Алгебраический аппарат квантовой информатики

Учебное пособие

Д.А.Кронберг, Ю.И.Ожигов, А.Ю.Чернявский
МГУ имени М.В.Ломоносова, факультет ВМК

Пособие основано на обязательных семинарах, проводимых авторами для студентов третьего курса кафедры квантовой информатики ВМК МГУ. В пособии кратко изложены элементарные основы квантовой информатики: формализм и свойства чистых и смешанных квантовых состояний, их преобразования и измерения. Рассмотрена запутанность между двумя подсистемами. Особое внимание уделено математическим фактам, выходящим за рамки программы первых двух курсов факультета ВМК (например, алгебра тензоров, SVD-разложение матриц). Приведены задачи для самостоятельного решения и примеры решения типовых задач. Учебное пособие предназначено для студентов 3-4 курсов факультета ВМК МГУ, а также других естественных и математических ВУЗов.

Оглавление

Введение

Целью данного пособия является краткое изложение базовых понятий квантовой информатики, а также их алгебраических основ. Определенной трудностью в изучении квантовой информатики является отсутствие во многих университетских курсах алгебры некоторых разделов, например тензоров. Поэтому особое внимание уделяется материалу по алгебре, не входящему в обязательную программу факультета ВМК.

Пособие содержит задачи для самостоятельного решения. Некоторые задачи представляют собой доказательства простейших теоретических свойств изучаемых объектов, некоторые же имеют практический характер. Сложные задачи помечены соответствующим количеством звездочек. Важные теоретические задачи, которые, по мнению авторов, вызывают наиболее частые затруднения, снабжены указанием на литературу, где можно найти решение, однако рекомендуется попытаться решить их самостоятельно. Одной из важных целей при решении представленных задач является освоение обозначений, используемых в квантовой информатике.

Пособие, как и задачи, необходимо прорабатывать последовательно, т.к. большинство материала связано между собой.

Для более глубокого изучения алгебры, используемой в квантовой информатике, рекомендуется прочесть какой-либо учебник, содержащий раздел, посвященный тензорам, например [1]. Сингулярное разложение матриц и способы его вычисления хорошо изложены в [2].

Основной литературой по квантовой информатике являются: [4][5][6].

Глава 1

Линейная алгебра

1 Гильбертово пространство и сопряженный оператор

Одним из важнейших объектов квантовой информатики является гильбертово пространство – обобщение евклидова пространства на бесконечномерный случай. Обычно гильбертово пространство рассматривается в курсе функционального анализа. В книге нам понадобится лишь конечномерный случай такого пространства, и, таким образом, мы под гильбертовым пространством будем понимать конечномерное линейное пространство (обычно комплексное) с введенным на нем скалярным произведением, обозначаемым (x, y).

Пусть оператор A действует в гильбертовом пространстве H, тогда *сопряженным* (или *эрмитово-сопряженным*) к нему оператором называется оператор A^*, такой что для любых двух векторов $x, y \in H$ выполняется соотношение

$$(x, Ay) = (A^* x, y).$$

Задача 1.1 *Покажите, что сопряженный оператор единственнен.*

Замечание 1.2 *Иногда через A^* обозначается комплексное сопряжение, а эрмитово сопряжение через $A^\dagger$. В книге A^* обозначает эрмитово сопряжение.*

Задача 1.3 *Покажите, что в матричном представлении эрмитово сопряжение означает комплексное сопряжение и транспонирование.*

2 Сопряженное пространство

Сопряженным пространством линейного пространства V над полем K называется пространство V^* его линейных функционалов, т.е. функций $f : V \to K$, таких что для любых $x, y \in V; a \in K$ выполняется $f(ax) = af(x), f(x + y) = f(x) + f(y)$.

Казалось бы, линейных функционалов больше, нежели векторов. Однако, если V – конечномерное, то $dim(V) = dim(V^*)$ (докажите это). Кроме того, если конечномерное пространство V имеет скалярное произведение, то имеется удобный изоморфизм между V и V^*. Т.к. этот изоморфизм важен для дальнейшего понимания, построим его. (Напомним, что изоморфизмом двух линейных пространств называется линейное биективное отображение одного пространства в другое.)

Рассмотрим произвольный вектор $x \in V$. Поставим в соответствие этому вектору линейный функционал $f_x(y)$: $f_x(y) = (y, x)$. Теперь необходимо показать, что для любого $f \in V^*$ существует $x \in V : f(y) = (y, x)$. Пусть $(e_1, e_2, \ldots, e_n)$ – ортонормированный базис пространства V. f в силу линейности полностью определяется своим действием на базисных векторах. Пусть $f(e_i) = c_i$, тогда в качестве x можно взять $x = \sum\limits_i c_i e_i$.

Задача 2.1 *Проверьте, что описанное выше соответствие действительно является изоморфизмом.*

В матричном представлении этот изоморфизм очень прост: для вектора x мы можем рассматривать его сопряженный вектор x^*, матричное умножение этого вектора на произвольный вектор $y \in V : x^* y = (y, x)$ – определяет линейный функционал.

Замечание 2.2 *В бесконечномерных гильбертовых пространствах подобный изоморфизм также существует. Об этом говорит теорема Рисса[3].*

3 Унитарные и эрмитовы операторы

Определение 3.1 *Оператор U называется унитарным, если $U^*U = I$.*

Задача 3.2 *Докажите, что $U^*U = I \Leftrightarrow UU^* = I \Leftrightarrow U$ – обратима и $U^* = U^{-1}$.*

В предыдущей задаче дается важное свойство унитарных матриц – они обратимы.

Унитарные матрицы обладают еще одним важным свойством:

Задача 3.3 *Докажите, что если $U : V \to V$ – унитарный оператор, то для любых $x, y \in V : (x, y) = (Ux, Uy)$.*

Т.е. унитарные операторы сохраняют скалярное произведение, а значит углы и длины. Таким образом унитарные преобразования являются поворотами пространства. Также унитарные операторы описывают переходы от одного ортонормированного базиса к другому.

Задача 3.4 *Докажите, что собственные значения унитарной матрицы по модулю равны единице.*

Следствием предыдущей задачи является то, что детерминант унитарной матрицы по модулю равен единице.

Определение 3.5 *Оператор H называется* эрмитовым *(или* самосопряженным*), если $H^* = H$.*

Задача 3.6 *Покажите, что определения унитарного и эрмитова оператора подходят и для матричного представления.*

Задача 3.7 *Докажите, что собственные значения эрмитовой матрицы вещественны.*

Одним из важнейших свойств эрмитовых матриц является спектральное разложение: $H = VDV^*$, где V – унитарная матрица, а D – вещественная диагональная. Т.к. собственные значения и вектора не зависят от базиса, можно заметить, что на диагонали D стоят собственные значения матрицы H, а матрица U состоит из собственных векторов.

Как следствие, мы видим, что эрмитовы матрицы имеют ортонормированный базис из собственных векторов.

4 Матричные функции

Пусть имеется квадратная матрица A и функция, представимая своим разложением в ряд Тейлора: $f(x) = \sum\limits_{i=0}^{\infty} a_i x^i$. Тогда можно определить $f(A)$, как $f(x) = \sum\limits_{i=0}^{\infty} a_i A^i$. При таком определении очень легко вычислять функции от эрмитовых матриц:

Задача 4.1 *Пусть H – эрмитова матрица,*

$$H = V \begin{pmatrix} d_1 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & d_n \end{pmatrix} V^*$$

– ее спектральное разложение. Тогда

$$f(H) = V \begin{pmatrix} f(d_1) & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & f(d_n) \end{pmatrix} V^*$$

Задача 4.2 $M = \begin{pmatrix} 7 & -1 & 0 \\ -1 & 7 & 0 \\ 0 & 0 & 4 \end{pmatrix}$, *вычислить* 2^M.

