МОСКОВСКИЙ ФИЗИКО-ТЕХНИЧЕСКИЙ ИНСТИТУТ
(ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ)

Кафедра философии

РЕФЕРАТ ПО ИСТОРИИ НАУКИ

КВАНТОВАЯ ТЕОРИЯ ИНФОРМАЦИИ

Аспирант — Филиппов Сергей Николаевич

Научный руководитель аспиранта _____ Манько В.И.
подпись

Преподаватель кафедры философии — Храмов О.С.

Москва 2010

Содержание

Введение

История науки как совокупности научного знания во всех его проявлениях (научные теории, гипотезы, экспериментальные факты, технологии, методы, парадоксы, открытые вопросы и нерешенные проблемы) представляет большой интерес не только для сообщества ученых, но и для всего человечества. Кроме того, историю науки следует рассматривать в неразрывной связи с историей человеческого общества и развитием философской мысли ввиду непрерывного взаимовлияния науки и общества. Ретроспектива научного знания (в контексте всего человеческого общества) и ее анализ позволяют не только выявить основные черты и особенности возникновения, периодов роста и упадка, но и подвести предварительные итоги, «извлечь уроки», ощутить методологию науки и способы ее совершенствования, наметить возможные пути дальнейшего развития или упадка, сделать более и менее реалистичные прогнозы. В данной работе предпринимается попытка рассмотреть все эти вопросы для относительно молодой, еще не совсем сформировавшейся, но претендующей на достойное место в «круге наук», дисциплине – квантовой теории информации (КТИ).

Изложение материала построено следующим образом.

Далее во Введении в общих чертах описывается круг проблем и задач, решаемых и рассматриваемых квантовой теорией информации. В главе 1 исследуются истоки «квантового происхождения» КТИ, а также обсуждаются проблемные места квантовой механики, которые затем переросли в злободневные вопросы КТИ. В главе 2 прослеживается информационная направленность КТИ и ее происхождение. В главе 3 производится синтез «квантовой» и «информационной» компонент в проекте «квантовый компьютер». В главе 4 излагаются истоки исследований по квантовой коммуникации. В главе 5 выясняется математическая нагруженность новой дисциплины, и отмечается роль КТИ на развитие математического аппарата. В Заключении дается краткая оценка основным этапам становления КТИ и полученным в рамках КТИ результатам, а также принимается попытка прогнозирования дальнейшего развития.

Хотя точного и общепринятого определения квантовой теории информации пока не существует, можно попытаться обозначить, чем именно этот новый раздел науки занимается. Именно, квантовая теория информации возникла на стыке квантовой механики и теории информации и по сути является результатом обобщения классической теории информации на мир квантовой физики. КТИ пытается ответить на следующий вопрос: «Что происходит, если информация закодирована в состоянии квантовой системы?» Для ответа на поставленный вопрос в первую очередь следует понять, как описывается и чем определяется

«состояние квантовой системы». Казалось бы, общепринятый курс квантовой механики даёт исчерпывающее объяснение тому, что подразумевается под этим словосочетанием, однако, внимательный анализ выявляет множество подводных камней и даже мин.[1] Без сомнений, фарватер «подводной лодки КТИ» очень извилист и непрост, но тем интереснее и актуальнее задачи, благороднее и выше цели. Итак, одним из вопросов, на который пытается ответить КТИ, является *формализм квантовой механики*. Не менее важен и процесс *кодирования* информации, поскольку этот процесс определяет переход от классического представления информации к квантовому. Здесь возникают проблемы организации квантового регистра, его физической реализации[2]. Далее, допустим, что информация закодирована каким-то образом в состоянии некоторой квантовой системы. Хотя кодирование важно само по себе, всё-таки возникают следующие естественные желания:

- Передавать информацию (*квантовая коммуникация и телепортация*);
- Сделать передачу информации по возможности секретной (*квантовая криптография*);
- Обрабатывать данные, решать задачи (*квантовые вычисления, квантовые алгоритмы, квантовые компьютеры*);
- Считывать информацию, содержащуюся в состоянии некой квантовой системы (*проблема измерения*);
- Сохранять информацию (*проблема декогерентизации*[3]).

Подытоживая вышесказанное, можем резюмировать, что квантовая теория информации есть междисциплинарное научное направление, в котором изучаются общие закономерности передачи, хранения и преобразования информации в системах, подчиняющихся законам квантовой механики.

Глава 1. О формализме квантовой механики в свете квантовой теории информации

Актуальность данной главы в тексте реферата как нельзя ярче демонстрирует меткое замечание из книги [11, стр. 7]: «Квантовая теория информации опирается на квантовую механику и поэтому получает в наследство весь букет проблем, связанных с основаниями квантовой механики». Более критическое суждение: «<…> квантовая механики (как физическая теория, а не как математический формализм) – это тяжело больной, но тщательно скрывающий свое заболевание человек» [11, стр. 7]. Автор реферата не совсем согласен с последним замечанием, хотя оно и содержит рациональное зерно, но здесь его

[1] Для иллюстрации этого факта упомянем лишь, что ежегодно уже в течение более десяти лет проводятся международные конференции по основаниям квантовой механики. Как замечает один из постоянных организаторов, «я был свидетелем бурных дебатов, в которых респектабельные профессора превращались в горячих юнцов, которые не лезут в карман за крепким словцом. До прямого рукоприкладства дело не доходило, но было близко к этому» [11, с. 137].

[2] Отметим, что задачи квантовой информатики сильно стимулировали экспериментальные исследования в области нанотехнологий и квантовой оптики (с середины 1990-х гг.). К примеру, для удовлетворения нужд квантовой информатики были разработаны уникальные установки и технологии: ловушки для ионов как в стандартном вакуумном исполнении, так и в твёрдотельном (микрочипы); квантовые электромагнитно-динамические резонаторы (КЭД-резонаторы) с колоссальной добротностью; создание квантовых точек на основе гетероструктур, двумерного электронного газа в других структурах, имплантации одиночных (!) атомов с высокой точностью; создание приборов, чувствительных к индивидуальным спинам электрона и присутствию/отсутствию элементарного заряда (новые типы одноэлектронных транзисторов, квантовых проволок).

[3] В русскоязычной литературе еще не сформировалось общепринятого перевода слова «decoherence», поэтому наряду с «декогерентизацией» можно встретить слово «декогеренция». Мы предпочтительно будем использовать первый вариант.

роль явно преувеличена[4]. «В квантовой механике складывается парадоксальная ситуация: имеется замечательный математический формализм, позволяющий делать предсказания о вероятностном поведении огромных ансамблей квантовых систем. Однако *интерпретация* этого формализма так и остается (уже на протяжении около ста лет) нерешенной проблемой» [11, стр. 8].

Проследим, как развивались основные идеи и трактовки квантовой механики, затем выявим «унаследованные» КТИ проблемы.

Своими корнями квантовая механика уходит в классическую статистическую механику. В литературе зачастую подчеркивается различие между формализмами квантовой и классической механик, здесь же мы попытаемся выявить и подчеркнуть аналогию между формализмами.

Второй закон Ньютона в современной форме записывается в виде обыкновенного дифференциального уравнения второго порядка, связывающего вторую производную координаты и силы, действующие на тело. Если заданы начальное положение тела в пространстве и его начальная скорость, то динамика такой частицы задается траекторий, которая находится как решение задачи Коши. Если сила как функция координаты является достаточно гладкой (с математической точки зрения достаточно, чтобы функция была непрерывно дифференцируема), то задача Коши имеет единственное решение. Это часто трактуется как присущий классической механике *детерминизм*. Стоит особо подчеркнуть, что детерминизм присущ не всем классическим системам. Если поле сил не удовлетворяет условию Липшица (но силы по-прежнему непрерывны), то решение задачи Коши, в общем случае, является неединственным. В этом случае начальные координата и импульс не определяют полностью траектории движения. С необходимостью особое внимание к себе приковывают такие задачи, в которых динамическая система неустойчива. Это сказывается в том, что малая погрешность в определении начального состояния может повлечь колоссальные отклонения траектории. В таком случае детерминизм выступает лишь как математическая абстракция, не имеющая воплощения в реальном мире.

Дальнейшее развитие идей Ньютона воплотилось в гамильтоновой механике, сформулированной в виде системы дифференциальных уравнений первого порядка с использованием функции Гамильтона на фазовом пространстве координат-импульсов. Функция Гамильтона имеет смысл полной энергии, что впоследствии нашло отражение в операторе полной энергии, используемом в квантовой механике. Одним из важных свойств гамильтоновой механики является то обстоятельство, что она *локальна*. При отсутствии взаимодействий в физическом пространстве частицы движутся независимо друг от друга. Если бы динамика была нелокальна, то это привело бы к следующей парадоксальной (с точки зрения классической физики) ситуации, когда несмотря на отсутствие взаимодействий в физическом пространстве, динамики частиц зависят друг от друга. Изменение состояния одной частицы проводило бы, в общем случае, к изменению состояний всех остальных частиц.

Имея дело с ансамблями многого числа частиц, в принципе, нет формальных ограничений для того, чтобы решить систему Гамильтона. Однако даже если абстрагироваться от порождаемых вычислительных трудностях, то не вполне ясно, как использовать информацию о траекториях многих частиц и как визуализировать эту информацию. Более того, представляет трудность предсказательный характер подобного описания. Например, как изменится динамика системы при изменении начальных условий. Поэтому было предложено рассмотреть вероятность нахождения частиц в какой-либо области фазового пространства. Была введена плотность вероятности $\rho(q,p,t)$ обнаружить частицу в области

[4] Продолжая сравнение квантовой механики с человеческим организмом, можно не без доли сарказма сказать, что сама жизнь – неизлечимое смертельное заболевание. Другими словами, квантовая механика – причина проблем самой себя. Последнее утверждение можно рассматривать как некий отголосок гегелевской абсолютной идеи – саморазвивающейся и самой о себе думающей.

фазового пространства (q÷q+Δq,p÷p+Δp) в момент времени t. Динамика плотности задается уравнением Лиувилля.

Одним из важных шагов в развитии классической механики было создание детерминистской модели электромагнитного поля[5]. Заметим, что если ввести новое обозначение: комплексная переменная = напряженность электрического поля + мнимая единица, умноженная на напряженность магнитного поля, то «фазовое пространство электромагнитного поля можно представить как пространство комплекснозначных суммируемых в квадрате функций …» [11, стр. 33].

Итак, «к концу 19 века сложилось впечатление, что с помощью классической механики можно описать все физические процессы[6]. Фундаментальные принципы – детерминизм и локальность – ни разу не подвергались сомнению, не было никаких экспериментальных данных, противоречащих этим принципам. Складывалась изумительно красивая картина Природы [*прим.*: в оригинале «природы» (строчными буквами), автор реферата решил подчеркнуть смысловую нагрузку слова]. Предыдущее состояние определяло последующие. Изменение состояния могло произойти лишь в результате воздействия сил. Для сложных систем, состоящих из подсистем, при отсутствии взаимодействия между системами изменение состояния одной системы не могло вызвать изменения состояния других систем. Впоследствии эти взгляды получили название локального реализма» [11, стр. 30].

