МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ИНСТИТУТ ЭЛЕКТРОННОЙ ТЕХНИКИ
(ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ)

КАФЕДРА КВАНТОВОЙ ФИЗИКИ И НАНОЭЛЕКТРОНИКИ

Ю.И. Богданов

Физико- статистические основы квантовой информатики

Москва 2010

УДК 519+530.145

Рецензенты: доктор физико- математических наук, профессор кафедры квантовой электроники МГУ им. М.В. Ломоносова *С.П. Кулик* ;
кандидат физико- математических наук, ведущий научный сотрудник Физико-технологического института РАН *В.В. Вьюрков*

Богданов Ю.И.

Б.73 Физико- статистические основы квантовой информатики. Учебное пособие. М.: МИЭТ, 2010, 163 с.

Рассматривается введение в новую область исследований- квантовую информатику, связанную с использованием законов квантовой физики для целей вычислений и связи.

Подробно описываются и анализируются физико- статистические модели квантовых систем. Существенное внимание уделяется фундаментальным аспектам квантовой информатики таким, как статистический характер законов микромира, принцип дополнительности Н. Бора, неравенства Белла и др.

Пособие основано на курсе лекций, читаемом для студентов старших курсов кафедры квантовой физики и наноэлектроники МИЭТ.

Введение

В настоящее время мы становимся свидетелями рождения новой фундаментальной научной дисциплины - квантовой информатики. Стимулом к рождению и развитию новой науки являются активно ведущиеся работы, основанные на применении квантовых систем к задачам вычислений и связи [1-6].

Следует отметить, что современные лазеры, твердотельные компьютеры и др. приборы также существенным образом базируются на законах квантовой физики. В чем же тогда специфика приборов квантовой информатики? Краткий (и упрощенный) ответ на этот вопрос может быть таким. Традиционные электронные приборы используют законы квантовой физики на уровне аппаратного обеспечения («железа»- hardware), новые же приборы квантовой информатики предполагают использование законов квантовой физики на уровне алгоритмов и программного обеспечения (software).

Технологическая революция XX века, связанная с использованием компьютеров, лазеров, ядерной энергии и др. достижений физики может быть названа первой квантовой революцией. Без преувеличения можно сказать, что развивающиеся в настоящее время методы и технологии квантовой информатики должны стать в XXI веке основой для новой (второй квантовой) технологической революции [5].

Оказывается, что использование законов квантовой теории не только на уровне “hardware”, но и на уровне “software” позволит квантовым компьютерам и приборам квантовой информатики решать задачи, недоступные никаким классическим компьютерам.

Направление квантовых вычислений стало активно развиваться после появления работ Р. Фейнмана [7,8]. Фейнман заметил, что моделирование квантовой физики на обычных компьютерах является экспоненциально сложной задачей. Отсюда он сделал вывод, что, возможно, компьютер,

основанный на квантовых принципах вычислений, окажется экспоненциально более мощным по сравнению со своими классическими собратьями. Ранее аналогичные соображения высказывал Ю.И. Манин [9].

Среди основных разработанных (и частично реализованных на простых физических системах) квантовых алгоритмов отметим следующие: алгоритм формирования запутанного состояния, алгоритм Дойча- Джозса (отличающий постоянные бинарные функции от переменных «сбалансированных» функций, имеющих различные значения для различных аргументов), алгоритмы квантовой телепортации и сверхплотного кодирования (dense coding), квантовый алгоритм поиска Гровера, квантовое дискретное преобразование Фурье и алгоритм факторизации П. Шора (разложение большого целого числа на простые множители) [10-12]. Среди наиболее важных результатов теории квантовых вычислений следует также отметить открытие универсального набора квантовых логических элементов (позволяющих выполнять любое унитарное преобразование- вычисление в системе квантовых битов- кубитов) [13,14], а также разработку квантовых алгоритмов коррекции ошибок [15].

Среди экспериментальных работ по реализации алгоритмов квантовой информатики отметим работы по таким направлениям, как квантовая телепортация и сверхплотное кодирование [16-18], а также приготовление белловских состояний [19,20].

Экспериментальные исследования по квантовому компьютингу ведутся в различных направлениях, среди которых отметим квантовую электродинамику резонаторов (КЭР) [21,22], линейные ионные ловушки [23-25] и ядерный магнитный резонанс – ЯМР (жидкостной и твердотельный) [26-28].

В настоящем пособии мы стремились показать, что квантовая информатика является основой не только для грядущих технологических достижений. Не менее важно то, что новая научная дисциплина оказывает

очень важное влияние на все теоретическое естествознание. Квантовая информатика позволяет лучше представить что такое квантовая физика, понять природу случайности, дать содержательное естественно- научное истолкование таким понятиям как информация, алгоритм, вычисление и др. Представления квантовой информатики могут существенно изменить физику, математику, информатику, химию, молекулярную биологию и другие естественные науки. Это будет уже не только технологическая, но и научная квантовая революция.

Пособие состоит из пяти глав. В первой главе рассматривается вероятностная интерпретация векторов гильбертова пространства (на примере взаимно- дополнительных прямого и обратного преобразований Фурье). Основанный на квантовой информатике подход позволяет осветить с новых и более общих позиций некоторые вопросы классической математической статистики. Так, оказывается, что аппарат характеристических функций классической математической статистики содержит в себе в рудиментарной форме представление об операторе координаты в импульсном представлении и аналогичные представления об операторе импульса в координатном представлении. Однако, в отрыве от представлений квантовой информатики, классическая статистика содержит эти понятия в сильно завуалированном виде. Неполнота и ограниченность классической теории становится очевидной с более общих позиций квантовой информатики. С точки зрения принципов квантовой информатики, недостаточность представлений классической математической статистики состоит в том, что последняя рассматривает только одно из возможных взаимно- дополнительных статистических распределений, игнорируя остальные. Только использование квантовых представлений позволяет увидеть за распределениями вероятностей более простой и фундаментальный геометрический объект – вектор состояния.

Во второй главе рассматриваются вопросы, связанные с точностью статистических характеристик гильбертова пространства. Геометрический аппарат квантовой информатики делает совершенно естественным рассмотрение наряду с обычными для статистики координатными величинами других (импульсных) величин, связанных с производными по координатам. При таком подходе соотношение неопределенностей оказывается неравенством типа Коши- Буняковского. Наряду с элементарными сведениями по неравенству Коши- Буняковского и соотношению неопределенностей, в настоящей главе рассматриваются также соотношение неопределенностей Шредингера- Робертсона и многомерное обобщение соотношения неопределенностей Гейзенберга. Кроме того, основываясь на аппарате квантовой информатики, изучаются вопросы, связанные с информацией Фишера, неравенством Рао- Крамера и корневыми статистическими оценками.

В третьей главе формулируются постулаты квантовой информатики. Здесь выбор постулатов аналогичен аксиомам квантовой физики, изложенным в известной монографии М. Нильсена и И. Чанга [1], однако, в отличие от указанных авторов, в формулировке и интерпретации каждого постулата мы делаем акцент на его статистической природе. Тем самым подчеркивается, что постулаты квантовой информатики есть реализация программы, заложенной в известной 6-ой проблеме Гильберта, которая направлена на построение особой теории вероятностей, основанной на геометрических понятиях и фундаментальных свойствах микромира. В качестве важного примера применения постулатов квантовой информатики рассматривается процедура перехода от классической механики к квантовой.

В четвертой главе принципы квантовой информатики прилагаются к описанию основных квантовых логических элементов. Рассматриваются произвольные унитарные вращения кубита, описываются элементы Паули,

Адамара, управляемое НЕ (CNOT) и др. Представлена теорема о невозможности клонирования неизвестного квантового состояния, изучается важное для квантовой информатики явление запутанности квантовых состояний, описываются состояния Белла и анализируется неравенство Белла.

В пятой заключительной главе представлены некоторые фундаментальные квантовые алгоритмы, призванные продемонстрировать радикальное преимущество квантовой информатики над классической. Рассмотрены сверхплотное кодирование и телепортация, описан квантовый параллелизм, изучены алгоритмы Дойча, Дойча- Джозса и квантового преобразования Фурье. Рассмотрены задачи нахождения периода функции и факторизации целых чисел, даны элементарные сведения по квантовой криптографии.

Данное учебное пособие написано для поддержки курса по физико-статистическим основам квантовой информатики, который читается для студентов кафедры квантовой физики и наноэлектроники МИЭТ.

Для понимания содержания от читателя требуется знание математики и физики в объеме стандартных программ для технических университетов. Важная составная часть курса – это задачи. Их решение призвано дать читателю более глубокое понимание излагаемой теории и научить простейшим навыкам самостоятельной осмысленной работы в данной области.

Автор благодарен академику К.А. Валиеву за поддержку, а также всем участникам семинара по физике квантовых компьютеров в Физико-технологическом институте РАН за обсуждение различных вопросов квантовой информатики. Особая благодарность В.В. Вьюркову, А.А. Кокину, С.П. Кулику, Ю.И. Ожигову, И.А. Семенихину и А.В. Цуканову, общение с которыми было очень полезным.

Глава 1. Квантовая случайность. Анализ взаимно- дополнительных статистических величин.

«Отыщи всему начало, и ты многое поймешь!»

(Козьма Прутков «Мысли и афоризмы», №247).

Вероятностную природу квантовой теории можно продемонстрировать на примере статистической интерпретации комплексной функции и её Фурье-образа.

1.1. Статистическая интерпретация прямого и обратного преобразований Фурье. Координатное и импульсное распределения.

Пусть $\psi(x)$ - произвольная комплексная функция, заданная в гильбертовом пространстве L_2. Такая функция обладает конечным интегралом от квадрата модуля

$$\int |\psi(x)|^2 dx < \infty$$

Прямое и обратное преобразования Фурье задаются следующими известными формулами:

$$\psi(x) = \frac{1}{\sqrt{2\pi}} \int \tilde{\psi}(p) \exp(ipx) dp \qquad (1.1)$$

$$\tilde{\psi}(p) = \frac{1}{\sqrt{2\pi}} \int \psi(x) \exp(-ipx) dx \qquad (1.2)$$

Задача 1.1 Непосредственным расчетом покажите, что комбинация прямого и обратного преобразований Фурье приводит к исходной функции (т.е является тождественным преобразованием).

Замечание: Воспользуйтесь следующим выражением для дельта- функции Дирака в виде интеграла Фурье:

$$\delta(x - x_1) = \frac{1}{2\pi}\int \exp(ip(x - x_1))dp \qquad (1.3)$$

Более подробно дельта- функция и ее свойства описываются в Приложении к настоящей главе.

С комплексной функцией $\psi(x)$ и её Фурье- образом $\tilde{\psi}(p)$ можно связать распределения вероятностей.

Определим плотность распределения вероятности в исходном (координатном) представлении как:

$$P(x) = |\psi(x)|^2 \qquad (1.4)$$

Выражение (1.4) называется формулой Борна.

С помощью Фурье- образа $\tilde{\psi}(p)$ можно задать некоторое другое (а именно так называемое импульсное) распределение вероятностей:

$$\tilde{P}(p) = |\tilde{\psi}(p)|^2$$

Известно, что для функции и ее Фурье- образа выполняется равенство Парсеваля:

$$\int |\psi(x)|^2 dx = \int |\tilde{\psi}(p)|^2 dp$$

Задача 1.2. Докажите равенство Парсеваля, используя Фурье-представление для дельта- функции

Равенство Парсеваля показывает, что полная вероятность не зависит от выбора представления. Её можно нормировать по выбору исследователя на произвольное положительное число. Как правило, условие нормировки выбирают в виде:

$$\int P(x)dx = \int \tilde{P}(p)dp = 1$$

Рассматриваемая формула предполагает, что полная вероятность равна единице. Заметим, что в исследовательской практике используются и другие

условия нормировки. В частности, в задачах распада и рассеяния микрообъектов полная вероятность может характеризоваться суммарным числом событий в единицу времени и, таким образом, быть размерной.

Заметим, что функция $\psi(x)$ и ее Фурье- образ $\tilde{\psi}(p)$ содержат в себе эквивалентную информацию (знание одной из них позволяет найти другую с помощью прямого или обратного преобразования Фурье). Их называют амплитудами вероятности в координатном и импульсном представлении соответственно (вместо термина амплитуда вероятности в зависимости от контекста задач используют и другие близкие по смыслу термины: волновая функция, пси- функция, вектор состояния).

1.2. Принцип дополнительности Н. Бора

Координатное $P(x)$ и импульсное $\tilde{P}(p)$ распределения называются взаимно- дополнительными статистическими распределениями, поскольку информационно эти распределения дополняют друг друга. Дело в том, что при измерении, скажем, в координатном представлении совершенно теряется информация о фазе волновой функции $\psi(x)$. Действительно, переход от $\psi(x)$ к $\psi(x)\exp(iS(x))$, где $S(x)$- произвольная действительная функция (фаза), никак не влияет на координатное распределение вероятности $P(x)$. Такой переход, однако, вообще говоря, будет влиять на импульсное распределение $\tilde{P}(p)$. В этом смысле $\tilde{P}(p)$ содержит в себе дополнительную информацию по отношению к $P(x)$.

Рассматриваемая терминология сформировалась под влиянием принципа дополнительности Н.Бора. Согласно этому принципу «данные, получаемые при разных условиях опыта, не могут быть охвачены одной- единственной картиной; эти данные должны скорее рассматриваться как *дополнительные* в

том смысле, что только совокупность разных явлений может дать более полное представление о свойствах объекта» [29].

В соответствии с квантовой теорией, полную информацию о статистической квантовой системе несет волновая функция (вектор состояния) $\psi(x)$. В то же время, чтобы экспериментально экстрагировать эту информацию, недостаточно использовать какое- либо одно фиксированное представление. Чтобы изучение квантовой системы было более полным, следует проводить измерения, отвечающие совокупности взаимно-дополнительных распределений. В этом и состоит со статистической точки зрения принцип дополнительности Н. Бора. Координатное и импульсное распределения являются примерами таких взаимно- дополнительных распределений. Статистический принцип дополнительности является ключевым для задач квантовой информатики.

Модель квантовой информатики предполагает определенные правила «игры» между Природой и человеком (исследователем). Пси- функция (вообще говоря, комплексная) содержит в себе полную информацию о квантовой системе. Её следует рассматривать как объект, аккумулирующий в себе возможные данные из различных взаимно- дополнительных распределений. В силу статистической природы квантовой механики, мы не имеем возможности измерить пси- функцию непосредственно (в противном случае, никакой статистики вообще бы не было). Все, что мы можем, это провести измерения над определенным числом представителей. Каждый из представителей находится в одном и том же состоянии $\psi(x)$ (это определяется тем, что все они были *приготовлены* в одних и тех же условиях, по одному и тому же рецепту). При этом, получаемые нами статистические данные, будут давать нам информацию о $|\psi(x)|^2$, $|\tilde{\psi}(p)|^2$ и др. распределениях в зависимости от выбранного представления.

С экспериментальной точки зрения, проверка справедливости квантовой теории, по- существу, основана на реконструкции (с помощью статистических измерений) свойств скрытого от непосредственного наблюдения вектора состояния в гильбертовом пространстве. Все проведенные до сих пор эксперименты находятся в согласии с представлениями квантовой информатики, основанными на взаимно- дополнительных статистических измерениях, за которыми стоит искомый вектор состояния квантовой системы в гильбертовом пространстве.

Заметим, что традиционная теория вероятностей и математическая статистика ограничиваются описанием только отдельных (не взаимно-дополнительных) распределений вероятностей (одномерных или многомерных). Принцип дополнительности приводит к нарушению так называемой аксиомы о составных случайных величинах классической теории вероятностей [30]. Следуя Г. Крамеру [31] сформулируем эту аксиому в следующем виде: “Если $\xi_1,...,\xi_n$ - случайные величины размерностей соответственно $k_1,...,k_n$, то каждый составной объект $(\xi_1,...,\xi_n)$ также является случайной величиной (размерности $k_1+...+k_n$)”. Таким образом, согласно аксиоме о составных случайных величинах, в классической теории вероятностей существует единственный способ перехода от описания отдельных свойств объектов к описанию совокупности таких свойств. Этот способ основан на переходе от одномерных распределений к многомерным. В квантовой информатике это не так. Поскольку распределения могут быть взаимно- дополнительными, их совокупность уже не есть распределение, а есть объект более общей природы- квантовое состояние. Так, за взаимно-дополнительными координатным $P(x)$ и импульсным $\widetilde{P}(p)$ распределениями не стоит никакого их совместного распределения $P(x,p)$. Существование такого распределения противоречит, как будет видно ниже, принципу

неопределенности Гейзенберга. Объединяющим началом всех взаимно-дополнительных распределений, согласно квантовой информатике, является вектор состояния в гильбертовом пространстве. Квантовое состояние можно рассматривать как естественное обобщение понятия статистического распределения. Согласно сказанному выше, квантовое состояние не может быть сведено к одному- единственному статистическому распределению, а описывает одновременно совокупность различных взаимно- дополнительных распределений.

1.3. Характеристическая функция. Вычисление среднего и моментов. Неполнота классической и полнота квантовой статистики.

Координатное и импульсное представления вектора состояния эквивалентны. В этой связи, интересно рассмотреть свойства координатного распределения вероятностей с точки зрения импульсного представления и наоборот – свойства импульсного распределения с позиции координатного представления.

С использованием волновой функции в импульсном представлении координатное распределение вероятностей можно записать в виде:

$$P(x)=\psi^*(x)\psi(x)=\frac{1}{2\pi}\int dpdp_1\tilde{\psi}^*(p)\tilde{\psi}(p_1)\exp(-ix(p-p_1))=$$

$$\frac{1}{2\pi}\int dudp\tilde{\psi}^*(p)\tilde{\psi}(p-u)\exp(-ixu)=\frac{1}{2\pi}\int f(u)\exp(-ixu)du$$

В последнем равенстве мы ввели характеристическую функцию (х.ф.):

$$f(u)=\int dp\tilde{\psi}^*(p)\tilde{\psi}(p-u)=\int dp\tilde{\psi}^*(p+u)\tilde{\psi}(p) \qquad (1.5)$$

Таким образом, мы получили, что плотность распределения можно рассматривать как обратное преобразование Фурье от характеристической функции:

$$P(x) = \frac{1}{2\pi}\int f(u)\exp(-ixu)du \qquad (1.6)$$

Тогда, сама характеристическая функция есть прямое преобразование Фурье от плотности или, что то же самое, математическое ожидание (среднее значение) от случайной величины $\exp(iux)$:

$$f(u) = \int P(x)\exp(ixu)dx = M(\exp(iux))$$

Выкладки, совершенно аналогичные проделанным выше, показывают, что характеристическая функция импульсного распределения вероятностей выражается через свертку от координатной пси- функции. Пусть $\widetilde{f}(t)$- характеристическая функция импульсного распределения, представляющая собой Фурье- образ от плотности распределения импульса $\widetilde{P}(p)$:

$$\widetilde{f}(t) = \int \widetilde{P}(p)\exp(ipt)dp = M(\exp(ipt))$$

В полной аналогии с (1.5) рассматриваемая характеристическая функция может быть представлена в виде свертки от координатной пси- функции:

$$\widetilde{f}(t) = \int dx\psi^*(x-t)\psi(x) = \int dx\psi^*(x)\psi(x+t)$$

Далеко не всякая функция может рассматриваться как характеристическая, поскольку обратное преобразование Фурье от характеристической функции должно давать действительную, неотрицательную функцию (а именно- плотность, нормированную на единицу).

Проведенные выше расчеты, по- существу, позволяют обосновать следующее утверждение: для того, чтобы функция $f(u)$ была характеристической, необходимо и достаточно, чтобы она представлялась в виде свертки (1.5) от комплексной функции $\widetilde{\psi}(p)$, удовлетворяющей условию нормировки:

$$\int dp|\tilde{\psi}(p)|^2 = 1 \qquad (1.7)$$

Необходимость: Пусть $f(u)$ характеристическая функция, тогда, согласно (1.6), она определяет некоторую плотность $P(x)$. Определим пси функцию как $\psi(x) = \sqrt{P(x)}\exp(iS(x))$, где $S(x)$ - произвольная действительная функция (в частности, можно положить $S(x) = 0$). Рассматриваемая процедура может быть названа дополнением классического статистического распределения до квантового состояния. Функция $\tilde{\psi}(p)$, определяемая формулой обратного преобразования Фурье (1.2), обеспечивает искомое представление характеристической функции в виде свертки (1.5). Таким образом, всякой характеристической функции можно сопоставить волновую функцию в импульсном пространстве (причем, такое представление неоднозначно).

Достаточность: Пусть $f(u)$ представлено в виде свертки (1.5) от некоторой функции $\tilde{\psi}(p)$, нормированной согласно (1.7). Определим волновую функцию в координатном пространстве $\psi(x)$ с помощью преобразования Фурье (1.1), а плотность распределения $P(x)$ посредством формулы Борна (1.4). Согласно проведенным выше выкладкам, функция $f(u)$ будет характеристической функцией распределения $P(x)$. Таким образом, всякой волновой функции импульсного пространства $\tilde{\psi}(p)$, можно поставить в соответствие единственную характеристическую функцию $f(u)$ и единственное распределение $P(x)$. Утверждение доказано.

Формула (1.5) уже в рамках классической (неквантовой) статистики вскрывает (хотя и в «свернутом» виде) существование импульсного пространства и соответствующей волновой функции $\tilde{\psi}(p)$. Указанное соотношение характеризует неполноту классических представлений о

вероятности. Действительно, как это было показано выше, свертка (1.5) не позволяет однозначно найти волновую функцию $\tilde{\psi}(p)$ в импульсном пространстве. Аналогично, соотношение (1.4) для плотности не позволяет однозначно найти волновую функцию $\psi(x)$ в координатном пространстве. Таким образом, за одним и тем же классическим распределением вероятности могут скрываться различные квантовые состояния, существенно отличающиеся друг от друга. Другими словами, классическое распределение вероятностей не дает полного описания случайного поведения реальных (квантовых) систем.

Как уже было отмечено выше, чтобы классическая теория стала полной, ее следует дополнить таким образом, чтобы распределение вероятностей превратилось в вектор квантового состояния (для этого можно, например, ввести фазовый множитель). В то же время, более глубокие по своей природе квантовые объекты полностью укладываются в структуру гильбертова пространства векторов состояния. Вектор квантового состояния не требует (да и не допускает) дополнения до каких- либо объектов более общей природы. Мы вернемся к вопросу о полноте квантовой статистической теории и неполноте классической теории вероятностей в главе 3 после рассмотрения основных постулатов квантовой информатики.

Представление характеристической функции в виде свертки является результатом, известным и в классической теории вероятностей (см. теорему 4.2.4 в [32], а также [33]). Однако, классическая теория вероятностей никак не комментирует природу комплексной функции $\tilde{\psi}(p)$, фигурирующей в данном представлении.

Остановимся коротко на важном для дальнейшего изложения способе вычисления моментов случайной величины посредством аппарата характеристических функций.

Нетрудно видеть, что значение х.ф. в точке ноль всегда равно единице:

$f(0)=1$

Моменты случайной величины выражаются через значения соответствующих производных х.ф. в точке ноль. Действительно:

$f'(u)=\int P(x)\exp(ixu)ixdx$, откуда

$f'(0)=iM(x)$.

Таким образом, первая производная х.ф. в точке ноль связана с математическим ожиданием.

Аналогично получаем, что производная k - го порядка связана с k -ым моментом случайной величины:

$f^{(k)}(0)=i^k M(x^k),\ k=0,1,2,...$

1.4. Операторы координаты и импульса в координатном и импульсном представлении. Фундаментальные коммутационные соотношения

Свойства х.ф. позволяют ввести оператор координаты в импульсном представлении. Действительно, рассматривая х.ф. как свертку (1.5), имеем:

$$M(x)=-if'(0)=-i\int dp\tilde{\psi}^*(p)\frac{\partial}{\partial u}\tilde{\psi}(p-u)_{u=0}=i\int dp\tilde{\psi}^*(p)\frac{\partial}{\partial p}\tilde{\psi}(p)$$

Таким образом, если в координатном представлении координата описывается оператором $\hat{x}$, сводящимся к умножению пси- функции на число x, (т.е. $\hat{x}\psi(x)=x\psi(x)$), то в импульсном представлении оператор координаты есть $\hat{x}=i\frac{\partial}{\partial p}$.

Аналогичным образом нетрудно показать, что, если в импульсном представлении импульс описывается оператором $\hat{p}$, просто сводящимся к умножению пси- функции на число p, т.е. $\hat{p}\tilde{\psi}(p)=p\tilde{\psi}(p)$, то в

координатном представлении оператор импульса есть $\hat{p} = -i\frac{\partial}{\partial x}$ (изменение знака перед мнимой единицей i соответствует отличию между прямым и обратным преобразованиями Фурье).

Заметим, что операторы координаты и импульса эрмитовы. Переход от координатного представления к импульсному оставляет инвариантным фундаментальное коммутационное соотношение:

$[\hat{p}, \hat{x}] = \hat{p}\hat{x} - \hat{x}\hat{p} = -i$

В случае нескольких степеней свободы представленное каноническое соотношение примет вид:

$\hat{p}_j \hat{x}_k - \hat{x}_k \hat{p}_j = -i\delta_{jk}$, $j, k = 1,2,...,s$

Здесь s - число степеней свободы

Рассматриваемое соотношение показывает, что каждый импульс не коммутирует только со своей (канонически сопряженной) координатой и коммутирует со всеми остальными координатами.

Все координаты коммутируют между собой, также как и все импульсы коммутируют между собой

$\hat{x}_j \hat{x}_k - \hat{x}_k \hat{x}_j = 0$

$\hat{p}_j \hat{p}_k - \hat{p}_k \hat{p}_j = 0$

Преобразование, сохраняющее фундаментальные коммутационные соотношения, называются каноническими.

Преобразование Фурье является частным случаем унитарных преобразований. Оказывается, что в квантовой информатике можно рассматривать произвольные унитарные преобразования. При этом будет происходить замена одного представления на другое, дополнительное по отношению к исходному. Измерения, проводимые в различных представлениях, порождают совокупность взаимно- дополнительных

распределений. Рассмотренные соображения, изложенные систематическим образом, являются основой постулатов квантовой информатики (см. главу 3).

1.П. Приложение. Дельта- функция и ее свойства.

Мы приведем только краткую сводку некоторых важных свойств дельта-функции. Более полное и строгое изложение вопроса можно найти в [34].

Дельта- функция является важным инструментом в квантовой информатике, поскольку находит широкое применение в таких вопросах, как теория преобразования Фурье, статистический анализ взаимно-дополнительных распределений и др.

Проведем исследования выражения (1.3) из раздела 1.1:

$$\delta(x - x_1) = \frac{1}{2\pi}\int \exp(ip(x - x_1))dp \qquad (1.8)$$

В точке $x_1 = x$ рассматриваемый интеграл заведомо расходится. Проведем его регуляризацию. Ограничим область интегрирования по переменной p в пределах от $-K$ до K. Регуляризованная версия исходного соотношения (1.8) есть:

$$\tilde{\delta}(x - x_1) = \frac{1}{2\pi}\int_{-K}^{K} \exp(ip(x - x_1))dp$$

Элементарное интегрирование сразу приводит к результату:

$$\tilde{\delta}(x - x_1) = \frac{1}{\pi}\frac{\sin(K(x - x_1))}{(x - x_1)}$$

Заметим, что интеграл от полученной функции по переменной x_1 всегда равен единице:

$$\int_{-\infty}^{+\infty} \tilde{\delta}(x - x_1)dx_1 = 1$$

Проанализируем характер поведения рассматриваемой функции $\tilde{\delta}(x-x_1)$. Её максимум находится в точке $x_1 = x$ и равен $\tilde{\delta}(0) = K/\pi$. При больших значениях обрезающего множителя K рассматриваемая функция локализована внутри интервала порядка π/K. При увеличении K функция становится все более и более локализованной вблизи ноля.

Последовательность функций $\tilde{\delta}(x-x_1)$, отвечающая бесконечно растущей последовательности значений K, называется дельта- образной. Дельта- функцию можно определить как обобщенную сингулярную предельную функцию дельта- образной последовательности.

Таким образом:

$$\delta(x) = \frac{1}{\pi}\lim_{K\to\infty}\frac{\sin(Kx)}{x}$$

Приведем также некоторые другие представления для дельта- функции:

$$\delta(x) = \frac{1}{\pi}\lim_{K\to\infty}\frac{\sin^2(Kx)}{Kx^2} \qquad (1.9)$$

$$\delta(x) = \lim_{\sigma\to 0}\frac{1}{\sqrt{2\pi}\sigma}\exp\left(-\frac{x^2}{2\sigma^2}\right) \qquad (1.10)$$

Задача 1.3 Обоснуйте представления (1.9) и (1.10) для дельта- функции.

Дельта- функция может рассматриваться как производная от ступенчатой функции (функции Хевисайда)

$$\delta(x) = \Theta'(x), \qquad \text{где}$$

$$\Theta(x) = \begin{cases} 1, x \geq 0 \\ 0, x < 0 \end{cases}$$

Основное свойство дельта- функции определяет способ ее интеграции с произвольной несингулярной функцией:

$$\int \delta(x) f(x) dx = f(0)$$

Нетрудно получить и некоторые другие свойства для дельта- функции

$$\int \delta(x - x_0) f(x) dx = f(x_0) \qquad (1.11)$$

$$\int \delta(ax) f(x) dx = \frac{1}{|a|} f(0) \qquad (1.12)$$

$$\int \delta(g(x)) f(x) dx = \sum_i \frac{1}{|g'(x_i)|} f(x_i), \qquad (1.13)$$

где x_i - простые корни функции $f(x)$

Задача 1.4. Обоснуйте приведенные формулы (1.11)- (1.13).

Глава 2. Точность статистических характеристик гильбертова пространства

В настоящей главе мы увидим, что различного вида неравенства Коши-Буняковского, соотношения неопределенностей, а также неравенства Рао-Крамера получаются, по- существу, с помощью одного и того же математического приема, сводящегося к элементарному требованию неотрицательности некоторого квадратного трехчлена. В разделах 2.1- 2.3 с использованием принципов квантовой информатики излагаются элементарные сведения, связанные с неравенством Коши- Буняковского и соотношением неопределенностей. В разделе 2.4 представлено так называемое соотношение неопределенностей Шредингера- Робертсона. В разделе 2.5 рассмотрено многомерное соотношение неопределенностей. Информация Фишера и неравенство Рао- Крамера, известные еще из классической математической статистики, изучаются в разделах 2.6- 2.8 с новой квантово- информационной точки зрения.

2.1. Неравенство Коши- Буняковского для векторов состояния и его статистическая интерпретация

Рассматриваемое неравенство имеет место для векторов произвольных линейных пространств, в которых определено понятие скалярного произведения. Приведем примеры таких пространств.

В комплексном конечномерном пространстве C^s размерности s скалярное произведение двух векторов определяется следующей формулой (в обозначениях Дирака):

$$\langle \varphi | \psi \rangle = \sum_{j=1}^{s} \varphi_j^* \psi_j$$

В бесконечномерном гильбертовом пространстве l_2 аналогичное определение имеет вид:

$$\langle \varphi | \psi \rangle = \sum_{j=1}^{\infty} \varphi_j^* \psi_j$$

Наконец, если $\psi(x)$ и $\varphi(x)$ - комплексные функции из пространства L_2, то их скалярное произведение есть:

$$\langle \varphi | \psi \rangle = \int \varphi^*(x) \psi(x) dx$$

Покажем, что для любых векторов линейного пространства со скалярным произведением выполняется следующее неравенство Коши- Буняковского:

$$\left| \langle \varphi | \psi \rangle \right|^2 \le \langle \varphi | \varphi \rangle \langle \psi | \psi \rangle$$

Для определенности, при проведении выкладок будем иметь ввиду функции из пространства L_2.

Предположим вначале, что скалярное произведение $\langle \varphi | \psi \rangle$- действительное число.

