hat{\pi}$ диагонален в базисе $\{|\psi_k\rangle\}$. Действительно, пусть

$$\hat{\pi} = \sum_n \mu_n |\varphi_n\rangle\langle\varphi_n| - \tag{46}$$

диагональное представление с использованием собственных состояний оператора $\hat{\pi}$. Для собственных значений из (39) имеем

$$0 \leq \mu_n \leq 1. \tag{47}$$

Если $\gamma_k \geq 0$, то по предположению (45)

$$0 = \langle\psi_k|\hat{\pi}|\psi_k\rangle = \sum_n \mu_n |\langle\varphi_n|\psi_k\rangle|^2. \tag{48}$$

Из этого равенства следует, что при $\mu_n \neq 0$ $\langle\varphi_n|\psi_k\rangle = 0$. Имеем, следовательно, при $k \neq k'$

$$\langle\psi_{k'}|\hat{\pi}|\psi_k\rangle = \sum_n \mu_n \langle\psi_{k'}|\varphi_n\rangle\langle\varphi_n|\psi_k\rangle = 0, \tag{49}$$

если $\gamma_k \geq 0$ или $\gamma_{k'} \geq 0$. Заметим теперь, что если бы вместо оператора $\hat{\pi}$, который есть ни что иное, как $\hat{\pi}_0$, искали бы оператор $\hat{\pi}_1 = \hat{1}_{\mathcal{H}_{out}} - \hat{\pi}$, мы пришли бы вместо условия (49) к условию

$$\langle\psi_{k'}|\hat{1}_{\mathcal{H}_{out}} - \hat{\pi}|\psi_k\rangle = -\langle\psi_{k'}|\hat{\pi}|\psi_k\rangle = 0 \tag{50}$$

при $\gamma_k < 0$ или $\gamma_{k'} < 0$. Вместе с (49) это даёт

$$\langle\psi_{k'}|\hat{\pi}|\psi_k\rangle \propto \delta_{k,k'}. \tag{51}$$

Искомое обобщённое измерение, наилучшим образом дискриминирующее состояния $\hat{\varrho}_0$ и $\hat{\varrho}_1$, оказалось обычным измерением фон Неймана с двумя исходами (0 и 1) и двумя проекторами

$$\begin{aligned} \hat{\pi} \equiv \hat{P}_0 &= \sum_{\substack{k \\ \gamma_k<0}} |\psi_k\rangle\langle\psi_k|, \\ \hat{1}_{\mathcal{H}_{out}} - \hat{\pi} \equiv \hat{P}_1 &= \sum_{\substack{k \\ \gamma_k\geq 0}} |\psi_k\rangle\langle\psi_k|. \end{aligned} \tag{52}$$

При этом измерении обеспечивается минимальная вероятности ошибки (40) в идентификации состояния:

$$P_{err} = p_0 + \sum_{\substack{k \\ \gamma_k<0}} \gamma_k. \tag{53}$$

Применим полученные результаты к проблеме различения двух чистых неортогональных состояний $|\phi_0\rangle$ и $|\phi_1\rangle$. В этом случае

$$\hat{\Gamma} = p_1 |\phi_1\rangle\langle\phi_1| - p_0 |\phi_0\rangle\langle\phi_0|. \tag{54}$$

Нахождение собственных значений и собственных состояний этого оператора не представляет никакой проблемы. Приведём только результат вычисления вероятности ошибки:

$$P_{err} = \frac{1}{2} - \frac{1}{2}\sqrt{1 - 4p_0p_1|\langle\phi_0|\phi_1\rangle|^2}. \tag{55}$$

Очевидно, что в случае $|\langle\phi_0|\phi_1\rangle| \to 0$, т.е. в пределе ортогональных состояний, P_{err} также стремится к нулю, а при практически тождественных состояниях ($|\langle\phi_0|\phi_1\rangle| \to 1$) и при $p_0 = p_1 = 0.5$ вероятность ошибки приближается к $1/2$.

5 Оптимальное универсальное копирование квантовых состояний

В предыдущем параграфе было показано, что различение неортогональных квантовых состояний возможно с неединичной вероятностью, т.е. с ошибками. Естественно ожидать, что приближённое копирование состояний также возможно. Далее мы рассмотрим простейший вариант операции клонирования состояний простейшей квантовой системы с двумерным пространством состояний – кубита (quantum bit или q-bit) $1 \to 2$, т.е. получения двух приближённых копий взамен оригинала. Но это клонирование окажется *универсальным* в том смысле, что осуществимо для всех возможных чистых состояний оригинала, и от этих состояний не зависит качество клонирования.

Поскольку клонирование предполагается универсальным, исходное состояние клонера должно быть изотропным, т.е. ни одно направление в пространстве состояний кубита, представляющего собой двумерную сферу, не должно быть преимущественным. Это можно обеспечить, если кубит, предназначенный на роль будущей копии, и некоторый третий кубит, так называемая *анцилла* (от латинского *ancilla* – служанка, рабыня), приготовлены в синглетном состоянии $|\Psi_0\rangle$. Таким образом, до начала процедуры клонирования имеем трёхкубитовое состояние

$$|\Phi^{(pre)}\rangle = |\psi\rangle_1 \otimes |\Psi_0\rangle_{2,3}, \tag{56}$$

где $|\psi\rangle_1$ – состояние оригинала, подлежащее клонированию. После процедуры клонирования состояние трёх кубитов можно представить в виде

$$|\Phi^{(post)}\rangle = \alpha|\psi\rangle_1 \otimes |\Psi_0\rangle_{2,3} + \beta|\psi\rangle_2 \otimes |\Psi_0\rangle_{1,3}. \tag{57}$$

Третье возможное слагаемое линейно зависит от двух из правой части (57):

$$|\psi\rangle_3 \otimes |\Psi_0\rangle_{1,2} = |\psi\rangle_2 \otimes |\Psi_0\rangle_{1,3} - |\psi\rangle_1 \otimes |\Psi_0\rangle_{2,3}. \qquad (58)$$

Преобразование состояния (56) в состояние (57) является линейным по $|\psi\rangle$ преобразованием. Для определения амплитуд вероятности α и β воспользуемся универсальностью записи синглетного состояния пары кубитов в любом ортонормированном базисе. Используем для этого базис $\{|\psi\rangle, |\psi^{\perp}\rangle\}$:

$$|\Psi_0\rangle = \frac{1}{\sqrt{2}}\Big(|\psi\rangle \otimes |\psi^{\perp}\rangle - |\psi^{\perp}\rangle \otimes |\psi\rangle\Big). \qquad (59)$$

Подставляя это выражение в (57), представим последнее в следующем виде:

$$|\Phi^{(post)}\rangle =$$

$$(\alpha+\beta)|\psi\rangle_1\otimes|\psi\rangle_2\otimes|\psi^{\perp}\rangle_3 - \Big(\alpha|\psi\rangle_1\otimes|\psi^{\perp}\rangle_2+\beta|\psi^{\perp}\rangle_1\otimes|\psi\rangle_2\Big)\otimes|\psi\rangle_3. \qquad (60)$$

Первое слагаемое в суперпозиции описывает появление двух *точных* копий исходного состояния первого кубита. Однако, обязательно присутствует также второе слагаемое, где одна из копий оказывается в ортогональном состоянии (самом неприемлемом в копировании). Третья частица называется антиклоном. В первом слагаемом состояние антиклона ортогонально оригиналу, а во втором именно он оказывается точной копией.

Коль скоро мы хотим иметь две равноценные (пусть и не идеальные) копии исходного состояния, мы должны сделать состояние $|\Phi^{(post)}\rangle$ симметричным относительно перестановки частиц 1 и 2. Следовательно, возникает условие

$$\alpha = \beta. \qquad (61)$$

Нормировка состояния $|\Phi^{(post)}\rangle$ даёт

$$|\Phi^{(post)}\rangle =$$

$$\sqrt{\frac{2}{3}}|\psi\rangle_1 \otimes |\psi\rangle_2 \otimes |\psi^{\perp}\rangle_3 - \frac{1}{\sqrt{6}}\Big(|\psi\rangle_1 \otimes |\psi^{\perp}\rangle_2 + |\psi^{\perp}\rangle_1 \otimes |\psi\rangle_2\Big) \otimes |\psi\rangle_3. \tag{62}$$

Состояние пары 1 и 2

$$\hat{\varrho}_{1,2} = Tr_3\, |\Phi^{(post)}\rangle\langle\Phi^{(post)}| \tag{63}$$

оказывается зацепленным, как следует из критерия Переса-Городецки (см. Часть 2). Одночастичные состояния $\hat{\varrho}_1$ и $\hat{\varrho}_2$ являются приближёнными копиями исходного состояния $|\psi\rangle\langle\psi|$ и оказываются, как и следовало, равными:

$$\hat{\varrho}_1 = \hat{\varrho}_2 = \frac{5}{6}|\psi\rangle\langle\psi| + \frac{1}{6}|\psi^{\perp}\rangle\langle\psi^{\perp}|. \tag{64}$$

С вероятностью $5/6$ каждая частица может оказаться в состоянии оригинала и с вероятностью $1/6$ – в ортогональном состоянии. Выражение (65) можно переписать в виде

$$\hat{\varrho}_1 = \hat{\varrho}_2 = \frac{2}{3}|\psi\rangle\langle\psi| + \frac{1}{3}\cdot\frac{1}{2}\hat{1} \tag{65}$$

как смесь с весом $2/3$ точного состояния оригинала[8] и взятого с весом $1/3$ максимально смешанного состояния кубита.

[8]Данная вероятность известна как "фактор Чёрной коровы" по названию кафе Black Cow в Кротоне-на-Гудзоне, где происходили оживлённые обсуждения проблемы копирования квантовых состояний.

6 О причинных петлях

В предыдущих параграфах мы рассматривали ограничения, налагаемые самой природой квантовых состояний на возможности оперирования с заложенной в них информацией. Были выявлены запреты на точное копирование и различение неортогональных состояний, тесно связанные с запретом на "сверхсветовой телеграф". Последнее обстоятельство указывает на пока не понятые глубокие связи квантовой теории со структурой пространства-времени. Руководствуясь этим намёком, мы воспользуемся очень мощным и тонким инструментом для лучшего понимания как природы квантовых состояний, так и свойств мира событий. Имеются в виду замкнутые времениподобные линии, называемые также причинными петлями или самопересекающимися мировыми линиями. В просторечьи такие феномены известны как "машины времени" и "червоточины". Мы будем пользоваться английской аббревиатурой CTC – closed time-like curve.

В общей теории относительности (ОТО) решения уравнений Эйнштейна могут давать структуру пространства-времени с особенностями в виде CTC, как было показано Куртом Гёделем и Патриком Керром. Несмотря на это CTC часто объявляются нефизичными из-за известных парадоксов, о которых пойдёт речь далее. Более правильно, пожалуй, рассматривать наличие парадоксов как повод для более глубокого анализа между свойствами реальности и свойствами нашего мышления.

Рассмотрим модель CTC в том виде, в каком она будет фигурировать дальше. Предположим, что в некоторый момент времени t_1 по часам нашей (по предположению – инерциальной) системы отсчёта всё материальное содержание внутренности некоторой 3-мерной сферы заменяется на

новое. Это новое содержание оказывается содержанием той же области в момент времени $t_2 > t_1$, когда мы наблюдаем вторичное мгновенное изменение внутренности сферы – исчезает содержание, соответствующее t_2 (отправляется назад во времени) и появляется содержание из прошлого момента t_1.