Теперь мы вплотную подошли к рождению новой теории – квантовой механики. «Как известно, первые шаги квантовой механики были робки и неосознанны. Ни о каком изменении философских оснований современной науки или создании принципиально нового математического описания природы и речи не шло. Все началось с графика, на котором был всплеск, который никак не удавалось объяснить в рамках классической статистической механики. Это экспериментальный график излучения абсолютно черного тела. Планк показал, что всплеск можно получить (в рамках классической статистической механики!!!), если считать, что энергия не непрерывна, а дискретна. Чисто формально энергетическое пространство было разбито на ячейки. Величина ячейки зависела от частоты колебаний электромагнитного поля. <…> Параметр h [постоянная Планка – прим. автора реферата] перестал быть просто параметром дискретизации и наполнился реальным содержанием только после работы Эйнштейна, 1905 г., в которой утверждалось, что передача электромагнитной энергии может происходить только порциями. <…> В принципе передача энергии порциями определенного размера отнюдь не влечет представления о «квантованной энергии». Энергия вполне может быть непрерывной, но передаваться порциями. В настоящее время Эйнштейну часто приписывается идея о корпускуле света – фотоне. Однако Эйнштейн никогда не рассматривал фотон как частицу. Для него фотон был порцией передачи энергии и не более. Итак, передача энергии дискретными порциями объясняет экспериментальные данные об излучении абсолютно черного тела (а также фотоэффект) и отнюдь не противоречит классической механике. <…> Допустим, что имеются какие-то дополнительные связи, которые запрещают системе двигаться по произвольной траектории, причем остается лишь дискретное множество «разрешенных траекторий» <…>. Энергия постоянна на каждой из этих траекторий. Получаем систему с дискретными уровнями энергии <…>. Дискретность обмена энергией фотонообразными порциями является следствием дискретной структуры множества орбит. С помощью такой схемы объяснял дискретный обмен энергией Нильс Бор, в частности в модели атома Бора. Разрешенные орбиты получались из специальной системы связей, «условия квантования». Основная

[5] Примечательно, что уравнения Максвелла не инвариантны по отношению к преобразованиям Галилея, однако инвариантны по отношению к преобразованиям Лоренца, предвещая тем самым теорию относительности. Аналогия подходов специальной теории относительности и томографического представления квантовой механики см. далее.

[6] «Забавно, что, когда Макс Планк после окончания гимназии пришел подавать документы в университет на физический факультет, профессор, принимавший документы, пытался его отговорить. По его мнению, развитие физики подошло к концу и было бы глупо погубить свою карьеру.» [11, стр. 30]

проблема этого подхода была в том, что условия квантования орбит не имели естественного объяснения в формализме классической механики. Они подгонялись под наблюдаемые спектры излучения» [11, стр. 34]. Нельзя в полной мере согласиться с последним цитируемым утверждением, поскольку *вся* серия Бальмера в спектре атома водорода была выражена через *одну* характеристическую константу, выражающейся через заряд и массу электрона, а также постоянную Планка. В связи с этим нельзя не упомянуть о принципе красоты. «В самой организации и формировании знаний происходит их сопоставление, выбор той или иной математической формулы, уравнения, содержательных концептов. При этом исследователь и в выборе знаний, и в ходе их построения, организации и функционировании, старается с помощью «малого» объяснить «многое» - большее число теоретических положений, событий, фактов и т.д. А это есть не что иное, кок ориентация на выполнение требования простоты. Так, например, при построении анализируемой нами квантово-механической теории Гейзенберг неоднократно проводил мысль о том, что он характеризует научную гипотезу и теоретическую систему как простую, если она позволяет комбинировать множество самых различных явлений, которые в каком-то аспекте выглядят теми же самыми и связанными. Такие системы, на его взгляд, более осмысленны и информативны, более гармоничны и *красивы*, так как действие по выполнению требования простоты связано с процессом подготовки и уменьшения числа вводимых аксиом, определений, ограничений, увеличением компактности и информативности формирующего знания.»[4, стр.209]

Вспомнив о Гейзенберге, мы тем самым подошли к матричной форме изложения квантовой механики, лежащей в основе копенгагенской интерпретации. Гейзенберг пытался разработать математический формализм для описания явлений, отражающих реально происходящие события атомного спектра излучения. «Первоначально Гейзенберг убежден, что самостоятельно разработал эту связь через созданную им «группу величин», что было описано в работе «О квантово-механическом переистолковании кинематических и механических отношений», опубликованной в 1925 г. Более зрелый и опытный Борн[7] в предложенном математическом аппарате Гейзенберга узнает уже известное в математике матричное исчисление» [4, стр. 202].

Альтернативой некоммутативному операторному представлению наблюдаемых в формализме Гейзенберга-Дирака-фон Неймана является волновая трактовка, опирающаяся на уравнение Шредингера. Здесь мы сделаем весьма важное замечание. «Механика Шрёдингера может в принципе (при желании) рассматриваться как естественное развитие теории броуновского движения» [11, с. 37]. В самом деле, в процессе броуновского движения молекулы имеют недифференцируемые траектории. «Здесь нельзя определить значение p(t) [импульс частиц – прим. автора реферата] для конкретного момента времени t. Поэтому бессмысленно пытаться рассмотреть распределение ρ(q,p,t) на фазовом пространстве. В то же время, если траектории частиц q(t) являются непрерывными функциями времени, то распределение на конфигурационном пространстве вполне определено. Возникает задача нахождения уравнения (которое должно будет заменить уравнение Лиувилля), описывающего эволюцию распределения ρ(q,t) [маргинального распределения, зависящего только от координаты и времени, но не от импульса – прим. автора реферата]» [11, с. 38]. Уравнения подобного вида были разработаны Эйнштейном, Смолуховским, Башилье. Для более общих диффузионных процессов уравнения для плотности ρ(q,t) были получены А.Н. Колмогоровым. Встает вопрос: можно ли написать уравнение не только для плотности вероятностей, но для траекторий частиц? Оказывается, это можно сделать с помощью стохастического дифференциального уравнения, в котором появляется случайный параметр ω и активно используется стохастический интеграл Ито[8]. «Таким образом, хотя гамильтонова механика уже неприменима, классическое описание с помощью траекторий по-прежнему возможно. Конечно, траектория q(t, ω) зависит от

[7] Именно Борн ввел термин «квантовая механика» в 1924 г.
[8] Введен в 40-е годы

случайного параметра ω и знание начального значения q(t=0, ω) не определяет траекторию однозначно. Таким образом, детерминизма в классическом его понимании уже нет. Имеет место лишь весьма ослабленный (стохастический) детерминизм: знание ω задает траекторию. Можно сказать, что стохастичность – это следствие нашего незнания» [11, с. 41]. Итак, еще раз обозначим идею рассуждения этого параграфа. Роль и значение уравнения Шредингера не принижается ни в коей мере. Кроме того, аксиоматика теории вероятностей была создана только в 1930-е годы, а стохастический интеграл Ито в 1940-х гг. Здесь лишь подчеркиваются *предпосылки*, схожие проблемы, общность подхода. Блистательный ум Шредингера, возможно, имплицитно оперировал понятиями теории вероятностей, физической картиной распределения ρ(q,t). Здесь мы подчеркиваем сходство, а не отличие классического и квантового описания. В самом деле, когда возникла задача описания динамики микроскопических частиц, «было бы естественно предположить, что их динамика уж никак не может быть проще, чем динамика броуновской частицы. Если броуновскую частицу так швыряет от столкновений, что ее импульс не определен в классическом смысле, то уж «квантовые частицы» должно швырять из стороны в сторону не меньше. Причем, в силу их микроскопических размеров, сталкиваться они могут не только друг с другом, но и с полями, например, электромагнитным полем. <…> Поэтому естественно предположить, что электрон, так же как и броуновская частица, имеет недифференцируемые траектории. Следует искать плотность распределения ρ(q,t) не на фазовом, а на конфигурационном пространстве. <…> Таким образом можно интерпретировать механику Шредингера. Он нашел динамику ρ(q,t) для микрочастиц. Единственный трюк состоял в том, что плотность распределения ρ(q,t) должна была представляться в виде квадрата модуля некоторой комплекснозначной функции ψ(q,t), а именно волновой функции. Это знаменитое правило Борна. И уравнение было получено не для ρ(q,t), а для ψ(q,t)» [11, с. 41]. С позиции сегодняшнего времени вполне резонно поставить вопрос: можно ли построить случайный процесс q(t, ω), реализующий траектории микрочастиц, для которого плотность вероятности ρ(q,t) вычислялась бы по правилу Борна? Согласно копенгагенской интерпретации, «уравнение Шредингера, в отличие от уравнения Колмогорова, не может быть основано на какой либо динамике для траекторий (ни в фазовом, ни в конфигурационном пространствах). Микрочастицы не имеют никаких траекторий в физическом пространстве. Формула $\rho(q,t)=|\psi(q,t)|^2$, вероятностный постулат Борна, дает отнюдь не вероятность того, что частица *находится* в точке q. На самом деле это вероятность *обнаружить* частицу в этой точке в результате измерения ее координаты. С одной стороны, частицы существуют, так как мы собираемся производить измерения над ними. С другой стороны, при копенгагенской интерпретации частицы сами по себе не имеют даже координаты в физическом пространстве. Следует отметить, что в первоначальной интерпретации Шредингера эта проблема не возникала. Интерпретация волновой функции ψ(q,t) как плотности вероятностей возникла позднее. Фактически она была навязана Шредингеру. Вначале он рассматривал ψ(q,t) как настоящую физическую волну, причем $\rho(q,t)=|\psi(q,t)|^2$ интерпретировалось (для электрона) как плотность заряда. Итак, для Шредингера «квантовая механика» была волновой теорией, которая шла на замену классической корпускулярной теории» [11, с. 43]. Положительный ответ на поставленный выше вопрос был получен лишь в 1960-е годы Нельсоном и получил название стохастической механики Нельсона. «Он показал, что для «квантовой частицы» можно построить случайный процесс q(t, ω), описывающий движение частицы как решение стохастического дифференциального уравнения. Картина движения очень интуитивна. Маленькая частица движется в случайной среде (поле). Взаимодействие со средой создает весьма сложные траектории. Но плотность вероятности ρ(q,t) может быть представлена в виде $\rho(q,t)=|\psi(q,t)|^2$, где комплекснозначная функция ψ (q,t) *удовлетворяет* решению Шредингера» [11, с. 44].

Таким образом, мы вплотную подошли к различным интерпретациям понятия «состояние системы» и к проблемам, которые они порождают.

1) Волновая интерпретация. Согласно Шредингеру состояние задается волновой функцией, рассматриваемой как физическая волна. Одна из проблем этой интерпретации – нелокальность. Волна для сложной системы «живет» в многомерном пространстве, а не в обычном трехмерном пространстве.

2) Копенгагенская интерпретация. Вектор состояния ψ дает наиболее полное описание состояния квантовой системы. При этом не предполагается, что система – это волна. Однако при этом и не предполагается, что система – это частица. Это проявление принципа дополнительности Бора. В отличие от шредингеровской картины здесь с самого начала и не предполагается, что исследуемый объект движется в физическом трехмерном пространстве. Согласно этой интерпретации, квантовая механика не описывает природу «как она есть сама по себе», она лишь описывает результаты наших измерений. Укреплению позиций копенгагенской трактовки способствовал личный авторитет Бора, а также теоремы[9] невозможности, разработанные фон Нейманом. Не вдаваясь в подробности этих теорем, заметим, что каждая такая теорема основывается на целом ряде условий, и показывается, что при этих условиях невозможно представить квантовую модель в виде образа классической статистической модели. «Однако некоторые из этих условий могут быть весьма сомнительными с физической точки зрения» [11, с. 12].