Пусть ξ- действительный параметр. Рассмотрим следующую заведомо неотрицательную функцию от ξ (эта функция представляет собой интеграл от заведомо неотрицательного выражения).

$$F(\xi) = \int (\psi(x) + \xi \varphi(x))(\psi^*(x) + \xi \varphi^*(x)) dx \ge 0$$

В обозначениях Дирака имеем:

$$F(\xi) = \left(\langle \psi | + \xi \langle \varphi | \right)\left(| \psi \rangle + \xi | \varphi \rangle \right)$$

В развернутой записи рассматриваемая функция представляет собой квадратный трехчлен:

$$F(\xi) = \xi^2 \langle \varphi | \varphi \rangle + 2\xi \langle \varphi | \psi \rangle + \langle \psi | \psi \rangle$$

Здесь мы учли предположение о действительности рассматриваемого скалярного произведения, т.е. $\langle \varphi | \psi \rangle = \langle \psi | \varphi \rangle$.

Условие неотрицательности означает, что дискриминант меньше или равен нулю:

$$4\left(\langle\varphi|\psi\rangle\right)^2 - 4\langle\varphi|\varphi\rangle\langle\psi|\psi\rangle \le 0$$

Таким образом в рассматриваемом случае выполняется неравенство Коши- Буняковского:

$$\left(\langle\varphi|\psi\rangle\right)^2 \le \langle\varphi|\varphi\rangle\langle\psi|\psi\rangle$$

Предположим теперь, что $\langle\varphi|\psi\rangle$ - комплексное число. Пусть $\langle\varphi|\psi\rangle = r\exp(i\alpha)$, где r и α - действительные числа.

Введем функцию, отличающуюся от $\varphi(x)$ только фазой

$$\tilde{\varphi}(x) = \varphi(x)\exp(i\alpha)$$

Тогда $\langle\tilde{\varphi}|\psi\rangle = r$ является действительным числом и для него выполняется доказанное выше неравенство:

$$\left(\langle\tilde{\varphi}|\psi\rangle\right)^2 \le \langle\tilde{\varphi}|\tilde{\varphi}\rangle\langle\psi|\psi\rangle$$

Учтем, что введенное фазовое преобразование не меняет модуля скалярного произведения, поэтому: $\left|\langle\varphi|\psi\rangle\right|^2 = \left(\langle\tilde{\varphi}|\psi\rangle\right)^2$, $\langle\tilde{\varphi}|\tilde{\varphi}\rangle = \langle\varphi|\varphi\rangle$.

Таким образом, неравенство Коши- Буняковского выполняется и в общем случае:

$$\left|\langle\varphi|\psi\rangle\right|^2 \le \langle\varphi|\varphi\rangle\langle\psi|\psi\rangle$$

Введем величину F, называемую согласованностью (fidelity) квантовых состояний $\varphi(x)$ и $\psi(x)$.

$$F = \frac{\left|\langle\varphi|\psi\rangle\right|^2}{\langle\varphi|\varphi\rangle\langle\psi|\psi\rangle}$$

Для состояний, нормированных на единицу, имеем просто:

$$F = \left|\langle \varphi | \psi \rangle\right|^2$$

Из неравенства Коши- Буняковского следует, что

$0 \le F \le 1$

Если исходить из этого неравенства, то заманчиво предположить, что F задает некоторую вероятность. Так оно и есть. Статистический смысл величины F заключается в том, что она задает вероятность *обнаружения* квантовой системы в состоянии $\varphi(x)$ при условии, что она была *приготовлена* в состоянии $\psi(x)$

Обмен информацией в природе предполагает, что состояние $\psi(x)$, приготовленное (созданное) на одном конце (в системе «передатчик») может быть обнаружено (воспринято) таковым в другой системе-«приёмнике». В идеальном случае «приемник» может быть настроен на получение того же квантового состояния, когда $\varphi(x) = \psi(x)$ (с точностью до фазового множителя). В этом случае $F = 1$. В действительности состояния $\psi(x)$ и $\varphi(x)$, на которые настроен приемник и передатчик соответственно, всегда хотя бы немного отличаются и $F < 1$. В рассматриваемом случае, таким образом, F задает вероятность «успеха» приемно- передающего акта.

2.2.Неравенство Коши- Буняковского в приложении к случайным величинам

Пусть $Y = Y(x)$ и $Z = Z(x)$ - действительные случайные величины, представляющие собой произвольные функции от координаты x. Пусть ξ - действительный параметр. Рассмотрим заведомо неотрицательную функцию от ξ:

$$F(\xi) = \langle \psi | (\xi Y + Z)^2 | \psi \rangle \ge 0$$

В развернутой записи рассматриваемая функция представляет собой квадратный трехчлен:

$$F(\xi) = \xi^2 M\left(Y^2\right) + 2\xi M(YZ) + M\left(Z^2\right)$$

Условие неотрицательности означает, что дискриминант меньше или равен нулю:

$$4\left(M(YZ)\right)^2 - 4M\left(Y^2\right)M\left(Z^2\right) \le 0$$

Таким образом для любых (коммутирующих) случайных величин выполняется неравенство Коши- Буняковского:

$$\left(M(YZ)\right)^2 \le M\left(Y^2\right)M\left(Z^2\right)$$

В частности, если в качестве случайных величин рассмотреть величины $Y - M(Y)$ и $Z - M(Z)$, приведенные к нулевым средним значениям, то для дисперсий получим неравенство:

$$D_Y D_Z \ge \left[M\left(\left(Y - M(Y)\right)\left(Z - M(Z)\right)\right)\right]^2 .$$

Из последнего выражения следует неравенство для коэффициента корреляции

$$r^2 \le 1$$

Напомним, что коэффициент корреляции между случайными величинами Y и Z определяется формулой:

$$r = \frac{M\left[\left(Y - M(Y)\right)\left(Z - M(Z)\right)\right]}{\sqrt{D_Y D_Z}}$$

Квадрат коэффициента корреляции иногда называют коэффициентом детерминации. Этот коэффициент показывает, в какой мере случайная величина Y определяет (детерминирует) случайную величину Z и наоборот.

Можно показать, что неравенство Коши- Буняковского обращается в равенство в том и только том случае, когда случайные величины Y и Z линейно связаны между собой.

2.3. Соотношение неопределенностей Гейзенберга для координаты и импульса

Модифицируем приведенный выше пример. Рассмотрим вместо $\xi Y + Z$ выражение $\xi \frac{\partial}{\partial x} + x$. Заметим, что оператор производной не является эрмитовым, потому что $\frac{\partial}{\partial x}^{+} = -\frac{\partial}{\partial x}$. Чтобы запись сделать более наглядной введем эрмитов оператор импульса $\hat{p} = -i\frac{\partial}{\partial x}$.

Рассмотрим как и при выводе неравенства Коши- Буняковского заведомо неотрицательную функцию от действительного параметра ξ

$$F(\xi) = \langle \psi | (-i\xi\hat{p} + \hat{x})(i\xi\hat{p} + \hat{x}) | \psi \rangle \geq 0$$

В развернутой записи имеем:

$$F(\xi) = \xi^2 M(\hat{p}^2) - i\xi M(\hat{p}\hat{x} - \hat{x}\hat{p}) + M(\hat{x}^2)$$

Учтем каноническое коммутационное соотношение

$$\hat{p}\hat{x} - \hat{x}\hat{p} = -i$$

В качестве наблюдаемых рассмотрим величины $\hat{x} - M(\hat{x})$ и $\hat{p} - M(\hat{p})$, которые, очевидно, удовлетворяют тому же коммутационному соотношению. Тогда для произведения дисперсий координаты и импульса получим искомое соотношение неопределенностей Гейзенберга :

$$D_x D_p \geq \frac{1}{4}$$

Дисперсия импульса есть средний квадрат импульса минус средний импульс в квадрате:

$$D_p = M\left(\hat{p}^2\right) - \left(M\left(\hat{p}\right)\right)^2$$

В развернутой записи средний квадрат импульса есть:

$$M\left(\hat{p}^2\right) = -\int \psi^*(x)\frac{\partial^2}{\partial x^2}\psi(x)dx = \int \frac{\partial}{\partial x}\psi^*(x)\int \frac{\partial}{\partial x}\psi(x)dx$$

Как следует из приведенных выкладок, неравенство обращается в равенство в том и только том случае, когда при некотором ξ:

$$\left(i\xi\hat{p} + \hat{x}\right)\left|\psi\right\rangle = 0$$

Это равенство имеет место только для гауссова состояния (основного состояния гармонического осциллятора).

Решение полученного уравнения в координатном и импульсном представлении соответственно есть:

$$\psi(x) = \frac{1}{\left(2\pi\sigma_x^2\right)^{1/4}}\exp\left(-\frac{(x-x_0)^2}{4\sigma_x^2}\right)$$

$$\tilde{\psi}(p) = \frac{1}{\left(2\pi\sigma_p^2\right)^{1/4}}\exp\left(-\frac{(p-p_0)^2}{4\sigma_p^2}\right)$$

Здесь x_0 и σ_x^2 - соответственно среднее и дисперсия для распределения координаты, а p_0 и σ_p^2 - соответственно среднее и дисперсия для распределения импульса.

Дисперсия координаты и импульса полученного гауссовского состояния определяются введенным параметром ξ

$$\sigma_x^2 = \frac{\xi}{2}\ ,\ \sigma_p^2 = \frac{1}{2\xi}$$

Таким образом, рассматриваемые величины оказываются связанными между собой минимальным соотношением неопределенностей:

$$\sigma_x^2\sigma_p^2 = \frac{1}{4}$$

Мы видим, что состояние, минимизирующее соотношение неопределенностей, описывается действительной функцией. Это обстоятельство неслучайно. Нетрудно видеть, что добавление произвольного фазового множителя к действительной координатной пси- функции не может уменьшить дисперсию импульса и, таким образом, не может усилить рассматриваемое неравенство.

2.4. Соотношение неопределенностей Шредингера- Робертсона

Неравенство, предложенное Шредингером и Робертсоном, отражает в себе свойства, присущие как неравенству Коши- Буняковского, так и соотношению неопределенностей Гейзенберга и, в известном смысле, может считаться их обобщением [35,36].

Пусть z_1 и z_2 - две произвольные наблюдаемые. Без ограничения общности будем считать их центрированными: $M(z_1) = M(z_2) = 0$.

Рассмотрим следующее заведомо неотрицательное выражение:

$$F(\xi) = \langle\psi|(\xi\exp(-i\varphi)z_2 + z_1)(\xi\exp(i\varphi)z_2 + z_1)|\psi\rangle$$

Здесь ξ - произвольное действительное число, φ - тоже действительное, но фиксированное число (фаза, выбор которой мы осуществим позднее).

Определим ковариацию величин как

$$\mathrm{cov}(z_1, z_2) = \frac{1}{2}\langle\psi|z_1z_2 + z_2z_1|\psi\rangle$$

Заметим, что симметризация произведения наблюдаемых потребовалась нам, чтобы сделать соответствующий оператор эрмитовым.

Пусть:

$$z_1 z_2 - z_2 z = iC,$$

где C - эрмитов оператор. Тогда:

$$M(C) = -i\langle\psi|z_1 z_2 - z_2 z_1|\psi\rangle$$

В развернутой записи выражение для $F(\xi)$ имеет вид:

$$F(\xi) = \xi^2 M\left(z_2^2\right) + \xi\left(2\,\mathrm{cov}(z_1, z_2)\cos(\varphi) - M(C)\sin(\varphi)\right) + M\left(z_1^2\right)$$

Пусть:

$$\rho^2 = 4\left(\mathrm{cov}(z_1, z_2)\right)^2 + \left(M(C)\right)^2,$$

Очевидно, можно найти такой угол β, чтобы выполнялись тождества:

$$2\,\mathrm{cov}(z_1, z_2) = \rho\cos(\beta)$$

$$M(C) = \rho\sin(\beta)$$

Тогда:

$$F(\xi) = \xi^2 M\left(z_2^2\right) + \xi\rho\cos(\varphi + \beta) + M\left(z_1^2\right) \geq 0$$

Распорядимся произволом в выборе фазы φ, чтобы обеспечить выполнение равенства $\cos(\varphi + \beta) = 1$. Указанный выбор, очевидно, обеспечит получение наиболее сильного неравенства:

$$M\left(z_1^2\right)M\left(z_2^2\right) = D(z_1)D(z_2) \geq \frac{\rho^2}{4} = \left(\left(\mathrm{cov}(z_1, z_2)\right)^2 + \frac{\left(M(C)\right)^2}{4}\right)$$

Определим коэффициент корреляции между наблюдаемыми z_1 и z_2 как:

$$r = \frac{\mathrm{cov}(z_1, z_2)}{\sqrt{D(z_1)D(z_2)}}$$

В результате, искомое неравенство (соотношение неопределенностей Шредингера- Робертсона) примет вид:

$$D(z_1)D(z_2) \geq \frac{\left(M(C)\right)^2 K^2}{4},$$

где $K = \frac{1}{\sqrt{1-r^2}}$

Введенный параметр K есть аналог известного числа Шмидта [37]. Это число имеет фундаментальное значение для описания квантовых корреляций и квантовой информации (см. Приложение к Главе 3).

Пусть теперь рассматриваемые наблюдаемые есть операторы координаты и импульса соответственно:

$z_1 = x$, $z_2 = p$.

Тогда, в силу фундаментального перестановочного соотношения для координаты и импульса, C есть тождественный оператор (единичная матрица).

В этом случае соотношение неопределенностей Шредингера- Робертсона будет иметь вид:

$$D(x)D(p) \geq \frac{K^2}{4}$$

Пусть $\Delta x = \sqrt{D(x)}$, $\Delta p = \sqrt{D(p)}$ - неопределенности (стандартные отклонения) для координаты и импульса. Тогда:

$$\Delta x \Delta p \geq \frac{K}{2}$$

Таким образом, если координата и импульс коррелируют друг с другом, произведение их неопределенностей возрастает в K раз по сравнению с величиной, определяемой неравенством Гейзенберга.

Заметим, что в силу некоммутативности координаты и импульса, их квантовая ковариация не может быть оценена по выборке подобно классической ковариации. Для вычисления соответствующей оценки нужно знать априори (или оценить по результатам взаимно- дополнительных измерений) вектор состояния (волновую функцию). Пусть:

$\psi(x) = \sqrt{P(x)}\exp(iS(x))$,

где действительные функции $P(x)$ и $S(x)$ есть соответственно плотность и фаза пси- функции. Заметим, что фаза $S(x)$ есть аналог классического действия механической системы.

Используя функции плотности и фазы, нетрудно получить следующее простое представление для ковариации координаты и импульса:

$$\mathrm{cov}(x,p)=\frac{1}{2}\langle\psi|\hat{x}\hat{p}+\hat{p}\hat{x}|\psi\rangle=\int x\frac{\partial S(x)}{\partial x}P(x)dx$$

Наглядность полученного результата обусловлена тем, что в классической механике производная от функции действия $\frac{\partial S}{\partial x}$ есть импульс.

2.5. Многомерное соотношение неопределенностей

Рассмотрим пространство размерности s.

Пусть $\hat{x}_j, \hat{p}_j$, $j=1,...,s$ - соответствующие операторы координат и импульсов.

Вывод соотношения неопределенности в многомерном случае аналогичен одномерному, но теперь вместо действительного числа ξ следует ввести действительную симметричную матрицу Ξ с элементами $\xi_{j\sigma}$, $j,\sigma=1,...,s$. Такое видоизменение диктуется необходимостью придать рассматриваемым величинам геометрически инвариантный вид в гильбертовом пространстве. Действительно для скалярного ξ, такая величина как $\left(i\xi\hat{p}_\rho+\hat{x}_l\right)|\psi\rangle$ неинвариантна, потому что индексы ρ и l, вообще говоря, различны. В то же время, для матрицы Ξ величина $\left(i\xi_{l\rho}\hat{p}_\rho+\hat{x}_l\right)|\psi\rangle$ будет кет- вектором в гильбертовом пространстве (по повторяющемуся индексу ρ предполагается суммирование). Введем также действительный вектор η (η_j $j=1,...,s$). С

его помощью, взяв скалярное произведение, преобразуем полученный кет-вектор в скаляр: $\left(i\xi_{l\rho}\hat{p}_\rho + \hat{x}_l\right)\eta_l\left|\psi\right\rangle = 0$.

Рассмотрим теперь следующее заведомо неотрицательное выражение (по повторяющимся индексам, как обычно, предполагается суммирование):

$$F(\xi) = \left\langle\psi\left|\eta_j\left(-i\xi_{j\sigma}\hat{p}_\sigma + \hat{x}_j\right)\left(i\xi_{l\rho}\hat{p}_\rho + \hat{x}_l\right)\eta_l\right|\psi\right\rangle \geq 0$$

В развернутом виде получим:

$$F(\xi) = \left\langle\psi\left|\eta_j\eta_l\left(\xi_{j\sigma}\xi_{l\rho}\hat{p}_\sigma\hat{p}_\rho - i\left(\xi_{j\rho}\hat{p}_\rho\hat{x}_l - \xi_{l\rho}\hat{x}_j\hat{p}_\rho\right) + \hat{x}_j\hat{x}_l\right)\right|\psi\right\rangle \geq 0$$

Чтобы использовать фундаментальные коммутационные соотношения между координатой и импульсом, перепишем последнее выражение, осуществив замену индексов j и l друг на друга, после чего сложим полученное выражение с исходным.

В качестве наблюдаемых будем использовать центрированные координаты и импульсы (имеющие нулевые средние).

В результате получим условие, согласно которому нижеследующее матричное выражение является неотрицательно определенным:

$$\Xi\Sigma_p\Xi - \Xi + \Sigma_x \geq 0$$

Напомним, что матрица A с элементами a_{jk} называется неотрицательно определенной, если для любого вектора $\left|z\right\rangle$:

$$\left\langle z\left|A\right|z\right\rangle = a_{jk}z_j^*z_k \geq 0$$

В полученном неравенстве мы ввели матрицы ковариаций координат и импульсов. Элементы этих матриц определяются выражениями

$$\left(\Sigma_x\right)_{jl} = \left\langle\psi\left|\hat{x}_j\hat{x}_l\right|\psi\right\rangle$$

$$\left(\Sigma_p\right)_{jl} = \left\langle\psi\left|\hat{p}_j\hat{p}_l\right|\psi\right\rangle$$

Учтем, что неотрицательная определенность матрицы ковариаций импульсов позволяет определить квадратный корень из нее.

Напомним, что произвольная эрмитова матрица A может быть приведена к диагональному виду, т.е. может быть представлена как:

$$A = UDU^{+},$$

где U - унитарная матрица, а D - действительная диагональная матрица.

Если, к тому же, матрица A неотрицательно определена, то неотрицательны и ее собственные значения, образующие диагональ матрицы D. В этом случае операция взятия квадратного корня из матрицы является хорошо определенной:

$$A^{1/2} = UD^{1/2}U^{+}$$

С использованием понятия матричного квадратного корня, полученное выше неравенство можно представить в виде:

$$\left(\Xi\Sigma_p^{1/2} - \frac{1}{2}\Sigma_p^{-1/2}\right)\left(\Sigma_p^{1/2}\Xi - \frac{1}{2}\Sigma_p^{-1/2}\right) - \frac{1}{4}\Sigma_p^{-1} + \Sigma_x \geq 0$$

Первое слагаемое слева заведомо неотрицательно определено (и обращается в ноль при $\Xi = \frac{1}{2}\Sigma_p^{-1}$). Отсюда следует, что и выражение $-\frac{1}{4}\Sigma_p^{-1} + \Sigma_x$ неотрицательно определено, т.е.

$$\Sigma_x \geq \frac{1}{4\Sigma_p}$$

Полученное неравенство и есть искомое многомерное соотношение неопределенностей. Его смысл заключается в следующем: каково бы ни было квантовое состояние, матрица, равная разности $\Sigma_x - \frac{1}{4}\Sigma_p^{-1}$ между матрицей ковариации координат и одной четвертой от матрицы, обратной к матрице ковариации импульсов, всегда является неотрицательно определенной.

Из приведенных расчетов следует, что неравенство обращается в равенство в том и только том случае, когда вектор состояния удовлетворяет следующему условию при $\Xi = \frac{1}{2}\Sigma_p^{-1}$:

$$\left(i\xi_{l\rho}\hat{p}_\rho + \hat{x}_l\right)\left|\psi\right\rangle = 0$$

Отсюда получаем, что соответствующее состояние является гауссовским с матрицей ковариаций Σ_p в импульсном представлении и матрицей ковариаций $\Sigma_x = \frac{1}{4\Sigma_p}$ - в координатном.

Мы ограничились рассмотрением многомерного соотношения неопределенностей, которое является непосредственным обобщением одномерного соотношения неопределенностей Гейзенберга. Другие примеры обобщенных соотношений неопределенностей и, в частности, связанные с обобщением соотношения Шредингера- Робертсона можно найти в [35,36]

2.6. Информация Фишера

Рассмотрим квантовую систему, для которой пси- функция действительна: $\psi(x) = \sqrt{P(x)}$. Использование таких пси- функций представляет собой простейший способ дополнения классической плотности распределения до квантового состояния. Для такой системы средний импульс равен нулю, а квадрат импульса есть:

$$M\left(\hat{p}^2\right) = \int \frac{\partial}{\partial x}\sqrt{P(x)}\frac{\partial}{\partial x}\sqrt{P(x)}dx = \frac{1}{4}\int \frac{\left(P'(x)\right)^2}{P(x)}dx$$

Здесь штрих означает производную по x.

Введем информацию Фишера, связанную с дисперсией импульса:

$$I_x = 4D_p = 4M\left(\hat{p}^2\right) = \int \frac{\left(P'(x)\right)^2}{P(x)}dx$$

Тогда соотношение неопределенностей запишется в виде следующего неравенства:

$$D_x I_x \geq 1$$

Полученное неравенство аналогично неравенству Рао- Крамера, рассматриваемому в следующем разделе

2.7. Неравенство Рао- Крамера

Рассмотрим снова ситуацию, когда плотность распределения дополняется до квантового состояния. Пусть распределение вероятностей и соответствующее квантовое состояние зависят от некоторого действительного параметра θ, т.е.:

$$\psi(x|\theta) = \sqrt{P(x|\theta)}.$$

Пусть $\hat{\theta}$ есть несмещенная оценка неизвестного параметра θ, основанная на выборке объема n в координатном пространстве, т.е. $\hat{\theta} = \hat{\theta}(x_1,...,x_n)$.

Условие несмещенности означает, что среднее значение (математическое ожидание) выборочной оценки $\hat{\theta}$ совпадает с истинным значением параметра θ, т.е.

$$M(\hat{\theta}) = \int P(x_1|\theta)\cdots P(x_n|\theta)\cdot\hat{\theta}(x_1,...,x_n)dx_1\cdots dx_n = \theta$$

Примерами несмещенных оценок могут служить известные оценки математического ожидания и дисперсии [31]:

$$\bar{x} = \frac{x_1 + ... + x_n}{n}$$

$$s^2 = \frac{1}{n-1}\sum_{k=1}^{n}(x_k - \bar{x})^2$$

Пусть $p_\theta = -i\frac{\partial}{\partial\theta}$ - оператор, канонически сопряженный параметру θ.

Нашей целью является вывод следующего соотношения, называемого неравенством Рао-Крамера:

$$D_\theta I_\theta \geq 1$$

Здесь введена информация Фишера, которая имеет вид:

$$I_\theta = n\int \frac{\left(\partial P\left(x|\theta\right)/\partial\theta\right)^2}{P\left(x|\theta\right)}dx = n\int\left(\frac{\partial \ln P\left(x|\theta\right)}{\partial\theta}\right)^2 P\left(x|\theta\right)dx$$

Воспользуемся тем, что вектор состояния для выборки может быть определен следующим выражением

$$\psi\left(x_1,...,x_n\right) = \sqrt{P\left(x_1|\theta\right)\cdots P\left(x_n|\theta\right)}$$

Проведем подробные вычисления. Пусть $\xi\frac{\partial\psi}{\partial\theta} + \left(\theta - \hat{\theta}\right)\psi$ - кет вектор, где ξ, как и ранее, произвольный действительный параметр, $\xi\frac{\partial\psi^*}{\partial\theta} + \left(\theta - \hat{\theta}\right)\psi^*$ - соответствующий бра- вектор.

Заведомо неотрицательное выражение есть:

$$F\left(\xi\right) = \int\left(\xi\frac{\partial\psi^*}{\partial\theta} + \left(\theta - \hat{\theta}\right)\psi^*\right)\left(\xi\frac{\partial\psi}{\partial\theta} + \left(\theta - \hat{\theta}\right)\psi\right)dx$$

Здесь для сокращения записи мы полагаем, что $dx = dx_1\cdots dx_n$, $\psi = \psi\left(x_1,...,x_n\right)$

В развернутой записи имеем:

$$F\left(\xi\right) = a\xi^2 + b\xi + c \geq 0,$$

где

$$a = \frac{I_\theta}{4} = \int\frac{\partial\psi^*}{\partial\theta}\frac{\partial\psi}{\partial\theta}dx$$

$$b = \int \left(\theta - \hat{\theta}\right)\left(\psi * \frac{\partial \psi}{\partial \theta} + \frac{\partial \psi *}{\partial \theta} \psi \right) dx$$

$$c = \int \left(\theta - \hat{\theta}\right)^2 \psi * \psi dx = D_\theta$$

Можно показать, что $b = -1$. Для этого достаточно представить подинтегральное выражение с помощью формулы для производной произведения в виде

$$\left(\theta - \hat{\theta}\right)\left(\psi * \frac{\partial \psi}{\partial \theta} + \frac{\partial \psi *}{\partial \theta} \psi \right) = \frac{\partial\left(\left(\theta - \hat{\theta}\right)\psi * \psi\right)}{\partial \theta} - \psi * \psi \frac{\partial\left(\theta - \hat{\theta}\right)}{\partial \theta} =$$

$$= \frac{\partial\left(\left(\theta - \hat{\theta}\right)\psi * \psi\right)}{\partial \theta} - \psi * \psi$$

Интеграл от первого слагаемого равен нулю в силу несмещенности оценки. В результате, учитывая условие нормировки, получаем, что $b = -1$.

Из условия $b^2 - 4ac \le 0$ для дискриминанта получаем искомый результат – неравенство Рао-Крамера [38- 40]:

$$D_\theta \ge \frac{1}{I_\theta}$$

Заметим, что мы провели вычисления не только для предполагаемого случая действительных векторов состояния, но и для более общего случая комплексных пси- функций.

В этом случае информация Фишера есть:

$$I_\theta = 4 \int \frac{\partial \psi^*}{\partial \theta} \frac{\partial \psi}{\partial \theta} dx$$

Информация Фишера является аналогом дисперсии импульса и отличается от последней множителем 4 и тем, что под интегралом идет дифференцирование по параметру, а не по координате.

Для случая действительных пси- функций, как нетрудно показать, имеет место приведенное выше выражение для информации Фишера (6). При

выводе следует воспользоваться легко проверяемым свойством аддитивности информации Фишера (информация от n независимых представителей в n раз превосходит информацию от одного представителя).

Полученное неравенство, очевидно, является наиболее сильным для случая, когда информация Фишера I_θ минимальна. Как и в случае соотношения неопределенности Гейзенберга, можно показать, что добавление произвольного фазового множителя к действительной пси- функции не может привести к уменьшению информации Фишера.

Выше мы видели, что соотношение неопределенностей из неравенства превращается в равенство для гауссова состояния. Аналогичный результат справедлив и для неравенства Рао- Крамера. Последнее превращается в равенство для оценок, имеющих нормальное распределение и только для них. Такие оценки называются эффективными.

Выше мы предполагали несмещенность статистической оценки. Однако, проведенные выкладки позволяют также получить более общее неравенство Рао- Крамера, пригодное и для смещенных оценок. В этом случае оно имеет вид:

$$M\left(\theta-\hat{\theta}\right)^2 \geq \frac{\left(1+\beta'(\theta)\right)^2}{I_\theta} \qquad (2.1)$$

где $\beta(\theta)=M\left(\hat{\theta}\right)-\theta$ - смещение оценки. (2.2)

Заметим, что в представленном неравенстве слева вместо обычной дисперсии стоит величина, которая характеризует рассеяние выборочной оценки $\hat{\theta}$ относительно истинного значения θ.

Задача 2.1 Обоснуйте неравенство Рао- Крамера (2.1)- (1.2), учитывающее возможную смещенность оценки.

2.8. Многомерное неравенство Рао- Крамера и корневая оценка

«Смотри в корень!» (Козьма Прутков «Мысли и афоризмы», №228).

Неравенство Рао- Крамера, также как и соотношение неопределенностей, может быть обобщено на многомерный случай.

Можно показать, что для любой несмещенной оценки $\hat{\theta}$ неизвестного многомерного параметра θ матрица $\Sigma_\theta - I_\theta^{-1}$ является неотрицательно определенной:

$$\Sigma_\theta - I_\theta^{-1} \geq 0$$

В случае оценок, близких к эффективным, соответствующая разность близка к нулю. Примером таких оценок могут служить оценки максимального правдоподобия, которые обладают свойством асимптотической эффективности [38- 40].

Здесь Σ_θ - матрица ковариации оценки $\hat{\theta}$. Элементы матрицы информации Фишера I_θ могут быть представлены в виде:

$$\left(I_\theta\right)_{jk} = n\int \frac{\partial \ln P\left(x|\theta\right)}{\partial \theta_j}\frac{\partial \ln P\left(x|\theta\right)}{\partial \theta_k}P\left(x|\theta\right)dx \qquad (2.3)$$

С точки зрения квантовой информатики принципиально важно, что выражение для информационной матрицы Фишера радикально упрощается, если ввести пси – функцию (здесь для простоты мы считаем ее действительной) [41,42].

$$\left(I_\theta\right)_{jk} = n\int \frac{\partial \psi\left(x|\theta\right)}{\partial \theta_j}\frac{\partial \psi\left(x|\theta\right)}{\partial \theta_k}dx$$

Для задач статистики фундаментальное значение имеет матрица, обратная к матрице информации Фишера. В силу сложности выражения (2.3) для многопараметрической матрицы информации Фишера, получаемые на его основе оценки обратной матрицы, как правило, являются плохо обусловленными. Единственным известным исключением является так называемая корневая оценка, основанная на введении пси – функции.

Приведем кратко соответствующие результаты. Более подробное изложение можно найти в [41,42].

Пусть разложение пси- функции по набору ортонормированных базисных функций $\varphi_j(x)\ \ j = 0,1,...,s-1$ имеет вид:

$$\psi(x) = \sqrt{1-\left(c_1^2 + ... + c_{s-1}^2\right)}\varphi_0(x) + c_1\varphi_1(x) + ... + c_{s-1}\varphi_{s-1}(x) \qquad (2.4)$$

Здесь мы исключили из числа оцениваемых параметров коэффициент $c_0 = \sqrt{1-\left(c_1^2 + ... + c_{s-1}^2\right)}$, так как, согласно условию нормировки, он рассчитывается через другие коэффициенты.

Величины $c_1, c_2, ..., c_{s-1}$ являются независимыми оцениваемыми параметрами.

В случае корневого разложения (2.4) информационная матрица I_{ij} имеет порядок $(s-1)\times(s-1)$ и выражается в следующем простом виде:

$$I_{ij} = 4n\left(\delta_{ij} + \frac{c_i c_j}{c_0^2}\right),$$

где $c_0 = \sqrt{1-\left(c_1^2 + ... + c_{s-1}^2\right)}$

Замечательной особенностью полученного выражения является его независимость от выбора базисных функций. Оказывается, что этим свойством обладает только корневая оценка плотности.

Матрица ковариаций оценки вектора состояния $\hat{c}$, в случае оценок, близких к эффективным, есть приближенно матрица, обратная к матрице информации Фишера:

$$\Sigma(\hat{c}) = I^{-1}(c)$$

Компоненты этой матрицы есть:

$$\Sigma_{ij} = \frac{1}{4n}\left(\delta_{ij} - c_i c_j\right) \qquad i, j = 1,...,s-1 \tag{2.5}$$

Полученную матрицу ковариаций можно расширить, добавив в нее ковариации компоненты $\hat{c}_0$ вектора состояния с остальными компонентами. Оказывается, что общая матрица ковариаций будет иметь тот же самый вид, что и (2.5), но теперь $i, j = 0,1,...,s-1$.