Далее мы будем пользоваться схемами с только одним пространственным измерением. Сфера превращается на этих схемах в отрезок прямой линии. На рис. 6 показаны мировые линии двух частиц, первая из которых оказываясь в момент t_1 внутри сферы, перебрасывается в будущее (рис. 6 слева). Вторая оказывается внутри сферы в момент t_2 и перебрасывается в прошлое. В принципе частица может оказаться "за-

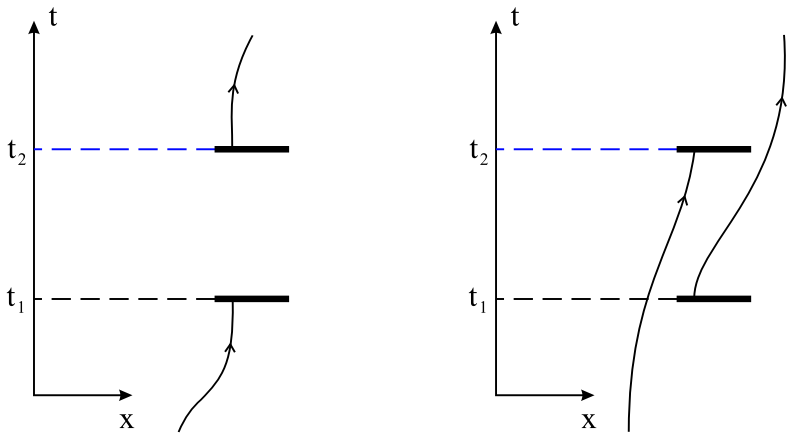

Рис. 6. Мировые линии частицы, перебрасываемой в будущее (слева) и возвращаемой в прошлое (справа).

пертой" внутри пространственно-временной области между t_1 и t_2, как на рис. 7 Это даёт основание использованию термина СТС. Фактически мы осуществили два разреза в на-

шем двумерном пространстве-времени и отождествили нижний край разреза при t_1 с верхним краем разреза при t_2 и наоборот. Заметим также, что описание феноменов на рис. 6 и 7 даётся с точки зрения наблюдателя, не попадающего в "червоточину". Рассматриваемая "машина времени" отличается от большинства своих литературных вариантов, т.к. она связывает всего два момента времени. В наших дальнейших рассуждения будет фигурировать правая схема рис. 6 с перемещением из будущего в прошлое.

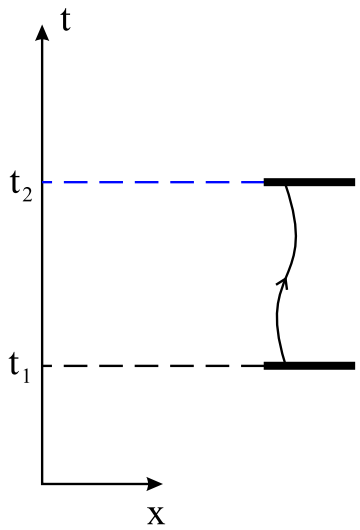

Рис. 7. Мировые линии частицы, запертой внутри "машины времени".

7 Парадоксы классической машины времени

Известные даже из научно-популярной литературы классические парадоксы путешествия в прошлое возникают при попытке описать взаимодействие системы (возможно, одушевлённой) со своей более ранней версией на интервале между моментами t_1 и t_2. Эта ситуация отражена на рис. 8. В области пространства-времени U происходит некоторое взаимодействие. Удобно представить себе частицы, двигающиеся по классическим траекториям и несущие внутренние дискретные степени свободы, описываемые параметрами со значениями 0 и 1. Дэвид Дойч (рис. 9), линии рассуждения которого

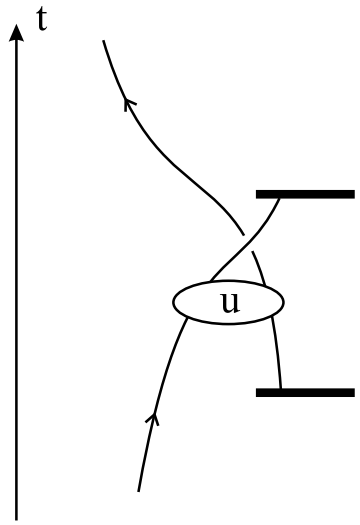

Рис. 8. Взаимодействие частицы с её версией, пришедшей из будущего.

мы будем пока следовать, широко использует такую модель.

Она позволяет привлекать для анализа методы теории вычислений и допускает квантовое обобщение. Взаимодействие между частицами сводится к изменению их внутренних состояний.

Рис. 9. Дэвид Дойч.

Несмотря на дискретность, мы пока будем считать внутреннее состояние (бит) частиц классическим, т.е. в каждой точке своей мировой линии частица обладает внутренним состоянием [0] или [1]. Такие обозначения помогут дистанцироваться от дальнейших квантовых обобщений, когда появятся кет-векторы $|0\rangle$ и $|1\rangle$. Однако, уже в классическом случае можно и полезно ввести сопоставление

$$[0] = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad [1] = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{66}$$

и операцию инвертирования (отрицания) бита

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \tag{67}$$

переводящую состояния (66) друг в друга.

Парадокс 1. Предположим, что инвертирование внутреннего бита частицы со схемы рис. 8 контролируется версией частицы уже совершившей перемещение из будущего, т.е. инвертирование произойдёт в том и только в том случае, если состояние поздней версии есть [1]. Такое взаимодействие называется контролируемым отрицанием (C-NOT) и является одной из основных двух(ку)битовых операций в классической (квантовой) теории вычислений. Соответствующая схема представлена рис. 10 с использованием общепринятого изображения контролируемого отрицания. Если внутренний бит частицы, пришедшей из безусловного прошлого (т.е. из времени $t < t_1$) обозначить $[x]_1$, а внутренний бит частицы, появившейся при t_1 из "червоточины" обозначить $[y]_2$, то взаимодействие со схемы рис. 10 выглядит следующим образом:

$$[x]_1\,[y]_2 \mapsto [x\dot{+}y]_1\,[y]_2, \tag{68}$$

где символ $\dot{+}$ обозначает сложение по $mod\,2$. После контролируемого инвертирования бита его носитель попадает при $t = t_2$ во вход "червоточины" и появляется в момент $t = t_1$ уже именем частицы 2. Следовательно, должно иметь место условие согласования состояний бита на входе и выходе "червоточины":

$$x\dot{+}y = y. \tag{69}$$

Это равенство возможно только при $x = 0$. Мы оказываемся невольны в приготовлении частицы при $t < t_1$ в состоянии [1].

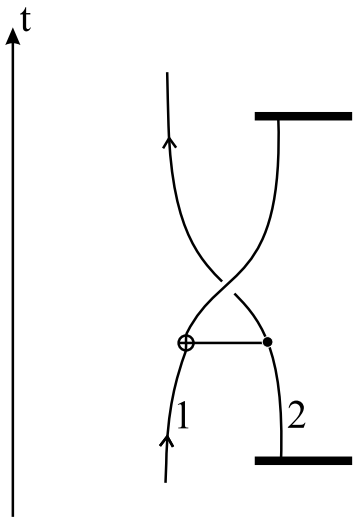

Рис. 10. Схема с контролируемым отрицанием, иллюстрирующая парадокс 1.

В этом и заключается парадокс. Частица в данном состоянии просто не сможет поучаствовать в описанном процессе.

Парадокс 2. Этот парадокс известен в литературе в несколько форме как "парадокс деда". А именно, человек возвращается в своё прошлое до времени рождения своего отца и убивает своего деда, тем самым делая невозможным собственное рождение и, естественно, путешествие в прошлое. Можно переформулировать этот парадокс, исключив смертоубийство: путешественник во времени встречает свою более молодую версию в интервале $t_1 < t < t_2$ и не допускает её ко входу в "червоточину" при $t = t_2$. В таком варианте "парадокс деда" допускает интерпретацию в терминах классических частиц – носителей внутреннего бита. Рассмотрим рис. 11 Частицы на траекториях 1 и 2 своими внутренними

битами моделируют эффективную *заселённость* траектории, т.е. при $x = 1$ заселена траектория 1, а при $x = 0$ – траектория 2. В пространственно-временной области, обведённой

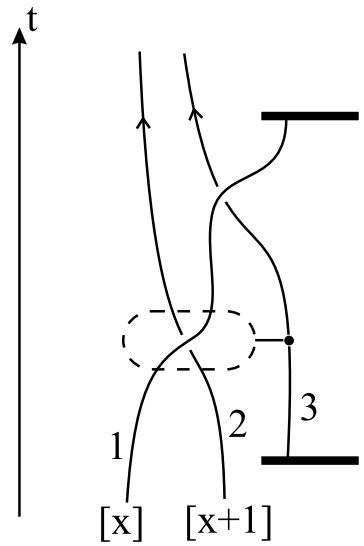

Рис. 11. Схема, иллюстрирующая парадокс 2. Состояние бита x моделирует заселённость траектории 1 или траектории 2.

пунктиром, происходит контролируемый частицей 3 обмен значениями битов (т.н. операция SWAPP). Обмен произойдёт, только если внутреннее состояние этой частицы, появившейся из "червоточины" при $t = t_1$ есть [1]. Траектория 1 проходит мимо входа в "червоточину" при $t = t_2$. Траектория 2 ведёт к этому входу. Поэтому если изначально была заселена траектория 2 и оказалась заселённой траектория 3, заселённость перемещается на траекторию 1. На языке внутренних состояний это описывается преобразованием

$$[x]_1\,[x\dot{+}1]_2\,[y]_3 \mapsto [x\dot{+}y]_1\,[x\dot{+}y\dot{+}1]_2\,[y]_3. \qquad (70)$$

Из данного выражения видно, что контролируемый обмен битами можно осуществить с помощью эквивалентной схемы рис. 12 с двумя контролируемыми отрицаниями. Условие согласования на входе и выходе из "червоточины" даёт

$$x\dot{+}y\dot{+}1 = y, \tag{71}$$

откуда следует

$$x = 1. \tag{72}$$

Таким образом, изначально заселённой может быть только траектория 1, которая минует вход в "червоточину". Парадокс, как и в предыдущем случае, заключается в ограничении на возможные начальные состояния: мы не можем приготовить при $t < t_1$ биты частиц 1 и 2 в состоянии $[0]_1\,[1]_2$.

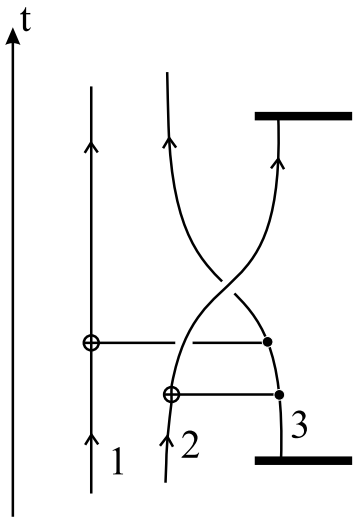

Рис. 12. Эквивалентная схема обмена заселённостей траекторий 1 и 2.

Заметим, что из условий согласования (69) и (71) получаются ограничения на значения x, но при этом остаётся свобода выбора значения y – состояния внутреннего бита частицы, вышедшей из "червоточины"[9]. Имеет место своеобразная ситуация одновременной переопределённости (ограничение на возможные начальные состояния – значения x), недоопределённости значения y.