3) Ансамбль-интерпретация. Следуя Эйнштейну, считается, что квантовая механика является некой специальной моделью классической статистической механики. Волновая функция приобретает физический смысл лишь через плотность вероятностей $\rho(q,t)=|\psi\ (q,t)|^2$. «В этом подходе квантовая механика не является окончательной теорией процессов в микромире. Как писали Эйнштейн, Подольский и Розен, она неполна и может быть дополнена теорией, описывающей траектории квантовых систем (например, в духе стохастической механики Нельсона)» [11, с. 49]. Проблемы с нелокальностью не возникает, однако основной проблемой ансамбль-интерпретации стало объяснение квантовой интерференции. «Поскольку интерференция вероятностей не появлялась в колмогоровской модели и других классических моделях теории вероятностей, а статистическая механика основана на классической теории вероятностей, то считалось, что классической статистическое описание неприменимо к интерференции вероятностей» [11, с. 49]. Недавно (в 2003 г.) Хренникову удалось получить интерференцию вероятностей в рамках классической теории вероятностей. Также ему удалось показать, что другая проблема ансамбль интерпретации – нарушение неравенства Белла[10] – также разрешатся в подходе, получившем название предквантовой классической статистической теории поля.

4) Теория ведущей волны де Бройля - Бома (современный вариант известен как бомовская механика). Де Бройль предложил скомбинировать ансамбль-интерпретацию и волновую интерпретацию (в историческом контексте де Бройль связал с каждой частицей волну еще до вывода уравнения Шредингера). «Де Бройль мечтал получить одно уравнение, в котором решение состояло бы из двух частей: гладкая часть описывает волну, а сингулярная - частицу» [11, с. 51]. Хорошей картиной к иллюстрации данного подхода был бы шарик, плавающий на волне.

5) Учет температурных флуктуаций в квантовой физике привел к модифицированному описанию квантового состояния матрицей плотности, введенной Ландау и фон Нейманом в 1927 г. Диагональные элементы матрицы плотности

[9] Как отмечается в [11, с. 11], в оригинальном немецком издании использовалось вовсе не слово «теорема», а «ansatz». «Ansatz» - *нем.* догадка, которая затем подтверждается своими результатами; установление исходных уравнений, которые описывают математическую или физическую проблему. Самый простой пример «возникновения» анзаца – решение текстовых задач, где сначала необходимо записать основную идею в виде некоторого соотношения, рассмотрение которого приводит в конечном счете к решению задачи [перевод и комментарий автора реферата].

[10] Мы вернемся к обсуждению неравенств Белла в разделе, посвященном коммуникации и криптографии.

трактуются как плотность вероятности. «Следует сказать, что интуитивное восприятие матрицы плотности еще более затруднительно, чем волновой функции. Состояние описывается полностью, если заданы не только диагональные элементы матрицы плотности, имеющие вероятностную интерпретацию, но и недиагональные элементы, такой интерпретации не имеющие. Таким образом, вывод, сделанный научным сообществом и существовавший до совсем недавнего времени, заключался в том, что между классическим и квантовым описанием состояния объекта существует непреодолимое различие, т.е. в классической статистической механике состояние задается плотностью вероятности, а в квантовой механике такое описание невозможно, причем невозможно принципиально в связи с соотношением неопределенностей.»[5, стр. 80].

6) В 1932 г. Вигнером была предпринята еще одна попытка сблизить классическую и квантовую механику. Вот что пишет по этому поводу В.И. Манько: «Касаясь истории вопроса, заметим, что с самого начала развития квантовой механики предпринимались попытки приблизить (или свести) описание состояния интуитивно трудно воспринимаемой волновой функцией (или матрицей плотности) к более понятным классическим образам, а именно, к каким-то траекториям или каким-то плотностям вероятности. Так, с целью найти вероятность, описывающую квантовое состояние, Ю. Вигнер в 1932 г. ввел функцию двух переменных W(q,p), называемую функцией Вигнера, аргументы которой трактуются как положение и импульс объекта. Функция Вигнера связана с матрицей плотности обратимым преобразованием Фурье. Тем самым, зная функцию Вигнера, мы знаем и матрицу плотности. Для состояний с волновой функцией мы по функции Вигнера восстанавливаем волновую функцию с точностью до несущественного фазового множителя. Функция Вигнера действительна, а не комплексна. При этом интеграл от нее по импульсу точно равен плотности вероятности в импульсном пространстве объекта. Точно такими же свойствами обладает положительная плотность вероятности в классической статистике. Однако наряду с этими «хорошими» свойствами у функции Вигнера имеется «дефект». А именно, будучи действительной, эта функция для некоторых состояний и в некоторых областях фазового пространства может принимать отрицательные значения. По этой причине ее никак нельзя интерпретировать как обычную вероятность, обязанную всегда быть неотрицательной. Одна из причин неудачи попытки Вигнера ввести классическую плотность вероятности лежит в несовместимости существования такой плотности вероятности с соотношением неопределенностей Гейзенберга. Для существования совместной функции распределения двух случайных величин необходима одновременная измеримость этих величин, а как мы уже отмечали, координата и импульс в квантовой механике одновременно неизмеримы. Поэтому предложенные позже и обладающие свойством неотрицательности модификации функции Вигнера (например, функция Хусими) также не являются плотностями вероятности. Поэтому их называют «квазивероятностями»»[5, стр.81].

7) В конце 1940-х гг. Р. Фейнману удалось построить выражение (интеграл по траекториям) для комплексной амплитуды вероятностей перехода между квантовыми состояниями, используя классическое действие и классические траектории, как реализуемые, так и нереализуемые. Тем самым амплитуда вероятности была связана с классической механикой явной формулой, содержащей классический лагранжиан. Позднее в 1958 г. Г.В. Рязанов дал для интеграла по траекториям другое и именно вероятностное представление, но с использованием отрицательных вероятностей, как и в случае функции Вигнера.

8) «В 1996-1997 гг. итало-российской группой исследователей[11] были опубликованы первые работы, в которых показано, что квантовое состояние может быть полностью задано положительной плотностью вероятности. Как ни странно, методика нахождения ключа к появлению такой возможности аналогична методике построения СТО[12]. В СТО все ее необычные предсказания (уменьшение длины движущегося объекта, замедление хода часов и т.п.) объясняются рассмотрением поведения физических тел в разных системах отсчета, движущихся с большими скоростями. Разумеется, системы отсчета в СТО понимаются как системы отсчета в обычном пространстве-времени, т.е. оси координат трактуются как оси, на которых откладываются время события и положение в пространстве, где это событие происходит. Оказалось, что в квантовой механике, включая все ее необычные предсказания, возможность построения вероятности, полностью задающей квантовое состояние, связана с рассмотрением положения объекта в ансамбле разных систем отсчета, но не в обычном, а в фазовом пространстве. В классической механике это означает, что на осях рассматриваемых систем отсчета откладываются координаты и импульсы, которыми в данный момент времени описывается объект. Если в СТО разные движущиеся системы отсчета связаны преобразованием Лоренца – гиперболическим поворотом на плоскости координата-время (одномерный случай), то в квантовой механике системы отсчета, о которых идет речь, связаны друг с другом не гиперболическим, а обычным поворотом на плоскости координата-импульс (фазовая плоскость).<…> Странным образом оказалось, что в квантовой механике роль и использование различных систем отсчета в фазовом пространстве частиц, хорошо изученные в классической статистике, долгое время оставались в тени. Это, по всей вероятности, связано с невозможностью измерить в квантовой области одновременно к координату, и импульс частицы в силу соотношения неопределенностей. По-видимому, соотношение неопределенностей координата импульс служило «психологическим тормозом», мешающим продолжить анализ роли различных систем отсчета в фазовом пространстве, хорошо развитый в классической механике, на квантовую область. Именно такой анализ дал возможность найти *новое представление квантовой механики, в котором квантовое состояние задается вероятностью, как и в классической статистике* [курсив автора реферата]. <…> Встает вопрос: как же удалось обойти трудность с соотношением неопределенностей Гейзенберга в новой формулировке обычной квантовой механики с использованием вероятности вместо волновой функции? Эта вероятность названа томографической вероятностью, а новая формулировка квантовой механики – ее «вероятностным представлением». Именно томографическая вероятность (томограмма) задает квантовое состояние полностью и содержит об этом состоянии столько же информации, сколько содержат волновая функция и матрица плотности, а также функция Вигнера. Дело в том, что повороты системы отсчета в фазовом пространстве с точки зрения математического формализма эквиваленты использованию для функции Вигнера известного преобразования Радона. Это самое преобразование используется в медицинских томографах (отсюда и взято название) для реконструкции реальной пространственной плотности интересующего медиков новообразования в теле пациента по экспериментальным томограммам. В квантовой механике роль измеряемого объекта играет функция Вигнера, которая преобразованием Радона связана с «томограммой» $w(X,\Theta)$, т.е. плотностью вероятности координаты X в повернутой на угол Θ системе отсчета в фазовом пространстве: <…> $X = q \cos\Theta + p \sin\Theta$. <…>Замечательным обстоятельством является обратимость написанных формул, т.е. знание томограммы позволяет вычислить по ней и функцию Вигнера и волновую функцию (с точностью до

[11] С. Манчини, В.И. Манько, П. Томбези.
[12] СТО - специальная теория относительности

несущественного постоянного фазового множителя). Как мы видим, томогрфическая вероятность, играющая ключевую роль в новой формулировке квантовой механики, содержит только координату X и угол Θ, задающий систему отсчета, в которой измеряется координата. При этом импульс (сопряженная координате переменная) в томограмму не входит. Измерение квантовой томограммы, определяющей волновую функцию, сводится к измерению только положения (координаты) объекта. Измерение импульса не является необходимым, а тем самым существование томографической вероятности прекрасно гармонирует с соотношением неопределенностей Гейзенберга»[5, стр. 81-84].

Подытоживая вышесказанное, можем констатировать, что в процессе развития квантовой теории так и не сложилось общепринятой точки зрения по поводу того, что считать «состоянием системы» и как его описывать. Здесь мы постарались проиллюстрировать, что есть много «за» и «против» для каждого из приведенных выше описаний. Читатель может упрекнуть автора, что мы отвлеклись от основной линии изложения. Хотя я и признаю, что для получения некоторых предсказаний поведения квантовых систем и не требуется иметь под рукой «словаря интерпретаций», что практические результаты порой гораздо важнее описания, но если в ходе строительства «здания квантовой теории информации» сэкономить на фундаменте, то результаты могут быть вполне печальными. Так или иначе, но в физике наибольшее распространение получила копенгагенская трактовка квантовой механики. Переходя от фундамента к первому этажу КТИ, отметим, что «проблема суперпозиции состояний трансформируется в проблему квантового параллелизма для квантовых компьютеров. Проблема полноты квантовой механики – в проблему квантовой нелокальности (действие на расстоянии)» [11, с. 9]. Первая проблема обсуждается в главе «Квантовые вычисления», вторая – в главе «Квантовая коммуникация». Однако прежде чем переходить к этим разделам, необходимо коснуться другого «кита» КТИ – теорию информации.

Глава 2. Теория информации: от классической к квантовой

«Цифровая революция началась в 1948 г., когда был изобретен транзистор, открывший дорогу миниатюризации электронных устройств и радикальному снижению материальных и энергетических затрат на создание систем обработки информации (hardware). В том же году был опубликован основополагающий труд американского инженера-математика Клода Шеннона, отца теории информации, обосновавшей переход к цифровому представлению и цифровой обработке данных (software). Еще раньше появились работы нашего ученого В.А. Котельникова по основам помехоустойчивой связи, которые предвосхитили некоторые идеи Шеннона.