Решение. Собственные вектора матрицы M будут $e_1 = (0,0,1), e_2 = (1,1,0), e_3 = (1,-1,0)$, а соответствующие собственные значения (2,4,8). Чтобы построить унитарную матрицу U спектрального разложения, необходимо взять нормированные собственные вектора. В итоге получим:

$$2^M = \begin{pmatrix} 0 & 1/\sqrt{2} & 1/\sqrt{2} \\ 0 & 1/\sqrt{2} & -1/\sqrt{2} \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix} \cdot$$

$$\cdot \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & 1/\sqrt{2} & -1/\sqrt{2} \end{pmatrix} = \begin{pmatrix} 160 & -96 & 1 \\ -96 & 160 & 0 \\ 0 & 0 & 16 \end{pmatrix}$$

Задача 4.3

$$M = \begin{pmatrix} 89 & -48 & 0 \\ -48 & 61 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

вычислить $log_5(M)$.

Следующие две задачи показывают связь между унитарными и эрмитовыми матрицами:

Задача 4.4 *Пусть* H *– эрмитова матрица, тогда* $U = e^{iH}$ *– унитарная.*

Задача 4.5 *Пусть* U *– унитарная матрица, тогда существует эрмитова матрица* H *такая, что* $U = e^{iH}$ *– унитарная.*

Глава 2

Пространство квантовых состояний

1 Основные понятия тензорной алгебры

Для того, чтобы описать формализм многочастичных квантовых состояний необходимо дать определения некоторых понятий тензорной алгебры. Для лучшего понимания рекомендуется прочесть соответствующий раздел какого-либо учебника по алгебре, например [1].

Перед тем, как перейти к формальным определениям, скажем несколько слов о том, что же такое тензоры и зачем они нужны. Вектор является строкой элементов, или, если рассматривать его программную реализацию, одномерным массивом. Матрица представляет собой таблицу, или двумерный массив. Кроме того матрицы соответствуют линейным операторам в конечномерных пространствах, т.е. описывают линейные преобразования над векторами - объектами меньшей размерности.

Несложно представить себе трехмерную таблицу, чуть сложнее многомерную, а понятие многомерного массива хорошо известно и активно используются в программировании. Тензоры как раз-таки представляют собой многомерное расширение понятия матрицы (или, что более полно, линейного оператора).

Перейдем к формальным определениям.

Определение 1.1 *Тензорным произведением векторных пространств V и W (обозначается $V \otimes W$) над общим полем K (для квантовой информатики важным является поле комплексных чисел) называется векторное пространство T вместе с билинейным отображением*

$$\otimes : V \times W \to T, (x, y) \mapsto x \otimes y,$$

удовлетворяющим следующему условию: если $e_i : i \in I$ и $f_j : j \in J$ – базисы пространств V и W соответственно, то $e_i \otimes f_j : i \in I, j \in J$ – базис пространства T.

Замечание 1.2 *Важно понимать, что запись $x \otimes y$ обозначает не пару векторов, а* ***один*** *вектор пространства T. А пара векторов (x, y) является лишь его прообразом. Вектор $x \otimes y$ называют тензорным произведением векторов x и y.*

Задача 1.3 *Пусть линейное пространство V имеет базис (a, b, c), а линейное пространство W базис (d, e). Каков базис пространства $V \otimes W$?*

Задача 1.4 *Пусть конечномерные пространства V и W над общим полем имеют размерности m и n соответственно. Какова размерность их тензорного произведения?*

Важно помнить, что если определение линейной алгебры опирается на какой-либо базис пространства, то оно должно быть независимо от этого базиса:

Задача 1.5 *Доказать, что Опр. 1.1 не зависит от выбора базисов пространств V и W.[1]*

Также важна единственность определения:

Задача 1.6 *Доказать, что для двух тензорных произведений пространств V и W $(T_1, \otimes_1)$, $(T_2, \otimes_2)$ имеется единственный изоморфизм $\psi : T_1 \to T_2$, удовлетворяющий условию $\psi(x \otimes_1 y) = (x \otimes_2 y)$, для любых $x \in V, y \in W$.[1]*

Указание. Для решения задачи необходимо вспомнить, что такое изоморфизм, построить тривиальный изоморфизм, удовлетворяющий требуемому условию на базисных векторах, и использовать свойство билинейности тензорного произведения.

Так как тензорное произведение единственно, мы можем рассматривать именно то, которое строится в самом определении. А именно, в качестве тензорного произведения пространств V и W мы можем взять линейное пространство T с базисом $e_i \otimes f_j$ и отображение, задаваемое на базисных векторах $(e_i, f_j) \mapsto e_i \otimes f_j$. На остальных векторах данное отображение строится из свойства билинейности. Обычно в качестве тензорного произведения пространств рассматривают именно такое построение, при этом не указывая явно билинейное отображение, а вместо этого описывая правила обращения со знаком тензорного произведения «$\otimes$»: дистрибутивность относительно сложения и вынесение числового множителя. Важно помнить об отсутствии коммутативности. Мы также будем использовать далее такую конструкцию.

Пример 1.7 *Рассмотрим два линейных пространства над полем действительных чисел: пространство*

V с базисом (v_1, v_2) и пространство W с базисом (w_1, w_2, w_3). Тогда их тензорное произведение $V \otimes W$ будет шестимерным пространством с базисом $(v_1 \otimes w_1, v_1 \otimes w_2, v_1 \otimes w_3, v_2 \otimes w_1, v_2 \otimes w_2, v_2 \otimes w_3)$. Любой вектор этого пространства будет иметь в

$$\begin{gathered} x = \sum_{i=1}^{2} \sum_{j=1}^{3} \alpha_{ij} v_i \otimes w_j = \\ \alpha_{11} v_1 \otimes w_1 + \alpha_{12} v_1 \otimes w_2 + \alpha_{13} v_1 \otimes w_3 + \\ + \alpha_{21} v_2 \otimes w_1 + \alpha_{22} v_2 \otimes w_2 + \alpha_{23} v_2 \otimes w_3, \end{gathered} \tag{2.1}$$

$\alpha_{ij} \in \mathbb{R}$.

Также можно рассматривать и произвольные вектора вида $x \otimes y$ и их линейные комбинации, при этом оперируя со знаком тензорного произведения также, как с обычным умножением, исключая коммутативность. Такие вектора легко записать в виде 1.7:

$$(3v_1 + 4v_2) \otimes (5w_1 + 6w_3) - v_2 \otimes v_3 =$$

$$= 15 v_1 \otimes w_1 + 18 v_1 \otimes w_3 + 20 v_2 \otimes w_1 + 23 v_2 \otimes w_3.$$

В силу ассоциативности определения тензорного произведения, т.е. $(U \otimes V) \otimes W$ изоморфно $U \otimes (V \otimes W)$, можно рассматривать тензорные произведения любого конечного числа пространств $V_1 \otimes V_2 \otimes \ldots \otimes V_n$. Важными представителями векторов такого пространства являются вектора, представимые в виде

$$x_1 \otimes x_2 \otimes \ldots \otimes x_n \tag{2.2}$$

Такие вектора имеют различные названия: разложимые, сепарабельные, мономы. В квантовой информатике состояния, соответствующие этим векторам, называются незапутанными. О таких состояниях речь пойдет в соответствующем параграфе.

Задача 1.8 *Приведите пример неразложимого вектора, для тензорного произведения пространств из Примера 1.7.*

2 Тензорное произведение операторов.