Парадокс 3 не похож на первые два, но основан на отмеченной выше недоопределённости состояния бита, чей носитель вышел из "червоточины" при $t = t_1$. Д.Дойч предлагает использовать термин "дополнительные данные" для описания состояния таких битов и применять его для формализации так называемого "парадокса доказательства теоремы". Дойч предлагает следующую цепочку рассуждений. В схеме парадокса 1 на рис. 10, повторенной многократно биты частиц, вышедших из "червоточины", можно рассматривать как некоторый текст в двоичной кодировке. Этот текст используется для контролируемого инвертирования битов частиц типа 1 (все они изначально находятся в состоянии [0] – единственно возможном, согласно (69)). Фактически происходит "саморепликация" текста, копия которого отправляется в прошлое. Этот текст может содержать решение некоторой сложной проблемы, например, доказательство ранее неизвестной теоремы. Возникает вопрос об авторе этого доказательства[10]. Здесь нарушается глубокий философский

[9]В анимированной форме второго парадокса, при $y = 0$ никто не появляется из машины времени и человек, находящейся на траектории 1, продолжает свою жизнь без путешествия в прошлое. Если $y = 1$, то из "червоточины" при $t = t_1$ появляется путешественник во времени и *заставляет* более молодую свою версию поменять траекторию и отправиться ко входу в "червоточину" при $t = t_2$. В обоих случаях при $t > t_2$, также как и при $t < t_1$, мы наблюдаем только одного человека.

[10]В анимированной версии парадокса путешественник во времени,

принцип об *эволюционной природе знания*. Весь наш опыт говорит, что знания (например, математические) не содержатся в окружающей природе и не извлекаются из неё путём некоторого процесса добычи.

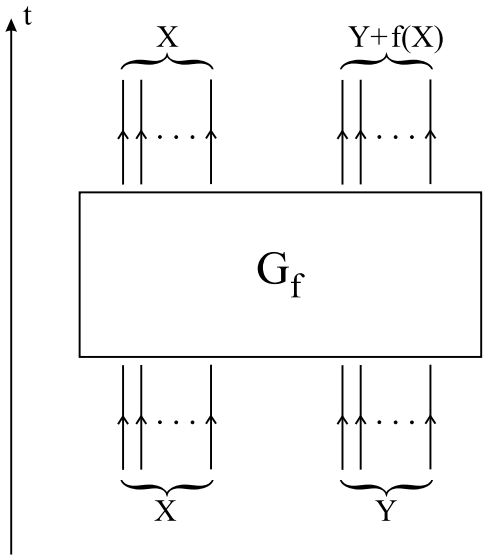

Рис. 13. Пространственно-временная схема вычисления функции f.

Приведённые рассуждения могут встретить возражения на основе некоторого сходства "самогенерации" доказательства теоремы в модели с СТС и в модели с обезьяной, случайным образом набирающей осмысленный текст, играя с компьютерной клавиатурой. Постараемся поэтому взглянуть на

прочитав перед отправлением в прошлое доказательство теоремы в книге, рассказывает затем об этом доказательстве математику, который и публикует его в той самой книге. Оба персонажа узнают содержание доказательства друг от друга.

проблему с несколько иной стороны. Рассмотрим устройство, вычисляющее функцию

$$f : \mathbb{Z}_{2^n} \to \mathbb{Z}_{2^n}. \tag{73}$$

Здесь $\mathbb{Z}_{2^n} = \{0, 1, \ldots, 2^n - 1\}$ – кольцо классов вычетов по $mod\, 2^n$. Для записи аргумента и значения функции f необходимы n-битовые регистры. Пусть область в (двумерном) пространстве-времени, где происходит вычисление функции выглядит как представленная на рис. 13. Здесь $Y \dot{+} f(X)$ – сложение по $mod\, 2^n$. В общем случае поиск неподвижной точки

$$X' = f(X') \tag{74}$$

есть непростая проблема, если не решать её простыми перебором всех возможных аргументов, что может оказаться практически невозможным, например, из-за очень большого времени. Однако, проблема нахождения неподвижной точки решается автоматически при использовании "червоточины". Действительно, организуем процесс вычисления функции f на интервале $t_1 < t < t_2$ (см. рис. 14). Мировые линии частиц, поставляющие к регистрам значения битов и различимые на рис. 13, обозначены на рис. 14 широкими полосами. Нетрудно заметить, что на выходе организованной таким образом вычислительной процедуры получается значение X, удовлетворяющее (74). Если функция f имеет несколько неподвижных точек, мы возвращаемся к проблеме недоопределённости – указания автора выбора той или иной неподвижной точки. Если, напротив, функция f не имеет неподвижных точек, мы приходим к парадоксу невозможности организовать вычислительную процедуру схемы рис. 14 с начальным условием $Y = 0$.

Предположим теперь, что устройство, вычисляющее функцию f, является системой искусственного интеллекта,

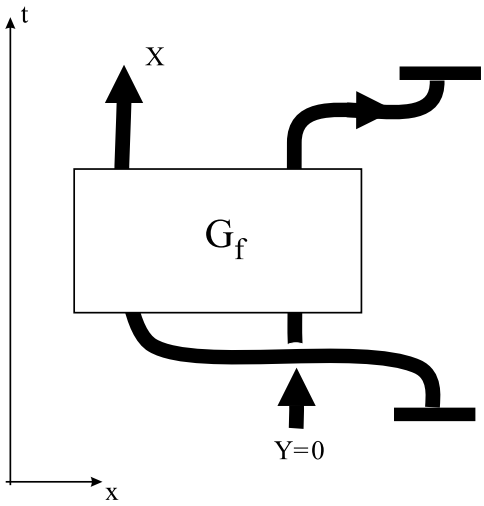

Рис. 14. Нахождение неподвижной точки функции f с помощью СТС.

воспринимающее входные данные X (последовательность нулей и единиц) как текст на некотором формальном языке. Система анализирует поступивший текст на предмет его статуса как доказательства определённой заранее сформулированной, но не доказанной теоремы, т.е. математической гипотезы. Сама система не обязана обладать каким-либо творческими способностями. От неё требуется только умение распознавать и проверять правильность чужой логики. Организуем работу системы так, что если она распознаёт текст как верное доказательство теоремы, она оставляет его неизменным, а если текст доказательством не является, система меняет некоторые его символы[11]. В соединении с "червоточиной" система приобретает способности *генерировать* доказа-

[11]То, что при этом может случайно появиться правильное доказательство, для нас сейчас не важно.

тельство. При этом отказ в срабатывании системы служит сигналом о несуществовании в данном формальном языке текста длины $\leq n$, являющегося доказательством теоремы.

Мы могли бы конечно без использования "червоточины" добавить к системе искусственного интеллекта устройство, генерирующее в лексикографическом порядке все возможные тексты и предлагающее их на проверку системе. При этом, естественно, обращаться к системе необходимо неоднократно. В комбинации с CTC система генерирует доказательство за одно обращение. Можно сказать, что "червоточина" позволяет повысить до единицы сколь угодно малую вероятность *случайной* генерации нужного текста.

В такой формулировке "парадокс доказательства теоремы" озадачивает несколько менее, если подходящих текстов длины $\leq n$ не более одного. Если это не так, снова появляется вопрос об "авторе" выбора конкретного текста.

8 Квантовый подход Д.Дойча к CTC

Предположим, что внутренние состояния частиц-носителей в построениях предыдущего параграфа имеют квантовую природу. Теперь они являются не битами, а кубитами. Состояния лежат, таким образом, в двумерном пространстве Гильберта, натянутом на пару ортонормированных векторов $|0\rangle$ и $|1\rangle$, заменивших классические состояния [0] и [1]. Кубит может находиться в любой суперпозиции $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$ своих базисных векторов. Это обстоятельство существенно расширяет картину эволюции с участием "червоточины".

Подражая Д.Дойчу, мы пока будем следовать онтологическому взгляду на природу квантового состояния. Рассмот-

рим рис. 15 – модифицированную схему рис. 8 с частицами-носителями квантовых состояний. Частица 1 приготавлива-

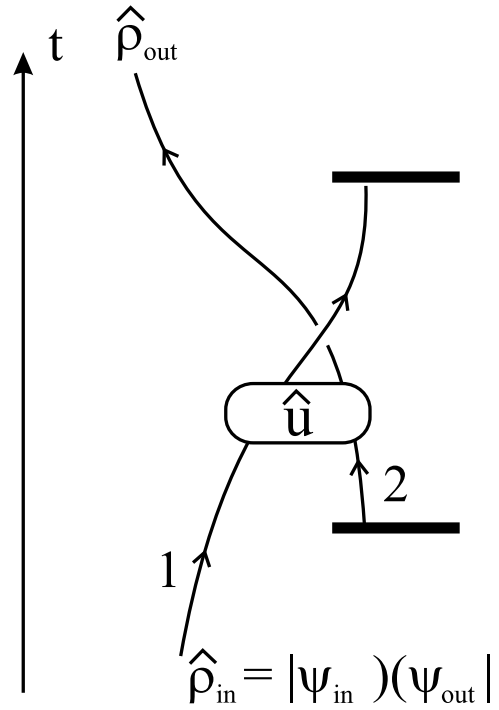

Рис. 15. Взаимодействие частицы с квантовым внутренним состоянием с её версией, пришедшей из будущего.

ется при $t < t_1$ в состоянии $|\psi_{in}\rangle$ (соответствующий статистический оператор $|\psi_{in}\rangle\langle\psi_{in}|$). Частица 2 появляется из выхода "червоточины" в некотором (в общем случае смешанном) состоянии $\hat{\varrho}$. Предполагается, что эволюция внутренних состояний частиц имеет место при их взаимодействии в отмеченной области. Эффект взаимодействия будем описывать унитарным оператором $\hat{U}$, действующим в пространстве состояний

пары частиц. Таким образом, взаимодействие сводится к следующему:

$$|\psi_{in}\rangle\langle\psi_{in}| \otimes \hat{\varrho} \mapsto \hat{U}(|\psi_{in}\rangle\langle\psi_{in}| \otimes \hat{\varrho})\hat{U}^{\dagger}. \tag{75}$$

До взаимодействия состояние сепарабельно, поскольку мы полагаем, что можем приготовить частицу 1 в *чистом* состоянии, не скоррелированным ни с какой другой системой[12]. После взаимодействия состояние пары частиц 1 и 2 в общем случае оказывается зацепленным. Частица 1 отправляется ко входу в "червоточину". Её состояние, рассматриваемое как *элемент квантовой физической реальности*, должно совпадать с состоянием $\hat{\varrho}$ частицы 2, появившейся из "червоточины" при $t = t_1$, т.е.

$$\hat{\varrho} = Tr_2[\hat{U}(|\psi_{in}\rangle\langle\psi_{in}| \otimes \hat{\varrho})\hat{U}^{\dagger}]. \tag{76}$$

Данное условие согласования представляет собой уравнение на статистический оператор $\hat{\varrho}$. Его решение зависти, естественно, как от типа взаимодействия $\hat{U}$, так и от начального состояния $|\psi_{in}\rangle$. Поэтому статистический оператор $\hat{\varrho}_{out}$ частицы при $t > t_2$

$$\hat{\varrho}_{out} = Tr_1[\hat{U}(|\psi_{in}\rangle\langle\psi_{in}| \otimes \hat{\varrho})\hat{U}^{\dagger}] \tag{77}$$

оказывается *нелинейной* функцией начального статистического оператора $\hat{\varrho}_{in} = |\psi_{in}\rangle\langle\psi_{in}|$. Мы столкнулись с необычным для квантовой физики явлением – нелинейным законом

[12]Мы уже сталкивались при обсуждении в предыдущем параграфе с ограничениями на возможные начальные состояния внутренних битов. Теперь мы имеем дело с кубитами. Нет оснований вводить какие-либо ограничения на их начальные состояния, пока мы не принуждены к этому обстоятельствами. В подходе Д.Дойча, как будет показано далее, такие обстоятельства не возникают.