<…> Любая схема передачи информации состоит из передатчика (возможно, включающего в себя устройство, кодирующее сообщения), канала связи и, наконец, приемника (вместе с возможным декодирующим устройством). Обычно все три названные компоненты описываются на языке классической физики и статистики. Посылаемый передатчиком сигнал (для простоты 0 или 1) подвергается в канале случайным помехам и может исказиться. Поэтому сигнал на выходе приемника не обязательно совпадает с посланным сигналом, а качество связи характеризуется вероятностью ошибки. Обычно требуется разработать такую конструкцию приемника, которая обеспечивала бы оптимальное обнаружение или оценивание посланного сигнала для заданного канала и метода передачи. Подобные задачи решаются методами теории статистических решений.

<…> Сильной и в то же время слабой стороной классической теории информации, обеспечивающей ее универсальность, стало абстрагирование от содержания и природы передаваемых данных. Такую теорию интересуют лишь два аспекта: количество передаваемой информации и качество передачи. Названные характеристики связаны

обратной зависимостью: чем точнее мы хотим передать сообщение при наличии помех в канале связи, тем более замедляется передача. Особое внимание в теории информации уделяется оптимальным характеристикам, таким как пропускная способность канала, т.е. максимально возможная скорость передачи при использовании кодирования-декодирования, обеспечивающего исправление ошибок, вызванных помехами» [9, с. 69].

Предвосхищая дальнейшие повествование А.С. Холево, приведем основной тезис: информация физична. В связи с этим важным заключением нельзя не упомянуть об онтологической проблеме информации. Ю.И. Семенов считает, что информация объектальна и существует въинобне[13], т.е. существует лишь в чём-то и через что-то. Другими словами, обязательно существует некий физический носитель информации. На строго поставленный вопрос «существует ли информация сама по себе?» вполне разумным ответом был бы «и да, и нет». «Да», поскольку мы не можем отрицать наличия информации, ее хранения, передачи, обработки и т.д., с чем мы ежедневно сталкиваемся даже в нашей повседневной жизни. Мы знаем, что информация имеет большое значение и может существенно повлиять на ход событий. Информация представляет собой порядок, упорядочивание элементов множества, она существует независимо от сознания людей. С другой стороны, ответ «нет» тоже имеет рациональное зерно. Можно ли «потрогать, пощупать» эту пресловутую информацию? Мне наиболее близок по духу следующий ответ: «информация существует объективно, но сама по себе не является материальной, она записана на материальном носителе. Она существует только через что-то и в чем-то (= въинобне), объектально={объективно, но не материально само по себе}.

«Один из пионеров физической теории информации Рольф Ландауэр, долгие годы проработавший в IBM, утверждал, что информация физична, и отвлекаясь от ее физической природы, исследователь делает далеко не всегда оправданное допущение. Фундаментальный носитель информации — это электромагнитное поле, например в форме видимого света, либо радиоволны. В обычных условиях помехи при передаче сигнала обусловлены хаотическим поведением квантов поля (фотонов), которое имеет тепловую природу. Оказывается, снижение температуры до абсолютного нуля не приводит к полному исчезновению шума: на первый план выходят так называемые вакуумные флуктуации, обусловленные квантовой природой излучения. Квантовые свойства света особенно ярко проявляются в когерентном излучении лазера, которое отличается от излучения естественного теплового источника так же, как упорядоченная колонна солдат отличается от пестрой ярмарочной толпы. Уже в 1950-х гг. ученые задумались о фундаментальных квантовомеханических пределах точности и скорости передачи информации. Дальнейшее развитие информационных технологий, достижения квантовой оптики, электроники и супрамолекулярной химии, исследующей кибернетические свойства высокомолекулярных соединений, заставляет предположить, что в скором будущем такие ограничения станут главным препятствием для дальнейшей экстраполяции существующих технологий и принципов обработки информации» [9, с. 69].

Таким образом, в течение 1950-1980 гг. был пройден начальный этап становления информационной компоненты КТИ, а именно, основное внимание уделялось выяснению фундаментальных ограничений на возможность передачи и обработки информации, обусловленных квантовомеханической природой ее носителя. Однако, не все на этом пути было так гладко. Как уже упоминалось выше, квантовая механика «варилась в собственном соку». К указанному периоду времени квантовая механика верно служила физическому сообществу, которое в свою очередь отошло от дебатов по основаниям и перешло к разработке технического аппарата. Надо отметить, что на этом пути были достигнуты колоссальные успехи. И все-таки назрела необходимость объединения теории информации и квантовомеханических рассмотрений. «Чтобы облечь качественные выводы физиков в точную форму, потребовался синтез математических идей теории информации и квантовой

[13] От слова «въинобытие», введенного Ю.И. Семеновым.

механики. В 1960-х гг. уже существовали квантовая статистическая механика и квантовая теория поля, однако эти дисциплины нацелены на иной круг задач, связанных с динамикой квантовых систем. Так, в статистической механике возникает и широко используется ближайший родственник информации — энтропия, однако она выступает там лишь как термодинамическая характеристика. Информационный смысл квантовой энтропии был прояснен в работе Бена Шумахера, посвященной квантовому сжатию данных и опубликованной в Physical Review в 1995 г. Ближе всего к потребностям еще не родившейся квантовой теории информации была теория квантового измерения, над которой работал Джон фон Нейман. Однако она нуждалась в существенном усовершенствовании и развитии

Исторически квантовая теория информации зародилась при рассмотрении фундаментальных квантовомеханических ограничений. Простейшим из них является известное с 1920-х гг. соотношение неопределенностей Гейзенберга. В 1970-е гг. были установлены более тонкие математические факты, такие как энтропийное неравенство, ограничивающее сверху количество информации, которое может быть передано носителем, подчиняющимся законам квантовой механики (например, излучением лазера). Однако в 1980-1990-е гг. ученые пришли к выводу, что квантовая теория не только вводит свои ограничения, но и открывает принципиально новые возможности, такие как квантовая телепортация и другие эффективные коммуникационные протоколы, физически стойкие протоколы квантовой криптографии, эффективные алгоритмы для решения трудных вычислительных задач и др. Идеи эти появились в результате логического развития аппарата квантовой теории, снабженного *статистической интерпретацией*, а если принять, что квантовая теория и ее минимальная интерпретация имеют неограниченную применимость, то нет оснований сомневаться и в принципиальной возможности новых эффективных приложений квантовой теории» [9, с. 71].

Здесь, под статистической интерпретацией подразумевается выполнение одного минимального требования – правила Борна[14], поэтому ее также называют «минимальной». Данная интерпретация «опирается только на возможную в принципе статистику квантовых измерений и не привлекает специальных допущений о механизме возникновения этой статистики. Статистическая интерпретация настолько органично сплавлена с математической структурой квантовой теории, что возникает как бы сама собой. Те объекты гильбертова пространства, которые ранее казались чисто математическими абстракциями, благодаря статистической интерпретации становятся двойниками физических идей и понятий. Так произошло с упомянутыми выше переполненными системами и вероятностными операторно-значными мерами, так же произошло и с абстрактным понятием вполне положительного отображения из теории операторных алгебр, которое оказалось адекватной математической моделью квантового канала с шумом» [9, с. 71].

В 1980-1990 гг. появляются идеи квантовых вычислений, квантовой криптографии и новых коммуникационных протоколов. Это стало возможным благодаря ломке взглядов на квантовую природу. Если раньше основное внимание уделялось ограничениям, накладываемым квантовым характером Природы, то впоследствии взгляды устремились к новым возможностям, заключенным в уникальных квантовых свойствах: запутанность[15] квантовых состояний, квантовый параллелизм и дополнительность между измерением и возмущением.

«*Дополнительность* означает наличие таких свойств одного и того же объекта, которые принципиально недоступны совместному наблюдению. Различные физические измерения

[14] Подобно данной ссылке, впервые постулат Борна $P(A=\lambda_j) = |\langle\psi \mid \psi_j\rangle|^2$ появился в его работе в виде сноски. Причем первоначально в нем содержалось абсолютное значение скалярного произведения, а не квадрат абсолютного значения. Здесь A – получаемое на эксперименте значение наблюдаемой, $\{ \lambda_j \}$ – собственные значения соответствующего эрмитова оператора $\hat{A}$, $| \psi_j \rangle$ - отвечающие этим собственным значениям собственные векторы, $| \psi \rangle$ - вектор состояния системы.

[15] Данный термин более или менее устоялся в русскоязычной литературе, однако наряду с данным словом употребляется также (в некотором отношении даже более корректное) слово «сцепленность». Оба слова являются грубым переводом английского «entanglement».

микрообъектов осуществляются разными макроскопическими экспериментальными установками, каждая из которых предполагает сложную и специфичную организацию пространственно-временной среды. Способы такой организации, отвечающие разным наблюдаемым свойствам, могут быть взаимно исключающими, т.е. дополнительными. На языке математики взаимно дополнительные величины, такие как координата и импульс, электрическое и магнитное поля, компоненты спина, изображаются неперестановочными (некоммутирующими) операторами. Для них имеют место соотношения неопределенностей, запрещающие точную совместную измеримость, так что именно дополнительность ответственна за специфические ограничения информационного характера. Дополнительность также приводит к тому, что состояния квантовой системы не могут быть заданы простым перечислением свойств, т.е. точкой в каком-либо фазовом пространстве. Вместо этого состояния описываются векторами в некотором линейном (гильбертовом) пространстве H, причем всякая суперпозиция (линейная комбинация) векторов также задает состояние.

Новые необычные возможности квантовых систем, как правило, связаны со *сцепленностью* (entanglement; в русской литературе используется также перевод «*запутанность*», «*перепутанность*»). В ее основе лежат необычные свойства составных квантовых систем, которые описываются тензорным (а не декартовым, как в классической механике)[16] произведением $H_A \otimes H_B$ пространств подсистем. В силу принципа суперпозиции пространство составной системы AB наряду с векторами-произведениями $\psi_A \otimes \psi_B$ должно содержать и всевозможные их линейные комбинации. Состояния составной системы, задаваемые векторами-произведениями, называются несцепленными, а все прочие — сцепленными. Сцепленность представляет собой квантовое свойство, отчасти родственное классической коррелированности, однако к ней не сводящееся (в физике говорят о корреляциях Эйнштейна-Подольского-Розена). Сцепленные состояния — не редкость в квантовой физике: обычно они возникают в результате взаимодействия или распада квантовых систем. Однако квантовая теория не исключает возможности сцепленного состояния для пары частиц, которые, однажды провзаимодействовав, разлетелись на макроскопическое расстояние. На необычные «телепатические» свойства такой пары и указали в свое время Эйнштейн, Подольский и Розен. Недавние эксперименты подтверждают возможность искусственного создания внутренней сцепленности фотонов и даже массивных микрочастиц на расстояниях порядка нескольких метров, хотя такое явление никогда не наблюдается в естественных условиях и противно самой природе классического макроскопического мира. Тот способ описания окружающего мира, который лежит в основе доквантовых представлений о пространстве-времени, получил название «локальный реализм». На чем бы ни основывалось объединение квантовой механики и общей теории относительности — на некоммутативной геометрии, теории струн, нелинейной квантовой механике, траекторных или иных подходах — оно должно будет разрешить противоречие между квантовой сцепленностью и локальным реализмом» [9, с. 73].