Определим тензорное произведение линейных операторов. Пусть даны два линейных пространства V и W над общим полем с базисами e_i и f_j. Тензорным произведением операторов $A : V \to V$ и $B : W \to W$ называется линейный оператор $A \otimes B : V \otimes W \to V \otimes W$, определенный на базисных векторах естественным образом: $(A \otimes B)(e_i \otimes f_j) = (Ae_i) \otimes (Bf_j)$.

Задача 2.1 *Докажите, что данное выше определение подходит под формальное определение 1.1 для пространств линейных операторов. (Необходимо построить соответствующие билинейное отображение.)*

Задача 2.2 *Пусть в данном выше определении в базисах e_i и f_j операторы A и B имеют матрицы $\{a_{ij}\}$ и $\{b_{ij}\}$ соответственно. Как будет выглядеть матрица оператора $A \otimes B$ в базисе $e_i \otimes f_j$ (тензорное произведение матриц).*

Задача 2.3 *Найти $tr(A \otimes B)$.*

Задача 2.4 *Найти $det(A \otimes B)$..*

Задача 2.5 **Матрица оператора Адамара имеет вид*

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Найдите формулу для (i,j)-го элемента матрицы $H^{\otimes n} = \underbrace{H \otimes \ldots \otimes H}_{n}$.

Задача 2.6 *Если обе матрицы A и B: а) унитарны б) эрмитовы в) положительно определены, то и матрица* $A \otimes B$ *обладает тем же свойством.*

3 Обозначения Дирака.

Для работы с тензорами в квантовой механике и особенно в квантовой информатике приняты удобные обозначения – обозначения Дирака. Пусть имеется гильбертово линейное пространство V, т.е. пространство со скалярным произведением, возможно бесконечномерное. В нашей книге мы ограничимся конечномерными пространствами. Будем обозначать вектора из пространства V как $|x\rangle$ («кет-вектор»), а соответствующие (см. параграф 2) вектора из сопряженного пространства V^* как $\langle x|$ (бра-вектор). В конечномерном пространстве это будет соответствовать обычному сопряжению вектора. Таким образом $\langle x||y\rangle$ - будет обозначать скалярное произведение. Для простоты одну из двух средних черт опускают и записывают $\langle x|y\rangle$. Например, можно рассмотреть трехмерное пространство с ортонормированным базисом $|1\rangle, |2\rangle, |3\rangle$. Тогда любой вектор пространства можно записать как $|v\rangle = x|1\rangle + y|2\rangle + z|3\rangle$, а условие ортонормированности выглядит, как $\langle i|j\rangle = \delta_{ij}$.

Теперь рассмотрим пространство $\underbrace{V \otimes \ldots \otimes V}_{p}$. Тогда базисом этого пространства будут вектора $|i_1\rangle \otimes |i_2\rangle \otimes \ldots \otimes |i_n\rangle$. Для векторов такого пространства обозначения Дирака допускает еще одно упрощение: вектора вида $|i_1\rangle \otimes |i_2\rangle \otimes \ldots \otimes |i_n\rangle$ можно записывать, как

$|i_1\rangle|i_2\rangle\dots|i_n\rangle$ или даже $|i_1 i_2 \dots i_n\rangle$. Т.е. можно убирать знак тензорного произведения и конструкцию $\rangle|$, если это не мешает читаемости и не производит путаницы, что к какому пространству относится (т.к. знак тензорного произведения векторов некоммутативен). В некоторых случаях можно для читаемости отделять индексы запятыми: $|i_1, i_2, \dots, i_n\rangle$.

4 Тензоры.

Пусть V – n-мерное векторное пространство над полем K.

Определение 4.1 *Пространство*

$$T^p_q(V) = \underbrace{V \otimes \dots \otimes V}_{p} \otimes \underbrace{V^* \otimes \dots \otimes V^*}_{q}$$

называется пространством тензоров типа (p, q) *на* V. $T^0_0(V)$ *полагают равным* K.

Задача 4.2 *Какова размерность* $T^p_q(V)$*?*

Важным примером, который еще ни раз встретится нам в книге является пространство тензоров типа (1,1). Читатель уже может догадаться, что это пространство представляет собой пространство линейных операторов, действующих в V. И действительно, каждый элемент пространства представляет собой линейную комбинацию элементов вида $x \otimes \alpha(.)$, где $\alpha(.)$ – линейный функционал, действующий в V. Если подействовать такой конструкцией на вектор y пространства V получим $x \otimes \alpha(y) = kx$, где k – элемент поля.

Если пространство гильбертово, то эквивалентность тензоров (1,1) операторам увидеть еще проще. Пусть V – гильбертово n-мерное пространство с ортонормированным базисом $(|1\rangle, |2\rangle, \dots, |n\rangle)$. Пространство тензоров (1,1) - это пространство $T_1^1 = V \otimes V^*$. Базис пространства V^* будет $(\langle 1|, \langle 2|, \dots, \langle n|)$. Общий вид состояния из T_1^1 будет $M = \sum\limits_{i,j=1}^{n} a_{ij}|i\rangle\langle j|$. Подействуем M на какое-либо базисное состояние $|k\rangle$:

$$M|k\rangle = \sum_{i,j=1}^{n} a_{ij}|i\rangle\langle j||k\rangle = \sum_{i}^{n} a_{ik}|i\rangle.$$

Как можно видеть M – линейный оператор. Причем матрица m_{ij} оператора M будет иметь элементы $m_{ij} = \langle i|M|j\rangle = a_{ij}$.

Т.е. запись $\sum\limits_{i,j=1}^{n} a_{ij}|i\rangle\langle j|$ можно рассматривать как матрицу.

Задача 4.3 *Как в дираковских обозначениях будет выглядеть диагональная матрица?*

Пример 4.4 *Рассмотрим пространство* $\mathbb{R}^2$ *со стандартным скалярным произведением с ортонормированным базисом* $(|0\rangle, |1\rangle)$. *Вектор* $|0\rangle$ *будет соответствовать вектору* $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$, *а вектор* $|1\rangle$ *вектору* $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$.

Рассмотрим матрицу

$$M = \begin{pmatrix} 1 & 0 \\ 3 & 4 \end{pmatrix}$$

и вектор

$$v = \begin{pmatrix} 2 \\ 5 \end{pmatrix} = 2|0\rangle + 5|1\rangle,$$

Тогда

$$Mv = \begin{pmatrix} 2 \\ 26 \end{pmatrix}.$$

Теперь в Дираковских обозначениях: $Mv = (|0\rangle\langle 0| + 3|1\rangle\langle 0| + 4|1\rangle\langle 1|)(2|0\rangle + 5|1\rangle) = = 2|0\rangle + 6|1\rangle + 20|1\rangle$.

Как мы видим вычисления эквивалентны. Нередко даже в матричных случаях для разреженных матриц удобнее использовать дираковские обозначения.