преобразования (77), который запишем в виде

$$\hat{\varrho}_{in} \mapsto \hat{\varrho}_{out} = \Lambda_{CTC}[\hat{\varrho}_{in}]. \tag{78}$$

Здесь введено обозначение Λ_{CTC} этого преобразования, созданного "червоточиной". Из отсутствия линейности следует важный факт: преобразование смеси $p_0\hat{\varrho}_0 + p_1\hat{\varrho}_1$ двух начальных состояний $\hat{\varrho}_0$ и $\hat{\varrho}_1$ с вероятностями p_0 и p_1 не является смесью преобразования каждого из этих состояний:

$$\Lambda_{CTC}[p_0\hat{\varrho}_0 + p_1\hat{\varrho}_1] \neq p_0\Lambda_{CTC}[\hat{\varrho}_0] + p_1\Lambda_{CTC}[\hat{\varrho}_1]. \tag{79}$$

Это происходит потому, что решение уравнения согласования (76) с $\hat{\varrho}_{in} = p_0\hat{\varrho}_0 + p_1\hat{\varrho}_1$ не совпадает с решениями для $\hat{\varrho}_{in} = \hat{\varrho}_0$ и $\hat{\varrho}_{in} = \hat{\varrho}_1$. Правильный учёт этого обстоятельства необходим, как будет показано далее, при анализе новых возможностей, создаваемых "червоточиной", в обработке квантовой информации.

Прежде чем обсуждать применения CTC в квантовой информатике, следует проверить, не накладывает ли условие согласования (76) каких-либо ограничений на множество возможных начальных состояний и возможных взаимодействий. Очевидно, ограничений не будет, если уравнение (76) всегда имеет решение. Доказательство последнего факта можно провести не только для кубитов на входе и выходе из "червоточины", но и для произвольной конечной размерности пространства $\mathcal{H}$ внутренних состояний частиц-носителей. Уравнение (76) можно рассматривать как условие

$$\hat{\varrho} = S[\hat{\varrho}] \tag{80}$$

на неподвижную точку отображения (супероператора)

$$S[\star] = Tr_2[\hat{U}(\hat{\varrho}_{in} \otimes \star)\hat{U}^{\dagger}], \tag{81}$$

действующего в пространстве статистических операторов[13] на $\mathcal{H}$. Пусть $\hat{\varrho}(0)$ – произвольный статистический оператор на $\mathcal{H}$. Строим последовательность $\{\hat{\varrho}(N)\}_{N=0}^{\infty}$:

$$\hat{\varrho}(N) = \frac{1}{N+1}\sum_{n=0}^{N} S^N[\hat{\varrho}(0)]. \tag{82}$$

Для конечномерных гильбертовых пространств соответствующие пространства статистических операторов компактны в топологии нормы. Согласно известной теореме функционального анализа бесконечные последовательности в таких пространствах обязательно имеют предельные точки, т.е. содержат сходящиеся подпоследовательности. Для величин

$$E(\hat{\varrho}(N)) \doteq Tr\left(S[\hat{\varrho}(N)] - \hat{\varrho}(N)\right)^2 = \tag{83}$$

$$\frac{1}{(N+1)^2} Tr\left(S^{N+1}[\hat{\varrho}(0)] - \hat{\varrho}(0)\right)^2.$$

Величина следа в правой части ограничена сверху некоторой константой C, зависящей от размерности пространства. Имеем поэтому

$$0 \leq E(\hat{\varrho}(N)) \leq \frac{C}{(N+1)^2}. \tag{84}$$

Ясно, что любая предельная точка $\hat{\varrho}$ последовательности $\{\hat{\varrho}(N)\}_{N=0}^{\infty}$ удовлетворяет условию

$$E(\hat{\varrho}) = 0 \tag{85}$$

и является, таким образом, неподвижной точкой отображения S.

[13]Тот факт, что результатом действия S является статистический оператор, т.е. эрмитовый, положительно-определённый и имеющий единичный след, нетрудно доказать методами из Части 2.

9 Ликвидация парадоксов в подходе Д.Дойча

Приведённые в предыдущем параграфе рассуждения показывают, что в рамках подхода Дойча к участию СТС в эволюции квантовых состояний нет ограничений на приготовление начальных состояний. Естественно, поэтому, что упомянутые выше классические парадоксы машины времени должны существенно трансформироваться.

Парадокс 1. Вместо выражения (68) для битов, мы имеем теперь аналогичное условие преобразования кубитов:

$$|x\rangle_1 \otimes |y\rangle_2 \mapsto |x\dot{+}y\rangle_1 \otimes |y\rangle_2. \tag{86}$$

Соответствующий унитарный оператор взаимодействия

$$\hat{U} = \sum_{x,y\in\mathbb{Z}_2} |x\dot{+}y\rangle_1\langle x| \otimes |y\rangle_2\langle y|. \tag{87}$$

Из условия согласования (76) получаем:

$$\hat{\varrho} = \frac{1}{2}\hat{1} + Re\langle 0|\psi_{in}\rangle\langle\psi_{in}|1\rangle\Big(|0\rangle\langle 1| + |1\rangle\langle 0|\Big), \tag{88}$$

а (77) даёт:

$$\hat{\varrho}_{out} = \frac{1}{2}\hat{1} + 2[Re\langle 0|\psi_{in}\rangle\langle\psi_{in}|1\rangle]^2\Big(|0\rangle\langle 1| + |1\rangle\langle 0|\Big). \tag{89}$$

Решение (88) существует для всех возможных начальных состояний $|\psi_{in}\rangle$, в том числе и для состояния $|1\rangle$, запрещённого в классическом случае. Для $|\psi_{in}\rangle = |0\rangle$ помимо решения (88), которое в этом случае есть просто $\hat{\varrho} = \hat{1}/2$, существует множество решений

$$\hat{\varrho} = p|0\rangle\langle 0| + (1-p)|1\rangle\langle 1|, \tag{90}$$

где $0 \leq p \leq 1$. Данная неопределённость есть квантовый аналог соответствующего явления в классическом случае (потребность в "дополнительных данных").

Парадокс 2. Как и в классическом варианте, мы предполагаем нахождение одного из входных кубитов в состоянии $|1\rangle$, что моделируют только одну занятую траекторию из пары 1 и 2. Это значит, что начальное состояние кубитов 1 и 2 лежит в подпространстве, натянутом на вектора $|1\rangle_1 \otimes |0\rangle_2$ и $|0\rangle_1 \otimes |1\rangle_2$. Вместо (70) имеем:

$$|x\rangle_1 \otimes |x\dot{+}1\rangle_2 \otimes |y\rangle_3 \mapsto |x\dot{+}y\rangle_1 \otimes |x\dot{+}y\dot{+}1\rangle_2 \otimes |y\rangle_3. \qquad (91)$$

Унитарный оператор, реализующий это преобразование и чьё действие определено только в описанном выше "одночастичном" подпространстве кубитов 1 и 2, имеет вид:

$$\hat{U} = \sum_{x,y \in \mathbb{Z}_2} |x\dot{+}y\rangle_1\langle x| \otimes |x\dot{+}y\dot{+}1\rangle_2\langle x\dot{+}1| \otimes |y\rangle_3\langle y|. \qquad (92)$$

Нетрудно убедиться, что этот оператор коммутирует с оператором

$$\hat{N}_{1,2} = |0\rangle_1\langle 0| \otimes |1\rangle_2\langle 1| + |1\rangle_1\langle 1| \otimes |0\rangle_2\langle 0| + 2|1\rangle_1\langle 1| \otimes |1\rangle_2\langle 1|. \quad (93)$$

эффективной заселённости первой и второй траекторий. Следовательно, взаимодействие $\hat{U}$ не изменит среднего значения оператора $\hat{N}_{1,2}$, но не обязано гарантировать, что конечное состояние кубитов 1 и 3 будет лежать в подпространстве состояний с единичной эффективной заселённостью.

Условие согласования

$$\hat{\varrho} = Tr_{1,3}\left[\hat{U}(|\psi_{in}\rangle_{1,2}\langle\psi_{in}| \otimes \hat{\varrho})\hat{U}^{\dagger}\right] \qquad (94)$$

для начального состояния $|\psi_{in}\rangle_{1,2} \in span\{|1\rangle_1 \otimes |0\rangle_2, |0\rangle_1 \otimes |1\rangle_2\}$ приводит к выражению

$$\hat{\varrho} =$$

$$\sum_{x\in\mathbb{Z}_2} |x\rangle\langle x| \Big(\langle x,\bar{x}|\psi_{in}\rangle\langle\psi_{in}|x,\bar{x}\rangle\langle 0|\hat{\varrho}|0\rangle + \langle \bar{x},x|\psi_{in}\rangle\langle\psi_{in}|\bar{x},x\rangle\langle 1|\hat{\varrho}|1\rangle \Big). \tag{95}$$

Всегда есть решение[14]

$$\hat{\varrho} = \frac{1}{2}\hat{1}. \tag{96}$$

Ему соответствует

$$\hat{\varrho}_{out} = \frac{1}{2}|0\rangle_1\langle 0| \otimes |0\rangle_3\langle 0| + \frac{1}{2}|1\rangle_1\langle 1| \otimes |1\rangle_3\langle 1|. \tag{97}$$

Это состояние является равновероятной смесью ситуации с отсутствием заселения траекторий и ситуации с обеими заселёнными траекториями. Ничего подобного в классическом варианте нет.

Решение (97) наводит на очень любопытную "многомировую" интерпретацию разрешения второго парадокса[15]: во всех мирах наблюдатель, чьё присутствие на той или иной траектории кодируется в нашей модели состоянием кубита, приближается ко входу в "червоточину" по траектории, которая должна отправить его (наблюдателя) назад во времени. Но только в половине миров (типа B) наблюдатель действительно отправляется в прошлое (см рис. 16), и в таких мирах он просто исчезает в "червоточине". Во второй половине миров (типа A) наблюдатель встречается со своим более

[14]Если $|\psi_{in}\rangle_{1,2} = |1\rangle_1 \otimes |0\rangle_2$, то, как и в парадоксе 1, дополнительно существует множество решений (90) – мы снова имеем дело с дополнительными данными в виде веса p.

[15]Эта идея в той или иной форме проникла в научно-фантастическую литературу. Одним из наиболее ярких и талантливых её воплощений является, пожалуй, роман "Меж двух времён" Джека Финнея. В кинематографе аналогичные мотивы прослеживаются в цикле "Назад в будущее".

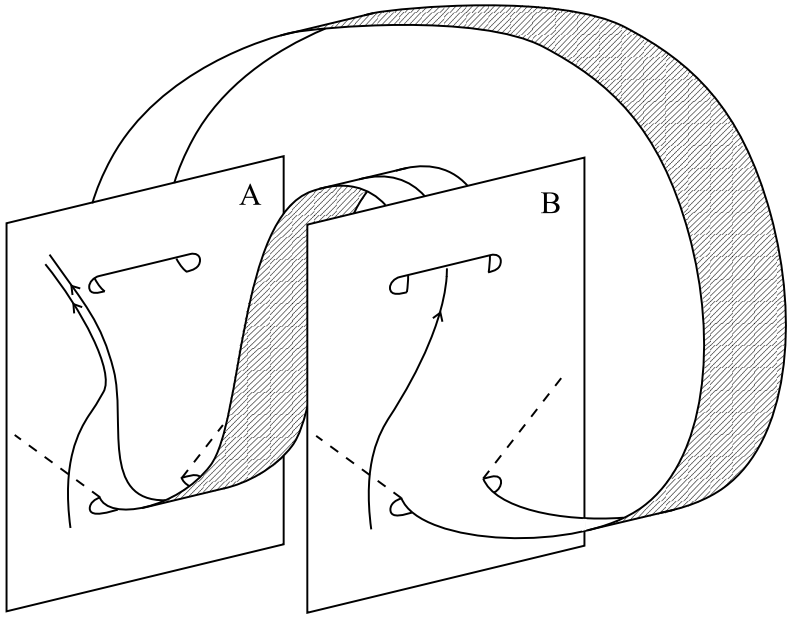

Рис. 16. "Многомировая" схема разрешения парадокса. Внешность двумерных световых конусов выхода из червоточины тождественна для обоих миров.