---

[16] В многих книгах данное утверждение возводится в ранг постулата, хотя и есть разумные аргументы в пользу такого предположения. Важность этого утверждения хорошо подчеркивается следующими математическими формулами. Для двух *классических* частиц состояние описывалось бы декартовым произведением $L_2(R^3) \times L_2(R^3)$, где $L_2(R^3)$ – множество интегрируемых в квадрате непрерывно дифференцируемых функций. Для двух *квантовых* частиц состояние задается тензорным произведением $L_2(R^3) \otimes L_2(R^3) \equiv L_2(R^3 \times R^3) = L_2(R^6)$. «Использование тензорного произведения вместо декартова для описания сложных систем – это одна из загадок квантовой теории. Именно это свойство квантовых систем влечет экспоненциальное возрастание вычислительных возможностей квантовых компьютеров по сравнению с классическими. Рассмотрим m квантовых битов, каждый из которых описывается гильбертовым пространством состояний $H_2 = C^2$. Тогда система из m квантовых битов описывается пространством $H_{2*2*2*\ldots*2} = C^2 \otimes C^2 \otimes C^2 \otimes \ldots \otimes C^2$. Здесь $\dim H_{2*2*2*\ldots*2} = 2^m$, а размерность пространства состояний сложной классической системы была бы 2m» [11, стр. 93].

Глава 3. Квантовые вычисления

Идея квантовых вычислений была, по-видимому, впервые высказана[17] Маниным в 1980 г. в его книге «Вычислимое и невычислимое». Эта идея стала активно обсуждаться в научном сообществе после знаменитой лекции Фейнмана «Моделирование физики на компьютерах», прочитанной в 1982г.[18] Вот отрывок из его рассуждений: «Правила моделирования, которые я бы хотел иметь, — такие, что число элементов компьютера, необходимое для моделирования большой физической системы, было бы пропорционально только пространственно-временному объему физической системы. Я не хочу иметь взрыв. То есть я хочу объяснить эту физику, я могу сделать это точно, и мне нужен компьютер определенного размера. Если удвоение объема пространства-времени означает, что мне понадобится *экспоненциально* увеличенный компьютер, то я посчитаю, что это против правил. (Я создаю правила, мне это позволено.) <…> Теперь я перехожу к вопросу, как мы можем моделировать на компьютере — универсальном автомате или что-то в этом роде — квантовомеханические эффекты. (Обычная формулировка — квантовая механика имеет некоторый тип дифференциального уравнения для функции ψ). Если у вас одна частица, ψ есть функция x и t, и это дифференциальное уравнение может быть смоделировано так же, как мое вероятностное уравнение <…>. Здесь все в порядке, и есть люди, которые сделали маленькие компьютеры, которые моделируют уравнение Шредингера для одной частицы. Но полное описание квантовой механики для большой системы с R частицами дается функцией $\psi(x_1, x_2, ..., x_R, t)$, которую мы называем амплитудой для нахождения частиц $x_1, x_2, ..., x_R$ и следовательно, поскольку переменных слишком много, ее *нельзя моделировать* обычным компьютером с числом элементов, пропорциональным R или N. Мы имеем те же трудности с вероятностями в классической физике. И, следовательно, проблема заключается в том, как можно моделировать квантовую механику.<…> Оказывается, насколько я могу судить, вы можете моделировать это с помощью квантовой системы из элементов квантового компьютера. Это не машина Тьюринга, а машина другого типа. Если мы не будем принимать во внимание непрерывность пространства и, как приближение, сделаем его дискретным (так же, как мы позволили себе сделать это в классическом случае), то похоже на правду, что все различные теории поля имеют один и тот же *тип* поведения и могут быть смоделированы в любом случае, видимо, работой решетки со спином и других вещей. Было замечено вновь и вновь, что явления теории поля (если мир создан на дискретной решетке) хорошо имитируются многими явлениями теории твердых тел (которые являются просто анализом работы решетки атомов кристалла, и в случае вроде твердого тела я подразумеваю, что каждый атом есть просто точка, с которой ассоциируются некоторые числа, в соответствии с квантовомеханическими правилами). Например, спиновые волны на спиновой решетке имитируют частицы Бозе в теории поля. Я, следовательно, полагаю, что верно то, что с помощью подходящего класса квантовых машин вы можете сымитировать любую квантовую систему, включая физический мир.[подчеркивание автора реферата]» [7, с. 82].

«Прогресс микроэлектроники и нанотехнологий приближается к рубежу, за которым игнорировать квантовую природу носителей информации будет уже невозможно. Элементы современной вычислительной техники лишь на два-три порядка превосходят характерные атомные размеры. Почетный председатель совета директоров и основатель корпорации Intel Гордон Мур считает, что на преодоление этой разницы уйдет всего 10–15 лет. Тогда волей-неволей придется искать новые решения, и фундаментальные результаты квантовой теории информации могут сыграть решающую роль.

[17] По личному впечатлению, эта идея была скорее всего выражена в имплицитной, а не в эксплицитной форме.
[18] С полным текстом этой наиинтереснейшей лекции (с вопросами и ответами) на русском языке можно ознакомиться в сборнике статей «Квантовый компьютер и квантовые вычисления», том 2, под ред. В.А. Садовничего – Ижевск: Ред. Журн. «Регулярная и хаотическая динамика», 1999, с. 96-124.

Квантовый компьютер — это гипотетическое вычислительное устройство, использующее специфически квантовые эффекты и поэтому намного превосходящее по своим возможностям любую классическую вычислительную машину. Его память (квантовый регистр) должна состоять из множества элементарных ячеек — кубитов, которые находятся в сцепленном состоянии, а операции предполагают управляемое квантовомеханическое взаимодействие между ними. Данные в процессе вычислений представляют собой квантовую информацию, которая по окончании процесса преобразуется в классическую путем измерения конечного состояния квантового регистра. Выигрыш в квантовых алгоритмах достигается за счет того, что при применении одной квантовой операции большое число коэффициентов суперпозиции квантовых состояний, которые в виртуальной форме содержат классическую информацию, преобразуется одновременно (квантовый параллелизм)» [9, с. 75].

Чтобы избежать недоразумений, прежде всего отметим, что основной целью создания квантовых компьютеров вовсе не является миниатюризация вычислительных устройств, как может показаться из чтения первого цитируемого параграфа. В то же самое время квантовый компьютер базируется на микроскопических системах, поскольку информация кодируется в квантовых состояниях (обычно электронов или ядер). Также ошибочно предполагать, что квантовые компьютеры придут на смену и вытеснят классические компьютеры. На самом деле квантовые и классические компьютеры должны работать в «тандеме»: классический компьютер должен контролировать внешними (классическими) сигналами, которые в свою очередь обеспечивают квантовую эволюцию регистра квантового компьютера (см. принципиальную схему квантового компьютера в Приложении 1). Квантовые компьютеры предназначены для решения весьма специфических задач. Здесь надо немного отклониться от основного изложения и обратиться к теории алгоритмов, рассмотреть классы алгоритмов и их сложности. «В теории сложности алгоритмов для классических компьютеров принято разделять алгоритмы на эффективные и неэффективные. Алгоритм относится к классу эффективных, если схема N_n состоит из полиномиального числа операций $O(n^d)$, где d=const, n - размер задачи. Время выполнения эффективного алгоритма возрастает с размером задачи полиномиально: $t_n \propto n^d$. В данном случае используемым для решения задачи ресурсом является время работы компьютера. К другим ресурсам относятся объем памяти компьютера и (в случае квантового компьютера) точность выполнения операций. Эффективный алгоритм должен использовать полиномиальное количество ресурсов, являющихся ограниченными. Эффективные алгоритмы называются также полиномиальными (класс P). Эффективным алгоритмам класса P противопоставляются неэффективные, требующие экспоненциально больших ресурсов (времени, памяти, точности). Например, если $t_n \propto 2^n$, алгоритм причисляется к неэффективным. Примером задачи, для которой не найдено эффективного алгоритма решения на классическом компьютере, является задача о вычислении простых множителей больших n-разрядных чисел (задача о факторизации чисел)[19]. Лучший известный вероятностный алгоритм для классических компьютеров требует $2^{\alpha(n\log_2 n)^{1/2}}$ операций.

В 1994 г. Шор построил алгоритм решения этой задачи на квантовом компьютере, который оказался. полиномиальной сложности: необходимое число операций $O(n^2 \log_2(\log_2 n \log_2 \varepsilon^{-1}))$, где ε — вероятность ошибочного результата вычислений. Результат Шора был сенсационным. Он опровергал так называемый тезис (эмпирический закон) Чёрча-Тьюринга: все компьютеры эквивалентны в том смысле, что переход от одного компьютера к другому не изменяет класса сложности задачи. Тезис был сформулирован для множества классических компьютеров. Тезис нарушается, если множество включает квантовые компьютеры» [2, стр. 5].

Упомянутый выше алгоритм Шора является наиболее ярким примером возможного приложения квантовых компьютеров. Заметим, что многие разновидности «секретных

[19] Заметим, однако, что не доказано, что не существует эффективного классического алгоритма этой задачи.

коммуникаций» основаны именно на факторизации больших чисел на простые множители. В немалой степени именно благодаря этому проект «квантовый компьютер» привлек к себе внимание со стороны специальных служб и получил поддержку государства (если не в России, то в других развитых странах). Алгоритм Шора не был первым квантовым алгоритмом: до этого был разработан квантовый алгоритм Дейча и Джоза (в 1992 г.) для решения весьма искусственной и не представляющей большого практического интереса задачи. Саймон усовершенствовал этот алгоритм для решения задачи о нахождении периода булевой функции, которая уже довольно важна. После алгоритма был также разработан алгоритм поиска Гровера (в 1996 г.), дающий ускорение в корень из N раз по сравнению с классическим компьютером.

Весьма важное отличие квантового и классического компьютеров заключается в том, что первый является цифровым вероятностным компьютером. Дело вот в чем. Перед выполнением алгоритма происходит инициализация начального состояния регистра. Суть инициализации – привести квантовую систему в определенное квантовое состояние, которое будет отправной точкой последующего «вычисления». Сам квантовый алгоритм есть унитарная эволюция вектора состояния квантовой системы. Желаемая унитарная эволюция обеспечивается с помощью *аналогового управления*. Унитарность эволюции обеспечивается при отсутствии шумов и нулевой температуре самим уравнением Шредингера. Произвольную унитарную эволюцию *всего* регистра можно получить с наперед заданной точностью с помощью лишь *одно*- и *двух*-кубитвых квантовых операций из стандартного набора. По окончании алгоритма остается конечный вектор состояния всего регистра, содержащий информацию о решении задачи. Получить эту информацию можно лишь с помощью измерения конечного состояния в вычислительном базисе (т.е. базисе, составленном из квантовых состояний 0 и 1 индивидуальных кубитов), причем в силу вероятностного характера квантовой механики, каждое из значений может быть получено с некоторой вероятностью. Вполне закономерен вопрос о том, как же можно получить единственное решение задачи в таком случае. Поэтому чтобы идея создания квантового компьютера вообще имела смысл, квантовый алгоритм должен приводить к такому конечному состоянию регистра, что вероятность получить в результате измерения правильное решение была намного больше суммы вероятностей ошибочных решений. «Все придуманные к настоящему времени квантовые алгоритмы обладают описанным свойством. Итак, квантовый компьютер дает цифровое решение задачи с определенной вероятностью, т.е. является цифровым вероятностным компьютером. <…> Такое сочетание свойств – аналоговый способ управления, вероятностный характер представления цифрового решения – не присутствует ни в одном типе классических компьютеров. Квантовый компьютер выглядит минотавром в мире компьютеров, сочетая несовместимые в классическом мире свойства аналоговых и цифровых классических компьютеров. На заре развития вычислительной техники (1950-1960 гг.) аналоговые (классические) компьютеры успешно дополняли цифровые ЭВМ. В последние годы они были вытеснены цифровыми ЭВМ из-за невысокой точности получаемых решений. Аналоговые переменные (токи и напряжения) удавалось контролировать с погрешностью порядка 10^{-2}. По современным оценкам параметры управляющих кубитами сигналов (импульсов) должны контролироваться с погрешностью 10^{-5} – 10^{-4}. Такую дорогую плату должны будут заплатить создатели квантовых компьютеров за сюрприз встречи с минотавром – цифровым компьютером с аналоговым управлением. <…> Высокая точность операций необходима, чтобы справиться с проблемой декогерентизации квантовых состояний» [2, стр. 11]