Задача 4.5 *Произвести такие же вычисления, как в предыдущем примере для* $M = \begin{pmatrix} 1 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 3 & 0 & 0 & 4 \end{pmatrix}$, $v = \begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \end{pmatrix}$

Опишем более точно производимые нами операции. Рассмотрим отображение $T_q^p \to T_{q-1}^{p-1}$, задаваемое на разложимых векторах как

$$x_1 \otimes x_2 \otimes \ldots \otimes x_p \otimes \alpha_1 \otimes \alpha_2 \otimes \ldots \otimes \alpha_q \mapsto$$

$$\mapsto \alpha_q(x_p) x_1 \otimes x_2 \otimes \ldots \otimes x_{p-1} \otimes \alpha_1 \otimes \alpha_2 \otimes \ldots \otimes \alpha_{q-1}.$$

Такое отображение называется сверткой, очевидно, что оно линейно. Можно производить свертку не только по последним, но и по любой другой паре пространств. Когда мы действуем элементом пространства $V \otimes V^*$ на элемент пространства V мы сначала «прикрепляем» его при помощи тензорного произведения, а затем производим свертку. В связи с произвольным выбором пары пространств для свертки при работе со сложными выражениями в кет-бра обозначениях важно помнить, что и с чем мы хотим сворачивать. Поэтому часто удобно индексировать пространства, например: $\big(|x\rangle_1\langle 0|_2|0\rangle_3 + |y\rangle_1\langle 1|_2|1\rangle_3\big)|1\rangle_4$ - вектор из пространства T_2^2. Произведем свертку по 2 и 4 пространствам и получим $|y\rangle_1|1\rangle_3$. Во многих случаях написание индексов довольно удобно и, например, позволяет переставлять пространства местами.

Задача 4.6 *Какой вектор будет являться сверткой*

$$\big(|0\rangle_1|0\rangle_2 + |1\rangle_1|1\rangle_1\big)\big(\langle 0|_3\langle 0|_4 + \langle 1|_3\langle 1|_4\big) \in T_2^2$$

по 1 и 4 пространствам. Какому пространству будет принадлежать этот вектор?

5 Многокудитные квантовые состояния

В основе принципа работы квантового компьютера лежит понятие кубит (qubit). Термин происходит от произношения «q-bit», сокращения от quantum bit. Кубит - математическое представление двухуровневой квантовой системы. Состояние кубита - нормированный вектор в гильбертовом пространстве $H = \mathbb{C}^2$ со стандартным скалярным произведением. В качестве базиса при описании кубита берется ортонормированный базис $(|0\rangle, |1\rangle)$. Таким образом состояние кубита - это нормированная суперпозиция базисных состояний: $|\psi\rangle = c_0|0\rangle + c_1|1\rangle, |c_0|^2 + |c_1|^2 = 1$. Комплексные коэффициенты c_0 и c_1 называются амплитудами. Возможность нахождения в суперпозиции является первым фундаментальным отличием кубита от классического бита, однако, возможности работы с этой суперпозицией имеют весьма серьезные ограничения.

Мы не можем достоверно узнать в каком состоянии находится кубит. Имеется возможность лишь измерить его, получив в результате $|0\rangle$ с вероятностью $|c_0|^2$ и $|1\rangle$ с вероятностью $|c_0|^2$. Подробнее об измерениях будет рассказано в соответствующем разделе.

Вторым фундаментальным отличием является то, что состояние нескольких кубитов лежит не в декартовом, а в тензорном произведении пространств кубитов. Т.е. состояние n-кубитов – нормированный вектор в пространстве $H^{\otimes n}$.

Следствием этого удивительного факта является экспоненциальный рост размерности пространства состояний в зависимости от числа кубитов (см. Задачу 1.4).

Итак, базисные состояния пространства n кубитов имеют вид

$$|i_1\rangle \otimes |i_2\rangle \otimes \ldots \otimes |i_n\rangle$$

или, что проще $|i_1 i_2 \ldots i_n\rangle$, где $i_j \in 0, 1$. Такой базис называют вычислительным.

А общий вид многокубитного состояния будет:

$$|\psi\rangle = \sum_{i_1, i_2, \ldots, i_n = 0}^{1} a_{i_1 i_2 \ldots i_n} |i_1 i_2 \ldots i_n\rangle,$$

$$|\psi\rangle = \sum_{i_1, i_2, \ldots, i_n = 0}^{1} |a_{i_1 i_2 \ldots i_n}|^2 = 1.$$

По аналогии с кубитом часто используется термин кудит - d-уровневая квантовая система. Состояния кудита – нормированные вектора в пространстве $\mathbb{C}^d$. Вычислительный ортонормированный базис обозначают, как $|0\rangle, |1\rangle, \ldots, |n-1\rangle$ или $|1\rangle, |2\rangle, \ldots, |n\rangle$. Трехуровневые и четырехуровневые системы называют кутрит и кукварт соответственно.

Для сопоставления с обычной записью векторов используется лексикографический порядок, т.е. обычные вектора упорядочены

$$(1, 0, \ldots, 0),$$

$$(0, 1, \ldots, 0),$$

$$\ldots$$

$$(0, 0, \ldots, 1),$$

а соответствующий им порядок многокудитного (или многокубитного) состояния задается лексикографически. Для кутритов с базисом

$$|0\rangle, |1\rangle, \ldots, |n-1\rangle$$

базисные вектора будут упорядочены так:

$$|000\rangle, |001\rangle, |002\rangle, |010\rangle, \ldots, |222\rangle.$$

Как можно заметить, если базис нумеруется с $|0\rangle$, то при лексикографическом порядке число внутри базисного кет-вектора – это d-ичное представление порядкового номера этого вектора плюс единица. В связи с этим состояние системы n кубитов иногда записывают как $|\psi\rangle = \sum\limits_{i=0}^{2^n-1} c_i|i\rangle$, подразумевая под i его двоичное представление.

Лексикографического правила стоит придерживаться и в случае системы кудитов с разными размерностями.

Пример 5.1 *Четырехкубитное базисное состояние* $|0101\rangle$ *будет соответствовать вектору (0,0,...,1,...,0) длины 16 с единицей на* $4 + 1 + 1 = 6$ *позиции.*

Задача 5.2 *Рассмотрим пространство трех кудитов разных размерностей* $\mathbb{C}^{10} \otimes \mathbb{C}^{11} \otimes \mathbb{C}^{12}$. *Какому вектору будет соответствовать базисный вектор* $|6,3,7\rangle$?. *Какому состоянию трехкудитной системы будет соответствовать вектор, у которого на 11, 125 и 531 позициях стоит* $1/\sqrt{3}$, *а в остальных позициях нули?*

Задача 5.3 *Даны состояния* $|\psi_0\rangle = |0\rangle$, $|\psi_1\rangle = \frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle$, $|\psi_2\rangle = \frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle$. *Найти* $\langle\psi_0|\psi_1\rangle$, $\langle\psi_1|\psi_2\rangle$, $\langle\psi_0|\psi_2\rangle$.

Задача 5.4 *Записать состояния из прошлой задачи в базисе Адамара:* $|\overline{0}\rangle = 1/\sqrt{2}(|0\rangle + |1\rangle)$, $|\overline{1}\rangle = 1/\sqrt{2}(|0\rangle - |1\rangle)$.

6 Преобразования квантовых состояний

Над квантовыми состояниями, описанными выше, можно производить унитарные преобразования. Унитарность гарантирует что мы не нарушим условие нормировки.

Преобразования в квантовой информатике записываются обычно в матричной форме. Однако, преобразовывать вектора состояний в матричную запись, умножать на матрицу, а затем преобразовывать обратно в кет-бра обозначения не всегда удобно, особенно, когда матрицы преобразований разрежены.

Посмотрим, как действуют матрицы на вектора в обозначениях Дирака на примере двухкубитных состояний. Важно помнить про лексикографический порядок векторов, который сохраняется и в записи матриц. Рассмотрим произвольную матрицу двухкубитных преобразований:

$$U = \left(\begin{array}{c|cccc} & |00\rangle & |01\rangle & |10\rangle & |11\rangle \\ \hline & & & & \\ |00\rangle & u_{00} & u_{01} & u_{02} & u_{03} \\ |01\rangle & u_{10} & u_{11} & u_{12} & u_{13} \\ |10\rangle & u_{20} & u_{21} & u_{22} & u_{23} \\ |11\rangle & u_{30} & u_{31} & u_{32} & u_{33} \end{array}\right) \qquad (2.3)$$

Такая матрица, действуя на базисное состояние, переводит его в соответствующий столбец, например: $|01\rangle$ в $u_{01}|00\rangle + u_{11}|01\rangle + |10\rangle u_{21} + |11\rangle u_{31}$.