пожилым двойником, который появляется из выхода "червоточины" при $t = t_1$ и препятствует путешествию в прошлое своей более молодой версии. После этого обе версии наблюдателя продолжают жить в таком мире при $t > t_2$. Таким образом, если в мире B наблюдатель исчезает в "никуда", то в мире A, вторая версия наблюдателя появляется "ниоткуда". Два описанных варианта соответствуют двум слагаемым в правой части выражения (97).

Дальнейшие спекуляции (в хорошем смысле) приводят к идее "асимметричного разделения", которую Д.Дойч оформил следующим образом. Алиса и Боб живут на необитаемом

острове и располагают машиной времени. Алисе хочется расширить свою компанию, включив в неё ещё одну свою версию. Для этого она намерена воспользоваться "червоточиной". С её точки зрения план имеет 100% вероятности успеха, т.к. либо она отправится в прошлое и встретит там себя и Боба, либо из выхода "червоточины" появится её чуть более взрослая копия. С точки зрения Боба он рискует с вероятностью 1/2 остаться в одиночестве. Таким образом, Алиса всегда будет в компании Боба, но Боб не всегда будет в компании Алисы.

Алиса и Боб могут воспользоваться "червоточиной" *независимо*. Это значит, что каждый из них отправится в путешествие во времени в том и только том случае, если из "червоточины" не появится его двойник. В этом случае для стороннего наблюдателя, воспринимающего всю совокупность миров, они делятся на четыре равновероятных типа: те миры, где присутствуют по паре версий Алисы и Боба, те, где есть только пара версий Алисы или пара версий Боба, и пустые миры.

Алиса и Боб могут организовать расставание, обменяв друг друга на копию самого себя. Это произойдёт, если (для определённости) Алиса поступает как описано выше, ориентируясь на появление или отсутствие своей копии, а Боб также ориентируется на появление копии Алисы и отправляется в "червоточину" в том и только том случае, если вторая версия Алисы появилась. Возникают два типа миров, населённых парой Алис или парой Бобов.

Фантазия Дойча рисует картину возможных реализаций таких сценариев в космических масштабах. Если технология "червоточин" позволит осуществлять путешествие по ним целым обитаемым звёздным системам, некая сверхцивилизация, осуществив n-кратное обращение к "червоточинам",

окажется в мире, где кроме неё присутствует ещё $2^n - 1$ её копия. Вероятность наблюдения именно этого мира другой менее развитой цивилизацией, вроде нашей, есть 2^{-n}. Более вероятно наблюдать исчезновение на некотором этапе из нашего мира совокупности копий сверхцивилизаций. Этим можно попытаться объяснить феномен "молчания Вселенной" – отсутствие наблюдаемой активности сверхцивилизаций.

Две сверхцивилизации, избегая конкуренции в борьбе за ресурсы, могут уйти с дороги друг друга, осуществив сценарий расставания, описанный выше на примере с Алисой и Бобом.

Д.Дойч является одним из самых активных сторонников многомировой (эвереттовской) интерпретации квантовой механики и убедительно продемонстрировал ценность подобных взглядов в проблеме парадокса 2. Данная схема его разрешения обнаруживает своеобразную относительность вероятности. С точки зрения стороннего наблюдателя (например, нас) обе версии участников эксперимента с "червоточиной" будут присутствовать с вероятностью 1/2 (в мирах типа A). С точки зрения самого кандидата в путешественники во времени он с единичной вероятностью встретит своего двойника (более молодого или более старого). Аналогичный относительный характер вероятности имеет место в *антропном принципе*, гласящем, что правильный подсчёт вероятности события должен осуществляться *при условии* существования его наблюдателя (возможно, наблюдателя, фиксирующего событие post factum). Прояснение статуса антропного принципа затрагивает глубокие философские вопросы, связанные с конечностью человеческой жизни. Например, следует ли руководствоваться этим принципом, соглашаясь на очень рискованную в обычном смысле игру, ставкой в которой является жизнь? Если верить антропному принципу,

с участник игры со своей точки зрения всегда будет наслаждаться выигрышем. С другой стороны, игрок должен помнить о тех мирах, где он трагически прекратил своё существование, и это несчастье случилось в определённом смысле с ним[16].

Парадокс 3. Схема на рис. ... в квантовом случае даёт следующее условие согласования

$$\hat{\varrho} = S_f[\hat{\varrho}], \tag{98}$$

где

$$S_f[\hat{\varrho}] = \sum_{X=0}^{2^n-1} |f(X)\rangle\langle X|\hat{\varrho}|X\rangle\langle f(X)|. \tag{99}$$

Естественно, что состояние $|X'\rangle\langle X'|$, отвечающее какой-нибудь неподвижной точке отображения f, является решением уравнения (98), но кроме него существуют и другие. Рассмотрим их. Ясно, что действие супероператора S_f всегда даёт статистический оператор, диагональный в базисе $\{|X\rangle\}$ $(X = 0, 1, \ldots, 2^n - 1)$. Поэтому общее решение уравнения (98) имеет вид

$$\hat{\varrho} = \sum_{X=0}^{2^n-1} p_X |X\rangle\langle X|, \tag{100}$$

где $\{p_X\}$ – некоторое распределение вероятностей. Подстав-

[16]Другой известный сторонник и пропагандист многомировой интерпретации, Макс Тегмарк, иллюстрировал аналогичные соображения с помощью идеи "квантового самоубийства", на которое он сам не идёт, т.к., хотя с ним ничего плохого не случится (произойдёт осечка), его жена может остаться вдовой.

ляя (100) в (98), получаем условие на данное распределение:

$$p_X = \sum_{\substack{Y=0 \\ Y=f(X)}}^{2^n-1} p_Y. \tag{101}$$

Пусть f – обратимая функция. Как легко заметить, в этом случае всю множество $\mathbb{Z}_{2^n}$ распадается на классы эквивалентности так, что каждый класс включает в себя числа, получаемые из любого другого числа из того же класса некоторым n-кратным действием отображения f. В частности, неподвижные точки отображения f и только они образуют классы из всего одного элемента. Условие (101) приобретает в случае обратимости f вид

$$p_X = p_{f(X)}. \tag{102}$$

Поэтому все состояния $|X\rangle$ для чисел из одного класса имеют одинаковую вероятность. Пронумеруем все классы эквивалентности C_i индексом i ($i = 1, 2, \ldots, I$). Имеем по определению

$$\mathbb{Z}_{2^n} = \bigsqcup_{i=1}^{I} C_i. \tag{103}$$

Здесь $\bigsqcup$ обозначает объединение взаимно-непересекающихся множеств. Общее решение уравнения (98) для обратимого f можно записать так:

$$\hat{\varrho} = \sum_{i=1}^{I} p^{(i)} \sum_{X \in C_i} |X\rangle\langle X|. \tag{104}$$

Здесь $p^{(i)}$ – вероятность для элементов из класса C_i. В множество этих решений входит, естественно, и максимально смешанное состояние $\hat{1}/2^n$. Все остальные решения требуют для своей спецификации дополнительных данных.

Во всех трёх квантовых версиях парадоксов с СТС возникают ситуации, в которых требуются дополнительные данные для описания эволюции на интервале между выходом и входом в "червоточину". Мы уже обсуждали в классическом контексте философский принцип об эволюционном генезисе знания и его нарушения при конкретизации дополнительных данных, что так беспокоит Д.Дойча.

Обсуждение эволюционного принципа затруднено отсутствием строгого математического определения объёма знания, аналогичного имеющемуся определению объёма информации. Понятие "знание" родственно понятию "информация", но явно не тождественно ему. Возможно, что знание следует определять как ту информацию, которую мы можем употреблять для достижения стоящих перед нами целей. Одной из основных целей, к которой в той или иной степени сводятся многие другие, является выживание. С этой точки зрения знание становится ещё одним и очень важным адаптивным механизмом, а эволюционное происхождение адаптивных механизмов представляется очень естественным.

Вынужденно упрощая рассмотрение и оперируя только с понятием объёма информации, Д.Дойч предлагает принцип максимума энтропии в подходе к проблеме дополнительных данных в системах с СТС. Это позволяет не рассматривать состояния $\hat{\varrho}$, получающиеся при решении уравнения согласования (76), отличные от также имеющегося решения с максимально смешанным состоянием, имеющим максимальную энтропию. Это состояние является единственной точкой максимума энтропии (энтропии фон Неймана), как показывается в Приложении. Это закрывает проблему в случае квантовых вариантов парадоксов 1 и 2 и в случае парадокса 3 при обратимом отображении f. Но как быть в случае необратимого f? Рассмотрим следующий пример. Пусть отображение f имеет

единственную неподвижную точку X' и при этом существует число X_0 такое, что последовательность $\{f^k(X_0)\}_{k=0}^{2^n-1}$ содержит все числа из $\mathbb{Z}_{2^n}$. Здесь $f^k(X_0) \doteq f(f^{k-1}(X_0))$. Первое число в этой последовательности есть $X_0 \equiv f^0(X_0)$, а последнее – X'. Из условия (101) следует в этом случае решение

$$p_{X_0} = p_{f(X_0)} = \ldots = p_{f^{2^n-2}(X_0)} = 0, \tag{105}$$

$$p_{f^{2^n-1}(X_0)} \equiv p_{X'} = 1.$$

Поэтому решение $\hat{\varrho} = |X'\rangle\langle X'|$ является единственным и драматически нарушающим эволюционный принцип.

Положение может спасти учёт неустранимого шума, присутствующего при любых вычислениях, в том числе и с участием СТС. Условие согласования (98) заменим на более сложное:

$$\hat{\varrho} = \frac{\varepsilon}{2^n}\hat{1} + (1-\varepsilon)S_f[\hat{\varrho}], \tag{106}$$

куда входит вероятность ε "забывания" состояния при путешествии в "червоточине". Уравнение 106) даёт вместо 101) условие

$$p_X = \frac{\varepsilon}{2^n} + (1-\varepsilon)\sum_{\substack{Y=0 \\ Y=f(X)}}^{2^n-1} p_Y. \tag{107}$$

Решая это уравнение для описанного выше отображения f, легко найти:

$$p_{f^i(X_0)} = \frac{1-(1-\varepsilon)^{i+1}}{2^n} \quad (i = 0, 1, \ldots, 2^n-2). \tag{108}$$

Для $p_{X'} = p_{f^{2^n-1}(X_0)}$ имеем из 107):

$$p_{X'} = \frac{\varepsilon}{2^n} + (1-\varepsilon)(p_{X'} + p_{f^{2^n-2}(X_0)}), \tag{109}$$

откуда с учётом 108) получаем

$$p_{X'} = \frac{1-(1-\varepsilon)^{2^n}}{\varepsilon 2^n}. \tag{110}$$

Заметим, что нарушение эволюционного принципа в системе с СТС тем значительнее, чем больше число n (т.е. чем меньше вероятность случайно угадать неподвижную точку). При фиксированном n и при уменьшении вероятности ошибки ε имеем из 110)

$$p_{X'} \to 1. \tag{111}$$

Это то самое "неприятное" нарушение эволюционного принципа. Если, напротив, фиксировать ε и неограниченно увеличивать n (так, что $(1-\varepsilon)^{2^n} \ll 1$), получим

$$p_{X'} \to \frac{1}{\varepsilon 2^n} \to 0. \tag{112}$$

Вес состояния $|X'\rangle\langle X'|$ в $\hat{\varrho}$ уменьшается из-за своеобразного эффекта усиления шума, хотя и остаётся больше $1/2^n$ – веса состояния $|X'\rangle\langle X'|$ в максимально смешанном статистическом операторе. Таким образом, драматическое нарушение эволюционного принципа устранено.