Возможно, читатель остался неудовлетворенным объяснением, в чем соль квантовых вычислений, и за счет чего достигается огромное ускорение вычислений на квантовых компьютерах. Стандартным ответом на этот вопрос является магическая фраза «квантовый параллелизм». Однако унаследованная от оснований квантовой механики проблема осталась. Вот что пишет один из исследователей этого вопроса: «Поскольку квантовая система может находиться в суперпозиции нескольких состояний, то при решении задач по вычислению

какой-либо функции f(x) естественно сначала приготовить состояние, содержащее суперпозицию всех значений аргумента x, а затем преобразовать это состояние в суперпозицию всех значений f(x). Каждый шаг вычислений описывается унитарным оператором. Обозначим через Uf оператор приготовления суперпозиции значений f(x). Как отмечает А.С. Холево: «очевидно, что однократное применение оператора Uf дает состояние, которое в латентной форме содержит все значения функции f и из которого интересующая нас информация может быть извлечена посредством квантового измерения. Такой прием называют квантовым параллелизмом». Самое туманное место в этом описании квантового параллелизма – это содержание всех значений f «в латентной форме». Вроде бы существование (даже в скрытой форме) должно всегда означать существование – наличие в действительности. Однако далее А.С. Холево продолжает: «Важно, однако подчеркнуть, что в отличие от параллелизма в классическом компьютере речь отнюдь не идет об одновременном вычислении всех значений функции». <…> Мне наиболее близки взгляды Джоза: «Квантовый параллелизм – это лишь удобный термин для использования суперпозиции при квантовых вычислениях. Никакого реального параллелизма здесь нет». <…> Необходимость хоть какого-то объективного обоснования хорошо понимают создатели квантовых вычислений. И многие из них (например, Дейч) склоняются к объяснению, которое, хотя и не так мистично, как копенгагенское, но все же должно быть отнесено к области научной фантастики. В основе этого объяснения квантового параллелизма (и преимуществ квантовых вычислений) лежит так называемая многомировая интерпретация квантовой механики. В этой интерпретации квантовые вычисления производятся в параллельных мирах. Поэтому квантовый параллелизм – это все же классический параллелизм, и все значения f действительно вычисляются. Однако вычисляются они в разных мирах. Акт измерения фиксирует мир и соответствующее значение f(x)» [11, стр. 22].

Испытывая некоторый дискомфорт при упоминании слова «интерпретация», постараемся больше не прибегать к нему и вернемся к истории обсуждаемого в этой главе вопроса. После сенсационного алгоритма Шора, открытого в 1994 г., *математическая сторона* квантовых вычислений была проработана во всех деталях. Предложены модификации упомянутых выше алгоритмов, найдены универсальные квантовые вентили, обеспечивающие одно- и двухкубитовые операции, разработаны методы коррекции ошибок (к 2000 г. Шором был предложен 9-кубитный код, позволяющий корректировать и амплитудные, и фазовые ошибки). Внимательный читатель может возразить: о каких ошибках вообще идет речь? Дело в том, что как бы мы ни старались изолировать квантовый регистр от внешних нежелательных воздействий, все-таки происходит взаимодействие регистра с окружением (которое к тому же имеет ненулевую температуру). Это приводит к тому, что состояние квантовой системы уже не описывается волновой функцией, и должно описываться матрицей плотности (см. различные интерпретации «состояния системы»). Происходит постепенное разрушение желаемого состояния системы – декогерентизация. В связи с этим необходимо, чтобы время, требующееся для одного шага квантового вычисления, было существенно меньше времени, в течение которого происходит декогерениция. Это и есть основная трудность (наряду с проблемой экспериментального измерения состояний кубитов – проблемы измерения) на пути по созданию *работающего на практике, а не на бумаге* квантового компьютера.[20]

[20] «Конференции по квантовой теории информации все еще сохраняют приятную и довольно редкую особенность: они объединяют как специалистов-теоретиков, вплоть до специалистов в весьма абстрактных разделах математики, так и физиков, непосредственно причастных к эксперименту. На одной из таких конференций ученый-экспериментатор начал доклад с иллюстрации, на которой были изображены роскошный «Кадиллак» с надписью «теория» и скромный «Трабант» — «эксперимент». Отрыв теории от экспериментальных реализаций действительно велик. Всякий эксперимент, предполагающий манипуляции состояниями индивидуальных микрочастиц, чрезвычайно сложен из-за их сверхчувствительности к любым внешним воздействиям. Более того, трудности реализации предписаний квантовой теории заложены и в самом ее фундаменте: она предоставляет математическую модель для любого реально наблюдаемого феномена микромира, однако дает лишь самые общие намеки на то, как можно двигаться в обратном направлении — от

«Квантовый компьютер находится на грани между микро- и макромиром, чем и обусловлены трудности его воплощения. Основным техническим препятствием для реализации квантового компьютера является декогерентизация — распад квантовых суперпозиций, обусловленный сверхчувствительностью микросистем к внешним воздействиям макромира. Если скорость декогерентизации не превосходит некоторого порогового значения, то применение квантовых кодов, исправляющих ошибки, теоретически позволяет сделать квантовые вычисления помехоустойчивыми. Однако при этом размер квантового регистра должен быть увеличен на порядки. *Сейчас*[курсив автора реферата] ведутся интенсивные поиски решения этих проблем: разработаны теоретические методы оптимизации архитектуры квантового компьютера, предложены схемы адиабатических вычислений, квантовых клеточных автоматов, вычислений, основанных на измерениях; обсуждается идея топологического квантового компьютера, физически устойчивого к ошибкам. Экспериментально исследуются модели кубитов, основанные на принципах ядерного магнитного резонанса, квантовой оптики и электродинамики, полупроводниковых квантовых точках, ионных ловушках, сверхпроводниковых мезо-структурах и т.д.» [9, с. 75].

Из истории экспериментальных усилий по созданию квантовых компьютеров отметим следующее. Успехи квантовой оптики в период 1990-2000 гг. дали мощный толчок квантовой теории информации. «Эксперименты по квантовой электродинамике резонаторов были особенно успешными при демонстрации фундаментальных особенностей квантовой механики, таких как квантовые осцилляции Раби, <…> состояния шредингеровского кота и квантовой декогерентизации. <…> Эти эксперименты демонстрируют прекрасный способ реализации основных квантовых логических операций; однако, представляется, что используя эти методы будет трудно осуществить большое количество таких операций» [1, с. 174]. В 1995 г. австрийскими физиками Цираком и Цоллером была высказана идея использования в качестве физической системы для реализации квантового компьютера совокупности ионов в ловушке в условиях лазерного охлаждения. Первые эксперименты были выполнены уже в том же году группой американских физиков. Запутывание 8 ионов кальция в ловушке было достигнуто в 2005 г. Сейчас активно обсуждается идея создания ловушек на основе твердотельных структур. Идея жидкостных ядерных магнитно-резонансных квантовых компьютеров была предложена в 1997 г. В 1998 г. были поставлены первые эксперименты по этой методике. Дальнейшие исследования выявили много сложностей на этом пути и работы «приутихли». В 1998 г. Кейном была предложена идея полупроводникового ядерно-магнитно резонансного квантового компьютера. К 2007 г. появились реальные экспериментальные методики по созданию таких структур (имплантация одиночных атомов), однако и на этом пути эксперты выявляют много проблем. В 1999 г. было предложено использовать зарядовые состояния электронов в квантовых точках для организации кубитов (Танамото и ряд других авторов). Эти идеи получили развитие, а экспериментальные результаты (хотя и неудовлетворительные с точки зрения декогерентизации) были получены в 2000-2005 гг. Сейчас работы в этом направлении продолжаются. Также в конце 1990-х гг. было предложено использовать

элемента математической модели к его материальному прототипу. В непревзойденном трактате Поля Дирака «Принципы квантовой механики» эта проблема описана следующим образом: «Возникает естественный вопрос: может ли быть измерена любая наблюдаемая? Теоретически на этот вопрос можно ответить — да. Практически может оказаться, что весьма затруднительно построить такой прибор, который мог бы измерять некоторую определенную наблюдаемую. Возможно, что экспериментатор не может сказать, как построить такой прибор, однако теоретик всегда может вообразить, что такое измерение может быть произведено». Другими словами, нет ни регулярного способа дать конструктивное описание соответствующей измерительной процедуры, ни даже гарантии, что такое описание возможно в принципе. Остается только верить, что оно рано или поздно будет найдено. Приведем пример из квантовой оптики. В теории хорошо известны состояния излучения с определенным числом фотонов (их называют состояниями Фока). Сегодня никто не сомневается в существовании фотонов, однако до сих пор не был известен способ генерирования таких состояний. Имелись теоретические предложения, в частности, основанные на использовании оптической обратной связи, и лишь недавно японским ученым удалось осуществить это в эксперименте» [9, с. 71]

сверхпроводниковые кубиты. Хотя данный вариант относительно прост в практическом исполнении, проблему декогерентизации не удалось решить до сих пор. Что касается адиабатического квантового компьютера на основе сверхпроводниковых кубитов, то в 2007 г. канадской фирмой D-wave было анонсировано «скандальное» заявление о создании квантового компьютера на основе 16 кубитов. Эксперты отнеслись к научной составляющей данного заявления довольно настороженно, тем самым отрицая то, что был продемонстрирован реальный квантовый компьютер.[21]

Глава 4. Квантовая коммуникация и криптография

Отметим, что квантовая теория информации применительно к коммуникации и криптографии преследует весьма амбициозную цель: «для заданного канала с помехами разработать такие методы кодирования и декодирования сигнала, которые позволили бы передавать за единицу времени как можно больше сообщений, практически неуязвимых для помех» [9, с. 70]. Под пропускной способностью канала будем понимать предельную максимальную скорость передачи информации. Далее выявляются и подчеркиваются (в прямом и переносном смысле) предпосылки рассмотрению квантовых каналов и разработке «хитроумных» методов исправления ошибок для передачи и надежного хранения информации. Вот какая ситуация сложилась в 1970 – 1980 гг.

«Изучать квантовые каналы связи необходимо, т.к. всякий физический канал в конечном счете является квантовым. В квантовом мире передатчик приготовляет квантовое состояние носителя информации в зависимости от поступающего сообщения. Например, передатчиком может быть лазер, который излучает либо вертикально, либо горизонтально поляризованные фотоны. Посылаемый двоичный сигнал кодируется соответствующим состоянием поля излучения. Однако в канале связи он, как правило, искажается, и на приемник поступают состояния, отличные от посланных передатчиком. Приемник осуществляет квантовое измерение той или иной физической величины, возможно, с последующей обработкой получаемой классической информации. Конечный результат такого измерения — выходной сигнал 0 или 1, дающий более или менее достоверную оценку посланного исходного сигнала, причем качество линии связи вновь характеризуется вероятностью ошибки. Аналогия с классической линией связи очевидна. Таким образом, возникает потребность в квантовой теории статистических решений и методах оптимального оценивания параметров квантовых состояний на основании результатов измерений. Очевидна и перспектива создания методов кодирования-декодирования, учитывающих квантовомеханическую природу носителя информации, которые позволяли бы компенсировать негативное влияние квантового шума. Возвращаясь к статистической механике, заметим, что такие процедуры вызывают ассоциацию со знаменитым «демоном Максвелла», создающим порядок из беспорядка, однако перед ними ставится более скромная, зато достижимая цель: сохранение островка порядка в море хаоса. Величина этого островка и определяет пропускную способность канала связи.