Таким образом, модель статистики, основанная на введении пси- функции, корневом разложении и методах квантовой информатики, является выделенной по отношению к любым другим мыслимым моделям. Её преимущества обусловлены простотой, универсальностью и хорошими вычислительными свойствами. Выражаясь в духе Дирака, можно сказать, что «Природа просто не могла не воспользоваться столь красивой математической моделью».

Эффективность корневого подхода в задачах восстановления квантовых состояний была подтверждена в работах [43-47]. Была показана возможность экспериментального восстановления оптических квантовых состояний так называемого бифотонного поля с высокой точностью, которая значительно превосходит уровень других известных экспериментов.

Опыт квантовой физики показывает, что при описании поведения микрообъектов целесообразно отказаться от явно ограниченных представлений, сводящих квантовые системы к механическим частицам, волнам и т.п. Вместо механистических картин явлений следует использовать статистическое описание квантовых состояний, которое оказывается наиболее

естественным и полным. При этом, само статистическое описание не должно ассоциироваться с механистическими моделями, основанными на случайном механическом выборе объектов, бросании монеты, игральной кости и т.п. Выше мы пытались показать, что наиболее фундаментальные представления о вероятности никак не связаны с такими механическими моделями и аналогиями. Статистическая модель, в основе которой лежит вектор состояния в гильбертовом пространстве и есть наиболее общая и универсальная модель теории вероятностей.

Глава 3. Принципы квантовой информатики и шестая проблема Гильберта

3.1 Постулаты квантовой информатики

«У всякого портного свой взгляд на искусство!» (Козьма Прутков «Мысли и афоризмы», №151).

Постулаты квантовой информатики должны вскрывать наиболее глубокие и наиболее фундаментальные идеи квантовой теории. Существуют различные точки зрения на то, какие понятия квантовой теории следует считать основными. В этой связи представляется интересным проследить эволюцию взглядов П. Дирака на парадигму квантовой физики. Именно Дирак еще в 1930 г. в своих выдающихся «Принципах квантовой механики» [48], по признанию фон Неймана, «дал столь краткое и элегантное изложение квантовой механики,…что оно вряд ли может быть превзойдено…» ([49], с.10). Отметим, что подобных же восторженных взглядов на формулировку Дираком основных положений квантовой теории придерживались и другие известные ученые. Тем ценнее то, что пишет сам Дирак в 1972 г. об эволюции собственных взглядов в работе «Теория относительности и квантовая механика» [50]:

«Возникает вопрос, действительно ли некоммутативность является главной новой идеей квантовой механики. Ранее я всегда полагал, что это так, но недавно я начал сомневаться в этом и думать, что, может быть, с физической точки зрения некоммутативность не является единственной важной идеей, и, возможно, существует некая более глубокая идея, некое более глубокое изменение наших обычных представлений, которое привносит квантовая механика» ([50], с.148).

Заметим, что идея некоммутативности была очень близка Дираку. Ведь именно она позволила ему сформулировать понятие квантовых скобок Пуассона взамен аналогичных классических скобок и, таким образом, очень красиво и элегантно преобразовать классическую механику в квантовую. И вот теперь, спустя более сорока лет после своих пионерских работ, Дирак приходит к выводу, что существует более глубокая по сравнению с некоммутативностью идея, и эта идея связана с существованием амплитуд вероятности. Нижеследующие слова Дирак выделяет курсивом: *«Я полагаю, что понятие амплитуды вероятности, по-видимому, является наиболее фундаментальным понятием квантовой теории»* ([50], с.148).

Интересно задать вопрос: как изменились бы «Принципы квантовой механики», если бы при их написании молодой Дирак придерживался таких же взглядов, к которым он пришел в зрелом возрасте? Анализ данного вопроса показывает, что для преобразования классической механики в квантовую не обязательно исходить из процедуры канонического квантования Дирака, в основе которой лежат квантовые скобки Пуассона. Достаточно придерживаться концепции амплитуд вероятностей и статистического требования соответствия в среднем результатов новой и старой теорий [30, 51, 52]. Этот вопрос рассматривается подробнее в следующем разделе.

Опираясь на изложенное выше, сформулируем первым следующий постулат.

Постулат 1. *Основной объект квантовой информатики – квантовая система. Поведение квантовой системы полностью описывается амплитудами вероятностей. Амплитуды вероятностей образуют вектор состояния в гильбертовом пространстве.*

Гильбертово пространство является линейным векторным пространством. Свойство линейности предполагает выполнение принципа суперпозиции. Это означает, что если $|a\rangle$ и $|b\rangle$ - векторы, описывающие некоторые состояния

системы, то и их произвольная линейная комбинация $c_1|a\rangle + c_2|b\rangle$ (где c_1, c_2 - произвольные комплексные числа) также есть возможное состояние системы (принцип суперпозиции).

Вектор состояния как геометрический объект в гильбертовом пространстве может быть задан в различных эквивалентных представлениях, унитарно связанных между собой подобно тому, как поведение объектов в обычном евклидовом пространстве можно описать в различных координатах, связанных между собой ортогональными преобразованиями. Эти соображения лежат в основе следующего постулата.

Постулат 2. *Амплитуды вероятностей как координаты вектора состояния в гильбертовом пространстве могут быть заданы в различных эквивалентных представлениях. Эквивалентные представления связаны друг с другом унитарными преобразованиями. Унитарное преобразование во времени описывает эволюцию квантовой системы*.

Унитарное преобразование может быть записано символически следующим матричным равенством:

$$|\psi'\rangle = U|\psi\rangle$$

Любая унитарная матрица U может быть представлена в виде матричной экспоненты

$$U = \exp(iH),$$

где H - эрмитова матрица.

В силу однородности времени, унитарное преобразование во времени должно удовлетворять условию:

$$U(t_1 + t_2) = U(t_1)U(t_2)$$

Матричная экспонента, удовлетворяющая условию однородности во времени, должна иметь вид:

$$U = \exp(iHt)$$

Введенный таким образом эрмитов оператор H называется гамильтонианом.

Из последнего соотношения следует, что унитарная эволюция квантовых состояний должна определяться уравнением Шредингера:

$$i\frac{\partial\psi}{\partial t} = H\psi$$

Вектор состояния является объективной статистической характеристикой квантовой системы и должен допускать возможность экспериментального изучения. Для такого изучения, однако, нужен не один, а множество представителей квантового статистического ансамбля. В таком ансамбле каждый представитель приготовлен по одному и тому же рецепту и, таким образом, находится в одном и том же квантовом состоянии. Нам недостаточно проводить измерения в каком- либо одном базисе. Нужно проводить измерения в различных унитарно- связанных между собой базисах. Результаты таких измерений регулируются следующим постулатом.

Постулат 3. *Измерения, проводимые в различных унитарно связанных друг с другом базисных представлениях, порождают совокупность взаимно-дополнительных статистических распределений. В фиксированном представлении квадрат модуля амплитуды вероятностей задает вероятность обнаружения квантовой системы в соответствующем базисном состоянии.*

Постулаты 2 и 3 тесно связаны друг с другом и образуют единое целое. С одной стороны, Постулат 3 служит тому, чтобы «материализовать» результаты преобразований, о которых говорится в Постулате 2. С другой стороны, проводя измерения согласно Постулату 3, мы должны позаботиться

о том, чтобы такие измерения давали наиболее полную картину явлений. Этого нельзя добиться, если ограничиться только каким- либо одним представлением. Таким образом, для того, чтобы провести измерения согласно Постулату 3, нужно использовать и Постулат 2, осуществляя переход между различными представлениями. Для каждого представителя статистического квантового ансамбля мы должны сделать выбор: провести измерение в исходном представлении или перейти путем унитарного преобразования к другому представлению и только потом провести измерение. Только совокупность измерений в различных взаимно-дополнительных представлениях способно дать полную картину для квантового состояния с экспериментальной точки зрения.

В изложенных выше соображениях мы предполагаем, что однажды измеренный представитель, далее не измеряется. Если бы мы даже провели такое измерение, то оно бы несло информацию не об исходном квантовом состоянии, а о состоянии, возникшем в результате первого измерения. В этом состоит свойство редукции квантовых состояний. «Однако даже при усердии одного яйца два раза не высидишь» (Козьма Прутков «Мысли и афоризмы», №258).

При рассмотрении квантовых состояний составных систем мы естественно приходим к понятию тензорного произведения пространств состояний отдельных подсистем. Рассмотрим для примера систему из двух двухуровневых квантовых систем (квантовых битов- кубитов). Естественно предположить, что данная система в качестве возможных состояний должна содержать следующие четыре базисные состояния:

$|00\rangle$ - оба кубита в состоянии $|0\rangle$,

$|01\rangle$ - первый кубит в состоянии $|0\rangle$, второй в состоянии $|1\rangle$,

$|10\rangle$ - первый кубит в состоянии $|1\rangle$, второй- в состоянии $|0\rangle$,

$|11\rangle$ - оба кубита в состоянии $|1\rangle$.

Указанные четыре базисных вектора порождают гильбертово пространство размерности 4. Это означает, что система из двух кубитов может находиться не только в одном из указанных состояний, но и в любом состоянии суперпозиции

$$|\psi\rangle = c_{00}|00\rangle + c_{01}|01\rangle + c_{10}|10\rangle + c_{11}|11\rangle$$

Такого рода соображения делают естественным следующий постулат.

Постулат 4. *Пространство состояний составной системы образовано тензорным произведением пространств состояний отдельных систем.*

Например, n кубитов, рассматриваемые как единая квантовая система, порождают 2^n базисных состояний и, соответственно, гильбертово пространство размерности 2^n. Произвольный вектор состояния в таком пространстве определяется 2^n комплексными амплитудами вероятности. Заметим, что если бы каждый кубит описывался некоторым состоянием независимо от остальных, то всего было бы $2n$ комплексных амплитуд вероятности, что гораздо меньше при больших n. Разность $2^n - 2n$ обусловлена специфическим квантовым ресурсом, называемым запутанностью (entanglement). Квантовое состояние системы называется запутанным, если оно не сводится к состояниям отдельных подсистем. Именно запутанность призвана сделать квантовые компьютеры экспоненциально более мощными по сравнению с их классическими собратьями.

Заметим, что Постулат 4 делает неизбежной вероятностную реализацию квантовой информационной модели. Действительно, например, для регистра из $n = 1000$ кубитов, имеет место состояние, описываемое $2^{1000} \approx 1{,}07 \cdot 10^{301}$ комплексными числами. Для Вселенной, имеющей в

своем распоряжении «только» $\sim 10^{78}$ нуклонов, нет никакой возможности записать подобное состояние детерминированным образом на каком- либо материальном носителе.

Постулат 4 позволяет нам на более высоком уровне вернуться к вопросу о полноте квантовой статистической теории и неполноте классической теории вероятностей (предварительно этот вопрос уже обсуждался в разделе 1.3).

Отметим следующую принципиальную разницу между описанием с помощью распределения вероятностей и с помощью вектора состояния.

Предположим в рамках классической теории вероятностей, что переменные $x_1, x_2, ..., x_s$ связаны между собой распределением вероятностей $P(x_1, x_2, ..., x_s)$. Наличие такого распределения никак не исключает возможного существования дополнительных r переменных $x_{s+1}, x_{s+2}, ..., x_{s+r}$, с которыми исходные переменные находятся в отношении статистической зависимости. Напомним, что рассматриваемые переменные являются статистически зависимыми, если совместное распределение размерности $s+r$ несепарабельно (нефакторизуемо), т.е. не может быть представлено в виде произведения распределений размерностей s и r. Для статистически зависимых систем имеем:

$$P(x_1, x_2, ..., x_s, x_{s+1}, ..., x_{s+r}) \neq P(x_1, x_2, ..., x_s) P(x_{s+1}, x_{s+2}, ..., x_{s+r}).$$

На менее формальном языке это свойство означает следующее. Любые статистические связи, обнаруженные внутри исходных переменных $x_1, x_2, ..., x_s$ на деле могут оказаться фикцией, поскольку истинные физические причины могут определяться не исходными, а дополнительными («скрытыми») переменными $x_{s+1}, x_{s+2}, ..., x_{s+r}$. Таким образом, любой классический статистический анализ не может сам по себе претендовать на получение объективных научных выводов. Высмеивая подобное положение

дел, еще 100 лет назад Бернард Шоу писал, что статистики могут легко доказать, что ношение цилиндров удлиняет жизнь и дает иммунитет против болезней [38]. Отмеченный внутренний недостаток классической статистики хорошо известен, поэтому добросовестные исследователи рассматривают статистический анализ только как вспомогательное средство.

Примечательно, что квантовая теория не имеет аналогичного порока. Пусть переменные $x_1, x_2, ..., x_s$ образует квантовое состояние $\psi(x_1, x_2, ..., x_s)$. Тогда, исключена возможность статистической зависимости рассматриваемых переменных от любых других переменных во Вселенной (включая «скрытые» переменные внутри самой системы). Другими словами, расширение исходной системы $x_1, x_2, ..., x_s$ путем включения любых дополнительных переменных $x_{s+1}, x_{s+2}, ..., x_{s+r}$ будет обязательно приводить к сепарабельному совместному квантовому состоянию, т.е. всегда совместное квантовое состояние будет представляться в виде произведения независимых векторов состояний, когда $\psi(x_1, x_2, ..., x_s, x_{s+1}, ..., x_{s+r}) = \psi(x_1, x_2, ..., x_s)\psi(x_{s+1}, x_{s+2}, ..., x_{s+r})$ Например, при введении спина в нерелятивистскую квантовую механику вектор состояния становится произведением координатной и спиновой функций. Понятно, что рассматриваемая факторизация состояния, приводящая к независимым «внутренним» и «внешним» переменным, возможна только как некоторая приближенная идеализация, справедливая только в пренебрежении некоторым относительно слабым взаимодействием (например спин- орбитальным). Заметим, что подобного рода идеализации и составляют основное содержание науки.

Предположим теперь, что, наоборот, рассматриваемое состояние несепарабельно (нефакторизуемо), т.е.

$$\psi(x_1, x_2, ..., x_s, x_{s+1}, ..., x_{s+r}) \neq \psi(x_1, x_2, ..., x_s)\psi(x_{s+1}, x_{s+2}, ..., x_{s+r}).$$

Тогда невозможно вообще приписать подсистемам $x_1, x_2, ..., x_s$ и $x_{s+1}, x_{s+2}, ..., x_{s+r}$ каких- либо векторов состояния. Такие системы не могут считаться независимыми замкнутыми системами, как бы далеко они не находились друг от друга. В квантовой информатике состояния указанного типа называются запутанными (entangled). Хорошо известный пример такого рода дают ЭПР состояния (состояния Эйнштейна, Подольского и Розена). Такие состояния впервые анализировались в знаменитой работе указанных трех авторов в 1935 г. в форме так называемого парадокса ЭПР [53]. Работа называлась «Можно ли считать квантовомеханическое описание физической реальности полным?» и была призвана показать несостоятельность квантовой теории. Парадокс, сформулированный авторами, заключается в том, что если имеются две частицы, которые взаимодействовали в прошлом, то, даже по прошествии сколь угодно большого времени по окончанию взаимодействия, эти частицы продолжают находиться в запутанном состоянии, характеризующимся специфической квантовой корреляцией. Так, производя измерения над одной из них, мы можем получить информацию и о второй частице. При этом частицы могут быть как угодно далеко разнесены в пространстве друг от друга. Таким образом, понятие замкнутости физической системы в квантовой теории существенно отличается от аналогичного понятия в классической теории. Пространственная изолированность больше не может служить признаком замкнутости. Вместо этого в квантовой теории существует внутренний статистический критерий: полное внутренне замкнутое описание системы, независимое от значений любых других переменных (внешних по отношению к рассматриваемой системе или внутренних, но «скрытых»), возможно только для квантовых систем, описываемых вектором состояния. По иронии судьбы, ЭПР состояния, вопреки замыслу их авторов, являются важным аргументом в пользу (а никак

не против) полноты квантовой теории. Подробнее ЭПР состояния будут рассмотрены в разделах 4.8- 4.10.

Изложенные соображения позволяют говорить о неполноте классической (колмогоровской) теории вероятностей и полноте квантовой. Заметим, что неполнота аксиоматики Колмогорова является известным фактом, который, однако, обычно не рассматривается специалистами по классической теории вероятностей как недостаток (см., например, [54]). С точки зрения квантовой информатики, однако, неполнота классической теории вероятностей – это, совершенно определенно, её недостаток. Это недостаток устраняется (правда, только на формальном математическом уровне) путем расширения классического распределения вероятностей до квантового вектора состояния (как это описано выше). Заметим также, что неполное описание нередко применяется и в квантовой теории. Этому описанию соответствует математический аппарат так называемой матрицы плотности. Краткое описание понятия матрицы плотности будет дано в следующем разделе и Приложении к настоящей главе. Необходимость введения матрицы плотности обусловлена тем, что часто квантовая физическая система может взаимодействовать сложным (и неконтролируемым) образом со своим окружением. Заметим, что с формальной точки зрения любая матрица плотности может быть дополнена до чистого состояния, подобно тому, как плотность распределения может быть дополнена до вектора квантового состояния. Процедура дополнения матрицы плотности до чистого состояния рассматривается в Приложении к настоящей главе.

3.2 От квантовой информатики к квантовой физике

В настоящем разделе мы покажем, что систематическое применение представленной выше парадигмы квантовой информатики к задачам механики

ведет к преобразованию классической механики в механику квантовую [30,51,52].

Основной закон динамики Ньютона есть:

$$\frac{d^2}{dt^2}\vec{x} = -\frac{1}{m}\frac{\partial U}{\partial \vec{x}}$$

Для того, чтобы применить постулаты квантовой информатики, достаточно предположить, что фигурирующие в основном законе динамики ускорение и сила есть некоторые средние величины. Усреднение обеспечивается посредством введения некоторой плотности распределения $P(x)$:

$$\frac{d^2}{dt^2}\left(\int P(x)\vec{x}dx\right) = -\frac{1}{m}\left(\int P(x)\frac{\partial U}{\partial \vec{x}}dx\right) \qquad (3.1)$$

Потребуем в соответствии с Постулатами 1 и 3, чтобы введенная плотность распределения допускала корневое разложение, естественное для квантовой информатики. Пусть всего имеется S компонент плотности, т.е.:

$$P(x) = \left|\psi^{(1)}(x)\right|^2 + \left|\psi^{(2)}(x)\right|^2 + ... + \left|\psi^{(s)}(x)\right|^2, \qquad (3.2)$$

где каждая из компонент представлена в виде разложения:

$$\psi^{(l)}(x) = c_j^{(l)}(t)\varphi_j(x), \quad l = 1,..,s \qquad (3.3)$$

Предположим, что зависимость коэффициентов разложения от времени определяется гармоническими функциями:

$$c_j^{(l)}(t) = c_{j0}^{(l)} \exp\left(-i\omega_j t\right) \qquad (3.4)$$

Базисные функции разложения и частоты заранее неизвестны. Их следует определить таким образом, чтобы выполнялись усредненные уравнения движения. Покажем, что модель, задаваемая уравнениями (3.1)- (3.4) приводит к стационарным функциям и частотам уравнения Шредингера.

Подставляя (3.2)-(3.4) в (3.1), получим:

$$m\left(\omega_j-\omega_k\right)^2\sum_{l=1}^{s}c_{j0}^{(l)}c_{k0}^{*(l)}\left\langle k\left|\vec{x}\right|j\right\rangle\exp\left(-i\left(\omega_j-\omega_k\right)t\right)=$$

$$=\sum_{l=1}^{s}c_{j0}^{(l)}c_{k0}^{*(l)}\left\langle k\left|\frac{\partial U}{\partial\vec{x}}\right|j\right\rangle\exp\left(-i\left(\omega_j-\omega_k\right)t\right) \qquad (3.5)$$

Здесь, как обычно, по повторяющимся индексам j и k предполагается суммирование.

Матричные элементы в выражении (3.5) определяются формулами:

$$\left\langle k\left|\vec{x}\right|j\right\rangle=\int\varphi_k^*(x)\,\vec{x}\,\varphi_j(x)dx \qquad (3.6)$$

$$\left\langle k\left|\frac{\partial U}{\partial\vec{x}}\right|j\right\rangle=\int\varphi_k^*(x)\frac{\partial U}{\partial\vec{x}}\,\varphi_j(x)dx \qquad (3.7)$$

Для того, чтобы соотношение (3.5) выполнялось в любой момент времени для произвольных начальных амплитуд, следует потребовать выполнения равенства левых и правых частей отдельно для каждого матричного элемента, поэтому:

$$m\left(\omega_j-\omega_k\right)^2\left\langle k\left|\vec{x}\right|j\right\rangle=\left\langle k\left|\frac{\partial U}{\partial\vec{x}}\right|j\right\rangle \qquad (3.8)$$

Последнее выражение представляет собой матричное уравнение Гейзенберга для квантовой динамики в энергетическом представлении. Базисные функции и частоты, удовлетворяющие соотношениям (3.8), есть стационарные состояния и частоты квантовой системы (в соответствии с эквивалентностью картин Гейзенберга и Шредингера).

Действительно, образуем диагональную матрицу из частот системы ω_j. Рассматриваемая матрица будет эрмитовой в силу того, что частоты – действительные числа. Эта матрица будет представлением некоторого эрмитова оператора, собственные значения которого суть ω_j, т.е.

$$\hat{\Omega}\left|j\right\rangle=\omega_j\left|j\right\rangle \quad , \qquad (3.9)$$

Найдем явный вид искомого оператора частоты $\hat{\Omega}$. В силу (3.9), матричное соотношение (3.8) можно переписать в виде операторного уравнения

$$\left[\hat{\Omega}\left[\hat{\Omega},\vec{x}\right]\right]=\frac{1}{m}\hat{\partial}U\,, \qquad (3.10)$$

где $\hat{\partial}=\dfrac{\partial}{\partial x}$ $\hat{\partial}=\dfrac{\partial}{\partial \vec{x}}$ - оператор дифференцирования, [ ]- коммутатор.

Выражение, стоящее в правой части (3.10), представим в виде некоторого коммутатора:

$$\frac{1}{m}\hat{\partial}U=\left[\frac{1}{\hbar}U,-\frac{\hbar}{m}\hat{\partial}\right]\,,$$

где $\hbar$ – произвольная константа, которая, в итоге, должна быть отождествлена с постоянной Планка (см. обсуждение ниже).

Рассматриваемый коммутатор, очевидно, не изменится, если к потенциальной составляющей $\dfrac{1}{\hbar}U$ добавить произвольную функцию от оператора производной $F_1\left(\hat{\partial}\right)$, т.е.

$$\frac{1}{m}\hat{\partial}U=\left[\frac{1}{\hbar}U,-\frac{\hbar}{m}\hat{\partial}\right]=\left[F_1\left(\hat{\partial}\right)+\frac{1}{\hbar}U,-\frac{\hbar}{m}\hat{\partial}\right]$$

Аналогичным образом имеем:

$$-\frac{\hbar}{m}\hat{\partial}=\left[-\frac{\hbar}{2m}\hat{\partial}^2,\vec{x}\right]=\left[-\frac{\hbar}{2m}\hat{\partial}^2+F_2\left(\vec{x}\right),\vec{x}\right],$$

где $F_2\left(\vec{x}\right)$- произвольная функция от координат.

Таким образом:

$$\left[\hat{\Omega}\left[\hat{\Omega},\vec{x}\right]\right]=\left[F_1\left(\hat{\partial}\right)+\frac{1}{\hbar}U,\left[-\frac{\hbar}{2m}\hat{\partial}^2+F_2\left(\vec{x}\right),\vec{x}\right]\right]$$

Последнее соотношение оказывается согласованным, если положить:

$$F_1\left(\hat{\partial}\right)=-\frac{\hbar}{2m}\hat{\partial}^2,\ \ F_2\left(\vec{x}\right)=\frac{1}{\hbar}U$$

Окончательно находим, что решением уравнения (3.10) является оператор:

$$\hat{\Omega}=-\frac{\hbar}{2m}\hat{\partial}^2+\frac{1}{\hbar}U(x) \qquad (3.11)$$

Для того, чтобы слагаемые в (3.11) имели одинаковую размерность, произвольная константа $\hbar$ должна иметь размерность постоянной Планка (эрг*с). Численное значение этой постоянной должно быть выбрано таким, чтобы собственные значения оператора частоты $\hat{\Omega}$ совпадали с реальными атомными частотами. Нетрудно видеть, что выбор численного значения постоянной Планка $\hbar$ связан с выбором единиц измерения для основных физических величин (длина, время, масса). С теоретической точки зрения единицы измерений можно выбрать так, чтобы было $\hbar=1$ (заметим, что в квантовой теории поля общеупотребительна система единиц, в которой $\hbar=c=1$).

Вместо оператора частоты $\hat{\Omega}$ в квантовой теории принято использовать гамильтониан $\hat{H}$.

$$\hat{H}=\hbar\hat{\Omega}=-\frac{\hbar^2}{2m}\hat{\partial}^2+U(x) \qquad (3.12)$$

Собственные значения гамильтониана согласно (10) есть:

$$\hat{H}\left|j\right\rangle=\hbar\omega_j\left|j\right\rangle \qquad (3.13)$$

Таким образом, если потребовать, чтобы корневая оценка плотности удовлетворяла в среднем классическим уравнениям движения, то базисные функции и частоты корневого разложения уже не могут быть произвольными,

а должны представлять собой соответственно собственные функции и собственные значения гамильтониана системы.

Нетрудно видеть, что динамика амплитуд вероятности, возникающая при описанном выше подходе, является унитарной в полном соответствии с Постулатом 2.

Постулат 4 квантовой информатики в приложении к изучаемой задаче требует, чтобы многочастичная квантовая система рассматривалась в соответствующем многомерном конфигурационном пространстве (детали такого описания содержатся в общеизвестных руководствах по квантовой механике [55, 56]).

Описанный выше подход представляет собой определенную альтернативу процедуре канонического квантования Дирака, в основе которой лежат квантовые скобки Пуассона [48].

Рассмотрим теперь матрицу плотности, элементы которой определим формулой:

$$\rho_{jk} = \sum_{l=1}^{s} c_j^{(l)} c_k^{*(l)} = \sum_{l=1}^{s} c_{j0}^{(l)} c_{k0}^{*(l)} \exp\left(-i\left(\omega_j - \omega_k\right)t\right) \qquad (3.14)$$

На основе представленных выше результатов нетрудно получить уравнение для динамики матрицы плотности, называемое обычно квантовым уравнением Лиувилля:

$$\frac{\partial \hat{\rho}}{\partial t} = -\frac{i}{\hbar}\left[\hat{H}, \hat{\rho}\right] \qquad (3.15)$$

С использованием полученного выражения (3.12) для гамильтониана уже нетрудно получить операторные представления для других динамических величин. Например, понятие импульса можно ввести на основе следующей легко проверяемой цепочки равенств:

$$m\frac{d}{dt}\left(\int P(x)\vec{x}dx\right)=-im\left(\omega_j-\omega_k\right)\sum_{l=1}^{s}c_{j0}^{(l)}c_{k0}^{*(l)}\langle k|\vec{x}|j\rangle\exp\left(-i\left(\omega_j-\omega_k\right)t\right)=$$

$$=\frac{im}{\hbar}\sum_{l=1}^{s}\left\langle\psi^{(l)}\left|\hat{H}x-x\hat{H}\right|\psi^{(l)}\right\rangle=\sum_{l=1}^{s}\left\langle\psi^{(l)}\left|\hat{\vec{p}}\right|\psi^{(l)}\right\rangle=Tr\left(\hat{\vec{p}}\hat{\rho}\right) \quad , \qquad (3.16)$$

где матрица плотности смеси (3.14) в обозначениях Дирака есть:

$$\hat{\rho}=\sum_{l}\left|\psi^{(l)}\right\rangle\left\langle\psi^{(l)}\right| \qquad (3.17)$$

В выражении (3.16) суммирование по индексам j и k предполагается автоматически, сумма по компонентам смеси (индекс l) выписана явно.

Первое из представленных в (3.16) равенств непосредственно следует из определения корневой оценки плотности, при получении второго равенства мы учли (3.13), наконец последние два равенства следуют из определения импульса (в нерелятивистской теории оператор импульса должен быть определен таким образом, чтобы его среднее значение совпадало с произведением массы на среднюю скорость).

Заметим, что в (3.17) компоненты смеси $\left|\psi^{(l)}\right\rangle$ нормированы таким образом, что $\left\langle\psi^{(l)}\left|\psi^{(l)}\right\rangle=\rho_l\right.$, где ρ_l - вес l - ой компоненты смеси.

Из соотношения (3.16) с необходимостью вытекает следующее определение импульса:

$$\hat{\vec{p}}=\frac{im}{\hbar}\left[\hat{H}\vec{x}\right]=-i\hbar\frac{\partial}{\partial\vec{x}}$$

Заметим, что выражения для операторов наблюдаемых величин мы не постулируем (как это делают при стандартном изложении квантовой механики), а выводим как необходимые следствия корневых статистических оценок.

С использованием понятия матрицы плотности, как это следует из (3.16) среднее значение импульса есть:

$$M(\vec{p}) = Tr(\vec{p}\rho)$$

Точно такая же формула имеет место для среднего значения любой другой наблюдаемой A

$$M(A) = Tr(A\rho)$$

Соотношения, согласно которым, уравнения классической механики выполняются в среднем и для квантовых систем, называют уравнениями Эренфеста [57]. Самих этих уравнений, конечно, недостаточно для описания квантовой динамики. Как было показано выше, дополнительное условие, которое позволяет преобразовать классическую механику в квантовую (т.е. условие квантования), есть, по- существу, требование корневого характера плотности.

3.3. Шестая проблема Гильберта

В знаменитом докладе Д. Гильберта «Математические проблемы», прочитанном 8 августа 1900 г. в Париже на 2-ом Международном конгрессе математиков, были сформулированы задачи, оказавшие существенное влияние на развитие математики и связанных с ней наук в XX веке.

Всего Гильберт поставил 23 проблемы, из которых для нас наибольший интерес представляет 6-ая проблема, сформулированная как «математическое изложение аксиом физики».

«С исследованиями по основаниям геометрии», говорится в докладе, «близко связана задача об аксиоматическом построении по этому же образцу тех физических дисциплин, в которых уже теперь математика играет выдающуюся роль: это в первую очередь теория вероятностей и механика.

Что касается аксиом теории вероятностей, то мне казалось бы желательным, чтобы параллельно с логическим обоснованием этой теории шло рука об руку строгое и удовлетворительное развитие метода средних

значений в математической физике, в частности в кинетической теории газов» ([58] с.415).

Сегодня, по прошествии более ста лет с момента постановки задачи, можно сказать, что слова Гильберта, прозвучавшие на рубеже XIX и XX веков, были почти пророческими.

Примечательно, что математическая формулировка основ теории вероятностей связывается Гильбертом в единый конгломерат с наукой о микромире. В то время в роли таковой выступала молекулярно- кинетическая теория, основы которой были заложены Максвеллом и Больцманом. Заметим, что всего через несколько месяцев после Гильберта был прочитан еще один доклад, который положил начало новой (квантовой) эре. Этот доклад был прочитан М. Планком 14 декабря 1900 г. на заседании немецкого физического общества.

Гильберт в своем докладе говорит, что искомая аксиоматическая теория вероятностей должна быть построена по аналогии с геометрией. Геометрия гильбертова пространства, заложенная в работах Гильберта, Шмидта и других ученых, как раз, и есть, как мы видели, основа квантовой информатики.

Заметим также, что при построении физических аксиом по образцу аксиом геометрии, как считает Гильберт, «возможно возникнет принцип классификации, который сможет использовать глубокую теорию бесконечных групп преобразования Ли» ([58], с.416). Очевидно, что Гильберт оказался прав и в этом своем предсказании, поскольку важность групп Ли в современной квантовой теории хорошо известна.