10 Разрушение зацепленности в подходе Д.Дойча

Подход Д. Дойча обнаруживает важное свойство "червоточины" – её способность разрушать зацепленность между квантовыми подсистемами, одна из которых перебрасывается в прошлое. До сих пор во всех конкретных примерах мы предполагали начальное состояние $\hat{\varrho}_{in}$ кубита, нацеленного

на вход в "червоточину", чистым: $\hat{\varrho}_{in} = |\psi_{in}\rangle\langle\psi_{in}|$. Ничего не мешает, однако, считать, что кубит находится в смешанном состоянии, т.е. представляет собой подсистему некоторой более широкой системы, приготовленной в чистом состоянии. На рис. 17 пара кубитов 1 и 3 приготавливается в синглет-

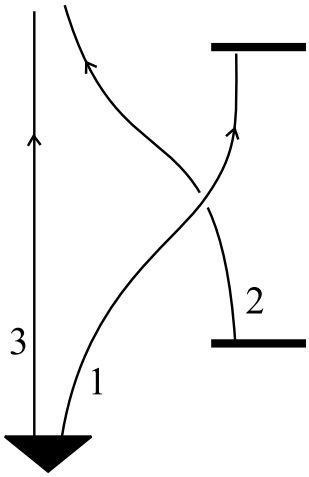

Рис. 17. Пара кубитов 1 и 3 приготавливается в зацепленном состоянии. Кубиты 1 и 2 оказываются незацепленными.

ном (для определённости) состоянии:

$$|\Psi\rangle_{1,3} = \frac{1}{\sqrt{2}}(|0\rangle_1 \otimes |1\rangle_3 - |1\rangle_1 \otimes |0\rangle_3). \qquad (113)$$

Мировая линия кубита 3 проходит в стороне от "червоточины", куда попадает кубит 1. Для простоты можно считать, что он не взаимодействует с кубитом 2, вышедшим из "червоточины". Условие согласования (76) выглядит в данном случае так:

$$\hat{\varrho} = Tr_{2,3}[|\Psi\rangle_{1,3}\langle\Psi| \otimes \hat{\varrho}]. \qquad (114)$$

Здесь можно сначала взять след по состояниям кубита 3. Тогда мы придём к простому выражению

$$\hat{\varrho} = Tr_2 \left[\hat{\varrho}_{in} \otimes \hat{\varrho}\right], \tag{115}$$

где

$$\hat{\varrho}_{in} = Tr_3 \left|\Psi\right\rangle_{1,3}\!\left\langle\Psi\right| = \frac{1}{2}\hat{1} \tag{116}$$

есть начальное смешанное состояние кубита 1. Из (115) тривиальным образом следует

$$\hat{\varrho} = \frac{1}{2}\hat{1}. \tag{117}$$

Мы получили, что после переброса в прошлое и превращения в кубит 2, кубит 1 утратил зацепленность с кубитом 3:

$$\left|\Psi\right\rangle\!\left\langle\Psi\right| \xrightarrow{\Lambda_{CTC}} \frac{1}{4}\hat{1} \otimes \hat{1}. \tag{118}$$

Преобразование (78), применённое к более широкому (чистому) начальному состоянию переводит его в смешанное состояние. Это ещё одно обстоятельство наряду с отмеченной ранее нелинейностью, отличающего его от привычных линейных и унитарных (для достаточно широко определённых систем) преобразований.

11 Однозначное различение неортогональных состояний с помощью CTC.

Необычные свойства пространства-времени с CTC предоставляют столь же необычные возможности для оперирования с квантовыми состояниями. Вспомним, что запрет на их

клонирование и однозначное различение вытекал из линейности и (при достаточно широком понятии системы) унитарности квантовых операций. Оба этих свойства оказываются нарушенными при участии СТС в подходе Д.Дойча. Поэтому не должно вызывать большого удивления возможность преодолеть (*с точки зрения данного подхода*) упомянутые запреты.

Рассмотрим алгоритм однозначного различения состояния $|0\rangle$ и $(|0\rangle - |1\rangle)/\sqrt{2}$. Это позволяет, в частности, "взламывать" протокол B92 секретного распределения ключа. В алгоритме используется элемент Адамара (Hadamard) – простейшая однокубитовая квантовая операция, фигурирующая во всех идеях квантовой информатики:

$$\hat{H}|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad \hat{H}|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \tag{119}$$

Организуем операцию Адамара, контролируемую кубитом, появившимся из выхода "червоточины" (см. рис. **??**), т.е. эта операция включается состоянием $|1\rangle$. Условие согласования (76) для данного взаимодействия кубитов даёт следующие выражения матричных элементов статистического оператора $\hat{\varrho}$:

$$\begin{gathered}
\varrho_{00} = \frac{1 + r_{01} + r_{10}}{1 + r_{01} + r_{10} + 2r_{11}}, \quad \varrho_{11} = \frac{2r_{11}}{1 + r_{01} + r_{10} + 2r_{11}}, \\
\varrho_{01} = \frac{r_{01}(1 + r_{01} + r_{10}) + r_{11}(r_{00} + r_{01} - r_{10} - r_{11})}{1 + r_{01} + r_{10} + 2r_{11}}, \\
\varrho_{10} = \frac{r_{10}(1 + r_{01} + r_{10}) + r_{11}(r_{00} - r_{01} + r_{10} - r_{11})}{1 + r_{01} + r_{10} + 2r_{11}}.
\end{gathered} \tag{120}$$

Здесь $r_{ij} \doteq \langle i|\hat{\varrho}_{in}|j\rangle$. Для состояния $\hat{\varrho}_{out}$ имеем:

$$\hat{\varrho}_{out} = |0\rangle\varrho_{00}\langle 0| + |1\rangle\varrho_{11}\langle 1| + \tag{121}$$

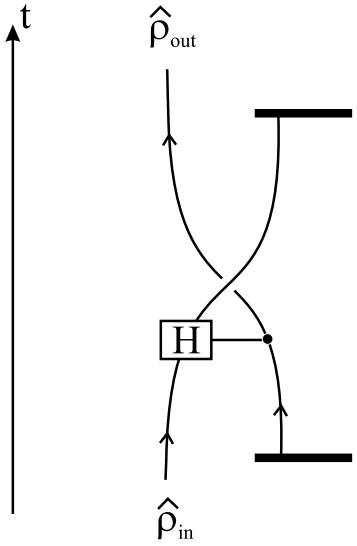

Рис. 18. Схема с контролируемой операцией Адамара для различения неортогональных квантовых состояний.

$$|1\rangle\varrho_{10}\langle 0|\,Tr\,\hat{H}\hat{\varrho}_{in} + |0\rangle\varrho_{01}\langle 1|\,Tr\,\hat{H}^{\dagger}\hat{\varrho}_{in}.$$

Здесь

$$Tr\,\hat{H}\hat{\varrho}_{in} = Tr\,\hat{H}^{\dagger}\hat{\varrho}_{in} = \frac{1}{\sqrt{2}}(r_{00} + r_{01} + r_{10} - r_{11}).$$

Для входных состояний $|0\rangle$ и $(|0\rangle - |1\rangle)/\sqrt{2}$ приведённые выражения дают следующий результат:

$$\begin{aligned} \hat{\varrho}_{in} = |0\rangle\langle 0| \quad &\Rightarrow \quad \hat{\varrho}_{out} = |0\rangle\langle 0| \\ \hat{\varrho}_{in} = \frac{1}{2}(|0\rangle - |1\rangle)(\langle 0| - \langle 1|) \quad &\Rightarrow \quad \hat{\varrho}_{out} = |1\rangle\langle 1|. \end{aligned} \qquad (122)$$

Проводя измерение выходного состояния в базисе $\{|0\rangle, |1\rangle\}$, мы можем однозначно различить входные состояния.

Данный алгоритм допускает расширение на любое конечное множество входных состояний. В частности, можно однозначно различить состояния поляризации $\{|V\rangle, |H\rangle, |R\rangle, |L\rangle\}$. Это означает преодоление секретности протокола BB84 и, что более впечатляет, возможность реализации "сверхсветового телеграфа" по проекту Н.Герберта. Действительно, с точки зрения Алисы в устройство-дискриминатор Боба, основанное на СТС, каждый раз поступает одно из четырёх перечисленных чистых состояний. Условие согласования (76), решаемое также с точки зрения Алисы, будет гарантировать правильное прочтение бита в лаборатории Боба.

12 Проблемы подхода Д.Дойча при наличии измерений.*

До сих пор мы анализировали схемы с СТС с позиций подхода Дойча, т.е. с позиций строго онтологического взгляда на природу квантового состояния. Способность различать неортогональняе состояния, вытекающая из такого подхода, можно рассматривать как некоторый настораживающий момент. И этот момент не единственный. Внесем в схему рис. 15 акт измерения состояния кубита при его выходе из машины времени, но до взаимодействия с более ранней версией (рис. 19). Рассмотрим вопрос о вероятности появления того или иного исхода измерения. Очевидно, что эти вероятности зависят от характера взаимодействия между кубитами, который следует конкретизировать. Рассмотрим один из простейших типов взаимодействия, фигурировавший ранее – контролируемое отрицание (C-NOT). Измерение проводится некотором

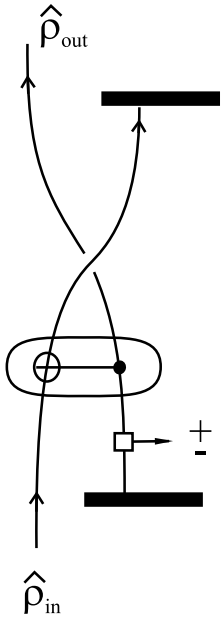

Рис. 19. Появление события измерения над кубитом, вышедшим из "червоточины".

базисе кубита, суперпозиционном по отношению к $\{|0\rangle, |1\rangle\}$:

$$\begin{aligned} |\psi_+\rangle &= \alpha|0\rangle + \beta|1\rangle \\ |\psi_-\rangle &= -\bar{\beta}|0\rangle + \bar{\alpha}|1\rangle. \end{aligned} \tag{123}$$

Здесь α и β – комплексные числа, связанные условием $|\alpha|^2 + |\beta|^2 = 1$. Согласно стандартному формализму квантовой механики при получении исхода $j = \pm$ измерения состояние кубита меняется:

$$\hat{\varrho} \mapsto \frac{\hat{P}_j \hat{\varrho} \hat{P}_j}{p_j}, \tag{124}$$

где $\hat{P}_j = |\psi_j\rangle\langle\psi_j|$ – проектор на состояние $|\psi_j\rangle$ и $p_j = \langle\psi_j|\hat{\varrho}|\psi_j\rangle$ – вероятность исхода j. Наличие причинной петли вносит существенную специфику: кубит подвергается измерению на выходе из нижнего разреза, уже неся в своем состоянии информацию об исходе предстоящего измерения. Поэтому в условии согласования следует рассматривать два состояния $\hat{\varrho}_\pm$ кубита:

$$\begin{aligned} p_+\hat{\varrho}_+ &= Tr_2\,\hat{U}(\hat{\varrho}_{in}\otimes\hat{P}_+\hat{\varrho}_+\hat{P}_+)\hat{U}^\dagger \\ p_-\hat{\varrho}_- &= Tr_2\,\hat{U}(\hat{\varrho}_{in}\otimes\hat{P}_-\hat{\varrho}_-\hat{P}_-)\hat{U}^\dagger. \end{aligned} \qquad (125)$$

Следуя идее Эверетта, мы предполагаем существование двух миров $W_\pm$, в которых реализуются альтернативные исходы измерения. Ситуация, соответствующая системе (125), изображена на рис. 20, где изображены две ленты вне плоского пространства-времени, соединяющие соответствующие края разрезов в каждом мире.