Пристальное рассмотрение понятия квантового измерения с информационно-статистической точки зрения привело к новому парадоксальному выводу: добавление независимого квантового шума в наблюдения позволяет увеличить количество получаемой информации. Парадокс в том, что такого никогда не бывает в классической статистике: добавление шума (рандомизация) только портит качество наблюдений. В квантовой оптике есть пример реальной измерительной процедуры, использующей независимый источник квантового шума (своего рода квантовую рулетку). Речь идет об оптическом гетеродинировании, при котором излучение, несущее информацию, складывается с опорным излучением от независимого источника. Такого рода процедура позволяет осуществить

[21] Подробности и мнения экспертов приведены на сайте http://offline.computerra.ru/2007/677/310169/

приближенное совместное измерение обеих компонент сигнала, электрической и магнитной, несмотря на то, что квантовая теория запрещает их точную совместную измеримость. С математической точки зрения такие измерения описываются переполненными системами векторов, отличными от полных ортонормированных систем (базисов) стандартной теории измерения фон Неймана. В частности, статистика оптического гетеродинирования описывается переполненной системой когерентных векторов, столь эффективно использованных в работах нобелевского лауреата Роя Глаубера. Всякую переполненную систему векторов в пространстве H можно описать как проекцию на H базиса в некотором объемлющем пространстве K, получающемся из H добавлением независимых (рандомизующих) степеней свободы. Оказалось, что переполненные системы представляют собой лишь частный случай более общего понятия вероятностной операторнозначной меры, исследованного советским математиком М.А. Наймарком еще в 1940 гг. и нашедшего естественное место в квантовой теории статистических решений, созданной в 1970–1980-х гг. »[9, с. 70].

Продолжая повествование о синтезе квантовой механики и теории информации, повторим, что с начала 1980-х гг. наметилась тенденция выявления «плюсов» квантовомеханической природы носителя информации, а не «минусов». Так, в 1982 г. Вутерсом и Зуреком была доказана невозможность клонирования неизвестного квантового состояния. «Под клонированием понимается создание точной копии исходного объекта при сохранении его в том состоянии, в каком он был до операции клонирования и которое изначально неизвестно» [3, с. 511]. «Простое рассуждение, основанное на линейности уравнений квантовой эволюции, показывает, что не существует «квантового ксерокса», т.е. физического устройства, позволяющего копировать произвольное квантовое состояние»[9, с. 74]. Это открыло дверь квантовой криптографии – одной из наиболее прикладных, но в то же время важных квантовой информатики. «Задача криптографии состоит в передаче информации между двумя сторонами (Алисой и Бобом) так, чтобы попытка перехватить передачу или узнать секретный код была обречена на неудачу. <…> В 1949 г. С. Шеннон, опираясь на разработанную им теорию информации, доказал теорему, что данная криптосистема является абсолютно секретной, если секретный код *истинно случайный* и он используется только один раз. Однако на практике реализация данной системы наталкивается на серьезные трудности. Одна из них — создание и передача большого секретного кода, необходимого каждый раз, когда посылается новое сообщение. Избежать этой сложности можно было бы при наличии физического канала, секретность которого обеспечивалась бы физическими законами. Именно такой канал и представляет квантовая физика. Квантовая криптография опирается <…> на невозможность клонирования отдельного квантового объекта. Если в качестве передатчика секретного кода выступают состояния отдельных частиц, то при попытке зарегистрировать эти состояния внешним наблюдателем они разрушаются. Факт попытки перехвата можно обнаружить, используя определенное соглашение (протокол) между Алисой и Бобом» [3, с. 514].

В 1984 г. Беннетом и Брассардом был теоретически разработан широко распространенный криптографический протокол, известный также как BB84, а в 1989 г. в IBM была успешно реализована первая криптографическая схема на этом протоколе. В качестве кубитов использовались поляризационные состояния одиночных фотонов[22], причем расстояние между источником и приемником составляло 32 см. Были разработаны и другие криптографические протоколы, использующие другие схемы распределения секретного ключа, например, в 1991 г. Экерт предложил протокол (позднее названный E91), который использует запутанные пары фотонов. Как и в случае с квантовыми компьютерами, основной преградой стало взаимодействие с окружением – поляризация фотонов относительно легко разрушается в

[22] «А ведь, в частности, надежность протокола квантовой криптографии основана на предположении, что секретный ключ распределяется с помощью единичных фотонов. В качестве реального источника используется слабый когерентный сигнал лазера, для которого вероятность появления более одного фотона мала. Но это оставляет лазейку для потенциального перехватчика «лишних» фотонов» [9, с. 73].

световоде. Однако технический прогресс позволил к 2000 г. осуществить криптографическую передачу данных по дну Женевского озера на расстояние 23 км. Длина кода, переданного за 11 часов, составила 20 кбит при скорости ошибок 1%, причем эти ошибки генерировались преимущественно германиевым фотодиодом. К 2007 г. максимальное расстояние составило 148 км. С 2000 г. стали появляться идеи коммерческого использования квантовой криптографии, и в 2004 г. в Вене был осуществлен первый в мире банковский квантовокриптографический перевод[23]. Отметим, что в России созданием и теоретическим исследованием криптографических схем занимается группа С.Н. Молоткова из МГУ им. М.В. Ломоносова.

Несмотря на то, что невозможность клонирования не позволяет создать точную копию неизвестного квантового состояния, она тем не менее не запрещает «телепортировать» его. В 1997 г. Цайлингеру и его сотрудникам удалось осуществить квантовую телепортацию – возможность переноса квантового состояния одного объекта на другой. «Хотя предложение о *квантовой телепортации* было сделано Чарлзом Беннетом с коллегами еще в 1993 г., именно эксперимент [Цайлингера] и последовавший за ним эксперимент [Боши] привлекли к себе широкое внимание научной (и не только) общественности» [3, с. 512].

Как и было обещано, обратимся теперь к неравенствам Белла.

Новый интерес к проблеме сведения квантовой случайности к классической «ансамбль-случайности» приходится на 1960 – 1980 гг. в связи с исследованиями Дж. Белла, статья которого «О парадоксе Эйнштейна-Подольского-Розена» была опубликована в 1964 г. Напомним, что парадокс Эйнштейна-Подольского-Розена (1935 г.) заставляет нас встать перед выбором между мгновенным действием на расстоянии и неполнотой квантовой механики. Эйнштейн считал, что квантовая механика неполна, и стремился найти некоторую статистическую модель. Джон Бэлл, отталкиваясь от того же мысленного эксперимента что и Эйнштейн с соавторами, пришел к выводу, что «или квантовая механика полна, или предквантовая механика нелокальна» [11, с. 133]. Хренников отмечает, что «Белл отнюдь не показал, что квантовая механика нелокальна и что квантовая случайность несводима к классической ансамбль-случайности <…> Для Белла наиболее естественной моделью, индуцирующей квантовую случайность, являлась бомовская механика. Случайность в бомовской механике чисто классическая. Таким образом, применима классическая теория информации. Однако модель нелокальна, и появляется возможность нелокальных атак. В принципе, содержание моего компьютера может стать известным другому лицу без какого-либо физического контакта с моим компьютером. Следовательно, квантовая криптография должна гарантировать защиту от подобных нелокальных атак. Таких гарантий квантовая криптография не дает. Конечно, можно возразить, что появление противника с нелокальными бомовскими возможностями весьма маловероятно и, более того, принадлежит области научной фантастики. Я согласен с такой точкой зрения. Однако весьма нелогично, с одной стороны, отвергать возможность классических нелокальных атак на квантовые криптографические схемы, а с другой стороны, ссылаться на Белла, рекламируя достоинства квантовой криптографии. Я считаю, что несводимость квантовой информатики к классической не следует из белловских рассмотрений. Поэтому заявления о 100-процентной секретности квантовых криптографических схем не слишком обоснованы. Это никоим образом не умаляет значения проекта «квантовая криптография». Даже если фундаментальной несводимости нет, то, оперируя с фотонами (чрезвычайно чувствительными к любым внешним воздействиям), мы весьма сужаем класс возможных атак на квантовые криптографические схемы. Итак, исследования Белла не могут быть использованы для обоснования превосходства квантовой криптографии над классической» [11, с. 135].

Эта весьма критическая, но откровенная и убедительная критика была озвучена в 2003-2008 гг. в противовес «устоявшейся» в научном сообществе трактовке, гласящей, что

[23] Важный чек, который требовал «абсолютной» секретности, был переведен мэром города в Банк Австрии.

квантовая механика нелокальна и квантовая случайность несводима к классической. Обсуждения этого вопроса не утихают и *по сей день*.

Приведем теперь дальнейшую историю неравенств Белла. В 1969 г. Клаузер, Хорн, Шимони и Холт модифицировали неравенство Белла и записали его в более удобном виде для экспериментальной проверки. По сути, и неравенство Белла, и КХШХ-форма этого неравенства были нацелены на проверку того, описываются ли предсказания квантовой механики некоторой теорией локальных скрытых переменных. Многие современные ученые считают, что в такой формулировке рассматриваются не все возможные теории скрытых локальных переменных, а их подкласс. Как бы то ни было, в 1981 г. Аспеку удалось экспериментально проверить выполнение неравенств на опыте. Оказалось, что экспериментальные данные нарушают неравенство Белла и тем самым отрицают возможность описания квантово-механических результатов с помощью определенного класса скрытых переменных. Многие считали это событие торжеством квантовой механики, однако некоторые усмотрели «нестыковки» и «некорректность» некоторых положений. Единого мнения на этот счет нет до сих пор.

Единого мнения удалось добиться в отношении запутанности. Так, в середине 2000-х гг. с помощью вероятностно-томографического представления было показано, что если неравенство Белла нарушается, то состояние не может быть сепарабельным и необходимо является запутанным (сцепленным). На деле это эффективный показатель запутанности, которая так необходима для работы квантового компьютера и некоторых криптографических схем.

Мой вывод о роли неравенств Белла в становлении квантовой теории информации таков: они привлекли внимание ученых к проблемам квантовой механики и передачи информации на квантовомеханических носителях, заставили сфокусироваться на поиске отличительных особенностей квантовомеханических систем, которые могли бы лечь в основу новых принципов организации обработки информации и ее передачи, и последним по порядку, но не последним по значению – стимулированию академического интереса к фундаментальным аспектам квантовой теории и теории информации.

Глава 5. Квантовая теория информации и математика

«В свое время появление квантовой механики оказало мощное взаимообогащающее влияние на ряд областей математики: в первую очередь на теорию операторов, операторных алгебр, представлений групп» [9, с. 75].