Задача 6.1 *Примените к состоянию* $|\psi\rangle = c_0|0\rangle + c_1|1\rangle$ *преобразование*

$$NOT = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Задача 6.2 *Примените к состоянию* $|\psi\rangle = c_{00}|00\rangle + c_{01}|01\rangle + c_{10}|10\rangle + c_{11}|11\rangle$ *оператор*

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

а) преобразовав состояние к вектору-столбцу и умножив на матрицу; б) определив, во что переходят базисные состояния под действием матрицы.

Замечание 6.3 *Иногда, чтобы сохранялась многочастичная структура преобразования, элементы абстрактной матрицы двухчастичного преобразования удобнее записывать не как* u_{ij}, *а как* u_{kl}^{mn}, *например,* u_{32} u_{11}^{10}. *Особенно, такая запись удобна, при большем количестве кубитов или кудитов. Такие обозначения будут удобны при решении некоторых задач данного параграфа.*

Тензорный формализм позволяет легко применять однокубитные преобразования к двухкубитным системам. Если однокубитные операторы из $H_U \otimes H_U^*$, действуют на первый кубит состояния из $H_1 \otimes H_2$, то мы производим свертку пространств H_U^* с H_1.

Если рассматривать матрицу, как преобразование базиса (как делалось выше), то применять такие преобразования очень просто:

Пример 6.4 *Применим преобразование*

$$U = \begin{pmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{pmatrix}$$

к первому кубиту состояния $|\psi\rangle = c_0|00\rangle + c_1|11\rangle$.

Оператор U *переводит* $|0\rangle$ *в* $u_{00}|0\rangle + u_{10}|1\rangle$, *а* $|1\rangle$ *в* $u_{01}|0\rangle + u_{11}|1\rangle$, *таким образом*

$$U|\psi\rangle = c_0(u_{00}|0\rangle + u_{10}|1\rangle)|0\rangle + c_1(u_{01}|0\rangle + u_{11}|1\rangle)|1\rangle =$$

$$= c_0u_{00}|00\rangle + c_1u_{01}|01\rangle + c_0u_{10}|10\rangle + c_1u_{11}|11\rangle.$$

Задача 6.5 *Покажите, что применение оператора* U *к первой частице двухчастичной чистемы эквивалентно применению* $U \otimes I$ *ко всей системе.*

Задача 6.6 *Проведите вычисления из Примера 6.4 в матричной форме, используя результат предыдущей задачи.*

Задача 6.7 *Существует ли унитарное преобразование, которое переводит состояние* $|000\rangle$ *в* $\frac{1}{\sqrt{2}}(i|001\rangle + |111\rangle)$, *а состояние* $\frac{1}{2}|000\rangle + \frac{\sqrt{3}}{2}|010\rangle$ *в* $\frac{1}{\sqrt{2}}(i|001\rangle + |101\rangle)$? *Если да, то привести пример такого преобразования.*

В следующих задачах используются:

- базис Адамара: $|\overline{0}\rangle = 1/\sqrt{2}(|0\rangle + |1\rangle)$, $|\overline{1}\rangle = 1/\sqrt{2}(|0\rangle - |1\rangle)$;

- преобразование Адамара:

$$H = 1/\sqrt{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix};$$

- Преобразование Тоффоли:

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

Задача 6.8 *Применить к первому и второму кубитам состояния* $\frac{1}{\sqrt{3}}(|000\rangle + |001\rangle + |111\rangle)$ *преобразование Адамара, затем к первому и третьему кубитам этого состояния применить двухкубитное унитарное преобразование* $U = \{u_{ij}\}$.

Задача 6.9 *Записать преобразование Адамара в базисе Адамара.*

Задача 6.10 *записать преобразование Тоффоли в базисе Адамара для первого и второго кубитов, и в вычислительном базисе для третьего кубита.*

Задача 6.11 * *Имеется многокубитное состояние*

$$|\psi\rangle = \sum_{i_1,i_2,\ldots,i_n=0}^{1} a_{i_1 i_2 \ldots i_n} |i_1 i_2 \ldots i_n\rangle$$

и унитарная матрица

$$U_k = \begin{pmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{pmatrix}.$$

Матрица U_k *действует на* $k-$ *кубит состояния* $|\psi\rangle$, *преобразуя его в*

$$|\varphi\rangle = \sum_{i_1,i_2,\ldots,i_n=0}^{1} b_{i_1 i_2 \ldots i_n} |i_1 i_2 \ldots i_n\rangle.$$

Выразить амплитуды $b_{i_1 i_2 \ldots i_n}$ *конечного состояния через амплитуды начального состояния и элементы матрицы* U_k.

Дополнительно:

а) U_k *размера* $d \times d$ *действует на многокудитное состояние*

$$|\psi\rangle = \sum_{i_1,i_2,\ldots,i_n=1}^{d} b_{i_1 i_2 \ldots i_n} |i_1 i_2 \ldots i_n\rangle;$$

б) Преобразование производится двухкубитной матрицей $U_{k,l}$ *над* k*-м и* l*-м кубитами.*

7 Фаза

Т.к. при измерениях играют роль модули квадратов амплитуд квантовых состояний, а преобразования квантовых состояний являются линейными, состояния отличающиеся лишь на общий фазовый множитель $e^{i\varphi}$ считаются эквивалентными (т.к. нет никакой физической возможности отличить их друг от друга). Однако важно помнить, что относительный фазовый множитель играет важную роль: например, состояния базиса Адамара

$1/\sqrt{2}(|0\rangle + |1\rangle)$ и $1/\sqrt{2}(|0\rangle - |1\rangle)$ легко отличить друг от друга, применив преобразование Адамара, а потом измерив в вычислительном базисе.

Задача 7.1 *Сколькими действительными параметрами можно задать состояние кубита? n кубитов? n кудитов размерности d?*

Глава 3

Измерения квантовых состояний

Важным свойством квантовых состояний является то, что мы не можем узнать амплитуды состояния. Мы можем лишь проводить *квантовые измерения*. Простейший тип измерений квантового состояния $|\varphi\rangle$ описывается следующим образом: зафиксируем некоторый ортонормированный базис пространства состояний $|\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_n\rangle$. Тогда измерение в этом базисе – случайная величина со значениями $|\psi_i\rangle$ и вероятностями $|\langle\varphi|\psi_i\rangle|^2$. Т.е. в результате измерения состояние $|\varphi\rangle$ перейдет в $|\psi_i\rangle$ (и мы будем знать об этом) с вероятностью $|\langle\varphi|\psi_i\rangle|^2$. Чаще всего рассматривают измерения в вычислительном базисе: при таком измерении исходами будут состояния вычислительного базиса с вероятностями равными квадрату модуля соответствующей амплитуды.

Задача 0.2 *Покажите, что процесс измерения не может быть описан унитарным преобразованием.*

Существуют различные формальные подходы к описанию квантовых измерений. Далее мы рассмотрим три таких подхода: проективные измерения, измерения общего вида, POVM-измерения. Эти типы измерений полностью эквивалентны друг другу.

1 Измерения общего вида

Измерения общего вида описываются набором операторов $\{M_m\}$. Вероятность получения результата m при измерении равна

$$p(m) = \langle\psi|M_m^* M_m|\psi\rangle.$$

После измерения система перейдет в

$$\frac{M_m|\psi\rangle}{\sqrt{p(m)}}.$$

Запомнить эти формулы довольно легко: мы рассматриваем ненормированный вектор $|m\rangle = M_m|\psi\rangle$. Квадрат нормы этого вектора $\langle m|m\rangle$ - вероятность, а его нормированный вариант – состояние после измерения.