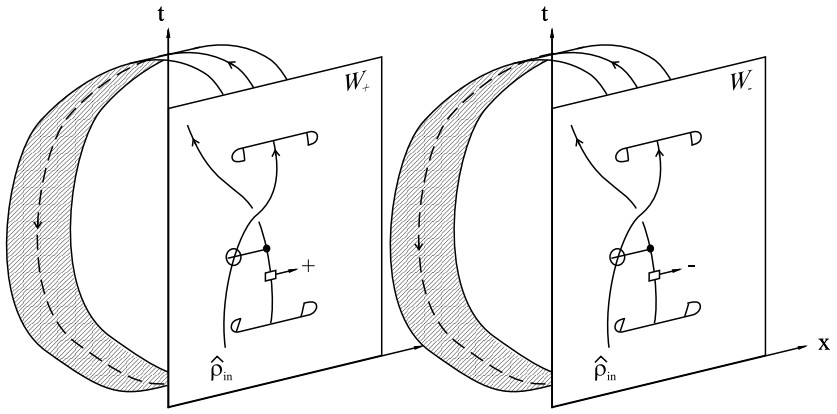

Рис. 20. Возможный вариант соединения миров, соответствующих альтернативным исходам измерения.

Решая уравнения (6), получаем для величин $p_\pm$:

$$p_+ = (|\alpha|^4 + |\beta|^4)\rho_{00} + 2|\alpha\beta|^2\rho_{11} + \tag{126}$$

$$+(\bar{\alpha}\beta|\alpha|^2 + \alpha\bar{\beta}|\beta|^2)\rho_{01} + (\bar{\alpha}\beta|\beta|^2 + \alpha\bar{\beta}|\alpha|^2)\rho_{10};$$

$$p_- = (|\alpha|^4 + |\beta|^4)\rho_{00} + 2|\alpha\beta|^2\rho_{11} - \tag{127}$$

$$-(\bar{\alpha}\beta|\beta|^2 + \alpha\bar{\beta}|\alpha|^2)\rho_{01} - (\bar{\alpha}\beta|\alpha|^2 + \alpha\bar{\beta}|\beta|^2)\rho_{10}.$$

Здесь $\rho_{kl} = \langle k|\hat{\varrho}_{in}|l\rangle$, $k, l = 0, 1$. Легко убедиться, что в общем случае $p_+ + p_- \neq 1$. Поэтому эти величины *не могут* быть вероятностями.

Можно попробовать исправить ситуацию, рассматривая иную топологию миров $W_\pm$. Пусть ленты соединяют верхний разрез одного мира с нижним разрезом другого (рис. 21). Для таких условий уравнения согласования принимают вид:

$$\begin{aligned} p_+\hat{\varrho}_- &= Tr_2\,\hat{U}(\hat{\varrho}_{in} \otimes \hat{P}_+\hat{\varrho}_+\hat{P}_+)\hat{U}^\dagger \\ p_-\hat{\varrho}_+ &= Tr_2\,\hat{U}(\hat{\varrho}_{in} \otimes \hat{P}_-\hat{\varrho}_-\hat{P}_-)\hat{U}^\dagger. \end{aligned} \tag{128}$$

Вычисление величин $p_\pm$ дает

$$p_+ = (|\alpha|^4 + |\beta|^4)\rho_{11} + 2|\alpha\beta|^2\rho_{00} + \tag{129}$$

$$+(\bar{\alpha}\beta|\beta|^2 + \alpha\bar{\beta}|\alpha|^2)\rho_{01} + (\bar{\alpha}\beta|\alpha|^2 + \alpha\bar{\beta}|\beta|^2)\rho_{10};$$

$$p_- = (|\alpha|^4 + |\beta|^4)\rho_{11} + 2|\alpha\beta|^2\rho_{00} - \tag{130}$$

$$-(\bar{\alpha}\beta|\alpha|^2 + \alpha\bar{\beta}|\beta|^2)\rho_{01} - (\bar{\alpha}\beta|\beta|^2 + \alpha\bar{\beta}|\alpha|^2)\rho_{10}.$$

Как и в предыдущем случае, сумма величин p_+ и p_- в общем случае не равна единице. Мы сталкиваемся с той же проблемой невозможности трактовать данные величины как вероятности исходов измерения.

Мы пришли к противоречивым результатам. Следовательно, какая-то из исходных посылок ошибочна. Их три: 1

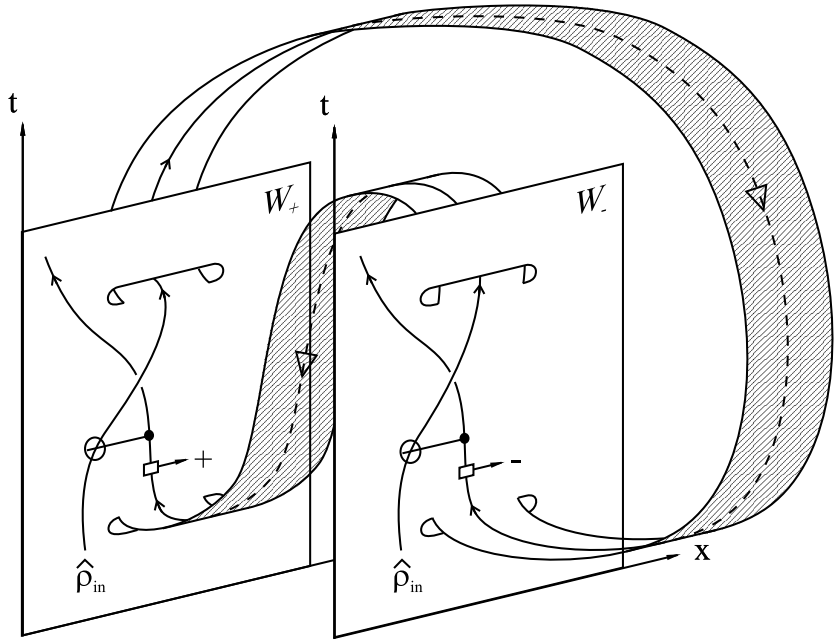

Рис. 21. Второй возможный вариант соединения миров, соответствующих альтернативным исходам измерения.

– предположение о возможности причинных петель, 2 – онтологическая трактовка понятия квантового состояния, 3 – применимость стандартного формализма описания квантовых измерений. Самым слабым представляется именно второй тезис и вытекающие из него условия согласования (125) и (128). Заметим, однако, что для этих условий остается некоторый шанс. А именно, нетрудно проверить, что имеет место следующее равенство:

$$\frac{1}{2}(p_+^{(I)} + p_+^{(II)}) + \frac{1}{2}(p_-^{(I)} + p_-^{(II)}) = 1, \qquad (131)$$

где величины $p_\pm^{(I)}$ и $p_\pm^{(II)}$ даются выражениями (126, 127) и

(129, 130), соответственно. Данное соотношение допускает несколько экстравагантную интерпретацию: если при возникновении причинной петли ее ленты случайным *равновероятным* образом либо замыкаются внутри каждого мира как на рис. 20, либо соединяют миры как на рис. 21, трактовка двух слагаемых из (131) как вероятностей исходов измерения может быть восстановлена. При такой интерпретации остается открытым вопрос о природе случайности выбора топологии соединения лент и миров. Если верен подход Д.Дойча, игнорировать этот вопрос не удастся.

Приложение. Свойства классической и квантовой энтропии.

В Приложении излагаются некоторые математические свойства энтропии и доказывается единственность состояния с максимальной энтропией. Данный результат, согласно гипотезе Д.Дойча, делает однозначным выбор состояния при необходимости дополнительных данных.

Пусть мы имеем некоторую классическую случайную наблюдаемую величину x. В зависимости от дополнительных условий, нумеруемых индексом σ, распределение этой величины есть $\rho_\sigma(x)$. Известны априорные вероятности $\{p_\sigma\}$ реализации тех или иных дополнительных условий. Примером может служить неидеальный канал связи, обсуждаемый в основном тексте. При этом индекс σ нумерует отправляемый символ, а случайная величина x представляет собой результат измерения на выходе из канала. Вероятности $\{p_\sigma\}$ задаются частотой появления того или иного символа в тексте[17].

[17]Для простоты считаем, что между появлениями различных симво-

Усреднение по вероятностям $\{p_\sigma\}$ (без ограничения общности каждую из них считаем ненулевой) порождает вероятность

$$\rho(x) = \sum_\sigma p_\sigma \rho_\sigma(x). \tag{132}$$

С этим распределением, которое называется выпуклой комбинацией распределений $\{\rho_\sigma(x)\}_\sigma$, можно связать энтропию

$$H[\rho] = -\sum_x \rho(x) \ln \rho(x) \tag{133}$$

также как и с каждым распределением $\rho_\sigma(x)$:

$$H[\rho_\sigma] = -\sum_x \rho_\sigma(x) \ln \rho_\sigma(x). \tag{134}$$

Имеет место следующая

Теорема 12.1. *Энтропия является строго выпуклой функционалом распределения вероятностей, т.е.*

$$H[\Sigma_\sigma\, p_\sigma \rho_\sigma] \geq \sum_\sigma p_\sigma H[\rho_\sigma],$$

и равенство имеет место только при условии $\forall\sigma \;\; \rho_\sigma(x) = \rho(x) \doteq \Sigma_\sigma\, p_\sigma \rho_\sigma(x)$.

Доказательство: Имеем

$$-\sum_x \rho(x) \ln \rho(x) + \sum_x \sum_\sigma p_\sigma \rho_\sigma(x) \ln \rho_\sigma(x) =$$

$$\sum_x \sum_\sigma p_\sigma \rho_\sigma(x) \ln \frac{\rho_\sigma(x)}{\rho(x)} =$$

лов корреляций нет.

$$\sum_x \sum_\sigma p_\sigma \rho_\sigma(x) \left(\ln \frac{\rho_\sigma(x)}{\rho(x)} - 1 + \frac{\rho(x)}{\rho_\sigma(x)} \right) \geq 0.$$

Доказана выпуклость. Если $H[\rho] = \sum_\sigma p_\sigma H[\rho_\sigma]$, то из последней строки следует, что для значений x таких, что $\rho_\sigma(x) \neq 0$, выражение в круглых скобках равно нулю и, следовательно $\rho_\sigma(x) = \rho(x)$. Из условия $\Sigma_x \rho_\sigma(x) = \Sigma_x \rho(x) = 1$ следует равенство распределений $\rho_\sigma(x)$ и $\rho(x)$ для всех x. Поскольку этот результат верен для всех σ, мы получаем строгую выпуклость энтропии. □

Квантовым вариантом энтропии (133) является энтропия фон Неймана. Для квантовой системы, находящейся в состоянии $\hat{\varrho}$, эта величина определяется следующим выражением:

$$S[\hat{\varrho}] \doteq -Tr\, \hat{\varrho} \ln \hat{\varrho}. \tag{135}$$

Диагональное представление

$$\hat{\varrho} = \sum_i \rho_i |e_i\rangle\langle e_i| \tag{136}$$

задаёт распределение вероятностей $\{\rho_i\}$ нахождения системы в том или ином собственном состоянии $|e_i\rangle$ статистического оператора. Если для взятия следа в (135) использовать базис этих собственных состояний, энтропия фон Неймана приобретает вид (133):

$$S[\hat{\varrho}] = -\sum_i \rho_i \ln \rho_i \equiv H[\rho]. \tag{137}$$

Выбор любого другого ортонормированного базиса $\{|e'_i\rangle\}$ порождает распределение вероятностей $\{\rho'_i\}$ нахождения системы в состояниях из этого нового базиса. С использованием

(136) получаем для вероятностей ρ'_i:

$$\rho'_i \equiv \langle e'_i|\hat{\varrho}|e'_i\rangle = \sum_j |\langle e'_i|e_j\rangle|^2 \rho_j \tag{138}$$

Матрица коэффициентов преобразования от распределения $\{\rho_i\}$ к распределению $\{\rho'_i\}$

$$q_{ij} \doteq |\langle e'_i|e_j\rangle|^2 \tag{139}$$

является *дважды стохастической*. Так называются квадратные матрицы с неотрицательными элементами и с равной единице суммой элементов из любой строки или любого столбца. Элементы матрицы (139) являются квадратами модулей элементов унитарной матрицы перехода от базиса $\{|e_i\rangle\}$ к базису $\{|e'_i\rangle\}$. Поэтому матрицу (139) называют также *унистохастической*.