Отметим, наконец, что в качестве важной задачи Гильберт видит математически строгое описание перехода от микромира к макромиру. Здесь, по мнению Гильберта, в основу может быть положена «книга Больцмана о принципах механики, в которой следовало бы строго математически обосновать и провести те изложенные в ней процессы предельного перехода,

которые ведут от атомистического понимания к теории движения твердого тела» ([58] с.415). Несмотря на колоссальный прогресс, достигнутый в понимании микромира в XX столетии, вопрос математического обоснования соответствующего предельного перехода от описания микроявлений к описанию макромира все еще остается дискуссионным (см., например, [59]).

Постановка 6-ой проблемы Гильбертом не была просто гениальной догадкой одного выдающегося человека. Актуальность рассматриваемой задачи определялась состоянием науки на рубеже XIX и XX веков. Так, знаменитая H- теорема, направленная на механико- статистическое обоснование второго начала термодинамики, была сформулирована Больцманом еще в 1872 г. [60]. Эта работа вызвала жаркие многолетние дискуссии. С резкой критикой работы Больцмана выступили многие известные ученые, в том числе выдающийся математик и теоретик естествознания А. Пуанкаре. Проблема заключалась в том, что обратимость законов классической механики вступала в противоречие с необратимым характером второго начала термодинамики. Хотя с физической точки зрения ответы Больцмана на возражения против его теории были весьма убедительны, с принципиальной математической точки зрения вопрос оставался открытым. Любой симбиоз представлений классической механики и статистики неизбежно оказывался непоследовательным и внутренне противоречивым. Отметим, в то же время, что подход Больцмана к статистической термодинамике не был чисто классическим. В той же, посвященной H- теореме работе [60], Больцман за 28 лет до Планка использовал (в методических целях) представления о квантованном характере энергии. Как мы теперь понимаем, любые попытки объединения механики и статистики логически должны были вести к квантовым представлениям (пусть и в неявной форме, как у Больцмана). Таким образом, на рубеже XIX и XX столетий, Гильберту и другим ученым было ясно, что развитие механики,

теории вероятностей и молекулярно- кинетической теории не могло далее проходить независимо. Прогресс науки настоятельно требовал объединения указанных разделов, однако такое объединение неизбежно оказывалось противоречивым. Формулируя свою знаменитую 6-ую проблему, Гильберт, вероятно, надеялся путем аксиоматизации снять имеющиеся трудности и получить единую универсальную непротиворечивую теорию. На роль такой теории, как мы видим сегодня, вполне может претендовать квантовая информатика.

3.4 Обсуждение

Рассмотрим коротко историю развития 6-ой проблемы Гильберта в XX веке.

Прежде всего, основываясь на своем тезисе о необходимости сочетания исследований по теории вероятностей с развитием кинетической теории газов, Гильберт применил свою теорию интегральных уравнений к кинетическому уравнению Больцмана. В рамках этих исследований Гильберту удалось найти эффективный способ приближенного решения кинетического уравнения [61]. Кинетическое уравнение Больцмана было для Гильберта примером такого уравнения, которое являлось интегральным по своей сути в том смысле, что не сводилось ни к каким дифференциальным уравнениям.

Возникновение квантовой механики, ознаменованное появлением 1925 г. работ В. Гейзенберга [62], Борна и Иордана [63], а также Гейзенберга, Борна и Иордана [64], побудило Гильберта заняться исследованием математических основ новой теории. Над этой задачей он работал совместно со своими ассистентами – фон Нейманом и Нордгеймом. Результаты исследований были опубликованы в работе [65], в которой авторы впервые попытались осмыслить принципы квантовой теории с математической точки зрения.

В свою очередь, сотрудничество с Гильбертом побудило фон Неймана к систематическим исследованиям по математическому обоснованию квантовой теории. Результатом работы, которая продолжалась несколько лет, стала книга [49]. Эта книга до сих пор считается основной среди работ, посвященных математическим аспектам квантовой механики. В своей монографии фон Нейман последовательно развил концепцию гильбертова пространства как арены, на которой развиваются квантовые события, ввел понятие матрицы плотности, развил теорию квантовых измерений, основанных на ортогональных разложениях единицы, провел исследование по обоснованию квантовой статистической механики.

Свое видение фундаментальных статистических основ квантовой механики фон Нейман попытался выразить в своей известной теореме о невозможности введения скрытых параметров в структуру квантовой теории. Эта теорема, по мнению фон Неймана, должна была обеспечить водораздел между квантовой и классической теориями статистики. Теорема о скрытых параметрах в течение долгого времени не вызывала никаких возражений, пока не была подвергнута жесткой критике со стороны Белла [66]. Позитивным итогом исследований Белла стали известные неравенства, носящие его имя. Эти неравенства показывают невозможность объяснения результатов статистических экспериментов над квантовыми объектами посредством концепции классического вероятностного пространства. С этой точки зрения неравенства Белла выражают в количественной форме то, что фон Нейман сформулировал в своей теореме на качественном уровне. Пример наиболее известного неравенства Белла будет рассмотрен в разделе 4.10.

Формальные математические инструменты, разработанные фон Нейманом, были существенно усовершенствованы и обобщены другими авторами. Так, в современной теории квантовых измерений рассматривают не только основанные на проекторах ортогональные разложения единицы,

введенные фон Нейманом, но и общие разложения единицы. Соответствующие объекты называют положительными операторнозначными мерами (Positive Operator- Valued Measure - POVM). Техника POVM будет кратко описана в нижеследующем Приложении.

Современное изложение математических аспектов квантовой механики содержится в книгах А.С. Холево [36, 67, 68]. История аксиоматики классической теории вероятностей излагается в [69].

3.П. Приложение. Разложение Шмидта и формализм матрицы плотности.

Пусть вектор состояния (амплитуда вероятности) составной системы $\left|\psi\right\rangle$ зависит от переменных двух подсистем. Оказывается, что вектор состояния составной системы может быть разложен по векторам, относящимся к отдельным подсистемам. Соответствующее представление называется разложением Шмидта [1,2,37]:

$$\left|\psi\right\rangle = \sum_k \sqrt{\lambda_k}\left|\psi_k^{(1)}\right\rangle \otimes \left|\psi_k^{(2)}\right\rangle \qquad (3.18)$$

Здесь λ_k - весовые (заведомо неотрицательные) множители, удовлетворяющие условию нормировки

$$\sum_k \lambda_k = 1$$

Мы предполагаем, что слагаемые в разложении (3.18) представлены в порядке убывания (невозрастания) коэффициентов λ_k .

Разложение Шмидта дает наглядный математический аппарат для исследования запутанности. Например, регистрация подсистемы №1 наблюдателем A в состоянии $\left|\psi_k^{(1)}\right\rangle$ означает, что подсистема №2 с

необходимостью будет зарегистрирована (наблюдателем B) в состоянии $\left|\psi_k^{(2)}\right\rangle$ (при том же самом k).

Функции (векторы) $\left|\psi_k^{(1)}\right\rangle$ и $\left|\psi_k^{(2)}\right\rangle$ называются модами Шмидта. Предположим, что каждая из подсистем описывается гильбертовым пространством размерности s. Тогда, каждый из наборов функций $\left|\psi_k^{(1)}\right\rangle$ и $\left|\psi_k^{(2)}\right\rangle$ ($k = 1,..., s$) будет полным набором, образующим ортонормированный базис.

Опишем алгоритм численной экстракции мод Шмидта. Пусть ψ матрица размера $s \times s$ с элементами $\psi_{j_1 j_2}$, задающими амплитуду вероятности найти подсистемы в базисных состояниях j_1 и j_2 соответственно. Введем матрицу M следующего вида:

$$M = \psi \cdot \psi^{+} \tag{3.19}$$

Найдем собственные функции и собственные значения матрицы M. В результате, рассматриваемая матрица будет представлена в виде:

$$M = UDU^{+}, \tag{3.20}$$

Здесь U - унитарная матрица, составленная из собственных векторов матрицы M (каждый столбец матрицы U есть некоторый собственный вектор матрицы M). Матрица D есть диагональная матрица, составленная из собственных значений λ_k матрицы M. Будем предполагать также, что λ_k выстроены на диагонали в порядке убывания (невозрастания).

Диагональные элементы матрицы D есть искомые весовые множители λ_k разложения Шмидта. При этом мода $\left|\psi_k^{(1)}\right\rangle$ дается k - ым **столбцом** матрицы U .

Для нахождения мод $\left|\psi_k^{(2)}\right\rangle$ введем матрицу V согласно формуле:

$$V = \sqrt{D^{-1}}U^{+}\psi \qquad (3.21)$$

В задачах высокой размерности матрица D, как правило, содержит элементы, практически равные нулю. Это может приводить к формальному делению на ноль при вычислении матрицы D^{-1}. Для предотвращения этого явления можно поступить двумя практически эквивалентными способами. Можно вводить небольшие ненулевые слагаемые (например, порядка 10^{-12} - 10^{-16}) в диагональ D. Результаты фактически не зависят от уровня «малости» вводимых величин (они нужны только для того, чтобы избежать деления на машинный ноль). Те же результаты можно получить, если «урезать» размерность матрицы D, оставив в ней на диагонали только r заведомо ненулевых элементов $\lambda_1, \lambda_2, ..., \lambda_r$ (при этом в матрице U также необходимо оставить только первые r столбцов).

Теперь для получения моды $\left|\psi_k^{(2)}\right\rangle$ остается только взять k - ую **строку** матрицы V .

С использованием матриц U и V матрица амплитуд вероятностей ψ может быть записана в виде:

$$\psi = U \cdot S \cdot V \qquad (3.22)$$

где $S = \sqrt{D}$ - диагональная матрица, неотрицательные диагональные элементы которой $\sqrt{\lambda_k}$ расположены в порядке убывания (невозрастания). Разложение (3.22) есть сингулярное разложение матрицы (singular value decomposition, сокращенно- svd), а параметры $\sqrt{\lambda_k}$ - сингулярные значения (singular values) матрицы.

Представленный алгоритм показывает, что определение мод Шмидта есть самосогласованная по переменным подсистем процедура. Так, каждый столбец матрицы U (каждая мода $\left|\psi_k^{(1)}\right\rangle$) определяется с точностью до независимого несущественного фазового множителя. Добавление такого множителя, однако, приведет, согласно (3.21), к согласованному изменению фазы моды $\left|\psi_k^{(2)}\right\rangle$, запутанной с исходной модой.

Задача 3.1 Явным расчетом покажите, что алгоритм, задаваемый формулами (3.19)- (3.22) действительно определяет разложение Шмидта (3.18) для составной системы.

Основная числовая характеристика, связанная с разложением Шмидта есть число Шмидта K, которое характеризует эффективное число мод в разложении:

$$K = \frac{1}{\sum_k \lambda_k^2}$$

По своему определению, в силу условия нормировки для λ_k, число K заведомо не ниже единицы (и равно единице только в том случае, когда в

разложении Шмидта имеется единственное ненулевое слагаемое). В случае систем, описываемых конечномерным вектором состояния, число K лежит в интервале $1 \le K \le s$, где s - размерность гильбертова пространства квантовой подсистемы.

Наблюдатель A, для которого доступна подсистема №1 и недоступна подсистема №2, не имеет возможности восстановить вектор состояния полной системы. Он вынужден ограничиться описанием подсистемы №1 посредством матрицы плотности:

$$\rho^{(1)} = \sum_k \lambda_k \left|\psi_k^{(1)}\right\rangle\left\langle\psi_k^{(1)}\right|$$

Аналогично, наблюдатель B, которому доступна только подсистема №2, имеет дело с матрицей плотности

$$\rho^{(2)} = \sum_k \lambda_k \left|\psi_k^{(2)}\right\rangle\left\langle\psi_k^{(2)}\right|$$

Матрица плотности является инструментом неполного описания квантовых систем. Такое описание может быть искусственно домыслено (дополнено) до описания посредством вектора состояния. Например, наблюдатель A, не имея возможности установить действительную систему №2, с которой запутана его система №1, может рассмотреть некоторую другую вспомогательную систему №2' и соответствующий ей базисный набор $\left|\psi_k'^{(2)}\right\rangle$. Вместо действительного вектора состояния составной системы $\left|\psi\right\rangle$, такой наблюдатель будет рассматривать некоторое другое состояние $\left|\psi'\right\rangle$

$$\left|\psi'\right\rangle = \sum_k \sqrt{\lambda_k}\left|\psi_k^{(1)}\right\rangle \otimes \left|\psi_k'^{(2)}\right\rangle$$

Важно отметить, что в отношении описания отдельно взятой системы №1 векторы состояния $|\psi\rangle$ и $|\psi'\rangle$ эквивалентны.

Унитарный оператор U, действующий на переменные подсистемы, задает следующее преобразование матрицы плотности (здесь и далее мы опускаем индекс №1, идентифицирующий рассматриваемую подсистему):

$$\rho' = U\rho U^{+}$$

Для оператора $U = \exp\left(-\frac{iHt}{\hbar}\right)$ рассматриваемое преобразование эквивалентно квантовому уравнению Лиувилля (3.15) из раздела 3.2.

В формализме матрицы плотности принято рассматривать следующие обобщенные измерения над системой [36,67,68]. Предположим, что результатом измерения может быть один из r исходов: $m = 1,2,...,r$. Вероятность исхода m дается формулой

$$P(m) = Tr(E_m \rho)$$

Здесь E_m ($m = 1,2,...,r$) набор эрмитовых операторов, образующих POVM (положительную операторнозначную меру).

По определению, операторы E_m неотрицательно определены:

$$E_m \geq 0$$

Кроме того, предполагается, что рассматриваемые операторы задают разложение единицы

$$\sum_m E_m = I,$$

где I - тождественный оператор (единичная матрица).

В силу эрмитовости и неотрицательной определенности, каждый оператор E_m может быть представлен в виде:

$E_m = X_m^+ X_m$,

где X_m ($m = 1,2,...,r$) – некоторые операторы измерения.

Частным случаем операторов E_m являются хорошо известные в квантовой механике ортогональные проекторы.

Пусть, например, задан ортонормированный базис $\left|\varphi_j\right\rangle$ $j = 1,...,s$. Каждому базисному вектору $\left|\varphi_j\right\rangle$ можно сопоставить свой оператор проектирования:

$$P_j = \left|\varphi_j\right\rangle\left\langle\varphi_j\right|, \quad j = 1,...,s \qquad (3.23)$$

(по индексу j нет суммирования!)

Задача 3.2 Покажите, что введенные посредством (3.23) операторы, удовлетворяют характерным для операторов ортогонального проектирования условиям:

$$P_j^2 = P_j \quad j = 1,...,s \qquad P_j P_k = 0 \quad j \neq k$$

Задача 3.3 Покажите, что введенные операторы проектирования задают ортогональное разложение единицы, т.е. выполняется условие:

$$\sum_j P_j = \sum_j \left|\varphi_j\right\rangle\left\langle\varphi_j\right| = I$$

Глава 4. Основные логические элементы квантовой информатики и их свойства

4.1 Квантовые биты

Квантовый бит или **кубит (qubit)** представляет собой двухуровневую квантовую систему [1-5]. Кубит описывается единичным вектором в двумерном комплексном векторном пространстве. Базис такого пространства задается всего двумя единичными ортогональными векторами, обозначаемыми соответственно $|0\rangle$ и $|1\rangle$. Кубит может быть реализован в различных физических системах.

Приведем только некоторые примеры. Ортонормированный базис $|0\rangle$ и $|1\rangle$ может соответствовать поляризациям фотонов (вертикальной $|\uparrow\rangle$ и горизонтальной $|\rightarrow\rangle$), а также любым другим взаимно ортогональным поляризациям, например $\left|\frac{3\pi}{4}\right\rangle$ и $\left|\frac{\pi}{4}\right\rangle$ (здесь в скобках указан угол между поляризацией фотона и горизонталью).

Базисные состояния кубита могут отвечать состояниям электрона со спином, направленным вверх (spin-up) и вниз (spin-down), в качестве $|0\rangle$ и $|1\rangle$ могут выступать основное и возбужденное состояния так называемого двухуровневого атома (модель двухуровневого атома предполагает, что за счет специального резонансного выбора частоты лазера накачки, в атоме эффективно оказываются задействованными только два определенные энергетические состояния).

Квантовые состояния $|0\rangle$ и $|1\rangle$, конечно, могут использоваться для записи значений 0 и 1 классического бита информации. Однако, возможности квантового описания информации гораздо шире. В отличие от классического

бита, квантовый бит (кубит) может быть представлен суперпозицией базисных векторов $|0\rangle$ и $|1\rangle$ в виде:

$$|\psi\rangle = a|0\rangle + \mathrm{b}|1\rangle,$$

где a и b – комплексные числа, такие что $|\mathrm{a}|^2 + |b|^2 = 1$.

Если над кубитом производится измерение в базисе $\{|0\rangle, |1\rangle\}$, то с вероятностью $|\mathrm{a}|^2$ кубит окажется в состоянии $|0\rangle$, а с вероятностью $|b|^2$ в состоянии $|1\rangle$.

Рассмотрим подробнее математическую модель кубита. Исторически приведенное ниже описание впервые применялось для рассмотрения поляризационных состояний частиц со спином ½ (электронов, протонов, нейтронов, определенных атомов и др.). Представленный формализм, однако, оказывается пригодным и для описания кубитов произвольной физической природы.

Пусть вектор состояния спина- кубита есть:

$$\psi = c_1\begin{pmatrix}1\\0\end{pmatrix} + c_2\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}c_1\\c_2\end{pmatrix}$$

Для описания математической модели кубита нам потребуются основные сведения из теории спина. Как известно [55,56], оператор спина есть:

$$\vec{s} = \frac{\hbar}{2}\vec{\sigma},$$

где введены матрицы Паули, которые в стандартном представлении задаются следующими формулами:

$$\sigma_1 = \sigma_x = \begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}\ \sigma_2 = \sigma_y = \begin{pmatrix}0 & -i\\i & 0\end{pmatrix}\ \sigma_3 = \sigma_z = \begin{pmatrix}1 & 0\\0 & -1\end{pmatrix}$$

Матрицы Паули удовлетворяют следующему соотношению:

$$\sigma_j \sigma_k = \delta_{jk} I + i\varepsilon_{jkl}\sigma_l \qquad j,k = 1,2,3$$

Здесь по повторяющемуся индексу l предполагается суммирование, δ_{jk} - символ Кронекера, ε_{jkl} - полностью антисимметричный тензор (символ Леви- Чивита). I - единичная матрица (для сокращения записи ее часто опускают).

В квантовой информатике удобно использовать систему единиц, в которой $\hbar = 1$.

Нетрудно видеть, что вектор $\psi = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ является собственным вектором оператора $s_z = \frac{1}{2}\sigma_z$, отвечающим собственному значению +½. Аналогично, вектор $\psi = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ является собственным вектором оператора $s_z = \frac{1}{2}\sigma_z$, отвечающим собственному значению -½

.

Задача 4.1 Покажите, что:

1. Состояния $\psi = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ $\psi = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix}$ отвечают соответственно собственным значениям + ½ и - ½ оператора $s_x = \frac{1}{2}\sigma_x$

2. Состояния $\psi = \frac{1}{2}\begin{pmatrix} 1-i \\ 1+i \end{pmatrix}$ $\psi = \frac{1}{2}\begin{pmatrix} 1+i \\ 1-i \end{pmatrix}$ отвечают соответственно собственным значениям + ½ и - ½ оператора $s_y = \frac{1}{2}\sigma_y$

Введем операторы проектирования спина на направление, задаваемое единичным вектором $\vec{n}$:

$$P_{\pm} = P\left(s_n = \pm 1/2\right) = \frac{1}{2}\left(1 \pm \vec{\sigma}\vec{n}\right)$$

Здесь и в других аналогичных случаях обозначение 1 символизирует единичную матрицу размером 2×2.

Знаки $\pm$ отвечают соответственно операторам проектирования на направление вдоль и против оси $\vec{n}$.

Примером оператора проектирования может служить оператор $\frac{1}{2}\left(1+\sigma_3\right) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, который выделяет из произвольного состояния амплитуду, отвечающую проекции спина +½ на ось z. Аналогично, оператор $\frac{1}{2}\left(1-\sigma_3\right) = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ выделяет из произвольного состояния амплитуду, отвечающую проекции спина -½ на ось z.

Говорят, что операторы проектирования задают разложение единицы, поскольку:

$P\left(s_n = +1/2\right) + P\left(s_n = -1/2\right) = I$ - единичный оператор

Задача 4.2 Покажите, что $\left(\vec{\sigma}\vec{n}\right)^2 = 1$ (единичная матрица)

Задача 4.3 Покажите, что введенные операторы проектирования являются ортогональными проекторами, т.е. удовлетворяют условиям:

$$P_{\pm}^2 = P_{\pm}, \;\; P_+P_- = P_-P_+ = 0$$

Вероятности иметь соответственно положительное и отрицательное значение проекции спина на направление $\vec{n}$ есть

$$P_+(\vec{n}) = \frac{1}{2}\langle\psi|P(s_n = +1/2)|\psi\rangle = \frac{1}{2}\langle\psi|1+\vec{\sigma}\vec{n}|\psi\rangle \qquad (4.1)$$

$$P_-(\vec{n}) = \frac{1}{2}\langle\psi|P(s_n = -1/2)|\psi\rangle = \frac{1}{2}\langle\psi|1-\vec{\sigma}\vec{n}|\psi\rangle \qquad (4.2)$$

Будем задавать $\vec{n}$ посредством сферических углов

$\vec{n} = (n_x, n_y, n_z) = (\sin\theta\cos\varphi, \sin\theta\sin\varphi, \cos\theta)$

Задача 4.4 Путем прямого расчета в стандартном представлении получите следующие выражения для вероятностей (4.1) и (4.2):

$$P_+(\vec{n}) = P_+(\theta,\varphi) = \frac{1}{2}\left[(1+\cos\theta)c_1^* c_1 + \sin\theta e^{-i\varphi} c_1^* c_2 + \sin\theta e^{i\varphi} c_2^* c_1 + (1-\cos\theta)c_2^* c_2\right]$$

$$P_-(\vec{n}) = P_-(\theta,\varphi) = \frac{1}{2}\left[(1-\cos\theta)c_1^* c_1 - \sin\theta e^{-i\varphi} c_1^* c_2 - \sin\theta e^{i\varphi} c_2^* c_1 + (1+\cos\theta)c_2^* c_2\right]$$

Представленные вероятности удовлетворяют следующему очевидному условию:

$$P_+(\theta,\varphi) + P_-(\theta,\varphi) = 1$$

Для каждого направления $\vec{n} = (n_x, n_y, n_z) = (\sin\theta\cos\varphi, \sin\theta\sin\varphi, \cos\theta)$ возникает свое распределение вероятностей. Все вместе эти направления образуют совокупность взаимно- дополнительных распределений в соответствии с принципом дополнительности Нильса Бора (раздел 1.2).

Операторы проекции спина на различные направления не коммутируют друг с другом:

$$\left[s_x, s_y\right] = i s_z$$

Другие аналогичные соотношения получаются циклической перестановкой индексов x, y и z.

Некоммутативность наблюдаемых означает, что проекции спина на различные направления не могут быть определены одновременно. Со

статистической точки зрения это означает, что не существует их совместного распределения $P(s_x, s_y, s_z)$.

Рассмотрим важный частный случай представленных выше общих формул. Пусть $c_1 = 1,\ c_2 = 0$ (состояние кубита $|0\rangle$, спин поляризован вверх вдоль оси z). При измерении в базисе $|0\rangle$ и $|1\rangle$ всегда будем получать состояние $|0\rangle$ (спин вверх). При измерении, задаваемом проекторами $P_{\pm}$, вероятности получения проекции спина вверх и вниз соответственно на направление, составляющее угол θ с вертикалью, будут даваться формулами:

$$P_+(\vec{n}) = P_+(\theta,\varphi) = \frac{1}{2}[(1+\cos\theta)] = \cos^2\left(\frac{\theta}{2}\right)$$

$$P_-(\vec{n}) = P_-(\theta,\varphi) = \frac{1}{2}[(1-\cos\theta)] = \sin^2\left(\frac{\theta}{2}\right)$$

Удобное представление для спиновых состояний можно получить на сфере Блоха, которая определяется посредством сферических углов Θ и Φ

$$\psi = \begin{pmatrix} \cos\left(\frac{\Theta}{2}\right)\exp\left(-i\frac{\Phi}{2}\right) \\ \sin\left(\frac{\Theta}{2}\right)\exp\left(i\frac{\Phi}{2}\right) \end{pmatrix} \qquad (4.3)$$

Указанное представление позволяет сопоставить любому состоянию кубита эквивалентное ему в математическом отношении квантовое состояние частицы со спином ½ (так называемый формализм фиктивного спина).

Любой точке на сфере Блоха соответствует некоторое квантовое состояние кубита и наоборот- любому (чистому) квантовому состоянию кубита можно сопоставить некоторую точку на сфере Блоха.

Заметим, что наряду с представленной выше используют и другие записи, отличающиеся от данной постоянным фазовым множителем.

Задача 4.5. Покажите, что вектор состояния кубита в представлении на сфере Блоха есть собственный вектор проектора $P_+ = \frac{1}{2}(1+\vec{\sigma}\vec{n})$ с собственным значением, равным единице. Здесь направление $\vec{n}$ задается сферическими углами Θ и Φ.

Заметим, что в случае спиновых состояний преобразования, задаваемые проекционными операторами $P_\pm$, могут быть физически реализованы с помощью установки типа Штерна- Герлаха. Эта установка задает в пространстве направление $\vec{n}$, вдоль которого прилагается сильно неоднородное магнитное поле, благодаря которому производится разделение исходного пучка частиц на два (соответствующих проекции спина +½ и –½).

Заметим, что с помощью соответствующих измерительных устройств, указанные операции проектирования могут быть реализованы и для кубитов любой другой физической природы (в этом случае геометрическое представление фиктивного спина на сфере Блоха играет только вспомогательную роль).

4.2. Реализация произвольного состояния кубита посредством унитарного поворота.

Любое состояние кубита может быть получено из состояния $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ посредством некоторого унитарного преобразования. Состоянию $|0\rangle$ на сфере Блоха соответствует «северный» полюс. Нетрудно видеть, что для того, чтобы из «северного» полюса попасть в точку (θ, φ)

на сфере Блоха нужно совершить поворот на угол θ относительно оси $\vec{n} = (-\sin\ \varphi, \cos\ \varphi, 0)$, лежащей в плоскости (x, y).

Введем следующий унитарный оператор:

$$R_{\vec{n}}(\theta) = \exp\left(-i\theta\frac{\vec{\sigma}\,\vec{n}}{2}\right) = \cos\left(\frac{\theta}{2}\right)I - i\sin\left(\frac{\theta}{2}\right)\vec{\sigma}\,\vec{n} \qquad (4.4)$$

Задача4.6 Докажите справедливость представленного тождества путем разложения матричной экспоненты в ряд.

Оказывается, что оператор $R_{\vec{n}}(\theta)$ осуществляет поворот исходного блоховского состояния относительно оси $\vec{n}$ на угол θ, что иллюстрируется следующей задачей.

Задача 4.7 Пусть исходное состояние есть $|0\rangle$. Подействуйте на него оператором $R_{\vec{n}}(\theta)$, где $\vec{n} = (-\sin\ \varphi, \cos\ \varphi, 0)$. Покажите, что в результате получится следующее состояние кубита, отвечающее точке (θ, φ) на сфере Блоха:

$$\psi(\theta,\varphi) = \begin{pmatrix} \cos\left(\frac{\theta}{2}\right) \\ \sin\left(\frac{\theta}{2}\right)\exp(i\varphi) \end{pmatrix}$$

Заметим, что представленная запись для состояния кубита на сфере Блоха отличается от формулы (4.3) раздела 4.1 только несущественным фазовым множителем.

4.3. Система кубитов

Анализ системы кубитов, состоящей более чем из одного кубита, позволяет выяснить природу преимущества квантовых вычислений по сравнению с классическими.

В классической физике, возможные состояния системы n частиц, индивидуальные состояния каждой из которых описываются вектором в двумерном векторном пространстве, образуют векторное пространство, содержащее $2n$ измерений. В то же время, для квантовых систем соответствующее результирующее пространство имеет гораздо большую размерность, а именно 2^n. Это обуславливает экспоненциальный рост размерности пространства состояний с увеличением числа частиц, что, в свою очередь, лежит в основе возможного радикального увеличения скорости вычислений квантового компьютера по сравнению с классическим. С математической точки зрения отличие квантовых систем от классических заключается в том, что в классической физике пространство состояний образуется посредством операции декартового произведения, в то время как в квантовой – посредством тензорного произведения.

Проиллюстрируем особенности квантовых систем на примере регистра из 3 кубитов. Базис такой системы состоит из $2^3 = 8$ векторов:

$$\{ |000\rangle, |001\rangle, |010\rangle, |011\rangle, |100\rangle, |101\rangle, |110\rangle, |111\rangle, \}$$

Например, запись $|000\rangle$ означает тензорное произведение $|0\rangle \otimes |0\rangle \otimes |0\rangle$. В стандартном представлении $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, поэтому:

$$|000\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad |001\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \ldots, \quad |111\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Число, стоящее в скобках Дирака, задает номер базисного квантового состояния в двоичном представлении. Например: $|011\rangle$ и $|3\rangle$ есть различная записи одного и того же базисного состояния.

Задача 4.8 Основываясь на определении тензорного (кронекеровского) произведения матриц, докажите следующее тождество:

$$(A \otimes B)\left(|\psi^{(1)}\rangle \otimes |\psi^{(2)}\rangle\right) = \left(A|\psi^{(1)}\rangle\right) \otimes \left(B|\psi^{(2)}\rangle\right)$$

Здесь считается, что оператор A и состояние $|\psi^{(1)}\rangle$ заданы в гильбертовом пространстве первой частицы, а оператор B и состояние $|\psi^{(2)}\rangle$- в гильбертовом пространстве второй частицы. Указанное тождество показывает, что в составной системе действие оператора $(A \otimes B)$ на двухчастичное состояние $\left(|\psi^{(1)}\rangle \otimes |\psi^{(2)}\rangle\right)$ сводится к тензорному произведению двух векторов $\left(A|\psi^{(1)}\rangle\right) \otimes \left(B|\psi^{(2)}\rangle\right)$, первый из которых описывает действие оператора A на первую частицу, а второй - действие оператора B на вторую частицу.

Неожиданным с точки зрения обычной интуиции является то, что состояние системы не всегда описывается в терминах состояния отдельных ее частей. Например, такое состояние из двух кубитов как $|00\rangle + |11\rangle$ не может быть разложено отдельно на состояния каждого из двух кубитов. Другими словами, мы не можем найти такие $a_1, b_{1,} a_2, b_2$, которые обеспечивали бы выполнение следующего равенства:

$$\left(a_1|0\rangle + b_1|1\rangle\right) \otimes \left(a_2|0\rangle + b_2|1\rangle\right) = |00\rangle + |11\rangle$$

Действительно:

$$\left(a_1|0\rangle + b_1|1\rangle\right)\otimes\left(a_2|0\rangle + b_2|1\rangle\right) =$$
$$= a_1a_2|00\rangle + a_1b_2|01\rangle + b_1a_2|10\rangle + b_1b_2|11\rangle$$

Отсюда следует, что $a_1b_2 = 0$, поэтому либо $a_1a_2 = 0$, либо $b_1b_2 = 0$, что невозможно.

Состояния системы, которые не могут быть представлены в виде произведения состояний ее частей, как уже указывалось ранее, называются **запутанными** (entangled) состояниями.

В соответствии с постулатами квантовой информатики полное описание каждого кубита в отдельности задается соответствующими однокубитовыми векторами состояний. Исходное состояние системы независимо приготовленных кубитов задается тензорным произведением однокубитовых состояний. При включении взаимодействия между кубитами возникают квантовые корреляции. В результате, совместное состояние регистра кубитов перестает быть сепарабельным, т.е. становится запутанным.

Запутанные состояния соответствуют ситуациям, которые не имеют классических аналогов и за которыми не стоит интуиция, подкрепленная наглядными механическими образами. Заметим, что такие состояния как раз и обеспечивают экспоненциальный рост размерности гильбертова пространства состояний в зависимости от числа кубитов.