Единственным условием, которому должны удовлетворять операторы $\{M_m\}$ является условие полноты: $\sum\limits_m M_m^* M_m = I$. Смысл этого условия заключен в следующей задаче.

Задача 1.1 *Покажите, что* $\sum\limits_m p(m) = 1$.

Задача 1.2 *Дан кубит* $|\psi\rangle = a_o|0\rangle + a_1|1\rangle$. *Покажите, что операторы* $M_0 = |0\rangle\langle 0|$ *и* $M_1 = |1\rangle\langle 1|$ *описывают обычное измерение в вычислительном базисе.*

Задача 1.3 *Покажите, что два измерения общего вида* $\{M_m\}$ *и* $\{L_l\}$.*, производимых друг за другом, эквивалентны одному измерению* $\{M_m L_l\}$.

2 Проективные (ортогональные) измерения

Рассмотрим эрмитов оператор M, называемый *наблюдаемой.* Пусть $M = \sum_m mP_m$ – его спектральное разложение. P_m – проекторы на собственные подпространства, m – собственные числа.

При измерении мы с вероятностью $p(m) = \langle\psi|P_m|\psi\rangle$ получим состояние $\frac{P_m|\psi\rangle}{\sqrt{p(m)}}$.

Задача 2.1 *Покажите, что проективные измерения являются частным случаем измерений общего вида.*

Задача 2.2 *Покажите, что повторение проективного измерения не меняет состояние.*

Задача 2.3 *Приведите пример непроективного измерения.*

3 Эквивалентность проективных и общих измерений

На самом деле проективные и ортогональные измерения сводятся друг к другу добавлением анциллы (дополнительного кудита) и запутывающими унитарными преобразованиями.

Задача 3.1 *Показать, что схема* добавление анциллы к системе $\to$ совместное унитарное преобразование анциллы и системы $\to$ ортогональное измерение анциллы *может быть описано общим (неортогональным) измерением системы.[4]*

Задача 3.2 *Показать, что любое измерение общего вида может быть представлено схемой* добавление анциллы к системе $\to$ совместное унитарное преобразование анциллы и системы $\to$ ортогональное измерение анциллы.*[4]*

Глава 4

Матрицы плотности

1 Матрица плотности как ансамбль квантовых состояний

Пусть квантовая система находится в одном из квантовых состояний $|\psi_i\rangle$ с вероятностью p_i. Такую систему называют *ансамблем* или *смесью* чистых квантовых состояний.

Матрицей (или *оператором*) плотности такой смеси называют:

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|.$$

Задача 1.1 *Если состояния* $|\psi\rangle$ *принадлежат пространству* H, *то какому пространству будет принадлежать оператор плотности, описывающий их смесь? Какова размерность этого пространства?*

Задача 1.2 *Пусть имеется смесь состояний* $|0\rangle$ *с вероятностью* $1/3$ *и* $1/\sqrt{2}(|0\rangle + |1\rangle)$ *с вероятностью* $2/3$ *запишите матрицу плотности этой смеси.*

Задача 1.3 *Пусть имеется смесь состояний* $|00\rangle$ *с вероятностью* $1/3$ *и* $1/\sqrt{2}(|00\rangle+|11\rangle)$ *с вероятностью* $2/3$ *запишите матрицу плотности этой смеси.*

Задача 1.4 *Докажите следующие два свойства:*

Свойство 1.5 *Оператор плотности имеет единичный след.*

Свойство 1.6 *Оператор плотности является неотрицательно определенным.*

Задача 1.7 *Докажите, что смесь состояний* ρ_i *с вероятностями* p_i *можно описать матрицей плотности* $\sum\limits_i p_i\rho_i$.

Задача 1.8 *Пусть вся система меняется под действием некоторого унитарного оператора* U, *тогда* ρ *меняется следующим образом:*

$$\rho \xrightarrow{U} U\rho U^*.$$

Задача 1.9 *Доказать, что при измерении* ρ, *описываемом операторами* $\{M_m\}$, *вероятность получить исход* m *будет*

$$p(m) = tr(M^*M),$$

а состояние перейдет в

$$\rho_m = \frac{M_m\rho M_m^*}{p(m)}.$$

Задача 1.10 *Единственно ли представление матрицы плотности в виде взвешенной суммы чистых состояний?*

2 Чистые и смешанные состояния

Квантовые состояния, соответствующие векторам, называются *чистыми*, остальные – *смешанными*. Т.е. матрица плотности, представимая в виде $|\psi\rangle\langle\psi|$ - является чистой.

Замечание 2.1 *Иногда под термином «смешанные состояния» подразумевают матрицы плотности (как чистые, так и смешанные), в противовес векторам состояний - чистым состояниям. Обычно из контекста ясно, какое из значений термина имеется ввиду.*

Указание. Для решения следующих задач данного параграфа удобно использовать спектральное разложение матрицы плотности.

Задача 2.2 *Доказать, что* $Tr(\rho^2) \leq 1$.

Задача 2.3 *Докажите, что следующие утверждения про матрицу плотности* ρ *эквивалентны (критерии чистоты состояния):*

а) ρ *– чистая;*
б) $rank(\rho) = 1$;
в) $\rho^2 = \rho$;
г) $Tr(\rho^2) = 1$.

Задача 2.4 *Доказать, что множество матриц плотности выпукло и его граничными точками являются чистые состояния.*

Глава 5

Редуцированная матрица плотности

Важным применением матриц плотности является то, что при помощи них можно описывать состояния подсистем составных (многочастичных) квантовых систем, что невозможно сделать при помощи векторов состояний.

Для начала нам необходимо дать понятие частичного следа оператора.

1 Частичный след

Рассмотрим матрицу плотности $\rho \in H \otimes H^*$. Вспомним, что след матрицы – это сумма диагональных элементов, и как хорошо известно, след не зависит от выбора базиса. Можно вычислить след пользуясь вычислительным базисом пространства H :

$$Tr(\rho) = \sum_i \langle i|\rho|i\rangle.$$

Теперь рассмотрим двухчастичные состояния. Чистые вектора-состояния принадлежат пространству $H_A \otimes H_B$, а матрицы плотности, соответственно, $H_A \otimes H_B \otimes H_A^* \otimes H_B^*$. Рассмотрим матрицу плотности $\rho_{AB} \in H_A \otimes H_B \otimes H_A^* \otimes H_B^*$. $\{|i\rangle_A\}$ и $\{|i\rangle_B\}$ – базисы пространств H_A и H_B соответственно.

След ρ_{AB}, соответственно, будет равен:

$$Tr(\rho_{AB}) = \sum_{ij} \langle j|_B \langle i|_A \rho_{AB} |i\rangle_A |j\rangle_B.$$

Используя двухчастичную структуру матрицы можно ввести понятие частичного следа.

Определение 1.1 Частичным следом *матрицы ρ по пространству H_A называется*

$$Tr_A(\rho_{AB}) = \sum_i \langle i|_A \rho_{AB} |i\rangle_A.$$

Матрицы $\rho_B = Tr_A(\rho_{AB})$ и $\rho_A = Tr_B(\rho_{AB})$ называются редуцированными матрицами плотности матрицы ρ_{AB}.

Замечание 1.2 *Операция частичного определена, конечно же, для произвольных матриц, а не только матриц плотности.*

Задача 1.3 *Убедитесь, что $\rho_A \in H_A$, $\rho_B \in H_B$.*

2 Вычисление частичного следа матрицы.