Теорема 12.2. *Для энтропий распределений* $\{\rho_i\}$ *и* $\{\rho'_i\}$, *связанных дважды стохастической матрицей,* $\rho'_i = \Sigma_j\, q_{ij}\rho_j$, *имеет место соотношение*

$$H[\rho'] \geq H[\rho].$$

Доказательство: Имеем

$$\begin{aligned} H[\rho'] &= -\sum_i \rho'_i \ln \rho'_i = -\sum_{i,j} q_{ij}\rho_j \ln \rho'_i, \qquad (140)\\ H[\rho] &= -\sum_j \rho_j \ln \rho_j = -\sum_{i,j} q_{ij}\rho_j \ln \rho_j. \end{aligned}$$

В последнем равенстве использовали стохастичность матрицы преобразования по столбцам:

$$\sum_i q_{ij} = 1. \tag{141}$$

Для разности энтропий получаем:

$$H[\rho'] - H[\rho] = \sum_{i,j} q_{ij}\rho_j \ln \frac{\rho_j}{\rho'_i} = \tag{142}$$

$$\sum_{i,j} q_{ij}\rho_j \left(\ln \frac{\rho_j}{\rho'_i} - 1 + \frac{\rho'_i}{\rho_j} \right) \geq 0.$$

При переходе к последней строке использовалась стохастичность по строкам:

$$\sum_j q_{ij} = 1. \tag{143}$$

Как следствие, мы получили утверждение о совпадении энтропии фон Неймана $\hat{\varrho}$ с минимальным возможным значением энтропии $H[q]$ для распределений, построенных согласно (138) по всевозможным ортонормированным базисам. □

Справедливо и более сильное утверждение, что равенство $H[\rho'] = H[\rho]$ имеет место только при условии различия распределений $\{\rho_i\}$ и $\{\rho'_i\}$ не более чем порядком своих членов. Для доказательства этого факта следует привлечь теорему Биркгофа о представимости любой дважды стохастической матрицы в виде выпуклой комбинации (с положительными и дающими в сумме единицу весами) перестановочных матриц, в каждой строке и каждом столбце которых присутствует только один ненулевой элемент, равный 1. После этого результат следует из теоремы (12.1).

Для энтропии фон Неймана имеет место утверждение, аналогичное теореме (12.1). Достаточно ограничиться случаем двух состояний $\hat{\varrho}_0$ и $\hat{\varrho}_1$, представленных с весами p_0 и $p_1 = 1 - p_0$:

Теорема 12.3. *Энтропия Неймана является строго выпуклой функционалом статистического оператора, т.е.*

$$p_0 S[\hat{\varrho}_0] + p_1 S[\hat{\varrho}_1] \leq S[p_0\hat{\varrho}_0 + p_1\hat{\varrho}_1],$$

и в случае $p_0 \neq 0 \neq p_1$ *равенство имеет место только при условии* $\hat{\varrho}_0 = \hat{\varrho}_1$.

Доказательство: Для $\hat{\varrho}_0$, $\hat{\varrho}_1$ и $\hat{\varrho} \doteq p_0\hat{\varrho}_0 + p_1\hat{\varrho}_1$ имеют место диагональные представления:

$$\begin{aligned} \hat{\varrho}_0 &= \sum_i \rho_i^{(0)} |e_i^{(0)}\rangle\langle e_i^{(0)}|, \\ \hat{\varrho}_1 &= \sum_i \rho_i^{(1)} |e_i^{(1)}\rangle\langle e_i^{(1)}|, \\ \hat{\varrho} &= \sum_i \rho_i |e_i\rangle\langle e_i|. \end{aligned} \tag{144}$$

Далее без ограничения общности будем считать, что множества собственных значений статистических операторов не вырождены. Согласно определения энтропии фон Неймана

$$S[p_0\hat{\varrho}_0 + p_1\hat{\varrho}_1] = -\sum_i \rho_i \ln \rho_i. \tag{145}$$

Из определения состояния $\hat{\varrho}$ имеем

$$p_0\langle e_i|\hat{\varrho}_0|e_i\rangle + p_1\langle e_i|\hat{\varrho}_1|e_i\rangle = \rho_i. \tag{146}$$

На этом основании из теоремы (12.1) следует

$$-p_0 \sum_i \langle e_i|\hat{\varrho}_0|e_i\rangle \ln\langle e_i|\hat{\varrho}_0|e_i\rangle - p_1 \sum_i \langle e_i|\hat{\varrho}_1|e_i\rangle \ln\langle e_i|\hat{\varrho}_1|e_i\rangle \leq \tag{147}$$

$$-\sum_i \rho_i \ln \rho_i.$$

Из теоремы (12.2) следует

$$\begin{aligned} S[\hat{\varrho}_0] &\leq -\sum_i \langle e_i|\hat{\varrho}_0|e_i\rangle \ln\langle e_i|\hat{\varrho}_0|e_i\rangle, \qquad (148)\\ S[\hat{\varrho}_1] &\leq -\sum_i \langle e_i|\hat{\varrho}_1|e_i\rangle \ln\langle e_i|\hat{\varrho}_1|e_i\rangle. \end{aligned}$$

На основе (147) и (149) получаем

$$p_0 S[\hat{\varrho}_0] + p_1 S[\hat{\varrho}_1] \leq S[p_0\hat{\varrho}_0 + p_1\hat{\varrho}_1]. \qquad (149)$$

Доказана выпуклость. Если здесь имеет место равенство, оно будет иметь место и в (147). При $p_0 \neq 0 \neq p_1$ из этого факта следует

$$\langle e_i|\hat{\varrho}_0|e_i\rangle = \langle e_i|\hat{\varrho}_1|e_i\rangle = \rho_i. \qquad (150)$$

Вместо неравенств (149) имеем

$$-\sum_i \rho_i^{(\sigma)} \ln \rho_i^{(\sigma)} = -\sum_i \langle e_i|\hat{\varrho}_\sigma|e_i\rangle \ln\langle e_i|\hat{\varrho}_\sigma|e_i\rangle. \qquad (151)$$

Здесь $\sigma = 0, 1$. При этом надо помнить, что величины $\langle e_i|\hat{\varrho}_\sigma|e_i\rangle$ связаны с $\rho_i^{(\sigma)}$ соотношением

$$\langle e_i|\hat{\varrho}_\sigma|e_i\rangle = \sum_j |\langle e_i|e_j^{(\sigma)}\rangle|^2 \rho_j^{(\sigma)}. \qquad (152)$$

Из равенств (151) и комментария к теореме (12.2) следует, что фигурирующая здесь унистохастическая матрица сводится к перестановочной и после подходящего изменения нумерации

$$|\langle e_i|e_j^{(\sigma)}\rangle| = \delta_{i,j}. \qquad (153)$$

Совпадают не только собственные числа операторов $\hat{\varrho}_0$ и $\hat{\varrho}_1$, но и соответствующие собственные состояния, т.е. $\hat{\varrho}_0 = \hat{\varrho}_1$. □

Строго выпуклые функции и функционалы обладают важным свойством. Доказательство можно провести, используя самые простые обозначения и не конкретизируя природу области определения. Достаточно считать, что это есть некоторое линейное топологическое пространство над полем действительных чисел.

Теорема 12.4. *Строго выпуклая функция $f(x)$, т.е. такая, что $f(px + (1-p)y) \geq pf(x) + (1-p)f(y)$ при всех $0 \leq p \leq 1$ и такая, что из $f(px + (1-p)y) = pf(x) + (1-p)f(y)$ при некотором $0 < p < 1$ следует $x = y$, имеет не более одной точки максимума*

Доказательство: Пусть имеется две точки $x_1 \neq x_2$ максимума функции f. Это означает, что существует некоторая окрестность точки x_1, в которой значения функции не превосходят её значения в x_1. Следовательно, существует достаточно малое значение параметра ε из интервала $(0, 1)$ такое, что

$$f((1-\varepsilon)x_1 + \varepsilon x_2) \leq f(x_1). \tag{154}$$

С другой стороны мы имеем по определению выпуклости:

$$(1-\varepsilon)f(x_1) + \varepsilon f(x_2) \leq f((1-\varepsilon)x_1 + \varepsilon x_2). \tag{155}$$

Из этих двух неравенств следует $f(x_2) \leq f(x_1)$. Меняя в этих рассуждениях местами x_1 и x_2, получаем в результате

$$f(x_2) = f(x_1). \tag{156}$$

Теперь комбинация неравенств (154) и (155) даёт:

$$f(x_1) \leq f((1-\varepsilon)x_1 + \varepsilon x_2) \leq f(x_1). \tag{157}$$

Следовательно

$$f((1-\varepsilon)x_1 + \varepsilon x_2) = (1-\varepsilon)f(x_1) + \varepsilon f(x_2). \qquad (158)$$

Это равенство при $x_1 \neq x_2$ противоречит строгой выпуклости функции. □

Данный результат позволяет утверждать, что энтропия фон Неймана может достигать максимума только в одной точке пространства состояний и, следуя гипотезе Дэвида Дойча о ненарушении эволюционного принципа, нет неоднозначности в выборе состояния в ситуации с СТС с дополнительными данными.

Список рекомендуемой литературы

1. *Everett H.* Relative State Formulation of Quantum Mechanics // Rev. Mod. Phys. 1957. Vol. 29. P. 454.

2. *Herbert N.* FLASH – A superluminal Communicator Based Upon a New Kind of Quantum Measurement // Foundations of Physics. 1982. Vol. 12. P. 1171.

3. *Wootters W.K. and Zurek W.H.* A Single Quantum Cannot Be Cloned // Nature. 1982. Vol. 299. P. 802.

4. *Dieks D.* Communication by EPR Devices // Phys. Lett. A 1982. Vol. 92. P. 271.

5. *Gisin N., Ribordy J., Tittel W., and Zbinden H.* Quantum Cryptography // Rev. Mod. Phys. 2002. Vol. 74. P. 145.

6. *Deutsch D.* Quantum Mechanics Near Closed Timelike Lines // Phys. Rev. D 1991. Vol. 44. P. 3197.

7. *Brun T.A., Harrington J., and Wilde M.* Localized Closed Timelike Curves Can Perfectly Distinguish Quantum States Phys. Rev. Lett. 2009. Vol. 102. P. 210402.

Список используемых сокращений

QM – quantum mechanics
ОТО – общая теория относительности
CTC – closed timelike curve
EPR – Einstein, Podolsky, Rosen
ЭПР – Эйнштейн, Подольский, Розен