4.4. Измерение кубитов

Измерение в квантовой системе, состоящей из одного или более кубитов, есть результат проектирования состояния системы до измерения в гильбертово подпространство, совместимое с измеренными значениями. При измерении, как уже отмечалось выше в главе 3, происходит редукция состояния. Амплитуда вероятности проекции, полученной в результате редукции, пересчитывается таким образом, чтобы снова быть нормированной на единицу.

В силу Постулата 3 (раздел 3.1), вероятность того, что результат измерения примет заданное значение, есть сумма квадратов модулей амплитуд вероятности всех компонент, совместимых с результатом измерения.

Рассмотрим для примера измерения в системе из двух кубитов. Вектор состояния такой системы в общем случае есть:

$$|\psi\rangle = c_{00}|00\rangle + c_{01}|01\rangle + c_{10}|10\rangle + c_{11}|11\rangle$$

Здесь $c_{00}, c_{01}, c_{10}, c_{11}$ - произвольные комплексные числа, удовлетворяющие условию нормировки:

$$|c_{00}|^2 + |c_{01}|^2 + |c_{10}|^2 + |c_{11}|^2 = 1$$

Пусть измеряется первый кубит. Вероятность обнаружить его в состоянии $|0\rangle$ есть $|c_{00}|^2 + |c_{01}|^2$, а в состоянии $|1\rangle$ соответственно $|c_{10}|^2 + |c_{11}|^2$. Если измерение первого кубита дало $|0\rangle$, то редуцированное состояние окажется пропорциональным вектору $c_{00}|00\rangle + c_{01}|01\rangle$. После нормировки получим окончательно для состояния после рассматриваемого измерения:

$$|\psi'\rangle = \frac{1}{\sqrt{|c_{00}|^2 + |c_{01}|^2}}\left[c_{00}|00\rangle + c_{01}|01\rangle\right]$$

Измерения запутанных и незапутанных состояний принципиально отличаются друг от друга. С точки зрения концепции измерений, кубиты оказываются незапутанными, если измерение одного из них никак не влияет на состояние другого и, напротив, кубиты обязательно будут запутаны, если такое влияние существует.

Рассмотрим, например, состояние $\frac{1}{\sqrt{2}}\left[|00\rangle + |01\rangle\right]$, которое не является запутанным, т.к. может быть представлено в виде тензорного произведения

отдельных кубитов $\frac{1}{\sqrt{2}}\left[|00\rangle+|01\rangle\right]=|0\rangle\otimes\frac{1}{\sqrt{2}}\left[|0\rangle+|1\rangle\right]$. Здесь, очевидно, измерение первого кубита никак не влияет на состояние второго и наоборот.

Рассмотрим, напротив, состояние $\frac{1}{\sqrt{2}}\left[|00\rangle+|11\rangle\right]$, которое является запутанным. Теперь, результат измерения одного из кубитов влияет на то, какое состояние возникнет у второго кубита. Так, если первый кубит окажется в состоянии $|0\rangle$, то и второй автоматически окажется в состоянии $|0\rangle$, если же в результате измерения первого кубита будет получено состояние $|1\rangle$, то и второй кубит обязательно будет обнаружен в состоянии $|1\rangle$. Рассматриваемое состояние является одним из так называемых состояний Белла. Подробнее свойства таких состояний будут описаны в разделах 4.8- 4.10

4.5. Простейшие квантовые логические элементы

Любые квантовые вычисления сводятся к унитарным преобразованиям системы кубитов. В силу линейности, преобразование полностью определяется действием на соответствующие базисные векторы.

Рассмотрим вначале некоторые полезные преобразования квантового состояния отдельных кубитов. Ниже приведены такие преобразования и соответствующие им матрицы.

Мы везде используем стандартный (канонический) базис:

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

Тождественное преобразование задается единичной двумерной матрицей

$$I:\ \begin{matrix}|0\rangle\to|0\rangle,\\ |1\rangle\to|1\rangle\end{matrix}\qquad I=\begin{pmatrix}1&0\\0&1\end{pmatrix}$$

Матрицы Паули задают следующие преобразования:

$$X: \begin{array}{l} |0\rangle \to |1\rangle, \\ |1\rangle \to |0\rangle \end{array} \quad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$Y: \begin{array}{l} |0\rangle \to i|1\rangle, \\ |1\rangle \to -i|0\rangle \end{array} \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

$$Z: \begin{array}{l} |0\rangle \to |0\rangle, \\ |1\rangle \to -|1\rangle \end{array} \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Заметим, что матрицы Паули одновременно являются эрмитовыми и унитарными, поэтому унитарны и все указанные выше преобразования.

Элемент Паули X есть оператор отрицания (negation), он осуществляет обмен состояниями, т.е. преобразует ноль в единицу и наоборот. Элемент Z задает оператор фазового сдвига (phase shift). Преобразование Y определяется произведением указанных операторов, поскольку $ZX = iY$.

Рассмотрим теперь важнейший для квантовых вычислений логический элемент- так называемое **управляемое – НЕ (Controlled-Not)** преобразование. Преобразование CNOT действует не на один, а одновременно на два кубита следующим образом: CNOT изменяет состояние второго (управляемого) кубита, если первый (управляющий) находится в состоянии $|1\rangle$, т.е.

$$CNOT: \begin{array}{l} |00\rangle \to |00\rangle, \\ |01\rangle \to |01\rangle, \\ |10\rangle \to |11\rangle, \\ |11\rangle \to |10\rangle. \end{array} \quad CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Оператор CNOT также унитарен и эрмитов одновременно. Рассматриваемое преобразование является принципиально новым по сравнению с однокубитовыми преобразованиями, т.к. матрица CNOT не

может быть разложена в тензорное произведение двух однокубитовых матриц.

Удобно иметь графическое представление преобразований квантового состояния, особенно когда эти преобразования связаны с взаимодействием нескольких кубитов. CNOT- элемент обычно изображается на квантовых логических схемах в виде следующей картинки

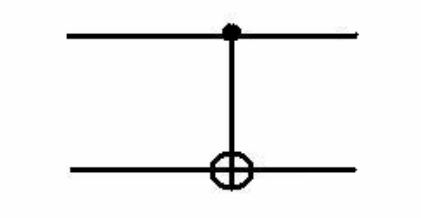

Рис. 4.1 Графическое изображение двухкубитового элемента CNOT

Здесь значок $\bullet$ соответствует управля**ющему** кубиту, а значок $\oplus$ - управля**емому** кубиту.

Аналогично можно определить элемент Control-Control-Not (CCNOT), который соответствует преобразованию, меняющему третий бит, когда оба первые есть $|1\rangle$ (см. рисунок). Это так называемый элемент Тоффоли.

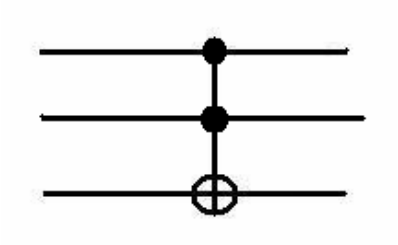

Рис. 4.2 Графическое изображение элемента Тоффоли

Действие элемента Тоффоли на базисные состояния и соответствующая унитарная матрица задаются следующим образом.

$CCNOT$:

$$|000\rangle \to |000\rangle,$$
$$|001\rangle \to |001\rangle,$$
$$|010\rangle \to |010\rangle,$$
$$|011\rangle \to |011\rangle,$$
$$|100\rangle \to |100\rangle,$$
$$|101\rangle \to |101\rangle,$$
$$|110\rangle \to |111\rangle,$$
$$|111\rangle \to |110\rangle$$

$$CCNOT = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

Однокубитовые преобразования изображаются графически, например, так:

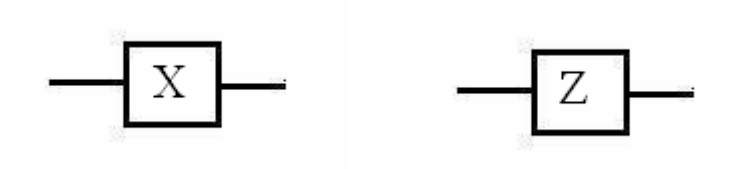

Рис. 4.3 Примеры графических изображений однокубитовых квантовых элементов.

Оказывается, что любое унитарное преобразование- вычисление в системе кубитов можно выполнить с помощью так называемых универсальных наборов квантовых логических элементов [13,14]. Например, произвольное унитарное вращение состояния отдельного кубита и двухкубитовая операция CNOT могут рассматриваться в качестве такого универсального набора.

4.6. Преобразование Уолша-Адамара (Walsh-Hadamar Transformation)

В квантовой информатике очень широко используется следующее однокубитовое преобразование – так называемое преобразование Адамара. Оно определяется как:

$$H : |0\rangle \to \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle),$$
$$|1\rangle \to \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Задача 4.9 Покажите, что

$$H = \frac{1}{\sqrt{2}}(X + Z) = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

Докажите следующие тождества:

$HX = ZH$

$HZ = XH$

$HY + YH = 0$

Преобразование, которое обеспечивает приложение H к каждому из n кубитов квантового регистра, называется преобразованием Уолша- Адамара:

$$W_1 = H, \quad \mathrm{W}_{\mathrm{m+1}} = H \otimes W_m, \quad m = 1,...,n-1$$

Задача 4.10 Докажите свойство преобразования Уолша- Адамара, которое дается формулой:

$$\left(\underbrace{\mathrm{H} \otimes \mathrm{H} \otimes \ldots \otimes \mathrm{H}}_{n \text{ раз}} \right) \left| \underbrace{00 \ldots 0}_{n \text{ раз}} \right\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle$$

Результат этой задачи часто используется при разработке квантовых алгоритмов (см. главу 5).

4.7. Теорема о невозможности клонирования неизвестного квантового состояния

Свойство линейности унитарных квантовых преобразований приводит к невозможности копирования (клонирования) информации в квантовом компьютере. Рассматриваемая теорема является одним из краеугольных камней квантовой информатики.

Доказательство проведем от противного. Предположим, что U - унитарное преобразование, осуществляющее клонирование. Такое преобразование действовало бы по правилу $U|a0\rangle = |aa\rangle$ для любого квантового состояния $|a\rangle$. Здесь запись $|a\rangle$ и $|0\rangle$ может означать не только однокубитовые, но и многокубитовые состояния.

Пусть $|a\rangle$ и $|b\rangle$ - два ортогональных квантовых состояния. Если U - оператор клонирования, то $U|a0\rangle = |aa\rangle$, $U|b0\rangle = |bb\rangle$. Рассмотрим теперь состояние, являющееся суперпозицией исходных состояний $|c\rangle = \frac{1}{\sqrt{2}}\left(|a\rangle + |b\rangle\right)$.

Тогда, в силу линейности унитарного преобразования

$$U|c0\rangle = \frac{1}{\sqrt{2}}\left(U|a0\rangle + U|b0\rangle\right) = \frac{1}{\sqrt{2}}\left(|aa\rangle + |bb\rangle\right) \qquad (4.5)$$

Кроме того, по предположению, U есть оператор клонирования, который должен действовать в том числе и на состояния $|c\rangle$. Поэтому:

$$U|c0\rangle = |cc\rangle = \frac{1}{2}\left(|aa\rangle + |ab\rangle + |ba\rangle + |bb\rangle\right) \qquad (4.6)$$

Состояние, задаваемое формулой (4.6), очевидно, не совпадает с состоянием, задаваемым формулой (4.5). Получено противоречие, что и доказывает теорему.

Важно понимать какое состояние возможно реализовать, а какое нет. Можно приготовить квантовое состояние, которое известно нам заранее. Принцип невозможности клонирования говорит о невозможности клонировать неизвестное состояние.

Заметим также, что можно создавать запутанное состояние $a|00...0\rangle + b|11...1\rangle$ из неизвестного состояния $a|0\rangle + b|1\rangle$. Пример реализации

такого рода запутанного состояния дается квантовой схемой, изображенной на рисунке.

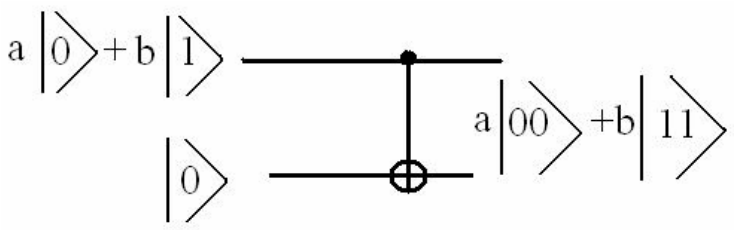

Рис. 4.4 Квантовая схема генерации запутанного состояния

Рассматриваемое двухкубитовое состояние не является, однако, реализацией схемы клонирования однокубитового состояния $a|0\rangle + b|1\rangle$. В силу запутанности, кубиты в состоянии $a|00\rangle + b|11\rangle$ оказываются связанными друг с другом: если один оказался при измерении, например, в состоянии $|0\rangle$, то и второй окажется в том же состоянии.

Задача 4.11 Обобщите представленную выше на рисунке квантовую схему, т.е. придумайте схему, позволяющую создавать запутанное состояние $a|00...0\rangle + b|11...1\rangle$ из неизвестного состояния $a|0\rangle + b|1\rangle$ для случая трех и более кубитов.

Настоящим клоном было бы состояние n частиц вида $(a|0\rangle + b|1\rangle)\otimes ...\otimes(a|0\rangle + b|1\rangle)$, созданное из неизвестного состояния $a|0\rangle + b|1\rangle$. Это, однако, невозможно в силу доказанной выше теоремы.

Теорема о невозможности клонирования неизвестного квантового состояния символизирует принципиально важную роль статистических методов в квантовой информатике. Действительно, если бы рассматриваемое здесь клонирование было возможно, то, имея в распоряжении только одного представителя, мы могли бы создать сколь угодно много его копий. Проведя измерения над этими копиями, мы смогли бы сколь угодно точно

восстановить квантовое состояние и любые его характеристики. Другими словами, нам не нужен был бы статистический ансамбль для проведения взаимно- дополнительных измерений, поскольку такой ансамбль всегда можно было бы воссоздать, имея под рукой всего одного представителя. Это противоречило бы таким принципам статистики, как неравенство Рао-Крамера. В действительности, уже простейшее однокубитовое состояние $a|0\rangle + b|1\rangle$ содержит в себе бесконечное (континуальное) количество информации в том смысле, что описывается комплексными бесконечно-значными числами (такими, как a и b). Измерение отдельного представителя приводит к редукции его квантового состояния и соответствующей потере информации о комплексных амплитудах. Однако, одновременно с этим исследователь получает некоторое элементарное количество информации (в каком из возможных базисных состояний обнаруживается квантовая система). Для точного восстановления квантового состояния потребуется бесконечное число представителей. В реальных задачах всегда имеется конечный объем экспериментальных данных и, соответственно, возможна только приближенная оценка квантового состояния. Точность восстановления квантового состояния оказывается тем выше, чем больше число представителей статистического ансамбля подвергается измерениям (и разрушению исходных квантовых состояний). Подробно задача статистического восстановления квантовых состояний рассмотрена в работах [30, 43, 44, 51, 52].

4.8. Состояния Белла

Состояниями Белла называют следующие четыре двухкубитовые состояния.

$$|\beta_{00}\rangle = |\Phi^+\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$

$$|\beta_{01}\rangle = |\Psi^+\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right)$$

$$|\beta_{10}\rangle = |\Phi^-\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle - |11\rangle\right)$$

$$|\beta_{11}\rangle = |\Psi^-\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right)$$

Задача 4.12 Покажите, что все состояния Белла являются запутанными

Указанные состояния могут быть созданы с помощью квантовой схемы, изображенной на рисунке.

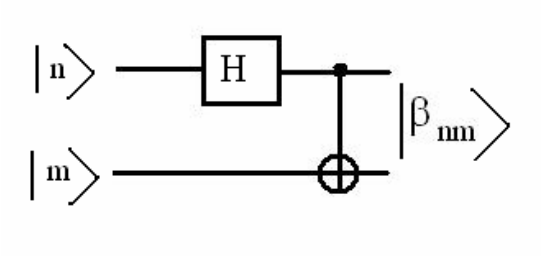

Рис. 4.5 Квантовая схема для генерации состояний Белла

Состояния Белла относят к классу так называемых ЭПР состояний. Такой термин возник в связи с парадоксом (эффектом) Эйнштейна - Подольского – Розена, который рассматривается ниже.

4.9 Парадокс (эффект) Эйнштейна - Подольского - Розена

Предположим, что источник генерирует пару частиц в состоянии Белла, например $\frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$. Такая пара частиц называется ЭПР – парой.

Пусть одна из этих частиц посылается в пункт А (к Алисе), а другая – в пункт В (к Бобу). Алиса и Боб могут находиться сколь угодно далеко друг от друга.

Предположим, что Алиса измеряет свою частицу и наблюдает состояние $|0\rangle$. Это означает, что совместное состояние частиц теперь оказывается состоянием $|00\rangle$ и, следовательно, при измерении своей частицы Боб обязательно получит $|0\rangle$.

Аналогично, если Алиса получит при измерении $|1\rangle$, то Боб также получит $|1\rangle$. Заметим, что изменение совместного квантового состояния частиц происходит мгновенно, даже если частицы находятся друг от друга сколь угодно далеко.

На первый взгляд кажется, что Алиса и Боб получают возможность обмениваться сообщениями со скоростью, большей скорости света в вакууме. Однако, это не так. Рассматриваемое явление нельзя использовать для налаживания линии связи, действующей быстрее света. Все что мы можем сказать – это то, что Алиса и Боб, используя эффект ЭПР, могут одновременно в разных местах наблюдать одинаковое случайное поведение.

Отметим, что первоначальная формулировка авторов ЭПР парадокса относилась к системам с непрерывными переменными. Здесь мы представили более простой пример, основанный на рассмотрении дискретных (спиновых) переменных. Такая формулировка ЭПР парадокса впервые была предложена Д. Бомом.

Заметим, что ЭПР парадокс на деле не является никаким парадоксом. Правильнее говорить об ЭПР эффекте. Он заключается в том, что части одной общей системы, даже после прекращения взаимодействия между ними, продолжают описываться единым квантовым состоянием. Это явление рассматривалось как парадокс на заре развития квантовой теории. В настоящее время ЭПР эффект находит свое естественное воплощение в задачах квантовой информатики.

4.10 Неравенство Белла

Рассмотрим следующее состояние Белла

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle\right) \qquad (4.7)$$

В обозначениях формулы (4.7) предполагается, что состояние образовано двумя спиновыми частицами. Это же состояние в других обозначениях есть:

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right) = \frac{1}{\sqrt{2}}\begin{pmatrix} 0 \\ 1 \\ -1 \\ 0 \end{pmatrix} \qquad (4.8)$$

В обозначениях формулы (4.8) рассматриваемое состояние Белла описывается как двухкубитовое состояние.

Будем в качестве оператора спина использовать оператор $\vec{\sigma}$ (т.е. будем опускать множитель $\frac{\hbar}{2}$). В таком представлении, результат измерения спина есть либо $+1$, либо -1.

Если при измерении на ось z Алиса получает $+1$, то Боб при измерении на ту же ось с необходимостью получает -1 и наоборот. То же самое будет происходить и при измерении на любую другую ось в пространстве. Данное состояние является так называемым синглетным состоянием. Оно отвечает суммарному спину системы из двух частиц, равному нулю (поэтому равна нулю и проекция спина системы на любую ось).

Заметим, что состояние $\frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right)$, отличающееся знаком от рассматриваемого, также отвечает нулевой проекции спина, но при этом суммарный спин равен единице. Набор из трех состояний $|00\rangle$,

$\frac{1}{\sqrt{2}}\left(|01\rangle+|10\rangle\right)$ и $|11\rangle$ образует так называемый триплет (триплетное состояние). Триплет отвечает суммарному спину двух частиц, равному единице ($j=1$), и трем значениям проекции спина соответственно: $m=+1,0,-1$.

Задача 4.13 Покажите инвариантность синглетного состояния относительно выбора оси квантования.

Дадим набросок решения задачи. Пусть $|0\rangle$ и $|1\rangle$ состояния, отвечающие проекциям спина (оператор σ_z) соответственно $+1$ и -1 на некоторую ось $\vec{n}$, $|0'\rangle$ и $|1'\rangle$- те же состояния при проектировании на ось $\vec{n}'$. Новые и старые базисные состояния связаны унитарным преобразованием

$$|0'\rangle=u_{00}|0\rangle+u_{01}|1\rangle$$

$$|1'\rangle=u_{10}|0\rangle+u_{11}|1\rangle$$

Здесь $U=\begin{pmatrix}u_{00} & u_{01}\\ u_{10} & u_{11}\end{pmatrix}$ - унитарная матрица.

Пусть её определитель равен единице: $u_{00}u_{11}-u_{10}u_{01}=1$

Тогда, нетрудно показать, что выполняется тождество:

$$|0'1'\rangle-|1'0'\rangle=|01\rangle-|10\rangle$$

Рассматриваемое тождество показывает, что синглетное состояние имеет один и тот же вид, независимо от оси квантования.

Заметим, что определитель унитарной матрицы может отличаться от единицы несущественным фазовым множителем.

Рассмотрим теперь некоторую процедуру измерения синглетного состояния. Пусть Алиса измеряет проекцию спина своей частицы на ось $\vec{a}$, а Боб- проекцию спина своей частицы на ось $\vec{b}$.

При измерении Алиса получает $+1$ с вероятностью $\frac{1}{2}$ и -1 с вероятностью $\frac{1}{2}$. После этого состояние редуцируется таким образом, что Боб при измерении на ту же ось $\vec{a}$ будет получать -1, если Алиса получает $+1$ и наоборот. Если же Боб проводит измерение на другую ось $\vec{b}$, расположенную под углом θ к оси Алисы, то в соответствии с полученными ранее результатами (см. разделы 4.1- 4.2), будем иметь следующее распределение вероятностей измерений:

$$P_{AB}(+1,-1)=\frac{1}{2}\cos^2\left(\frac{\theta}{2}\right) \qquad (4.9)$$

$$P_{AB}(+1,+1)=\frac{1}{2}\sin^2\left(\frac{\theta}{2}\right) \qquad (4.10)$$

$$P_{AB}(-1,+1)=\frac{1}{2}\cos^2\left(\frac{\theta}{2}\right) \qquad (4.11)$$

$$P_{AB}(-1,-1)=\frac{1}{2}\sin^2\left(\frac{\theta}{2}\right) \qquad (4.12)$$

Здесь $P_{AB}(+1,-1)$ означает, что Алиса получает $+1$, а Боб -1 и т.д.

Задача 4.14 Докажите приведенные выше формулы (4.9)- (4.12). Указание: воспользуйтесь результатами, описывающими реализацию произвольного состояния кубита посредством унитарного поворота.

Задача 4.15 Покажите, что маргинальные распределения, описывающие показания отдельно Алисы и Боба, есть:

$$P_A(+1)=P_A(-1)=\frac{1}{2} \qquad P_B(+1)=P_B(-1)=\frac{1}{2}$$

Покажите, что математические ожидания этих распределений равны нулю, а дисперсии единице.

Пусть X и Y - случайные величины, регистрируемые соответственно Алисой и Бобом. Покажите, что коэффициент корреляции случайных величин X и Y есть:

$$R_{AB}=M(XY)=-\cos(\theta)=-\vec{a}\vec{b}$$

Напомним, что классические (неквантовые) представления о вероятности исходят из того, что случайность является «ненастоящей» (субъективной). На самом деле объект, якобы, обладает данным значением параметра и до измерения, только оно скрыто от нас, а измерение просто проявляет то, что было ранее скрыто (шар в урне был либо черным, либо белым и до того, как мы его вынули).

Оказывается, что квантовые корреляции, проявляемые в синглетном состоянии Белла, опровергают такие представления, поскольку подобные корреляции не могут быть смоделированы никакой классической моделью, т.е. моделью со скрытыми (латентными) параметрами (типа рулетки).

Чтобы показать это рассмотрим так называемое неравенство Белла-Клаузера- Хорна- Шимони [1,66].

Пусть X_1, X_2, Y_1, Y_2 - произвольные действительные числа, не превышающие по модулю 1. $\left|X_j\right|\le 1$, $\left|Y_j\right|\le 1$, $j=1,2$

Покажем, что

$$-2 \le X_1Y_1 + X_1Y_2 + X_2Y_1 - X_2Y_2 \le 2$$

Пусть, например, все параметры неотрицательны и $Y_1 \ge Y_2$, тогда

$$X_1Y_1 + X_1Y_2 + X_2Y_1 - X_2Y_2 = X_1(Y_1 + Y_2) + X_2(Y_1 - Y_2) \le$$
$$\max(X_1, X_2)(Y_1 + Y_2 + Y_1 - Y_2) = 2Y_1 \max(X_1, X_2) \le 2$$

Задача 4.16 Проведите до конца рассуждения, доказывающие неравенство Белла- Клаузера- Хорна- Шимони.

Пусть теперь X_1, X_2, Y_1, Y_2 - действительные случайные величины, удовлетворяющие тем же неравенствам.

Задача 4.17 Покажите, что неравенства, справедливые для некоторых случайных величин, останутся справедливыми и для соответствующих средних значений (математических ожиданий).

С учетом результатов последней задачи, усредняя неравенство Белла- Клаузера- Хорна- Шимони, получим:

$$\left|M(X_1Y_1) + M(X_1Y_2) + M(X_2Y_1) - M(X_2Y_2)\right| \le 2$$

Оказывается, что полученное неравенство нарушается при измерениях синглетного состояния Белла. Действительно, выберем направления измерений в одной плоскости так, чтобы полярные углы были:

$\varphi = 0$ для $\vec{a}_1$, $\varphi = \frac{\pi}{2}$ для $\vec{a}_2$, $\varphi = -\frac{3\pi}{4}$ для $\vec{b}_1$, $\varphi = \frac{3\pi}{4}$ для $\vec{b}_2$.

Тогда:

$$M(X_1Y_1) = M(X_1Y_2) = M(X_2Y_1) = -\cos\left(\frac{3\pi}{4}\right) = \frac{\sqrt{2}}{2}$$

$$M(X_2Y_2) = -\cos\left(\frac{\pi}{4}\right) = -\frac{\sqrt{2}}{2}$$

В результате получим:

$$M(X_1Y_1) + M(X_1Y_2) + M(X_2Y_1) - M(X_2Y_2) = 2\sqrt{2} > 2$$

Таким образом, неравенство Белла нарушается.

Проясним статистический смысл неравенства Белла и факта его нарушения. При усреднении неравенства Белла- Клаузера- Хорна- Шимони, когда вычислялись средние значения $M(X_1Y_1), M(X_1Y_2), M(X_2Y_1)$ и $M(X_2Y_2)$, неявно предполагалось, что существует совместное распределение случайных величин $P(X_1, Y_1, X_2, Y_2)$ (всего 16 вероятностей). Реально же такого распределения в представленном примере не существует. Другими словами, в приведенном примере нельзя подобрать 16 таких неотрицательных чисел (вероятностей), чтобы описать все корреляции (некоторые из «вероятностей» обязательно будут отрицательными, т.е. не будут на деле вероятностями).

С физической точки зрения результат Белла служит еще одной иллюстрацией к принципу дополнительности Н. Бора и связанной с ним некоммутативностью наблюдаемых. Действительно, измерениям Алисы на оси $\vec{a}_1$ и $\vec{a}_2$ отвечают некоммутирующие спиновые переменные, поэтому совместное двумерное распределение $P(X_1, X_2)$ не существует. Аналогично, не существует двумерного распределения $P(Y_1, Y_2)$, которое отвечало бы результатам измерений Боба на оси $\vec{b}_1$ и $\vec{b}_2$. Уже отсюда следует, что не существует и совместного четырехмерного распределения этих величин, т.е. не существует $P(X_1, Y_1, X_2, Y_2)$.

Остановимся коротко на методологической стороне неравенства Белла. Возникает вопрос: зачем Беллу потребовалось конструировать достаточно

сложный пример, доказывающий, что совместного распределения $P(X_1, Y_1, X_2, Y_2)$ не существует, если этот факт заведомо известен, поскольку принцип дополнительности и некоммутативность спиновых операторов приводят к неправомочности уже более простых распределений $P(X_1, X_2)$ и $P(Y_1, Y_2)$?

Попробуем ответить на этот вопрос. Дело в том, что довольно часто при слишком упрощенном изложении предмета всю специфику квантовых явлений пытаются свести к неустранимому взаимодействию микросистемы с измерительным прибором. В частности, нередко говорят, что некоммутирующие переменные (например, X_1 и X_2) не могут быть определены одновременно только потому, что измерение одной из них приводит к физическому воздействию на микрообъект и разрушению его квантового состояния, что, как следствие, ведет к невозможности измерения другой переменной (X_2). При таком понимании квантовых явлений считают, что каждый микрообъект, якобы, всегда обладает определенными значениями характеризующих его переменных, но эти переменные могут находиться в скрытом (латентном) состоянии. В таких моделях, называемых теориями со скрытыми параметрами, имеют смысл и распределения для некоммутирующих переменных типа $P(X_1, X_2)$, но существуют эти распределения не в явной, а в скрытой (латентной) форме. В этой связи, пример Белла может рассматриваться как аргумент против подобного рода теорий со скрытыми параметрами.

Действительно, Белл не вводит в рассмотрение несуществующих распределений $P(X_1, X_2)$ и $P(Y_1, Y_2)$, относящихся к измерениям над одной частицей. Он рассматривает только измерения над различными частицами, пространственно удаленными друг от друга. Этим измерениям соответствуют

коммутирующие спиновые переменные, отвечающие различным частицам, поэтому хорошо определенны и соответствующие распределения $P(X_1, Y_1)$, $P(X_1, Y_2)$, $P(X_2, Y_1)$ и $P(X_2, Y_2)$. Согласно логике теории со скрытыми параметрами, измерения Алисы никак не должны влиять на скрытые параметры Боба и наоборот, поэтому должно выполняться неравенство Белла. Многочисленные проведенные эксперименты, однако, согласуются с предсказаниями квантовой теории и убедительно демонстрируют факт нарушения неравенства Белла. Таким образом, нарушение неравенства Белла свидетельствует против теорий со скрытыми параметрами (против так называемого скрытого реализма).

Поясним, в каком контексте здесь используется термин реализм. Согласно квантовой теории, в соответствии с принципами статистики, микрообъект, находящийся в квантовом состоянии суперпозиции, не обладает до измерения определенным значением физической переменной (представленной в суперпозиции). В результате соответствующего проекционного измерения микрообъект переходит в другое состояние, с определенным значением рассматриваемой физической переменной. Согласно же так называемому реализму (в разрез с принципами квантовой информатики и опытом) считается, что микрообъект всегда обладает определенным набором свойств (хотя и, возможно, в скрытой и сложной форме). Именно такого рода реализм и отвергается фактом нарушения неравенства Белла.

В теориях со скрытыми параметрами рассматриваемые переменные X_1, Y_1, X_2, Y_2 могут быть сложными функциями большого числа (например, миллиона) других неизвестных скрытых параметров. Однако, и в этом случае (в предположении однозначности и гладкости соответствующих зависимостей), для наших переменных X_1, Y_1, X_2, Y_2 возникнет некоторое распределение $P(X_1, Y_1, X_2, Y_2)$, которое будет следствием более глубокого

неизвестного распределения для скрытых микропараметров. Все проведенные выше рассуждения останутся справедливыми и для этого гипотетического случая. Таким образом, неравенство Белла для переменных X_1, Y_1, X_2, Y_2 останется в силе независимо от того, стоят или нет за рассматриваемыми скрытыми переменными еще более «скрытые». Таким образом, усложнение модели, связанное с введением распределений все большего и большего числа переменных ничего не может дать для объяснения факта нарушения неравенства Белла в принципе. Как мы уже видели выше, для объяснения различия между классической и квантовой статистикой нужны качественно новые идеи. Эти идеи связаны с принципом дополнительности и соответствующим рассмотрением некоммутирующих наблюдаемых. Объектом, объединяющим свойства всех взаимно- дополнительных распределений, как мы уже видели ранее, служит вектор квантового состояния (который не может быть заменен ни на какое распределение сколь угодно высокой размерности).