Рассмотрим три способа вычисления частичного следа матрицы.

1. Если матрицу удобнее записывать в дираковских обозначениях, то вычислять редуцированную матрицу плотности удобнее по определению.

Пример 2.1 *Пусть H_A и H_B – 20-мерные гильбертовы пространства с вычислительным базисом $|1\rangle, \ldots, |20\rangle$. Пусть дана матрица (не являющаяся матрицей плотности) $M = |3\rangle_A|5\rangle_B\langle 3|_A\langle 6|_B + 2|7\rangle_A|8\rangle_B|7\rangle_A|11\rangle_B$.*

Подставим первое слагаемое в записи матрицы в определение Tr_A, получим:

$$\sum_{i=1}^{5} \langle i|_A|3\rangle_A|5\rangle_B\langle 3|_A\langle 6|_B|i\rangle_A.$$

Ненулевым будет только 3-й член суммы $\langle 3|_A|3\rangle_A|5\rangle_B\langle 3|_A\langle 6|_B|3\rangle_A = |5\rangle_B\langle 6|_B$. Во втором слагаемом останется только $|7\rangle_B\langle 11|_B$.

Таким образом мы получим $Tr_A(M) = |5\rangle_B\langle 6|_B + 2|8\rangle_B\langle 11|_B$. Аналогично вычислив, получим $Tr_B(M) = 0$.

Задача 2.2 *Вычислить по определению частичные следы для матрицы:*

$$\rho = |1\rangle_A|2\rangle_B\langle 1|_A\langle 3|_B + 5|2\rangle_A|8\rangle_B|4\rangle_A|8\rangle_B + 3|2\rangle_A|2\rangle_B|2\rangle_A|3\rangle_B$$

Такой метод вычисления можно выразить формулой: пусть имеется матрица $M = \sum\limits_{i,j,k,l} a_{ijkl}|i\rangle_A|j\rangle_B\langle k|_A\langle l|_B$, тогда $Tr_A(M) = \sum\limits_{i,j,l} a_{ijil}|j\rangle_B\langle l|_B$.

2. Второй метод является аналогом первого, но в случае матричной записи. Рассмотрим матрицу плотности двухкубитного состояния. Общий вид такой матрицы будет $M = \sum\limits_{i,j,k,l=0}^{1} a_{ijkl}|i\rangle_A|j\rangle_B\langle k|_A\langle l|_B$, что в матричной записи будет

$$\begin{pmatrix} a_{0000} & a_{0001} & a_{0010} & a_{0011} \\ a_{0100} & a_{0101} & a_{0110} & a_{0111} \\ a_{1000} & a_{1001} & a_{1010} & a_{1011} \\ a_{1100} & a_{1101} & a_{1110} & a_{1111} \end{pmatrix}.$$

Рассмотрим Tr_B. Первое слагаемое в сумме частичного следа будет

$$\langle 0|_A M|0\rangle_A$$

– это подматрица, где в индексах на первом и третьем местах стоит 0 - т.е. блок 2×2

$$\begin{pmatrix} a_{0000} & a_{0001} \\ a_{0100} & a_{0101} \end{pmatrix},$$

стоящий в верхнем левом углу на диагонали. Аналогично

$$\langle 1|_A M|1\rangle_A$$

– блок стоящий ниже на главной диагонали. Сложив эти блоки, получим:

$$Tr_A(M) = \begin{pmatrix} a_{0000} + a_{1010} & a_{0001} + a_{1011} \\ a_{0100} + a_{1110} & a_{0101} + a_{1111} \end{pmatrix}$$

Задача 2.3 *Аналогичным методом вычислите* $Tr_B(M)$.

Задача 2.4 **Как применять такой метод для больших размерностей? Для трехчастичных (многочастичных) систем, когда мы хотим взять частичный след по какой-либо частице? По двум частицам?*

3. Третий метод подходит для вычисления редуцированных матриц плотности чистых двухчастичных состояний.

Пусть дано чистое двухчастичное состояние $|\psi\rangle \in H_A \otimes H_B$, и нам необходимо вычислить редуцированную матрицу плотности второго кубита (т.е. частичный след по первому кубиту). Такое состояние можно представить в виде $|\psi\rangle = \sum\limits_i a_i|i\rangle|\psi_i\rangle$, где $|\psi_i\rangle \in H_B$ – нормированные состояния второго кубита, возможно неортогональные.

Задача 2.5 *Докажите, что* $\rho_B = Tr_A(|\psi\rangle\langle\psi|) = \sum\limits_i |a_i|^2|\psi_i\rangle\langle\psi_i|$.

Замечание 2.6 *В данном методе состояния* $|\psi_i\rangle$ *можно и не нормировать.*

3 Подсистемы квантовых состояний

Рассмотрим запутанное двухкубитное состояние $|\psi\rangle = 1/\sqrt{2}(|0\rangle_1|0\rangle_2 + |1\rangle_1|1\rangle_2)$. Предположим, что мы рассматриваем только первый кубит данного состояния. Может ли он быть описан вектором? Ответ на этот вопрос отрицательный.

Задача 3.1 *Покажите, что первый кубит состояния* $|\psi\rangle = 1/\sqrt{2}(|0\rangle_1|0\rangle_2 + |1\rangle_1|1\rangle_2)$ *не может быть описан вектором.*

Указание. *Необходимо рассмотреть измерения первого кубита в различных базисах. Такие измерения описываются операторами вида* $M_0 = |\widetilde{0}_1\rangle\langle\widetilde{0}_1|, M_1 = |\widetilde{1}_1\rangle\langle\widetilde{1}_1|$. *Необходимо рассмотреть несколько таких измерений и вычислить соответствующие вероятности для состояния* $|\psi\rangle$. *После чего показать, что ни один однокубитный вектор состояния не может давать таких вероятностей.*

Из предыдущей задачи следует, что вектора состояний не подходят для описания подсистем запутанных квантовых систем. Объектом, который описывает такие состояния, является редуцированная матрица плотности.

Задача 3.2 *Докажите, что произвольное измерение первого кубита дает одинаковые результаты* *для состояния* $|\psi\rangle = 1/\sqrt{2}(|0\rangle_1|0\rangle_2 + |1\rangle_1|1\rangle_2)$ *и* $\rho_A = Tr_B(|\psi\rangle\langle\psi|)$.

Задача 3.3 *Докажите, что произвольное измерение первого кудита дает одинаковые результаты для произвольного чистого двухчастичного состояния* $|\psi\rangle \in H_A \otimes H_B$ *и* $\rho_A = Tr_B(|\psi\rangle\langle\psi|) \in H_A \otimes H_A^*$.

Задача 3.4 *Докажите, что произвольное измерение первого кудита дает одинаковые результаты для произвольной двухчастичной матрицы плотности* $\rho \in H_A \otimes H_B \otimes H_A^* \otimes H_B^*$ *и* $\rho_A = Tr_B(\rho) \in H_A \otimes H_A^*$.

Задача 3.5 *** Докажите, что оператор частичного следа является единственным оператором, приводящий к правильному описанию наблюдаемых подсистемы составной системы [4]*

Таким образом, если имеется составная система (чистая или смешанная), имеющая матрицу плотности $\rho \in H_A \otimes H_B \otimes H_A^* \otimes H_B^*$, то ее подсистемы описываются соответствующими редуцированными матрицами плотности.