«Математическая традиция в теории информации восходит к А.Н. Колмогорову и А.Я. Хинчину. Для математика, которому небезразлична естественнонаучная сторона его исследований, теория информации является источником глубоких идей и новых трудных задач, имеющих достойную мотивацию. В равной, если не в большей мере это относится и к квантовой теории информации, проблематика которой оказывается тесно связанной с некоммутативным анализом, асимптотической теорией конечномерных нормированных операторных пространств и алгебр, тонкими свойствами структур положительности и тензорного произведения, а также с методами случайных матриц. В 2002 г. <…> вышла книга [8], посвященная математическому изложению основ квантовой теории информации. В ней, в частности, были затронуты две открытые проблемы: А) аддитивность энтропийных характеристик квантового канала, связанных с его классической пропускной способностью; Б) теорем кодирования для квантовой пропускной способности. Прошедшие годы ознаменовались быстрым прогрессом, в частности, усилиями разных исследователей было получено полное решение проблемы Б. Квантовая пропускная способность оказалась тесно связанной с криптографическими характеристиками канала, такими как пропускная способность для секретной передачи классической информации и скорость распределения случайного ключа. Был выделен важный класс деградируемых каналов, для которых эти две

характеристики совпадают и зачастую могут быть вычислены в явном виде. Значительный прогресс был достигнут и в решении проблемы аддитивности» [10].

Будучи вовлеченным в математическую части квантовой теории информации, могу отметить, что вполне существенные результаты получены не только в положительных отображениях операторов на операторы, но также и в биективных отображениях операторов на томографические символы разного вида. В частности, недавно было показано, сколько направлений в пространстве необходимо выбрать для построения конечномерного вероятностного вектора с ясной физической интерпретацией, содержащего ту же информацию о состоянии спиновой системы, что и оператор плотности. Влияние КТИ на математическое русло было значительным.

«Процесс продолжается и сейчас, и в нем все большую роль играют достижения квантовой теории информации. Так, исследование сцепленности стимулировало прогресс в понимании геометрии тензорных произведений, а каналы и теоремы кодирования оказались тесно связаны со структурами положительности в операторных пространствах и алгебрах. Новый импульс получил некоммутативный анализ; даже в такой, казалось бы, хорошо изученной области, как теория матриц, появились новые яркие результаты и новые трудные и интересные проблемы. На Европейском конгрессе математиков 2008 г. в Амстердаме квантовая теория информации выделена в специальное направление, которому посвящен ряд приглашенных докладов» [9, с. 75].

Заключение

«Мы немного познакомились с историей и современным состоянием квантовых вычислений и квантовой информации. Что ждет нас в будущем? Что могут предложить квантовые вычисления и квантовая информация науке, технике и всему человечеству? Что нового дает эта область по сравнению с ее родительскими дисциплинами – информатикой, теорией информации и физикой? <…> Квантовые вычисления и квантовая информация научили нас думать о вычислениях физически, и мы обнаружили, что этот подход открывает много новых возможностей в области связи и обработки информации. <…> Фактически мы поняли, что любая физическая теория, а не только квантовая механика, может служить базисом для теории обработки информации и теории связи. В результате этих исследований однажды могут быть созданы устройства обработки информации, намного превосходящие по своим возможностям современные вычислительные и коммуникационные системы, что будет иметь свои положительные и отрицательные последствия для всего общества. Конечно, квантовые вычисления и квантовая информация ставят перед физиками массу задач, но при этом не совсем понятно, что эта область предлагает физике в долгосрочной перспективе. Мы полагаем, что точно так же, как мы научились думать о вычислениях физически, мы можем научиться думать о физике в терминах вычислений. Физика традиционно является дисциплиной, где основное внимание сосредоточено на понимании «элементарных» объектов и простых систем, однако многие интересные аспекты Природы проявляются лишь с ростом размеров и сложности. <…> Квантовые вычисления и квантовая информация предоставляют новые инструменты, позволяющие перебрасывать мост от простого к относительно сложному: в сфере вычислений и алгоритмов есть систематические средства для построения и изучения таких систем. Применение этих идей из этих областей уже начинает приводить к выработке новых взглядов на физику. Мы надеемся, что в последующие годы этот подход будет успешно применяться во всех ее разделах» [6, стр. 32].

В заключение приведем слова А.С. Холево: «Квантовая информатика стала новым междисциплинарным научным направлением на стыке физики, информатики и математики, которое поднимает новые важные вопросы и дает ключ к пониманию некоторых фундаментальных закономерностей Природы, до недавних пор остававшихся вне поля зрения исследователей. Ее теоретические разработки стимулируют как новые достижения в

области математики, так и развитие экспериментальной физики, значительно расширяющее возможности манипулирования состояниями микросистем и потенциально важное для появления новых эффективных технологий» [9, с. 75].

Действительно, к этому выводу не добавить и не отнять. Заметим только, что даже если многие объекты исследований квантовой теории информации так и не будут никогда воплощены в жизнь (например, квантовый компьютер), то сами исследования в этой области стали таким катализатором для развития многих естественных наук (математика, физика), техники и технологии, и, в немалой степени, гуманитарных наук (философские аспекты квантовой механики встают здесь на первый план), что план-минимум уже можно считать выполненным. «Дорогу осилит идущий»[24]. Я искренне верю в эту мудрость.

Литература:

1. *Бауместер Д., Экерт А., Цайлингер А. (ред).* Физика квантовой информации. – М.: ПостмаркетМир, 2002.
2. *Валиев К.А.* Квантовые компьютеры и квантовые вычисления // Успехи физических наук, том 175, с. 3-39 (2005).
3. *Килин С.Я.* Квантовая информация // Успехи физических наук, том 169, с. 507-527 (1999).
4. *Котина С.В.* Поиск красоты. Роль эстетических ориентиров в формирующейся научной теории. – М.: Вестком, 2002.
5. *Манько В.И.* Квантовая механика: соотношение неопределенностей + вероятность вместо волновой функции. В сборнике статей «Исследования по истории физики и механики» (под ред. Г.М. Идлиса) – М.: Наука, 2003, стр. 78-87.
6. *Нильсен М., Чанг И.* Квантовые вычисления и квантовая информация: Пер. с англ. – М.: Мир, 2006.
7. *Фейнман Р.* Моделирование физики на компьютерах. В сборнике статей «Квантовый компьютер и квантовые вычисления», том 2, под ред. Садовничего В.А. – Ижевск: Регулярная и хаотическая динамика, 1999, стр. 96-124.
8. *Холево А.С.* Введение в квантовую теорию информации. – М. МЦНМО, 2002.
9. *Холево А.С.* Квантовая информатика: прошлое, настоящее, будущее // В мире науки, № 7, стр. 68-75 (2008).
10. *Холево А.С.* Квантовые системы, каналы, информация. – М.: МЦНМО, 2010.
11. *Хренников А.Ю.* Введение в квантовую теорию информации. – М.: Физматлит, 2008.

[24] По-моему, это высказывание также относится и к реферату. И хотя на нашей дороге (я имею в виду изложение текста) не раз встречались кочки и разбитость колеи, все же, следуя возвратно-поступательным образом по ленте времени как по нити Ариадны, нам удалось выйти из чащи хаотического переплетения физических, математических и информационных лиан на поляну. Теперь мы знаем, где мы находимся и какие проблемы-деревья нас окружают, а также слышим стук дровосеков-исследователей, которые тоже иногда заблуждаются в этом все еще темном, но таком манящем и полном чудес лесу – квантовой теории информации.

Приложение 1. Принципиальная схема квантового компьютера

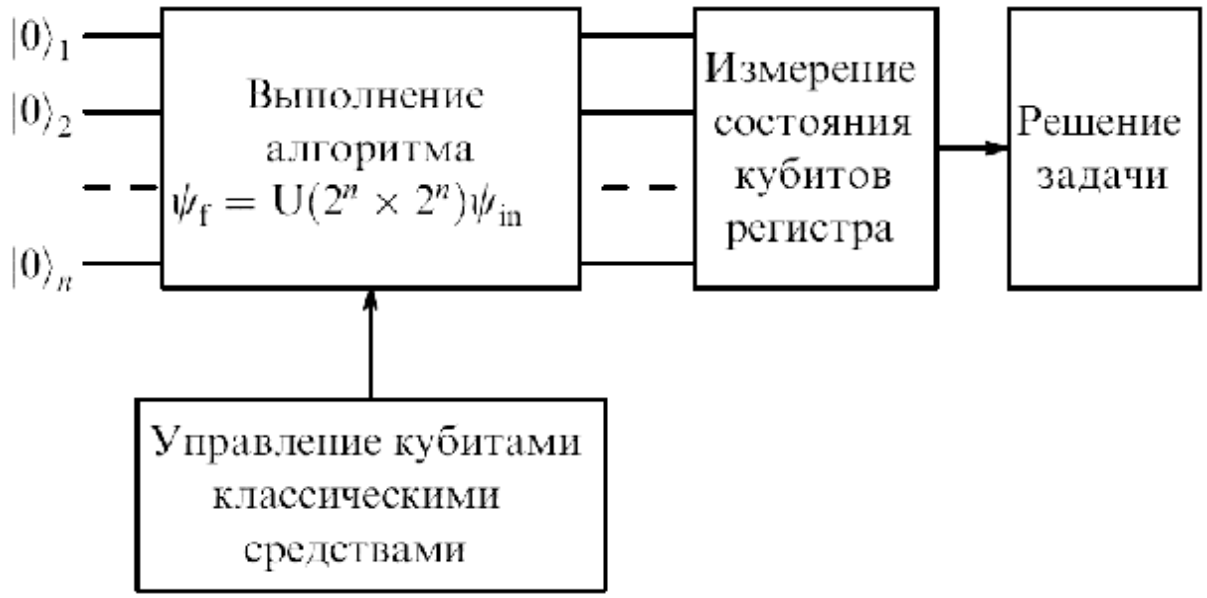

Рисунок заимствован из работы [2]

Приложение 2. Рассуждения на тему: «Человеческий мозг как Природный квантовый компьютер»

«Не исключено, что в природе квантовый компьютер давно уже существует. Высказывается мнение, что элементы квантового компьютинга присутствуют в человеческом мышлении, и тогда квантовая информатика открывает новые перспективы для принципиального объяснения возможных алгоритмов мышления. Остановимся на тех особенностях человеческого мышления, которые действительно вызывают ассоциации с квантовыми закономерностями.

1) Способность целостного восприятия информации в противоположность разложению на составляющие свойства; возможно, глаз способен принимать не только классические состояния входящего света, но и непосредственно квантовые состояния фотонов, чем и объясняются особая мощь и пропускная способность визуальных коммуникаций, а также их органическая связь с распознаванием образов.

2) Сходство дополнительности между действием и размышлением и квантовой дополнительностью между положением и скоростью, на которое обращал внимание еще Нильс Бор в своих физико-философских эссе. Примечательно, что при разработке концепции квантовой дополнительности Бор исходил из уже существовавшей аналогичной концепции витализма в биологии.

3) Черты сцепленности (или нелокальности), когда информация, содержащаяся в объединении подсистем некоторой сложной системы, превосходит арифметическую сумму количеств информации, получаемых из подсистем.

4) Феномен сознания-подсознания. Трудно удержаться от такой (конечно, крайне упрощенной) аналогии: некоммутативная алгебра квантовомеханических наблюдаемых, в которой в каждый момент времени «сканируется» некоторая доступная наблюдению коммутативная (классическая) подалгебра.

5) Органическое сочетание аналоговых и цифровых методов, эффективный параллелизм обработки информации.

Разумеется, эти и другие соображения, такие как наличие интуиции и свободной воли, носят косвенный характер и не влекут с неизбежностью вывода, что в мозгу человека или в нервной системе других живых существ присутствуют «квантовые микрочипы» или другие квантово-физические механизмы, ответственные за неклассические вычисления и соответствующее поведение. Но они, возможно, свидетельствуют о том, что работа мозга принципиально несводима к функциям сколь угодно совершенного и сложного классического суперкомпьютера, и тогда теоретические модели таких систем должны принимать во внимание эту неклассичность» [9, с. 72].