Стоит уточнить, что факт нарушения неравенства Белла свидетельствует против так называемого локального реализма (т.е. остается еще возможность для «нелокального реализма», когда некоторые из скрытых параметров могут быть де- локализованы, т.е. будут одновременно принадлежать обеим частицам, поэтому измерение Алисой своей частицы неведомым и нелокальным образом будет влиять и на частицу Боба).

Резюмируя аргументы, представленные выше, отметим, что сама постановка вопроса о скрытых параметрах и связанная с этим многолетняя полемика в физической литературе, на наш взгляд, свидетельствуют о еще недостаточном понимании принципа дополнительности и статистического характера квантовой теории. Можно предположить, что действительный прогресс в понимании смысла квантовой теории будет достигаться не столько тем, что с помощью сложных расчетов и хитроумных экспериментов будут

отвергнуты все возможные различные теории со скрытыми параметрами, сколько тем, что будет осознана изначальная искусственность и практическая бессмысленность подобного рода построений (подобно тому, как в свое время была осознана бессмысленность многочисленных теорий электродинамического эфира).

4.11. Физическая реализация кубита. Спиновой магнитный резонанс.

Мы рассмотрим физическую реализацию кубита на примере квантовой системы со спиновым магнитным резонансом.

На основе уравнения Дирака можно показать, что наличие спина у электрона приводит к появлению у него магнитного момента. Соответствующий гамильтониан взаимодействия магнитного момента $\vec{\mu}$ с магнитным полем $\vec{H}$ есть:

$$\mathrm{H}_{\mathrm{int}} = -\vec{\mu}\vec{H} \text{ , где } \vec{\mu} = \frac{e\hbar}{2mc}\vec{\sigma}$$

Пусть магнитное поле $\vec{H}$ есть комбинация однородного поля $\vec{H}_0$, направленного вдоль оси z и поля $\vec{H}_1$, вращающегося в плоскости x, y:

$$\vec{H} = H_0\vec{e}_z + H_1\left(\vec{e}_x \cos\omega t + \vec{e}_y \sin\omega t\right)$$

Для определенности будем иметь ввиду электрон. С учетом отрицательного знака заряда электрона, имеем:

$$\mathrm{H}_{\mathrm{int}} = \mu\vec{\sigma}\vec{H} \text{ , где } \mu = \frac{|e|\hbar}{2mc}$$

Уравнение Паули, представляющее собой модификацию уравнения Шредингера с учетом спина электрона, есть:

$$i\hbar\frac{\partial\varphi}{\partial t}=\mathrm{H}_{\mathrm{int}}\varphi,$$

где $\varphi=\begin{pmatrix}\varphi_1\\ \varphi_2\end{pmatrix}$ - двухкомнонетнный спинор.

Пусть $\omega_0=\frac{\mu H_0}{\hbar}$, $\omega_1=\frac{\mu H_1}{\hbar}$ - соответственно продольная и поперечная частоты.

Тогда уравнение Паули примет вид:

$$i\frac{\partial\varphi}{\partial t}=\Omega\varphi,$$

где $\Omega=\omega_0\sigma_z+\omega_1\left(\sigma_x\cos(\omega t)+\sigma_y\sin(\omega t)\right)$ - оператор частоты.

Осуществим переход к другим (медленным) переменным посредством преобразования

$$\tilde{\varphi}=\exp\left(i\frac{\omega t}{2}\sigma_z\right)\varphi$$

Рассматриваемое преобразование называется переходом во вращающуюся систему координат. Для новой переменной получим уравнение:

$$i\frac{\partial\tilde{\varphi}}{\partial t}=\left[\exp\left(i\frac{\omega t}{2}\sigma_z\right)\Omega\exp\left(-i\frac{\omega t}{2}\sigma_z\right)-\frac{\omega}{2}\sigma_z\right]\tilde{\varphi}$$

Учтем, что (см. формулу (4.4) раздела 4.2):

$$\exp\left(i\frac{\omega t}{2}\sigma_z\right)=\cos\left(\frac{\omega t}{2}\right)+i\sin\left(\frac{\omega t}{2}\right)\sigma_z$$

Тогда, рассматриваемое уравнение примет вид:

$$i\frac{\partial\tilde{\varphi}}{\partial t}=\left[\left(\omega_0-\frac{\omega}{2}\right)\sigma_z+\omega_1\sigma_x\right]\tilde{\varphi}$$

Его решение, очевидно, есть:

$$\tilde{\varphi}(t)=\exp\left[-it\left(\left(\omega_0-\frac{\omega}{2}\right)\sigma_z+\omega_1\sigma_x\right)\right]\tilde{\varphi}_0$$

Последняя формула описывает поворот квантового состояния на сфере Блоха.

Ось поворота и угол вращения есть:

$$\vec{n}=\frac{2\left(\left(\omega_0-\frac{\omega}{2}\right)\vec{e}_z+\omega_1\vec{e}_x\right)}{\Omega_R},\ \theta=\Omega_R t,$$

Где $\Omega_R=2\sqrt{\left(\omega_0-\frac{\omega}{2}\right)^2+\omega_1^2}$ - частота Раби

Наиболее простая динамика спина- кубита будет наблюдаться в условиях резонанса, когда

$\omega_0=\frac{\omega}{2}$. Практически такой резонанс достигается обычно путем медленного изменения продольного поля $\vec{H}_0$.

В условиях резонанса в рассматриваемом примере происходит вращение состояния кубита вокруг оси x

Задача 4.18 Пусть начальное состояние кубита есть $\tilde{\varphi}_0=|0\rangle=\begin{pmatrix}1\\0\end{pmatrix}$, что соответствует «северному полюсу» на сфере Блоха. Покажите, что в условиях резонанса, чтобы перевести кубит из состояния $|0\rangle$ в состояние $|1\rangle$,

достаточно выждать в течении времени $t = \frac{\pi}{\Omega_R}$ (так называемый π - импульс). Аналогично, покажите, что воздействие в течении $t = \frac{\pi}{2\Omega_R}$ приводит к повороту состояния на угол $\pi / 2$ вокруг оси x, что соответствует преобразованию состояния $\tilde{\varphi}_0 = |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ в состояние $\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -i \end{pmatrix}$

Динамика кубита может быть представлена в виде:

$$\tilde{\varphi}(t) = \left(\cos\left(\frac{\Omega_R t}{2}\right) - i\vec{\sigma}\vec{n}\sin\left(\frac{\Omega_R t}{2}\right)\right)\tilde{\varphi}_0$$

Задача 4.19 Пусть начальное состояние кубита есть $\tilde{\varphi}_0 = |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$. Покажите, что вероятность переворота спина (спин- флип) есть:

$$P = 4\left(\frac{\omega_1}{\Omega_R}\right)^2 \sin^2\left(\frac{\Omega_R t}{2}\right)$$

Среднее по времени от полученной вероятности есть:

$$\overline{P} = 2\left(\frac{\omega_1}{\Omega_R}\right)^2 = \frac{\omega_1^2}{2\left(\left(\omega - \frac{\omega}{2}\right)^2 + \omega_1^2\right)}$$

Последнее выражение, рассматриваемое как функция ω_0, описывает резонанс на частоте $\omega_0 = \frac{\omega}{2}$.

Заметим, что в реальных экспериментах, как правило, $\omega_1 << \omega_0$

Приведём некоторые данные, необходимые для проведения численных оценок

Магнитный момент электрона:

$\mu_e / \mu_B = 1.001159652$, где

$\mu_B = \frac{|e|\hbar}{2m_e c} = 9.274015 \cdot 10^{-21}$эрг/гс$= 9.274015 \cdot 10^{-24}$Дж/Тл - магнетон Бора.

Небольшое отличие отношения μ_e / μ_B от единицы называется аномальным магнитным моментом электрона. Теоретическое объяснение этого эффекта, согласующееся с экспериментом с очень высокой точности, является важным достижением квантовой электродинамики.

Магнитный момент протона есть:

$\mu_p / \mu_N = 2.792847$, где

$\mu_N = \frac{|e|\hbar}{2m_p c} = 5.050786 \cdot 10^{-24}$эрг/гс$= 5.050786 \cdot 10^{-27}$Дж/Тл - ядерный магнетон

Большое отличие магнитного момента протона от ядерного магнетона является следствием сложной (кварковой) структуры частицы (заметим, что в теории Дирака частица предполагается точечной).

Нейтрон, несмотря на нулевой заряд, также обладает магнитным моментом, который равен (в ядерных магнетонах)

$\mu_n / \mu_N = -1.913042$

Оценим типичные частоты, возникающие при магнитном резонансе

Пусть продольное поле есть: $H_0 = 1$Тл

Тогда для электрона получаем: $\nu_{0e} = \frac{\omega_{0e}}{2\pi} = \frac{\mu_e H_0}{2\pi\hbar} = 14.0125$ ГГц,

Резонансная частота есть: $\nu_e = 2\nu_{0e} = 28.025$ ГГц

Аналогично для протона:

$$\nu_{0p} = \frac{\omega_{0p}}{2\pi} = \frac{\mu_p H_0}{2\pi\hbar} = 21.29 \text{ МГц},$$

Резонансная частота протона: $\nu_p = 2\nu_{0p} = 42.58$ МГц

Глава 5. Некоторые алгоритмы квантовой информатики

5.1. Сверхплотное кодирование.

Алгоритмы сверхплотного кодирования и телепортации (разд. 5.2) идейно близки между собой.

Сверхплотное кодирование (dense coding) применяют для того, чтобы посредством физического перемещения одного кубита в ЭПР - паре осуществить передачу двух классических битов информации.

Телепортацию (teleportation), наоборот, используют для того, чтобы с помощью двух классических битов информации осуществить передачу произвольного неизвестного квантового состояния одного кубита. В этом случае не происходит перемещение квантового бита в пространстве от передающей к принимающей стороне. Передача неизвестного квантового состояния кубита на расстояние, в силу теоремы о невозможности клонирования, неизбежно сопровождается разрушением квантового состояния исходного кубита.

Рассмотрим алгоритм сверхплотного кодирования. Алиса и Боб стремятся наладить между собой линию связи. Каждый из них получает одну из частиц в ЭПР- паре:

$$\frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$

Допустим, что Алиса получает первую частицу, а Боб – вторую. Пока частицы разделены, Алиса может делать преобразования только над своей частицей (кубитом), а Боб только над своей.

Пусть Алиса хочет передать сообщение из двух бит классической информации. Это эквивалентно передаче целого числа от 0 до 3. В зависимости от этого числа Алиса выполняет над своим кубитом одно из четырех преобразований {I, X, Y, Z}. При этом второй кубит, принадлежащий

Бобу, испытывает тождественное преобразование. Трансформация квантового состояния в зависимости от кодируемого Алисой значения представлена в таблице 5.1.

Таблица 5.1 Двухбитовое кодирование ЭПР состояния Алисой		
Значение	Преобразование	Новое состояние
0	$I \otimes I$	$\frac{1}{\sqrt{2}}(\|00\rangle + \|11\rangle)$
1	$X \otimes I$	$\frac{1}{\sqrt{2}}(\|10\rangle + \|01\rangle)$
2	$Y \otimes I$	$\frac{i}{\sqrt{2}}(\|10\rangle - \|01\rangle)$
3	$Z \otimes I$	$\frac{1}{\sqrt{2}}(\|00\rangle - \|11\rangle)$

Затем Алиса посылает свой кубит Бобу. Боб прикладывает CNOT к системе двух кубитов, которые находятся в запутанном состоянии. После операции CNOT состояние перестает быть запутанным (см. табл.5.2).

Таблица 5.2 Результат действия CNOT при декодировании информации Бобом			
Исходное состояние	CNOT	Первый кубит	Второй кубит
$\frac{1}{\sqrt{2}}(\|00\rangle + \|11\rangle)$	$\frac{1}{\sqrt{2}}(\|00\rangle + \|10\rangle)$	$\frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)$	$\|0\rangle$
$\frac{1}{\sqrt{2}}(\|10\rangle + \|01\rangle)$	$\frac{1}{\sqrt{2}}(\|11\rangle + \|01\rangle)$	$\frac{1}{\sqrt{2}}(\|1\rangle + \|0\rangle)$	$\|1\rangle$
$\frac{i}{\sqrt{2}}(\|10\rangle - \|01\rangle)$	$\frac{i}{\sqrt{2}}(\|11\rangle - \|01\rangle)$	$\frac{i}{\sqrt{2}}(\|1\rangle - \|0\rangle)$	$\|1\rangle$
$\frac{1}{\sqrt{2}}(\|00\rangle - \|11\rangle)$	$\frac{1}{\sqrt{2}}(\|00\rangle - \|10\rangle)$	$\frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)$	$\|0\rangle$

Заметим, что теперь Боб может безбоязненно измерить второй кубит, не нарушая квантового состояния. Если в результате измерения он получит $|0\rangle$, то это значит, что Алиса послала 0 или 3. Если, напротив, он получит $|1\rangle$, то это значит, что Алиса послала 1 или 2.

Далее Боб совершает преобразование Адамара H над первым кубитом (табл.5.3)

Таблица 5.3. Результат действия оператора Адамара на первый кубит

Первый бит	H
$\frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)$	$\frac{1}{2}(\|0\rangle + \|1\rangle + \|0\rangle - \|1\rangle) = \|0\rangle$
$\frac{1}{\sqrt{2}}(\|1\rangle + \|0\rangle)$	$\frac{1}{2}(\|0\rangle - \|1\rangle + \|0\rangle + \|1\rangle) = \|0\rangle$
$\frac{i}{\sqrt{2}}(\|1\rangle - \|0\rangle)$	$\frac{i}{2}(\|0\rangle - \|1\rangle - \|0\rangle - \|1\rangle) = -i\|1\rangle$
$\frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)$	$\frac{1}{2}(\|0\rangle + \|1\rangle - \|0\rangle + \|1\rangle) = \|1\rangle$

Теперь Боб сможет отличить 0 от 3, а также 1 от 2.

Заметим, что для реализации протокола сверхплотного кодирования принципиально важным является наличие ресурса запутанности. Другими словами, для того, чтобы Алиса смогла закодировать в свой кубит два бита классической информации, необходимо, чтобы ее кубит был изначально запутан с кубитом, имеющимся у Боба. Поскольку кубит, изначально имевшийся у Боба, не использовался для передачи информации, то, очевидно, суммарно мы получаем передачу двух битов классической информации посредством двух кубитов.

Задача 5.1 Пусть исходное двухкубитовое состояние является незапутанным. Покажите, что рассмотренный выше протокол кодирования не сможет привести к передаче более чем одного бита классической информации (тем самым, Вы обоснуете принципиально важную роль ресурса запутанности в рассматриваемом протоколе).

Задача 5.2 Нарисуйте квантовую цепь, соответствующую рассмотренному выше протоколу сверхплотного кодирования.

5.2. Телепортация

Цель телепортации заключается в том, чтобы передать на расстояние квантовое состояние частицы, используя классические биты и реконструируя точно квантовое состояние в приемнике.

Поскольку квантовое состояние не может быть клонировано, квантовое состояние исходной частицы обязательно будет разрушено.

Рассмотрим алгоритм квантовой телепортации с использованием ЭПР – пар.

Пусть Алиса хочет переслать неизвестное состояние кубита Бобу

$$\phi = a\left|0\right\rangle + b\left|1\right\rangle$$

Алиса и Боб имеют также по одному кубиту из ЭПР – пары:

$$\frac{1}{\sqrt{2}}\left(\left|00\right\rangle + \left|11\right\rangle\right)$$

Стартовое состояние есть:

$$\left(a\left|0\right\rangle + b\left|1\right\rangle\right) \otimes \frac{1}{\sqrt{2}}\left(\left|00\right\rangle + \left|11\right\rangle\right) =$$

$$= \frac{1}{\sqrt{2}}\left(a\left|000\right\rangle + a\left|011\right\rangle + b\left|100\right\rangle + b\left|111\right\rangle\right)$$

В этом состоянии Алиса может управлять первыми двумя кубитами, а Боб – третьим.

Пусть теперь Алиса прикладывает CNOT к своим кубитам, а затем преобразование Адамара H к первому кубиту.

После действия CNOT на первые два кубита имеем:

$$\frac{1}{\sqrt{2}}\left(a|000\rangle + a|011\rangle + b|110\rangle + b|101\rangle\right)$$

После приложения оператора Адамара H к первому кубиту получим следующее состояние:

$$\frac{1}{2}\left(a|000\rangle + a|100\rangle + a|011\rangle + a|111\rangle + b|010\rangle - b|110\rangle + b|001\rangle - b|101\rangle\right) =$$

$$\frac{1}{2}\left(|00\rangle\left(a|0\rangle + b|1\rangle\right) + |01\rangle\left(a|1\rangle + b|0\rangle\right) + |10\rangle\left(a|0\rangle - b|1\rangle\right) + |11\rangle\left(a|1\rangle - b|0\rangle\right)\right)$$

Теперь Алиса измеряет свои два кубита (разрушая квантовое состояние исходной частицы). Она получает при этом один из возможных результатов измерения: $|00\rangle$ $|01\rangle$ $|10\rangle$ $|11\rangle$. Именно эту информацию она и посылает Бобу. Для декодирования Бобу остается проделать соответственно всего одну из операций: I, X, Z, iY

Задача 5.3 Нарисуйте квантовую цепь, соответствующую рассмотренному выше протоколу телепортации.

5.3. Квантовый параллелизм. Алгоритмы Дойча и Дойча- Джозса.

Пусть функция $f(x)$ имеет однобитовую область определения и однобитовое множество значений. Нетрудно видеть, что таких функций всего четыре. Две из них постоянны:

1. $f(0)=0$, $f(1)=0$, 2. $f(0)=1$, $f(1)=1$

Две другие функции переменны:

3. $f(0)=0$, $f(1)=1$, 4. $f(0)=1$, $f(1)=0$

Квантовая реализация функции $f(x)$ состоит в том, что двухкубитовое состояние $|x,y\rangle$ преобразуется в состояние $|x,y\oplus f(x)\rangle$, т.е.

$$|x,y\rangle \xrightarrow{f} |x,y\oplus f(x)\rangle$$

Здесь символ $\oplus$ означает сложение по модулю 2.

В частности, если во втором кубите исходно записан ноль ($|y\rangle = |0\rangle$), то функция $f(x)$ задает следующее преобразование:

$$|x,0\rangle \xrightarrow{f} |x,f(x)\rangle$$

Графическое представление для квантового вычисления функции $f(x)$ показано на рисунке.

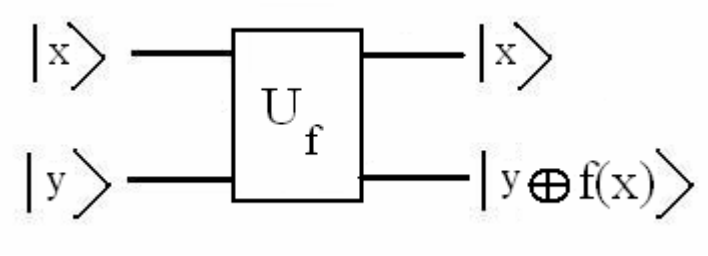

Рис.5.1 Схема квантового вычисления функции $f(x)$

Рассмотрим для примера четвертую из представленных выше функций: $f(0)=1$, $f(1)=0$. Нетрудно видеть, что рассматриваемая функция задает следующее преобразование:

$$|0,0\rangle \to |0,0\oplus f(0)\rangle = |0,1\rangle$$

$$|0,1\rangle \to |0,1\oplus f(0)\rangle = |0,1\oplus 1\rangle = |0,0\rangle$$

$$|1,0\rangle \to |1,0 \oplus f(1)\rangle = |1,0\rangle$$

$$|1,1\rangle \to |1,1 \oplus f(1)\rangle = |1,1\rangle$$

Задача 5.4 Покажите, что введенное определение квантовой реализации функции задает унитарное преобразование входного состояния в выходное. Найдите соответствующие унитарные матрицы для каждой из четырех представленных выше функций.

Принцип суперпозиции позволяет подавать на вход схемы квантового вычисления функций не только определенное базисное состояние $|x\rangle$, но и произвольную суперпозицию таких состояний. Эта возможность обеспечивает так называемый квантовый параллелизм, которой означает, что (в определенном смысле) квантовый алгоритм позволяет вычислять функцию $f(x)$ для многих значений аргумента $|x\rangle$ одновременно. Квантовый параллелизм, таким образом, обеспечивает принципиально важное преимущество квантовых схем вычислений над классическими. Заметим, в то же время, что результаты квантовых параллельных вычислений не могут быть непосредственно экстрагированы из квантовой системы из-за неизбежной редукции квантового состояния при измерениях.

Задача 5.5 Докажите справедливость результата, представленного на следующем рисунке.

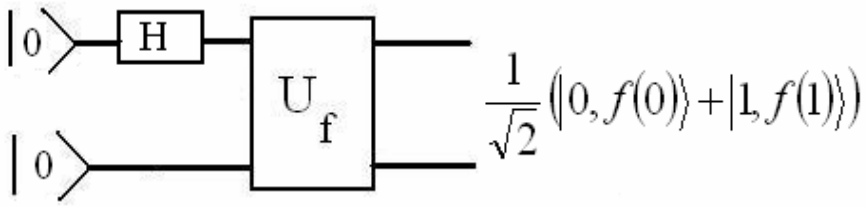

Рис. 5.2 Демонстрация квантового параллелизма для функции с однокубитовой областью определения.

Результаты, полученные в задаче, являются простейшей демонстрацией свойства квантового параллелизма. Благодаря действию элемента Адамара H на первый кубит, на вход вычислителя функции U_f поступает суперпозиция состояний $\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$. В итоге, выходное состояние системы представляет собой суперпозицию результатов вычислений при значениях аргумента $x=0$ и $x=1$.

Представленный результат может быть обобщен на вычисление функции $f(x)$ с n- битовой областью определения и 1- битовым множеством значений. Квантовая реализация функции $f(x)$ в этом случае определяется тем же преобразованием $|x,y\rangle \xrightarrow{f} |x, y\oplus f(x)\rangle$, где символ $\oplus$ означает сложение по модулю 2, но теперь $|x\rangle$- не один кубит, а n- кубитовый регистр данных.

Задача 5.6 Докажите справедливость результата, представленного на рисунке.

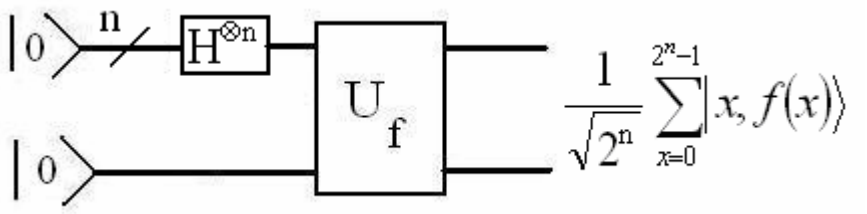

Рис.5.3 Демонстрация квантового параллелизма для функции с n-кубитовой областью определения.

Указание к задаче: воспользуйтесь результатами задачи 4.10.

Здесь обозначение 

символизирует n- кубитовый провод (регистр запроса). Каждый кубит рассматриваемого провода подвергается преобразованию Адамара H, что обеспечивается тензорным произведением $H^{\otimes n}$. Область определения функции $f(x)$ задана 2^n базисными состояниями $|x\rangle = |0\rangle, |1\rangle, \ldots, |2^n - 1\rangle$. Множество значений функции $f(x)$ определяется всего двумя состояниями $|0\rangle$ и $|1\rangle$. Квантовый параллелизм обеспечивает одновременное вычисление функции в 2^n точках от $x = 0$ до $x = 2^n - 1$.

Алгоритм Дойча описывается квантовой схемой, приведенной на рисунке.

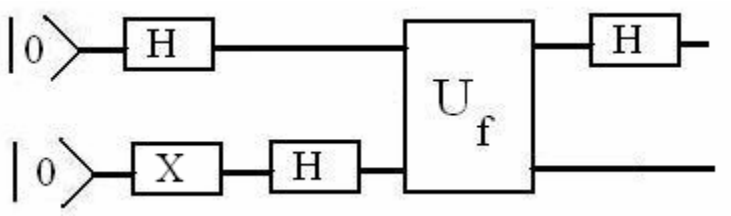

Рис.5.4 Квантовая схема для алгоритма Дойча

Задача 5.7 Покажите, что состояние на выходе схемы Дойча есть:

$$\psi_{out} = \pm|0\rangle \frac{(|0\rangle - |1\rangle)}{\sqrt{2}},$$

когда функция постоянна, т.е. $f(0) = f(1)$

$$\psi_{out} = \pm|1\rangle \frac{(|0\rangle - |1\rangle)}{\sqrt{2}},$$

когда функция переменна, т.е. $f(0) \neq f(1)$

Указание к задаче: покажите, что действие оператора U_f на состояние $|x\rangle \frac{(|0\rangle - |1\rangle)}{\sqrt{2}}$ приводит к состоянию $(-1)^{f(x)}|x\rangle \frac{(|0\rangle - |1\rangle)}{\sqrt{2}}$

Произведем измерение первого кубита выходного состояния ψ_{out}, полученного в представленной выше задаче. В результате измерения с достоверностью получится $|0\rangle$, если функция постоянна и $|1\rangle$, если функция переменна. Полученный результат весьма поучителен: посредством одного-единственного вычисления мы смогли идентифицировать определенное глобальное свойство функции (ее постоянство или переменность). При классическом рассмотрении задачи нам, очевидно, потребовалось бы два вычисления для решения той же самой задачи.

Заметим, что схема Дойча не ставит цели восстановить неизвестную функцию целиком: она ориентирована только на идентификацию рассматриваемого глобального свойства неизвестной функции.

Можно констатировать, что в алгоритме Дойча двухбитовая неопределенность, соответствующая четырем возможным функциям f, снижается до однобитовой неопределенности, соответствующей только двум возможным функциям f. Измерение на выходе схемы Дойча позволяет отличить пару функций (1,2) от пары (3,4). Очевидно, что для того, чтобы отличить пару (1,3) от пары (2,4), достаточно измерить $f(0)$. Аналогично, что для того, чтобы отличить пару (1,4) от пары (2,3), достаточно измерить

$f(1)$. Два последних алгоритма аналогичны в классическом и квантовом случае. Возникает резонный вопрос: почему нет аналога алгоритму Дойча в классической теории информации? Дело в том, что в действительности нет двух раздельных теорий информации (классической и квантовой). Существует только одна последовательная теория информации- это квантовая информатика. Классическая теория информации- есть «урезанная» версия квантовой (в классической теории бит может находиться только в состояниях $|0\rangle$ или $|1\rangle$, но не их суперпозиции). Такое «урезание», как мы видим уже на примере алгоритма Дойча, делает теорию логически менее привлекательной, менее последовательной и фактически неполной. Напомним, что точно в таком же отношении друг к другу находятся классическая и квантовая теории вероятностей. Это неслучайно: ведь любое количественное определение информации (например, определение Шеннона) базируется на статистических соображениях.

Оказывается, что задача Дойча допускает простое обобщение на многокубитовый случай. Рассмотрим функцию $f(x)$ с n- битовой областью определения и 1- битовым множеством значений. Теперь переменная x может принимать N различных значений $x=0,1,...,N-1$, где $N=2^n$. Предположим, что нам заранее известно, что функция $f(x)$ может быть только одного из двух типов: постоянная функция или так называемая сбалансированная функция. Для постоянной функции $f(0)=f(1)=...=f(N-1)$. Если функция сбалансирована, то $f(x)=0$ для некоторых x и $f(x)=1$ для остальных значений аргумента, причем значения $f(x)=0$ и $f(x)=1$ встречаются одинаково часто (в этом и

заключается сбалансированность). Пусть, например, имеется функция $f(x)$ с 10-ти битовой областью определения. Тогда для некоторых 512 значений x получим $f(x)=0$, а для остальных 512 значений x получим $f(x)=1$. Задача Дойча- Джозса состоит в том, чтобы отличить постоянную функцию от сбалансированной.

Алгоритм Дойча- Джозса является непосредственным обобщением алгоритма Дойча на случай многокубитовых систем. Он описывается следующей квантовой схемой, приведенной на рисунке.

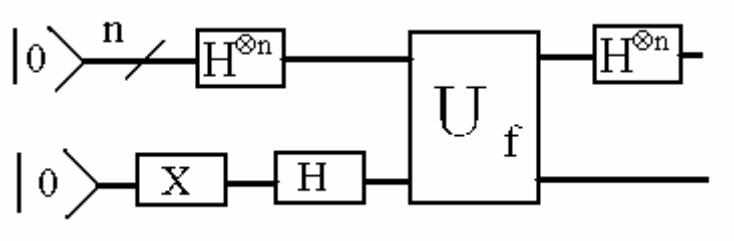

Рис. 5.5 Квантовая схема алгоритма Дойча- Джозса

Задача 5.8 Покажите, что на вход вычислителя U_f в схеме Дойча-Джозса поступает состояние $\sum_{x=0}^{2^n-1}\frac{|x\rangle}{\sqrt{2^n}}\frac{\left(|0\rangle-|1\rangle\right)}{\sqrt{2}}$.

Задача 5.9 Покажите, что на выходе вычислителя U_f в схеме Дойча-Джозса возникает состояние

$$\sum_{x=0}^{2^n-1}\frac{(-1)^{f(x)}|x\rangle}{\sqrt{2^n}}\frac{\left(|0\rangle-|1\rangle\right)}{\sqrt{2}}$$

Задача 5.10 Убедитесь, что действие оператора Адамара H на базисные состояния $|x\rangle = |0\rangle, |1\rangle$ отдельного кубита описывается формулой: $H|x\rangle = \sum_{z=0}^{1} (-1)^{xz} \frac{|z\rangle}{\sqrt{2}}$. Покажите, что непосредственно из указанной формулы следует ее n- кубитовое обобщение: действие оператора Уолша- Адамара $H^{\otimes n}$ на базисные состояния n- кубитового регистра $|x\rangle = |0\rangle, |1\rangle, ..., |2^n - 1\rangle$ описывается формулой:

$$H^{\otimes n}|x\rangle = \sum_{z=0}^{2^n-1} (-1)^{xz} \frac{|z\rangle}{\sqrt{2^n}}.$$

Здесь $x = (x_1, x_2, ..., x_n)$ и $z = (z_1, z_2, ..., z_n)$ - запись номеров состояний в двоичном представлении, x и z представляют собой n- компонентные строки из нолей и единиц, $xz = x_1 z_1 + x_2 z_2 + ... + x_n z_n$ - скалярное произведение соответствующих строк.

Непосредственно из результатов представленных выше задач следует, что на выходе схемы Уолша- Адамара возникает следующее $n+1$- кубитовое состояние:

$$|\psi_{out}\rangle = \sum_{z=0}^{2^n-1} \sum_{x=0}^{2^n-1} (-1)^{xz+f(x)} \frac{|z\rangle}{2^n} \frac{(|0\rangle - |1\rangle)}{\sqrt{2}}$$

Проведем теперь измерение первых n кубитов (регистра запроса). Амплитуда вероятности найти регистр запроса в состоянии $|z=0\rangle = \left|\underbrace{0,0,...,0}_{n}\right\rangle = |0\rangle^{\otimes n}$, очевидно, есть:

$$M_{\underbrace{0,0,...,0}_{n}} = \sum_{x=0}^{2^n-1} \frac{(-1)^{f(x)}}{2^n}.$$

Пусть функция $f(x)$ постоянна, т.е. $f(0)=f(1)=...=f\left(2^n-1\right)$. В этом случае все 2^n слагаемых в рассматриваемой сумме одинаковы (происходит их конструктивная интерференция), в итоге суммарная амплитуда вероятности оказывается равной $+1$ или -1, а соответствующая вероятность равной единице. Таким образом, если неизвестная функция $f(x)$ постоянна, то все n кубитов регистра запроса с достоверностью оказываются в состоянии $|0\rangle$.

Пусть теперь неизвестная функция $f(x)$ переменна и сбалансирована. Сбалансированность означает, что для половины из 2^n возможных значений аргумента x функция равна нулю ($f(x)=0$), а для другой половины возможных значений аргумента x - единице ($f(x)=1$). В этом случае в сумме $M_{\underbrace{0,0,...,0}_{n}} = \sum_{x=0}^{2^n-1} \frac{(-1)^{f(x)}}{2^n}$ положительные и отрицательные слагаемые полностью скомпенсируют друг друга (деструктивная интерференция). Теперь суммарная амплитуда и соответствующая вероятность окажутся равными нулю. Таким образом, если неизвестная функция $f(x)$

сбалансирована, то регистр запроса никогда не будет обнаружен в состоянии $\left|\underbrace{0,0,...,0}_{n}\right\rangle$. Другими словами, хотя бы один из n кубитов регистра запроса окажется при измерении в состоянии $|1\rangle$.

Мы видим, что алгоритм Дойча- Джозса позволяет с достоверностью отличить постоянную функцию от сбалансированной посредством одного-единственного обращения к вычислителю U_f.

Задача 5.11 Покажите, что при классическом рассмотрении задачи Дойча-Джозса для того, чтобы с достоверностью отличить постоянную функцию от сбалансированной может потребоваться до $2^{n-1}+1$ обращений к устройству, производящему вычисление функции $f(x)$.

Результат представленной задачи показывает, что алгоритм Дойча-Джозса обеспечивает квантовому компьютеру экспоненциальное преимущество в скорости по сравнению с классическим компьютером.

Это преимущество, однако, имеет место только для идеальной задачи абсолютно безошибочной классификации. В реальных задачах нам, как правило, достаточно ограничиться правдоподобным ответом, который является правильным лишь с вероятностью, очень близкой к единице. Кроме того, получать абсолютно достоверные ответы на вопросы при помощи вычислений невозможно и по чисто техническим причинам, поскольку преобразование данных в компьютере (классическом или квантовом) неизбежно сталкивается с возможными технологическими ошибками, шумами и сбоями. Если же мы ограничиваемся правдоподобными (с вероятностью, близкой к единице) ответами, то в задаче Дойча- Джозса пропадает

экспоненциальное преимущество квантового алгоритма по сравнению с классическим вероятностным алгоритмом. Последний заключается в том, что на вход классического вычислителя функции $f(x)$ подается последовательность случайных чисел $x_1, x_2, \ldots, x_m$ объема m и по результатам $f(x_1), f(x_2), \ldots, f(x_m)$ вырабатывается правдоподобный ответ на вопрос о виде функции (постоянная она или сбалансированная).

Задача 5.12 Пусть задача Дойча- Джозса решается на классическом вероятностном компьютере, причем допускается некоторая малая вероятность ε ошибки (когда сбалансированная функция принимается за постоянную). Какой объем m последовательности случайных чисел следует взять?

Алгоритм Дойча- Джозса относится к так называемым квантовым вычислениям с оракулом (прорицателем). Роль оракула здесь играет вычислительное устройство U_f. Фактически это устройство представляет собой черный ящик, содержание которого неизвестно и несущественно в данной задаче. Все что мы знаем- это то, что оракул обеспечивает выполнение унитарного преобразования U_f, где f - постоянная или сбалансированная функция. Любое устройство U_f - это, конечно, некоторый квантовый код (алгоритм), который обеспечивает выполнение заданного преобразования. Мы можем считать, что синтаксически рассматриваемый код настолько сложен, что мы не в состоянии понять какую функцию он вычисляет (постоянную или сбалансированную). Не имея возможности понять код, мы используем его как черный ящик в квантовой схеме, при этом вопрос о постоянстве или сбалансированности неизвестной функции f решается экспериментально посредством алгоритма Дойча – Джозса. Заметим, однако, что такая постановка задачи несколько искусственна.

Главное значение алгоритмов Дойча и Дойча- Джозса методическое: они раскрывают сущность квантового параллелизма и демонстрируют возможности квантовых вычислений.

5.4. Квантовое преобразование Фурье.

Пусть имеется система из n кубитов. Ее состояние представляет собой вектор в гильбертовом пространстве размерности $N=2^n$. Базисные состояния квантовой системы есть $|j\rangle$, где $j=0,1,...,N-1$

Квантовое преобразование Фурье задается следующим унитарным преобразованием базисных состояний:

$$|j\rangle \underset{QFT}{\longrightarrow} \frac{1}{\sqrt{N}}\sum_{k=0}^{N-1}\exp\left(\frac{i2\pi jk}{N}\right)|k\rangle$$

Преобразование Фурье базисных функций определяет соответствующее преобразование вектора состояния

$$|\psi\rangle=\sum_{j=0}^{N-1}c_j|j\rangle \underset{QFT}{\longrightarrow} \frac{1}{\sqrt{N}}\sum_{k=0}^{N-1}\sum_{j=0}^{N-1}\exp\left(\frac{i2\pi jk}{N}\right)c_j|k\rangle=\sum_{k=0}^{N-1}\widetilde{c}_k|k\rangle$$

Здесь

$$\widetilde{c}_k=\frac{1}{\sqrt{N}}\sum_{j=0}^{N-1}\exp\left(\frac{i2\pi jk}{N}\right)c_j$$

Последняя формула представляет собой преобразование Фурье комплексных амплитуд вероятности. Результат в точности соответствует так называемому классическому дискретному преобразованию Фурье,

примененному к столбцу комплексных чисел c_j, где $j = 0,1,...,N-1$ (см. например [70]).

Обратное преобразование Фурье для амплитуд вероятности есть

$$c_j = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \exp\left(-\frac{i2\pi jk}{N}\right) \tilde{c}_k$$

Квантовое преобразование Фурье принципиально отличается от аналогичного дискретного преобразования Фурье классического сигнала (несмотря на тождество соответствующих формул). Дело в том, что в квантовой информатике мы имеем дело со специфическим «сигналом», который образован амплитудами вероятности (а не электрическими или механическими напряжениями как в классическом случае). В отличии от классического сигнала, квантовый «сигнал» нельзя измерить никаким «осциллографом» (при измерении квантовое состояние редуцируется в одно из базисных состояний). В то же время, в квантовой информатике мы можем оперировать векторами данных экспоненциально большой размерности (например при $N = 2^{1000}$).

Для простоты изложения остановимся более подробно на трехкубитовом преобразовании Фурье ($n = 3$, $N = 2^3 = 8$).

Например, базисное состояние $j = 5$ будет претерпевать следующее изменение

$$|5\rangle \xrightarrow[QFT]{} \frac{1}{\sqrt{8}}\left(|0\rangle + \exp\left(\frac{i10\pi}{8}\right)|1\rangle + ... + \exp\left(\frac{i70\pi}{8}\right)|7\rangle\right) =$$

$$= \frac{1}{\sqrt{8}}\left(|0\rangle + \exp\left(\frac{i5\pi}{4}\right)|1\rangle + \exp\left(\frac{i\pi}{2}\right)|2\rangle + \exp\left(\frac{i7\pi}{4}\right)|3\rangle + \right.$$

$$\left. + \exp(i\pi)|4\rangle + \exp\left(\frac{i\pi}{4}\right)|5\rangle + \exp\left(\frac{i3\pi}{2}\right)|6\rangle + \exp\left(\frac{i3\pi}{4}\right)|7\rangle\right)$$

Квантовое преобразование Фурье может быть построено на основе элементов Адамара и контролируемого преобразования фазы.

Пусть R_k - следующее однокубитовое преобразование фазы:

$$R_k = \begin{pmatrix} 1 & 0 \\ 0 & \exp\left(i\frac{2\pi}{2^k}\right) \end{pmatrix}$$

На рисунке 5.6 изображен двухкубитовый элемент, осуществляющий контролируемое фазовое преобразование. Управляемый кубит (нижний) подвергается преобразованию R_k, если управляющий кубит (верхний) находится в состоянии $|1\rangle$

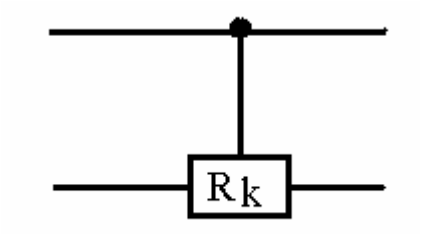

Рис. 5.6 Двухкубитовый элемент, осуществляющий управляемое фазовое преобразование.

На рисунке 5.7 представлена квантовая цепь, обеспечивающая трехкубитовое преобразование Фурье

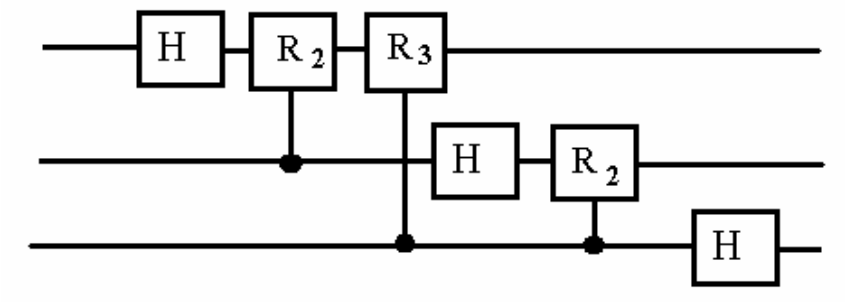

Рис. 5.7 Квантовая цепь для трехкубитового преобразования Фурье

Задача 5.13 Пусть на вход трехкубитовой квантовой схемы, изображенной на представленном выше рисунке, подается состояние $\left|\psi_{in}\right\rangle = \left|5\right\rangle$. Покажите, что на выходе квантовой схемы будет состояние:

$$\left|\psi_{out}\right\rangle = \frac{1}{\sqrt{8}}\left(\left|000\right\rangle + \exp\left(\frac{i5\pi}{4}\right)\left|100\right\rangle + \exp\left(\frac{i\pi}{2}\right)\left|010\right\rangle + \exp\left(\frac{i7\pi}{4}\right)\left|110\right\rangle + \right.$$
$$\left. + \exp(i\pi)\left|001\right\rangle + \exp\left(\frac{i\pi}{4}\right)\left|101\right\rangle + \exp\left(\frac{i3\pi}{2}\right)\left|011\right\rangle + \exp\left(\frac{i3\pi}{4}\right)\left|111\right\rangle\right)$$

Решите ту же задачу для других входных состояний $\left|j\right\rangle \quad j = 0,1,...,7$.

Решение задачи свидетельствует о том, что квантовая схема на рисунке действительно дает трехкубитовое преобразование Фурье с одной существенной оговоркой. Легко видеть, что для того, чтобы результат был правильный, на выходе схемы порядок следования кубитов должен быть обращен. Другими словами, двоичное представление состояний на выходе следует читать не слева направо, а справа налево: например $\left|100\right\rangle$ означает состояние $\left|1\right\rangle$ и т.д.

Конечно, на выходе схемы можно ввести дополнительные операции обмена состояниями кубитов, но с практической точки зрения это нецелесообразно (лучше договориться об инверсии порядка нумерации кубитов).

Представленная выше трехкубитовая схема допускает простое обобщение на произвольное число кубитов.

Общий алгоритм квантового преобразования Фурье может быть реализован с помощью схемы, изображенной на рисунке.

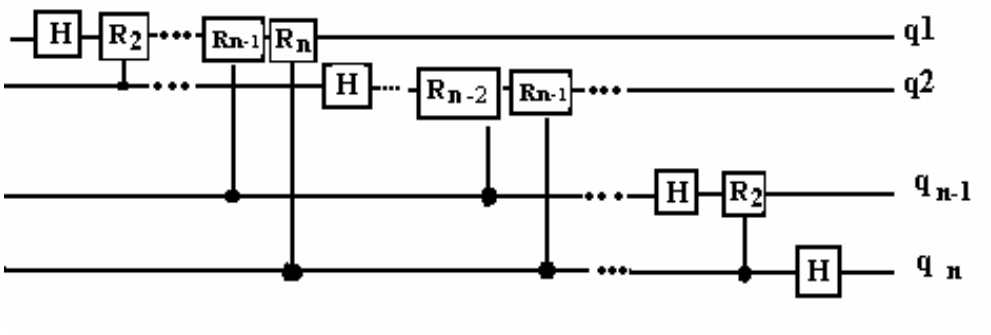

Рис. 5.8 Квантовая цепь для n - кубитового преобразования Фурье

Подсчитаем число операций, необходимых для осуществления квантового преобразования Фурье. Из схемы видно, что с первым (верхним) кубитом можно связать n преобразований (преобразование Адамара и $n-1$ фазовое преобразование), аналогично со вторым (сверху) кубитом можно связать $n-1$ преобразование и т.д. Полное число преобразований, равное сумме арифметической прогрессии, есть $\frac{(n+1)n}{2}$. Таким образом, число операций, необходимых для осуществления квантового преобразования Фурье, есть величина порядка $O(n^2) \sim O((\log N)^2)$. Отметим, что самые быстрые классические алгоритмы выполняют преобразование Фурье за порядка $O(N(\log N))$ операций (так называемое быстрое преобразование Фурье). Таким образом, квантовый алгоритм имеет экспоненциальное преимущество по сравнению со своим классическим аналогом.

Пример. Пусть имеется 1000- кубитовое состояние ($n=1000$). Ему отвечает вектор состояния, описывающийся $N=2^n=1{,}07\cdot 10^{301}$ комплексными числами. Для осуществления классического быстрого преобразования потребуется проделать порядка $N\log_2 N=1{,}07\cdot 10^{304}$

операций. В то же время, квантовое преобразование над рассматриваемым вектором осуществляется примерно за $(\log_2 N)^2 = 1 \cdot 10^6$ операций.

Таким образом, экспоненциальное преимущество квантового алгоритма по сравнению с классическим позволит на квантовом компьютере ставить и решать задачи, которые никогда не будут решены на классическом компьютере.

5.5. Нахождение периода функции

Задача определения периода функции является важным примером применения квантового преобразования Фурье.

Предположим, что имеется периодическая функция $f(x)$ с периодом T. Это означает, что для всех x выполняется тождество:

$$f(x+T) = f(x)$$

В последней формуле под операцией сложения подразумевается сложение по модулю N. Предположим дополнительно, что все значения функции $f(x)$ на одном периоде различны. Очевидно, что функция может быть в точности периодической только в том случае, когда N делится на T без остатка, т.е. если $M = N/T$ - целое число.

В качестве начального состояния возьмем следующую однородную суперпозицию (квантовая схема для получения такого состояния представлена в задаче 5.3.3):

$$|\psi_{in}\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x, f(x)\rangle$$

Проведем измерение второго регистра (регистра функции). Предположим, что при этом мы получим некоторое значение функции f_0. Пусть x_0 - одно из значений аргумента, при котором $f(x_0)=f_0$. В результате редукции вектора состояния в суперпозиции «выживут» только слагаемые, отвечающие $x=x_0+mT$, где $m=0,1,..,M-1$, поскольку только для них $f(x_0+mT)=f_0$. В результате первый регистр (отвечающий аргументу x) перейдет в следующее квантовое состояние:

$$|\psi\rangle=\frac{1}{\sqrt{M}}\sum_{m=0}^{M-1}|x_0+mT\rangle$$

Выполним теперь квантовое преобразование Фурье над полученным состоянием. Согласно определению, каждое отдельно взятое базисное состояние будет подвергнуто следующему преобразованию:

$$|x_0+mT\rangle \xrightarrow[QFT]{} \frac{1}{\sqrt{N}}\sum_{k=0}^{N-1}\exp\left(\frac{i2\pi k(x_0+mT)}{N}\right)|k\rangle$$

Суперпозиция, представляющая состояние $|\psi\rangle$, в результате квантового преобразования Фурье примет вид:

$$|\psi_{out}\rangle=\frac{1}{\sqrt{NM}}\sum_{k=0}^{N-1}\sum_{m=0}^{M-1}\exp\left(\frac{i2\pi k(x_0+mT)}{N}\right)|k\rangle$$

Задача 5.14 Пусть $F(k)=\sum_{m=0}^{M-1}\exp\left(\frac{i2\pi km}{M}\right)$, где $k=0,1,...,N-1$ и $N=MT$. Покажите, что $F(k)=M$, если $k=j\frac{N}{T}=jM$, где $j=0,1,...,T-1$ и $F(k)=0$ при всех остальных значениях k.

Результаты представленной выше задачи показывают, что выходное состояние регистра может быть записано в виде:

$$\left|\psi_{out}\right\rangle = \frac{1}{\sqrt{T}}\sum_{j=0}^{T-1}\exp\left(\frac{i2\pi x_0 j}{T}\right)\left|j\frac{N}{T}\right\rangle$$

Последний шаг процедуры – это измерение полученного состояния. Мы видим, что с равной вероятностью возможно любое из T состояний $\left|j\frac{N}{T}\right\rangle$, где $j = 0,1,...,T-1$.

Пусть Природа «выбрала» некоторое j_0 и в результате измерения возникло состояние $\left|l_0\right\rangle = \left|j_0\frac{N}{T}\right\rangle$. Тогда, имеем следующее тождество для четырех целых чисел:

$$\frac{j_0}{T} = \frac{l_0}{N}$$

Здесь l_0 и N доступные исследователю числа, в то время как j_0 и T - числа, неизвестные ему. Наша цель- определить T. Полученное тождество показывает, что исследователь не может гарантированно определить T при однократном выполнении процедуры. Чтобы его поиски оказались продуктивны, ему следует уповать на то, что «выбранное» Природой число j_0 и период T окажутся взаимно простыми (т.е. не будут иметь общих делителей, кроме единицы). Тогда, приведя дробь l_0 / N к несократимой, он сможет восстановить j_0 и T. В этом случае нам удастся с помощью одного уравнения (7) найти два неизвестных целых числа. Если же исследователю не

повезет и Природа «выберет» такое j_0, что дробь j_0/T окажется сократимой, то вместо истинного периода T он получит меньшее значение.

Приведем пример. Пусть $N=2^{10}=1024$ - заранее известное число. $T=64$ - период, неизвестный исследователю. Природа может «выбрать» любое j_0 от 0 до 63. Пусть, например, она «выбрала» $j_0=21$. Тогда исследователь получит $l_0=j_0\frac{N}{T}=336$. Сократив дробь $\frac{336}{1024}$ до $\frac{21}{64}$, исследователь правильно определит, что $j_0=21$ и $T=64$. Пусть теперь, Природа «выбрала» $j_0=12$. Этот выбор неудачен для исследователя, поскольку числа 12 и 64 имеют общий делитель, равный 4. Теперь $l_0=j_0\frac{N}{T}=192$. Сократив дробь $\frac{192}{1024}$ до $\frac{3}{16}$, исследователь может сделать неправильный вывод, будто бы $j_0=3$ и $T=16$. Для того, чтобы с высокой вероятностью получить правильный ответ, исследователь будет вынужден повторять описанную процедуру многократно. Тогда, очевидно, в качестве ответа ему следует взять период, отвечающий наибольшему из возможных значений (максимальный знаменатель в дроби l_0/N после ее сокращения).

Оценим, сколько раз исследователь должен проделать описанную выше процедуру, чтобы определить неизвестный период T с высокой гарантией. Для этого нужно оценить вероятность того, что «выбранное» Природой число j_0 окажется взаимно простым с T. Известно, что при больших T количество простых чисел, не превышающих T можно оценить как $T/\log T$. Отсюда следует, что вероятность удачи при отдельном испытании больше или порядка $1/\log T \geq 1/\log N$. Таким образом, если исследователь

повторит процедуру $O(\log N)$ раз, то с высокой гарантией, он сможет найти неизвестный период. Например, если $N = 2^{1000}$, то потребуется всего порядка 1000 испытаний (в оценках такого рода мы не делаем различия между натуральным и двоичным логарифмами).

Резюмируем полученный результат. Квантовый алгоритм нахождения периода функций требует всего $O\left((\log N)^3\right)$ операций (для квантового преобразования Фурье требуется $O\left((\log N)^2\right)$ операций и $O(\log N)$ операций требуется для описанной выше процедуры угадывания). Рассматриваемый алгоритм является полиномиальным по числу кубитов и, соответственно, по количеству знаков в числе N (поскольку число шагов алгоритма определяется полиномом третьей степени).

Для экспоненциально больших N полиномиальный квантовый алгоритм обладает радикальным преимуществом по сравнению с любыми известными классическими алгоритмами. Важный пример использования отмеченного преимущества рассмотрен в следующем разделе.

5.6 Факторизация чисел

Алгоритм нахождения периода функции, рассмотренный выше, может быть с успехом применен для разложения заданного целого числа на множители. Эта задача решается с помощью алгоритма, придуманного П. Шором в 1994 г.

В настоящее время алгоритм Шора- самый знаменитый из известных квантовых алгоритмов. Он позволяет за $O\left((\log N)^3\right)$ шагов осуществить разложение целого числа N на множители и, таким образом, является

алгоритмом полиномиальной сложности. Заметим, что аналогичный классический полиномиальный алгоритм неизвестен.

Пусть N - целое нечетное число (при четном N имеем тривиальное решение задачи). Нам требуется разложить данное число на простые множители или показать, что оно простое.

Выберем случайно число $a < N$. Вычислим наибольший общий делитель (НОД) чисел a и N (это можно сделать с помощью алгоритма Евклида, который изложен в конце настоящего раздела).

Если НОД чисел a и N оказался большим, чем единица, то задача решена.

Предположим, что НОД чисел a и N равен единице. Тогда, согласно известной в теории чисел теореме Эйлера, существует такое r, что:

$$a^r = 1 \bmod N$$

Выберем минимальное r, удовлетворяющее указанному тождеству. Оно называется порядком числа a по модулю N.

Рассмотрим теперь функцию

$$f(x) = a^x \bmod N$$

Заметим, что утверждение о том, что r есть порядок числа a по модулю N и утверждение о том, что функция $f(x)$ периодична с периодом r, эквивалентны.

Таким образом, задача о вычислении порядка сводится к задаче о нахождения периода функции (для чего можно применить алгоритм раздела 5.5).

Сделаем одно замечание. Чтобы применить алгоритм из разд. 5.5., следует ограничить область определения функции $f(x)$ некоторым конечным интервалом $0 \le x < x_0$. Алгоритм из раздела 5.5 предполагает, что x_0 делится на r без остатка. Заметим, что это предположение несущественно, если только x_0 выбрать достаточно большим так, чтобы на нем укладывалось большое число периодов функции $f(x)$.

Предположим, что найденное r - четное, тогда (1) можно переписать в виде:

$$\left(a^{r/2}-1\right)\left(a^{r/2}+1\right)=0 \bmod N$$

Это означает, что число $\left(a^{r/2}-1\right)\left(a^{r/2}+1\right)$ должно делиться на N без остатка.

Предположим дополнительно, что каждое из чисел $\left(a^{r/2}\pm 1\right)$ не делится на N без остатка. Тогда у каждого из этих чисел есть общие делители с числом N.

Находя соответствующие наибольшие общие делители числа N с числами $\left(a^{r/2}-1\right)$ и $\left(a^{r/2}+1\right)$, мы решаем поставленную задачу.

Мы видим, что изложенный метод срабатывает не всегда. Чтобы метод сработал, нам нужно, чтобы r было четным и, одновременно, числа $\left(a^{r/2}\pm 1\right)$ не делились на N без остатка. Можно показать, что это происходит с вероятностью ≥ 0.5, если только a выбирается случайно.

Такой вероятности достаточно, чтобы путем повторения добиться гарантированно успеха.

Приведем пример. Пусть $N=85,\ a=7$

Прямым вычислением получаем (по модулю 85): $7^1=7,\ 7^2=49,$ $7^3=3,\ 7^4=21,\ 7^5=62,\ 7^6=9,\ 7^7=63,\ 7^8=16,\ 7^9=27,\ 7^{10}=19,$ $7^{11}=48,\ 7^{12}=81,\ 7^{13}=57,\ 7^{14}=59,\ 7^{15}=73,\ 7^{16}=1,\ 7^{17}=7$ и т.д.

Таким образом $r=16$

Далее:

$\left(a^{r/2}-1\right)=\left(7^8-1\right)=5764800 \quad \left(a^{r/2}+1\right)=\left(7^8+1\right)=5764802$

Вычислим теперь необходимые наибольшие общие делители. НОД(5764800, 85)=5, НОД(5764802, 85)=17.

Окончательно имеем разложение 17*5=85.

В рассмотренном демонстративном примере мы нашли r посредством прямого расчета. В реальных задачах с большим N для этого может потребоваться квантовый компьютер.

Для справок приводим алгоритм Евклида нахождения наибольшего общего делителя.

Пусть a и b - натуральные числа. Без ограничения общности будем считать, что $a>b$.

Пусть ρ_1 - остаток от деления a на b. Вместо пары $[a;b]$ рассмотрим пару $[b;\rho_1]$ и, проделав с ней тоже самое, получим ρ_2. Далее рассмотрим пару $[\rho_1;\rho_2]$ и т.д. до тех пор, пока остаток от деления первого числа на

второе не станет равным нулю. Тогда возникнет пара $[\rho_n;0]$, в которой число ρ_n и будет искомым наибольшим общим делителем чисел a и b. Всего требуется $n \sim O(\log a)$ итераций для достижения результата.

Пример: Найдем наибольший общий делитель чисел 315 и 168. Алгоритм Евклида приведет нас к последовательности пар чисел: [315;168] [168;147] [147; 21] [21;0]. Число 21 и есть наибольший общий делитель чисел 315 и 168 : НОД(315, 168)=21

Резюмируем полученный результат. Мы описали полиномиальный квантовый алгоритм разложения целого числа на множители. Примечательно, что подобный классический алгоритм неизвестен. Рассматриваемый результат имеет важное теоретическое и практическое значение.

В теоретическом плане можно констатировать, что классическая арифметика (без алгоритма Шора) конструктивно (алгоритмически) неполна. Действительно, в арифметике хорошо известны простые конструктивные способы сложения, вычитания и умножения целых чисел. В то же время, операция разложения целого числа на множители, которая является обратной по отношению к умножению, оказывается сложной в вычислительном отношении. Получается, что в классической арифметике мы легко можем вычислить произведение двух больших простых чисел, но сталкиваемся с практически неразрешимой проблемой при попытках решения обратной задачи. Алгоритм Шора делает арифметику алгоритмически полной, поскольку теперь мы можем говорить и о факторизации чисел как о конструктивно решаемой задаче.

Отмеченная алгоритмическая неполнота классической арифметики лежит в основе современных криптографических методов защиты информации, которые нашли широкое применение в банковской сфере, Интернете и др. Речь, в частности, идет о так называемом коде RSA, который, как раз основан

на сложности задачи разложения большого целого числа на множители. Как следует из представленных выше результатов, создание квантовых компьютеров сделает классические криптографические системы беззащитными. Таким образом, встает вопрос о разработке новых (квантовых) способов защиты информации. Этому вопросу посвящен следующий раздел.

5.7. Квантовая криптография

Одним из практически важных направлений квантовой информатики является квантовая криптография. Задача криптографии состоит в разработке таких методов передачи информации между двумя сторонами (Алисой и Бобом), чтобы любые попытки с третьей стороны (Ева) перехватить и рассекретить сообщение были обречены на провал.

Остановимся на передаче сообщений с помощью так называемого секретного ключа. Секретный ключ – это последовательность случайных цифр, известных только Алисе и Бобу, например такая (нижеследующий пример взят из [71]):

K={12793 41169 42357 … }

Допустим, что Алиса хочет послать Бобу сообщение, представляющее собой, например, следующую последовательность цифр.

P={73997 68279 65867 …}

В сообщении P, например, каждой букве ставится в соответствие некоторое десятичное число. Если послать в эфир непосредственно сообщение P, то оно может быть легко перехвачено и расшифровано. Для

того, чтобы этого не произошло, сообщение P вначале шифруется, а только потом передается в эфир.

При шифровании к каждой цифре из сообщения P прибавляется цифра ключа K, если результат больше 10, то берется последняя цифра, в результате получаем криптограмму C:

C={85680 09338 07114 …}

Боб, получив криптограмму C и, зная секретный ключ K, легко расшифрует ее, преобразовав ее в сообщение P.

Ева, которая не знает ключа K, никогда не сможет расшифровать криптограмму, если только секретный ключ K абсолютно случайный и используется только один раз (факт абсолютной секретности таких сообщений доказал Шеннон в 1949 г.)

Приведенные выше последовательности цифр соответствуют реальному письму, которое направлял Че Гевара из Боливии Ф. Кастро на Кубу в 1967 г. [71]

Трудность описанной схемы состоит в передаче ключа (длинной последовательности цифр) от Алисы к Бобу: если они не встречаются непосредственно, то при передаче через эфир ключ может перехватить Ева.

Чтобы избежать отмеченной трудности, хорошо было бы иметь канал, секретность которого гарантируется самой Природой. Именно такой канал предоставляет квантовая информатика.

Покажем. каким образом последовательность отдельных кубитов может быть использована для передачи секретных ключей по несекретным каналам.

Рассмотрим следующую ситуацию. Алиса и Боб связаны между собой посредством обычной двухсторонней открытой линии связи и односторонним

(от Алисы к Бобу) квантовым каналом. Оба эти канала доступны наблюдениям со стороны Евы, которая способна перехватывать сообщения.

Рассмотрим очень простой и широко используемый протокол передачи секретного ключа BB84 (название протокола отражает фамилии его авторов – Беннет (Bennett) и Брассар (Brassard), а также год, когда он был предложен- 1984).

Опишем передачу секретного ключа от Алисы к Бобу в рамках протокола BB84. Алиса посылает последовательность кубитов Бобу, кодируя их следующим образом. Для каждого посылаемого фотона Алиса случайным образом использует один из следующих базисов (второй базис повернут относительно первого на 45°):

$\{0 - |\rightarrow\rangle;\ \ 1 - |\uparrow\rangle\}$ или $\{0 - |\nearrow\rangle;\ 1 - |\nwarrow\rangle\}$

Боб не знает о том, какой из двух базисов выбирает Алиса для каждого фотона. Он измеряет состояние получаемых фотонов также посредством случайно выбранного базиса.

После того, как передача по квантовому каналу заканчивается, Боб сообщает по открытому каналу информацию о последовательности своих базисов, а Алиса сообщает ему, в каких случаях он выбирал правильный (то есть совпадающий с ее) базис. В своей последовательности цифр Боб оставляет только те, которые соответствуют согласованному с Алисой базису. Именно эту последовательность они могут использовать как ключ.

Случайность в выборе базисов, которой придерживаются наши герои, служит цели обеспечения случайности ключа.

В среднем Алиса и Боб будут иметь согласованность базисов в 50% случаев.

Предположим теперь, что Ева измеряет состояние фотонов, переданных Алисой, и пересылает Бобу новые фотоны, соответствующие измеренной ею

поляризации. В этом процессе она будет использовать неверный базис в 50% случаев и пересылать фотоны в этом же базисе Бобу. Это приведет к тому, что Боб, измеряя в правильном базисе, будет иметь ошибку с вероятностью 25%.

Таким образом, подслушивание приводит к большому количеству ошибок (25%), что легко смогут обнаружить Алиса и Боб, обмениваясь достаточно длинной последовательностью.

Заметим, что вмешательство Евы может сделать связь между Алисой и Бобом невозможной. Однако, если Алиса и Боб будут действовать правильно, то никакое вмешательство Евы не сможет разрушить секретность их связи.

Задача 5.15 Придумайте схему, основанную, например, на БЧХ- кодах, которая могла бы обеспечивать (сколь угодно) высокую секретность протоколу BB84.

Современная оптико – волоконная связь позволяет, в принципе, передавать квантовые сообщения на расстояние до 100 км и далее. Принципиальное ограничение связано с невозможностью усиления сигнала (из теоремы о невозможности клонирования следует, что попытки усиления сигнала неизбежно приведут к его разрушению).

С целью преодоления указанного ограничения предложены возможные различные технологические решения, в том числе связанные с разработкой квантовых криптографических протоколов на когерентных оптических состояниях. Когерентные оптические состояния могут нести в себе большое число фотонов. Это, с одной стороны, способствует увеличению дальности передачи секретных сообщений, а с другой стороны, создает дополнительные проблемы с защитой информации. Рассмотрение этих вопросов выходит за рамки нашего изложения.

5.8. Алгоритм Гровера

Алгоритм Гровера направлен на поиск записи в неструктурированной базе данных. Он обеспечивает поиск решения за $O\left(\sqrt{N}\right)$ шагов в базе из N элементов. Заметим, что классический алгоритм способен решит задачу только за $O(N)$ шагов.

Рассмотрим квантовую постановку задачи. Пусть имеется N состояний.

$|0\rangle,|1\rangle,...,|N-1\rangle$

Допустим, что задача имеет M решений ($1 \le M \le N$). $M=1$- частный случай в рассматриваемой постановке.

Рассмотрим функцию такую, что $f(x)=1$, если x - решение и $f(x)=0$, если x не есть решение. Унитарный оператор U_f, обеспечивающий рассматриваемую функцию, называется оракулом и обозначается буквой O. Действие оракула поясняется схемой

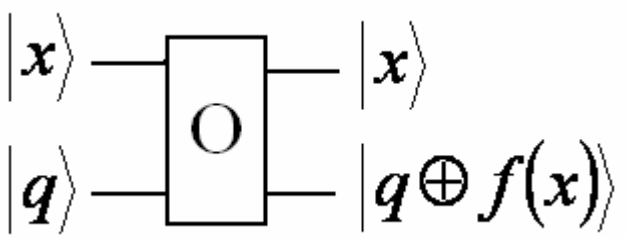

Рис. 5.9 Схема действия оракула

Таким образом, оракул выполняет следующее преобразование

$|x\rangle|q\rangle \to |x\rangle|q \oplus f(x)\rangle$

Оракул способен распознать решение и пометить его:

$|x\rangle|0\rangle \to |x\rangle|1\rangle$, если x - решение

$|x\rangle|0\rangle \to |x\rangle|0\rangle$, если x не есть решение

Пусть состояния $|x\rangle$, где $x=0,1,...,N-1$ мы поочередно подаем на вход оракула и ждем, когда кубит оракула перевернётся и тем самым будет получено решение. Очевидно, что таким образом будет реализован небыстрый алгоритм поиска и он будет обеспечивать решение за $O(N)$ шагов.

Наша задача состоит в том, чтобы за счёт квантового параллелизма (т.е. за счет подачи на вход некоторой суперпозиции состояний) предложить быстрый алгоритм, обеспечивающий поиск за $O(\sqrt{N})$ шагов.

Последовательность осуществления алгоритма следующая.

Пусть $|q\rangle=\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$. Такое состояние уже использовалось нами в реализации алгоритма Дойча. Это состояние играет роль «катализатора», который сам не меняется, но обеспечивает изменение состояния других кубитов. Действительно, действие оракула в рассматриваемом случае сводится к преобразованию:

$$|x\rangle|q\rangle\to(-1)^{f(x)}|x\rangle|q\rangle$$

Договоримся о сокращенной записи (опуская неизменный кубит-«катализатор»)

$$|x\rangle\to(-1)^{f(x)}|x\rangle$$

Таким образом, мы видим, что оракул помечает решение посредством фазы π.

Введем теперь некоторый унитарный оператор (так называемый оператор условного сдвига фазы)

$U=2|0\rangle\langle 0|-I$,

где I - единичный (тождественный) оператор.

Покажем, что введенный выше оператор действительно является унитарным. Используем условие полноты системы базисных функций

$$\sum_{x=0}^{N-1}|x\rangle\langle x| = I$$

Тогда для оператора условного сдвига фазы получаем

$$U = 2|0\rangle\langle 0| - I = |0\rangle\langle 0| - \sum_{x\neq 0}|x\rangle\langle x|$$

Отсюда видим, что

$U|0\rangle = |0\rangle$ и

$U|x\rangle = -|x\rangle$, если $x \neq 0$

Рассмотрим теперь состояние, играющее центральную роль в квантовых алгоритмах и неоднократно использовавшееся нами ранее. Это состояние представляет собой равномерную суперпозицию всех базисных состояний:

$$|\psi\rangle = \frac{1}{\sqrt{T}}\sum_{x=0}^{N-1}|x\rangle$$

Далее значком $|\psi\rangle$ будем обозначать это конкретное состояние.

Задача 5.16 Докажите справедливость тождества

$$H^{\otimes n}\left(2|0\rangle\langle 0| - I\right)H^{\otimes n} = 2|\psi\rangle\langle\psi| - I$$

Теперь мы готовы ввести оператор Гровера. Он определяется последовательностью двух операторов: действием сперва оракулом O, а затем оператором $2|\psi\rangle\langle\psi| - I$, в результате получаем оператор Гровера:

$$G = \left(2|\psi\rangle\langle\psi| - I\right)O$$

Решение задачи поиска сводится к последовательному действию оператором Гровера на исходное состояние $|\psi\rangle$. Опишем подробности алгоритма.

Заметим вначале, что состояние $|\psi\rangle$ можно представить в виде суперпозиции двух состояний, одно из которых есть сумма всех решений, а другое- сумма всех «не- решений»:

$$|\psi\rangle = \sqrt{\frac{N-M}{N}}|\alpha\rangle + \sqrt{\frac{M}{N}}|\beta\rangle$$

Здесь $|\beta\rangle$ - нормированная сумма всех решений

$$|\beta\rangle = \frac{1}{\sqrt{M}}\sum_{x'}|x'\rangle$$

Аналогично, $|\alpha\rangle$ - нормированная сумма всех «не- решений»

$$|\alpha\rangle = \frac{1}{\sqrt{N-M}}\sum_{x''}|x''\rangle$$

В представленных формулах мы помечаем решения одним штрихом, а «не- решения»- двумя штрихами.

Действие оператора Гровера лучше всего изображать графически на двумерном графике, оси которого образованы состояниями $|\alpha\rangle$ и $|\beta\rangle$. Действие оператора оракула O сводится к отражению относительно оси $|\alpha\rangle$. Аналогично, действие оператора $2|\psi\rangle\langle\psi| - I$ сводится к отражению относительно состояния $|\psi\rangle$. Первая итерация Гровера изображена на рисунке

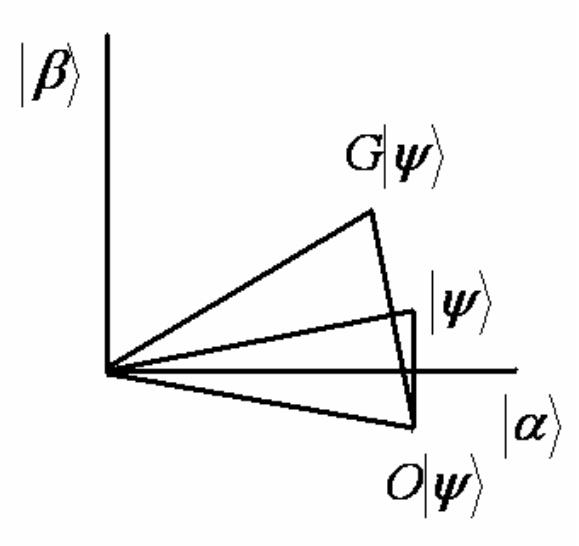

Рис.5.10 Графическая иллюстрация алгоритма Гровера

Задача 5.17 Пусть $\cos\left(\frac{\theta}{2}\right)=\sqrt{\frac{N-M}{N}}$, $\sin\left(\frac{\theta}{2}\right)=\sqrt{\frac{M}{N}}$. Покажите, что результат действия k итераций Гровера может быть представлен в виде:

$$G^{(k)}|\psi\rangle=\cos\left(\frac{(2k+1)\theta}{2}\right)|\alpha\rangle+\sin\left(\frac{(2k+1)\theta}{2}\right)|\beta\rangle$$

Из полученного результата мы видим, итерации Гровера приводят к постепенному вращению вектора состояния в сторону вертикальной оси $|\beta\rangle$ (т.е. в сторону решений задачи). Итерационный процесс следует закончить, когда будет приближенно выполняться равенство:

$$\frac{(2k+1)\theta}{2}=\frac{\pi}{2}$$

Отсюда следует, что необходимое число итераций задается приближенно условием:

$$k\approx\frac{\pi}{4}\sqrt{\frac{N}{M}}$$

В результате измерения, проведенного после k итераций Гровера с высокой (хотя и не равной единице) вероятностью будет найдено одно из решений задачи поиска.

Алгоритм Гровера имеет важное значение в области квантового моделирования

5.9 Введение в квантовое исправление ошибок

Повышение надежности передачи и хранения информации достигается посредством избыточности. Например, в трехбитовом коде каждый логический бит информации задаётся тремя физическими битами

$$0 \to 000$$

$$1 \to 111$$

В рассматриваемом случае реализуется мажоритарная система исправления ошибок (принятие решения на основе большинства голосов). В случае трехбитового кодирования сообщение (логический бит) передаётся правильно, если число ошибок в физических битах равно нулю или единице. Соответственно, сообщение может быть передано неверно, если ошибок две или три.

Рассмотрим в качестве простого введения двоичный симметричный канал. Пусть p - вероятность ошибки в одном физическом бите: вероятность превращения нуля в единицу ($0 \to 1$), либо наоборот, единицы в нуль ($1 \to 0$). Будем считать обе эти вероятности одинаковыми (отсюда название-симметричный канал). Вероятность безошибочной передачи информации ($0 \to 0$, либо $1 \to 1$), соответственно, равна $1 - p$.

Задача 5.18 Покажите, что классический трёхбитовый код характеризуется следующей вероятностью ошибки передачи одного логического бита информации

$$P_e = 3p^2 - 2p^3$$

Покажите далее, что избыточность увеличивает надежность передачи информации (т.е. $P_e < p$, если $p < 0.5$).

Перейдем теперь к рассмотрению квантового бита (кубита). Рассмотрим вначале так называемый канал с классической ошибкой (название «классическая ошибка» довольно условно).

Такая ошибка описывается действием оператора X (NOT), когда состояние 0 меняется на 1, а состояние 1 меняется на 0:

$X|\psi\rangle$, т.е. $\begin{matrix} |0\rangle \to |1\rangle \\ |1\rangle \to |0\rangle \end{matrix}$

Таким образом, действие ошибки описывается следующим преобразованием состояния кубита

$$a|0\rangle + b|1\rangle \to a|1\rangle + b|0\rangle$$

Трёхбитовый код в квантовом исполнении (резервирование одного логического кукубита тремя физическими кубитами) выглядит следующим образом:

$a|0\rangle + b|1\rangle \to a|000\rangle + b|111\rangle$, т.е.

$$|0\rangle \to |0_L\rangle \equiv |000\rangle$$

$$|1\rangle \to |1_L\rangle \equiv |111\rangle$$

Реализация рассматриваемого способа кодирования посредством квантовой схемы представлена на рисунке.

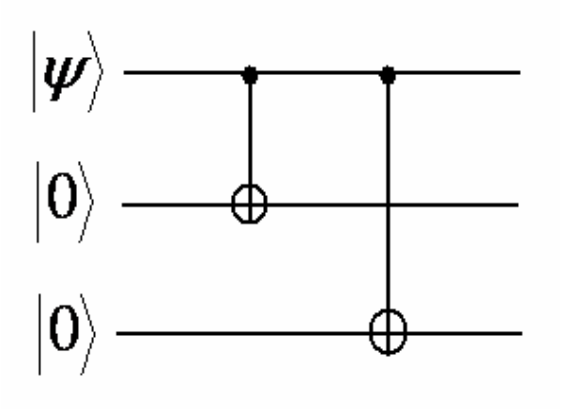

Рис. 5.11 Квантовая схема кодирования для защиты от классической ошибки

Квантовая схема обеспечивает следующую последовательность преобразований

$$|\psi\rangle|0\rangle|0\rangle \equiv \left(a|0\rangle + b|1\rangle\right)|00\rangle \equiv a|000\rangle + b|100\rangle \to a|000\rangle + b|110\rangle \to a|000\rangle + b|111\rangle$$

Рассмотрим каким образом добавление вспомогательной системы из двух кубитов в исходном состоянии ноль позволяет детектировать возможное наличие ошибки.

Дополним схему кодирования схемой декодирования и измерения вспомогательной системы.

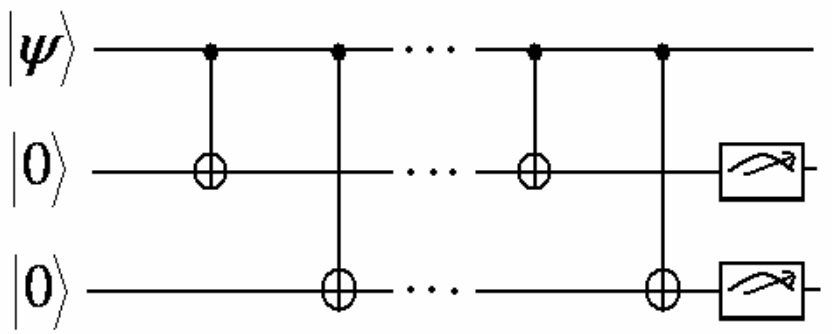

Рис. 5.12 Квантовая схема кодирования, дополненная схемой декодирования и измерения.

Специфика квантового исправления ошибок состоит в том, что мы не можем подвергать измерениям кубиты, несущие информацию (в противном

случае эта информация будет утеряна в результате редукции состояния). Вместо измерения информационной системы производится измерение вспомогательной системы. Измерение вспомогательной системы позволяет идентифицировать возможную ошибку и исправить её.

Оказывается, что измерение двух вспомогательных (второго и третьего) кубитов допускает 4 следующие возможности: 11 (когда произошла ошибка в первом кубите), 00 (когда ошибок нет), 10 (ошибка во втором кубите), 01 (ошибка в третьем кубите).

Предположим, например, что возникла ошибка в первом (информационном) кубите, т.е.

$$a|000\rangle + b|111\rangle \to a|100\rangle + b|011\rangle$$

Тогда, декодирование (правая часть рисунка) приведёт к следующей последовательности преобразований:

$$a|100\rangle + b|011\rangle \to a|110\rangle + b|011\rangle \to a|111\rangle + b|011\rangle = \left(a|1\rangle + b|0\rangle\right)|11\rangle$$

Измерение второго и третьего кубитов дадут результат 11. Это будет означать, что в первом (информационном) кубите произошла ошибка. Для исправления этой ошибки нужно выполнить преобразование X над информационным кубитом.

Рассмотрим три остальных случая. Если ошибок нет, то последовательность преобразований будет следующей:

$$a|000\rangle + b|111\rangle \to a|000\rangle + b|101\rangle \to a|000\rangle + b|100\rangle = \left(a|0\rangle + b|1\rangle\right)|00\rangle$$

Убеждаемся, что в результате преобразований информационный кубит не изменился, а вспомогательная система оказалась в состоянии 00.

Если возникла ошибка во втором кубите, то имеем цепочку преобразований:

$$a|010\rangle + b|101\rangle \to a|010\rangle + b|111\rangle \to a|010\rangle + b|110\rangle = \left(a|0\rangle + b|1\rangle\right)|10\rangle$$

Снова информационный кубит не изменился, а вспомогательная система оказалась теперь в состоянии 10.

Если возникла ошибка в третьем кубите, то аналогично получим:

$$a|001\rangle + b|110\rangle \to a|001\rangle + b|100\rangle \to a|001\rangle + b|101\rangle = \left(a|0\rangle + b|1\rangle\right)|01\rangle$$

Информационный кубит опять не изменился, а вспомогательная система оказалась теперь в состоянии 01.

Таким образом, рассматриваемые четыре возможности идентифицируют 4 ситуации (отсутствие ошибок, либо ошибка в одном из трёх кубитов).

Рассмотрим теперь случай двух ошибок. Пусть, например, ошибки возникли в 1-ом и 2-ом кубитах. Тогда

$$a|110\rangle + b|001\rangle \to a|100\rangle + b|001\rangle \to a|101\rangle + b|001\rangle = \left(a|1\rangle + b|0\rangle\right)|01\rangle$$

Если мы будем действовать по схеме, указанной выше, то мы ошибочно сделаем вывод о наличии ошибки в третьем кубите и, таким образом, не сможем идентифицировать ошибку в информационном кубите.

Мы видим, что рассмотренный трёхкубитовый код исправляет гарантированно не более одной ошибки.

Рассмотрим теперь так называемую фазовую ошибку. Эта ошибка сводится к несанкционированному действию оператора сдвига фазы Z. Таким образом, действие фазовой ошибки описывается следующим преобразованием состояния кубита (меняется знак у базисного состояния $|1\rangle$)

$$a|0\rangle + b|1\rangle \to a|0\rangle - b|1\rangle$$

Покажем, что рассмотрение фазовой ошибки можно свести к рассмотрению классической ошибки:

Выполнив преобразование Адамара, перейдем к новому базису:

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

$$|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Мы видим, что в новом базизе действие фазовой ошибки сводится к тому, что состояния $|+\rangle$ и $|-\rangle$ переходят друг в друга ($|+\rangle \to |-\rangle$, $|-\rangle \to |+\rangle$). Таким образом, в новом базисе фазовая ошибка сводится к классической ошибке.

Схема кодирования фазовой ошибки изображена на рисунке. Она представляет собой схему кодирования классической ошибки, дополненную преобразованием Адамара для каждого кубита

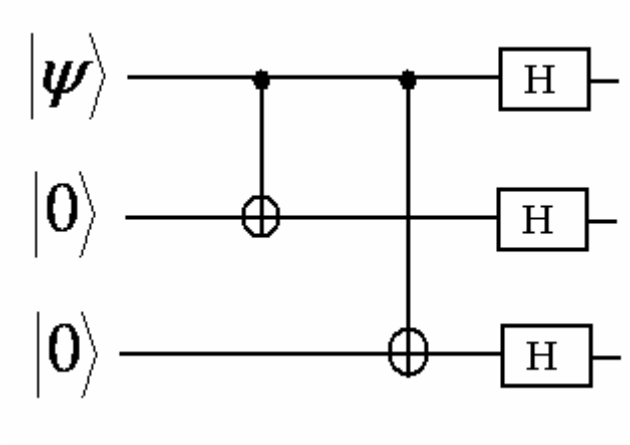

Рис. 5.13 Квантовая схема кодирования для защиты от фазовой ошибки

СПИСОК ЛИТЕРАТУРЫ

1. *Нильсен М, Чанг* И. Квантовые вычисления и квантовая информация: Пер. с англ. Под ред. М.Н. Вялого и П.М. Островского с предисловием К.А. Валиева. - М.: Мир. 2006. 824 с.
2. *Валиев К.А.*, *Кокин А.А.* Квантовые компьютеры: Надежды и реальность. 2-е изд., исп. М.–Ижевск: НИЦ РХД, 2002. 320 с.
3. Физика квантовой информации. Квантовая криптография. Квантовая телепортация. Квантовые вычисления // Под. ред. *Д.Боумейстера, А.Экерта, А. Цайлингера;* Пер. с англ. под ред. *С.П.Кулика и Т.А.Шмаонова.* М. Постмаркет. 2002. 376с.
4. *Прескилл Дж*. Квантовая информация и квантовые вычисления. Том.1. М.-Ижевск. РХД. 2008. 464с.
5. *Валиев К.А.* Квантовые компьютеры и квантовые вычисления // Успехи Физических Наук. 2005. Т.175. №1. С.3-39.
6. *Ожигов Ю.И.* Квантовые вычисления. М. МГУ. 2003.
7. *Feynman R.* Simulating Physics with Computers // Int. J. Theor. Phys. 1982. V.21. №6/7. P.467-488. См. перевод *Фейнман Р.* Моделирование физики на компьютерах // сб. «Квантовый компьютер и квантовые вычисления». Т.2. Ижевск. РХД. 1999. с.96-124.
8. *Feynman R.* Quantum Mechanical Computers // Found. of Phys. 1986. V.16. №6. P.507-531. См. перевод *Фейнман Р.* Квантовомеханические компьютеры // сб. «Квантовый компьютер и квантовые вычисления». Т.2. Ижевск. РХД. 1999. с.125-156.
9. *Манин Ю.И.* Вычислимое и невычислимое. М. Советское Радио. 1980. 128с.
10. *Китаев А., Шень А., Вялый М.* Классические и квантовые вычисления М. МЦНМО. ЧеРо. 1999. 192 с.

11. *Grover L.K.* Quantum Mechanics Help in Searching for a Needle in a Haystack // Phys. Rev. Lett. 1997. V.78. №2. P.325-328. См. перевод *Гровер Л.К.* Квантовая механика помогает найти иголку в стоге сена // сб. «Квантовый компьютер и квантовые вычисления». Т.1. Ижевск. РХД. 1999. с.101-109.
12. *Shor P.* Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. LANL Report quant-ph/ 9508027.1995. 28p.
13. *Deutsch D.* Quantum Theory, the Church- Turing Principle and the Universal Quantum Computer // Proc. Roy. Soc. London. 1985. V.A400. №1818. P.97-117. См. перевод *Дойч Д.* Квантовая теория принципа Черча- Тьюринга и универсальный квантовый компьютер // сб. «Квантовый компьютер и квантовые вычисления». Т.2. Ижевск. РХД. 1999. с.157-189.
14. *Barenco A., Bennett C.H., Cleve C., DiVincenzo D.P., Margolus N., Shor P., Sleater T., Smolin J.A., Weinfurter H.* Elementary Gates for Quantum Computation // Phys. Rev. A. 1995. V.52. №5. P.3457-3467.
15. *Preskill J.* Fault-tolerant quantum computation. LANL Report quant-ph/ 9712048.1997. 58p.
16. *Kim Y.H., Kulik S.P., Shih Y.H.* Quantum teleportation of a polarization state with a complete Bell state measurement // Phys. Rev. Lett. 2001. V.86. P.1370-1373
17. *Bartlett S.D., Munro W.J.* Quantum Teleportation of Optical Quantum Gates // Phys. Rev. Lett. 2003. V.90. 117901.
18. *Mattle K., Weinfurter H., Kwiat P.G., and Zeilinger A.* Dense Coding in Experimental Quantum Communication // Phys. Rev. Lett. 1996. V76. P.4656-4659.

19. *Kim Y.H., Kulik S.P., Shih Y.H.* Bell state preparation using pulsed nondegenerate two-photon entanglement // Phys. Rev.A. 2001. V.63. 060301. 4p.
20. *Kim Y.H., Chekhova M.V., Kulik S.P., Rubin M., Shih Y.H.* Interferometric Bell state preparation using femtosecond pulse pumped spontaneous parametric down-conversion. 2001. // Phys. Rev. A. V.63. 062301. 11p.
21. Cavity Quantum Electrodynamics. Advances in atomic, molecular and optical physics // *Berman P.* (editor). Academic Press. San Diego. 1994. 497 p.
22. *Münstermann P., Fischer T., Maunz P., Pinkse P.W.H., and Rempe G.* Observation of cavity-mediated long-range light forces between strongly coupled atoms // Phys. Rev. Lett. 2000. V.84. P.4068-4071.
23. *Beige A.* Ion-trap quantum computing in the presence of cooling // Phys. Rev. A. 2004. V.69. 012303. 11p.
24. *Pachos J., Walther H.* Quantum computation with trapped ions in an optical cavity // Phys. Rev. Lett. 2002. V.89. 187903. 4p.
25. *Childs A., Chuang I.L.* Universal quantum computation with two-level trapped ions // Phys. Rev. A. 2001. V.63. 012306. 4p.
26. *Gershenfeld N.*A., Chuang I.L. Bulk Spin-Resonance Quantum Computation // Science. 1997. V. 275. №1. P.350-356.
27. *Vandersypen L.M.K., Steffen M., Breyta G., Yannoni C.S., Sherwood M.H., Chuang I.L.* Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance // Nature. Dec. 2001. V.414. P. 883-887.
28. *Кокин А.А.* Твердотельные квантовые компьютеры на ядерных спинах. Институт компьютерных исследований. Москва- Ижевск. 2004. 204 с.
29. *Bohr N.* Discussion with Einstein on epistemological problems in atomic physics // in Schilp P.A. (editor), Albert Einstein, Philosopher-Scientist (Library of Living Philosophers, Evanston, Illinois, 1949), P.200-241.

Перевод на русский язык: *Бор Н.* Дискуссия с Эйнштейном по проблемам теории познания в атомной физике. Избранные научные труды в 2-х томах. Т.2. С. 399-433. М. Наука. 1971.

30. *Богданов Ю.И.* Многопараметрические статистические модели в задачах квантовой информатики // Труды ФТИАН. М. Наука. 2005. Т.18. с.91-118
31. *Крамер Г.* Математические методы статистики. М.: Мир, 1975. 648 с.
32. *Lukacs E.* Characteristic Functions. London. Charles Griffin & Company Limited. 1960.216 p.
33. *Прохоров Л.В.* Квантовая механика- проблемы и парадоксы. СПб. НИИХ СПбГУ. 2003. 120 с.
34. *Владимиров В.С.* Обобщенные функции в математической физике. М. Наука. 1979. 320с.
35. *Robertson H.P.* An Indeterminacy Relation for Several Observables and Its Classical Interpretation // Phys.Rev. 1934. V.46. P.794-801
36. *Холево А.С.* Статистическая структура квантовой теории. М.–Ижевск: Ин-т комп. исслед., 2003. 192 с.
37. *Богданов А.Ю., Богданов Ю.И., Валиев К.А.* Информация Шмидта и запутанность квантовых систем //Вестн. Моск. ун-та. Сер.15. Вычислительная математика и кибернетика. 2007.№1; LANL report quant-ph/0512062
38. *Кендалл М., Стьюарт А.* Статистические выводы и связи. М. Наука. 1973. 900 с.
39. Вероятность и математическая статистика. Энциклопедия. // Под ред. *Ю.В. Прохорова.* М:. Большая Российская энциклопедия, 1999. 911 с.
40. *Крянев А.В., Лукин Г.В.* Математические методы обработки неопределенных данных. М. Физматлит. 2003. 216 с.

41. *Богданов Ю.И.* Основная задача статистического анализа данных: Корневой подход. М.: МИЭТ, 2002. 96с. Пер. на англ.: *Bogdanov Yu. I.* Fundamental problem of statistical data analysis: Root approach. M.: MIEE, 2002. 84 p.; *Bogdanov Yu. I.* Statistical inverse problem // LANL E-print, 2002, arXiv: phys/0211109. 39p.
42. *Bogdanov Yu.I.* Quantum mechanical view of mathematical statistics // Proceedings of SPIE. 2006. V.6264. 62640E; LANL E-print, 2003, arXiv: quant-ph/0303013. 26 p; New Topics in Quantum Physics Research. Nova Science. 2006. pp. 1-36.
43. *Ю.И. Богданов,* Унифицированный метод статистического восстановления квантовых состояний, основанный на процедуре очищения // ЖЭТФ. 2009. Т.135. Вып.6.с.1068-1078.
44. *Богданов Ю.И., Кривицкий Л.А., Кулик С.П.* Статистическое восстановление квантовых состояний оптических трехуровневых систем // Письма в ЖЭТФ. 2003. Т. 78, вып. 6. С. 804–809.
45. *Bogdanov Yu.I., Chekhova M.V., Kulik S.P.* et al. Statistical reconstruction of qutrits // Phys. Rev. A. 2004. Vol. 70. 042303. 16 p.
46. *Bogdanov Yu.I., Chekhova M.V., Kulik S.P.* et al. Qutrit state engineering with biphotons // Phys. Rev. Lett. 2004. Vol. 93. 230503. 4p.
47. *Bogdanov Yu.I., Brida G, Genovese M., Kulik S.P., Moreva E.V., Shurupov A.P.* Statistical Estimation of the Efficiency of Quantum State Tomography Protocols // Phys. Rev. Lett. 2010. V.105. 010404. 4p.
48. *Дирак П.А.М.* Принципы квантовой механики // Собрание научных трудов. Т.1: Квантовая теория. М.: Физматлит, 2002. С. 7–320.
49. *Von Neumann J.* Mathematische Grudlagen der Quantenmechanik. Berlin. Springer. 1932. См. перевод *Фон Нейман И.* Математические основы квантовой механики. М. Наука. 1964. 368с.

50. *Dirac P.A.M.* Relativity and Quantum Mechanics // Fields and Quanta. 1972. V3. P.139-164. (см. перевод *Дирак П.А.М.* Теория относительности и квантовая механика // Собрание научных трудов. Том III. М. Физматлит. 2004. с. 141-152.)
51. *Bogdanov Yu.I.* Root estimator of quantum states // LANL E-print, 2003, arXiv: quant-ph/0303014. 26 p; New Topics in Quantum Physics Research. Nova Science. 2006. pp. 129-162.
52. *Богданов Ю. И.* Основные понятия классической и квантовой статистики: Корневой подход // Оптика и спектроскопия. 2004. Т.96, №5. С.735–746.
53. *Einstein A., Podolsky B., Rosen N.* Can quantum-mechanical description of physical reality be considered complete? // Phys. Rev. 1935. V.47. P.777-780. Перевод на русский язык: Эйнштейн А., Подольский Б., Розен Н. Можно ли считать квантовомеханическое описание физической реальности полным? А. Эйнштейн Собрание научных трудов в 4-х томах. Т.3. С. 604-611. М. Наука. 1966.
54. *Гнеденко Б.В.* Курс теории вероятностей. М. Эдиториал УРСС. 2005. 448 с.
55. *Коэн-Таннуджи К., Диу Б., Лалоэ Ф.* Квантовая механика // Пер. с фр. Л.Н. Новикова. В 2-х т. Екатеринбург. Изд-во Урал. Ун-та. 2000.
56. *Ландау Л.Д., Лифшиц Е.М.* Квантовая механика. Нерелятивистская теория М. Наука. 1974. 752 с.
57. *Ehrenfest P.* Bemerkung über die angenaherte Gültigkeit der klassischen Mechanik innerhalb der Quanten Mechanik // Z. Phys. 1927. **45**. S. 455-457. См. перевод: *Эренфест П.* Замечание о приближенной справедливости классической механики в рамках квантовой механики // в сб. *Эренфест П.* Относительность. Кванты. Статистика. Сборник статей. М. Наука. 1972. с.82- 84.

58. *Гильберт Д.* Математические проблемы // Избранные труды. Т2. М. Факториал. 1998. с.401- 436.
59. *Zee H.D.* Roots and Fruits of Decoherence // Seminaire Poincare. 2005. p.115-129.; *Zurek W.H.* Decoherence and the Transition from Quantum to Classical- Revisited// Ibid. p.1-23.
60. *Больцман Л.* Дальнейшие исследования теплового равновесия между молекулами газа // Избранные труды. М. Наука. 1984. с.125-189.
61. *Гильберт Д.* Основы общей теории линейных интегральных уравнений. Глава XXII Обоснование кинетической теории газов // Избранные труды. Т2. М. Факториал. 1998. с.350- 364.
62. *Гейзенберг В.* О квантовотеоретической интерпретации кинематических и механических соотношений. Избранные труды. М. УРСС. 2001. с. 86-98.
63. *Борн М., Иордан П.* К квантовой механике. Там же. С. 99-126.
64. *Гейзенберг В., Борн М., Иордан П.* К квантовой механике. II. Там же. С. 127-175.
65. *Hilbert D., Neumann J., Nordheim L.* Űber die Grundlagen der Quantenmechanik. 1928. Math. Ann. Bd. 98. s. 1-30.
66. *Bell J.S.* Speakable and unspeakable in quantum mechanics. Collected papers on quantum phylosophy. Cambridge University Press. 1993.
67. *Холево А.С.* Введение в квантовую теорию информации. М. МЦНМО. 2002. 128с.
68. *Холево А.С.* Вероятностные и статистические аспекты квантовой теории. Издание 2-е, дополненное. Москва- Ижевск. Институт компьютерных исследований. 2003. 410 с.
69. *Гнеденко Б.В.* К шестой проблеме Гильберта // Проблемы Гильберта (сб. статей под ред. Александрова П.С.) М. УРСС. 2000. с.117- 119.

70. *Блейхут Р.* Быстрые алгоритмы цифровой обработки сигналов. М. Мир, 1989. 448 с.
71. *Килин С.Я.* Квантовая информация // Успехи Физических Наук. 1999. Т.169. №5. С.507-527.

Содержание **стр.**