Глава 6

Двухчастичная запутанность квантовых состояний

1 Критерий запутанности

Пусть имеется чистое двухчастичное квантовое состояние в пространстве $H_A \otimes H_B$, $d_A = dim(H_A)$, $d_A = dim(H_A)$, $d = min(d_A, d_B)$.

$$|\psi\rangle = \sum_{i=1}^{d_A} \sum_{j=1}^{d_B} a_{ij} |i\rangle_A |j\rangle_B. \tag{6.1}$$

Напомним, что *незапутанным* называется состояние, представимое в виде $|\psi\rangle = |\psi\rangle_A \otimes |\psi\rangle_B$ (соответственно, все остальные состояния называются *запутанными*)

Задача 1.1 *Докажите, что двухчастичное состояние является запутанным тогда и только тогда, когда существуют унитарные матрицы U_A и U_B такие, что $U_A \otimes U_B |\psi\rangle = |00\rangle$.*

Как можно узнать, запутанно ли какое-либо квантовое состояние или нет? Ответ содержится в следующей задаче.

Задача 1.2 **Рассмотрим состояние 6.1 и матрицу* $A = \{a_{ij}\}$*, составленную из амплитуд этого состояния. Доказать, что состояние* $|\psi\rangle$ *запутано тогда и только тогда, когда* $rank(A) > 1$.

Указание. Если ранг матрицы равен единице, значит все ее столбцы (строки) пропорциональны друг другу.

Задача 1.3 *Запутано ли состояние* $|\varphi\rangle = 1/\sqrt{2}(|00\rangle + |11\rangle)$?

Решение. Матрица, соответствующая этому состоянию будет

$$A = \begin{pmatrix} 1/\sqrt{2} & 0 \\ 0 & 1/\sqrt{2} \end{pmatrix}$$

$rank(A) = 2$, значит состояние запутано.

Задача 1.4 *Когда будет запутано двухкубитное состояние* $|\varphi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$?

Можно рассматривать двухчастичную запутанность между различными подсистемами многочастичной системы (т.е. различными разбиениями множества пространств кудитов на два подпространства). Например для трехкубитной системы $|\varphi\rangle = \sum\limits_{i_1,i_2,i_3=0}^{1} a_{i_1 i_2 i_3}|i_1 i_2 i_3\rangle$ можно рассмотреть три различных двухчастичных запутанности: между 1 и (2 и 3) кубитами; (1 и 2) и 3 кубитом; 2 и (1 и 3) кубитами. Для проверки запутанности между 2 и (1 и 3) кубитами нужно вычислить ранг матрицы

$$\begin{pmatrix} a_{000} & a_{001} & a_{100} & a_{101} \\ a_{010} & a_{011} & a_{110} & a_{111} \end{pmatrix}.$$

Задача 1.5 *Выпишите матрицы для проверки запутанности между: а) 1 и (2 и 3) кубитами; б) (1 и 2) и 3 кубитом;*

Задача 1.6 *Пусть имеется n – кудитная система (каждый кудит размерности d). а) Какого размера будет матрица для проверки запутанности между произвольными k и l $(k + l = n)$ кудитами? б) Сколько различных разбиений такой системы на две подсистемы?*

Задача 1.7 *Исследовать на запутанность обобщенное GHZ состояние*

$$|GHZ\rangle = a_0|000\rangle + a_1|111\rangle, |a_0|^2 + |a_1|^2 = 1.$$

Решение. Исследовать на запутанность означает узнать, по каким разбиениям на два подпространства запутана система. Для данного состояния все три матрицы проверки на запутанность с точностью до перстановки столбцов и транспонирования будут равны

$$\begin{pmatrix} a_0 & 0 & 0 & 0 \\ 0 & a_1 & 0 & 0 \end{pmatrix}.$$

А значит это состояние запутано по всем подпространствам (полностью запутанно), если выполняется условие $a_0a_1 > 0$ и полностью незапутанно, если это условие не выполняется.

Задача 1.8 *Исследовать на запутанность обобщенное W состояние*

$$|W\rangle = a_0|001\rangle + a_1|010\rangle + a_2|001\rangle, |a_0|^2 + |a_1|^2 + |a_2|^2 = 1.$$

Задача 1.9 Пример. *Исследовать на запутанность состояние (в зависимости от параметров $a \neq 0, b \neq 0, c \neq 0, d \neq 0$)*

$$\frac{1}{|a|^2 + |b|^2 + |c|^2 + |d|^2}(a|000\rangle + b|010\rangle + c|101\rangle + d|111\rangle).$$

Задача 1.10 *Исследовать на запутанность n-кубитное состояние*

$$|\psi\rangle = 1/\sqrt{2^n} \sum_{i_1,i_2,\ldots,i_n=0}^{1} |i_1 i_2 \ldots i_n\rangle.$$

Задача 1.11 *Рассмотрим n-кубитное ненормированное состояние*

$$|\psi\rangle = \sum_{i=0}^{2^n} \frac{1}{2^i} |i\rangle.$$

Нормировать состояние и исследовать его на запутанность.

2 Сингулярное разложение матриц

Важную роль для запутанности двучхастичных состояний играет сингулярное разложение матриц (или SVD-разложение, от Singular Value Decomposition)

Теорема 2.1 *Для любой комплексной матрицы A размера $m \times n$ существует разложение*

$$A = U \cdot S \cdot V^*,$$

где U – унитарная матрица порядка m, V – унитарная матрица порядка n, S – диагональная матрица $m \times n$ с неотрицательными действительными числами $\{s_1, s_2, \ldots, s_n\}$ на диагонали (эти числа называют сингулярными числами матрицы A). Причем набор этих чисел однозначно определяется матрицей A.

Определение 2.2 *Столбцы матрицы $U(V)$ называются левыми (правыми) сингулярными векторами матрицы A.*

Замечание 2.3 *Обычно принято записывать диагональные элементы* $\{s_1, s_2, \ldots, s_n\}$ *матрицы* S *в порядке невозрастания, тогда и матрица* S *определена однозначно.*

Сингулярное разложение обладает множеством полезных свойств:

Задача 2.4 *Число ненулевых сингулярных чисел матрицы равно ее рангу:*

$$dim(s_i : s_i > 0) = rank(A).$$

Задача 2.5 *Покажите, что собственные значения матрицы* A^*A *являются квадратами сингулярных чисел матрицы* A. *Каковы будут собственные вектора матрицы* A^*A?

Свойство 2.6 *Пусть* $s_1 \geq s_2 \geq \ldots \geq s_n$. *Рассмотрим диагональную матрицу* S'_k *размера* $m \times n$ *с диагональными элементами* $\{s_1, s_2, \ldots, s_k, 0, 0, \ldots, 0\}$, *где* $k < n$. *Тогда матрица* $A_k = US'_K V^*$ *будет наилучшим приближением матрицы* A *среди всех матриц ранга* k *в смысле матричной нормы* $||.||_2$.

Доказательство 2.7 *Т.к. матрица* $A - A_k = US''V^*$, *где* S'' *является диагональной с элементами* $\{0, \ldots, 0, s_{k+1}, \ldots, s_n\}$, *то* $||A - A_k||_2 = s_{k+1}$. *Рассмотрим произвольную матрицу* K *ранга* k. *Ядро этой матрицы имеет размерность* $n - k$, *а размерность линейной оболочки строк* $v_1, v_2, \ldots, v_{k+1}$ *матрицы* V *равна* $k + 1$. *Т.к.* $(n - k) + (k + 1) > n$, *указанные подпространства имеют нетривиальное пересечение, и для нормированного вектора* h *из этого пересечения*

$$||A - K||_2^2 \geq ||(A - K)h||_2^2 = ||Ah||_2^2 =$$

$$= ||USV^*h||_2^2 = ||S(V^*h)||_2^2 \geq s_{k+1}^2 ||V^*h||_2^2 = s_{k+1}^2.$$

Приведенное выше свойство (аппроксимация матрицами меньших рангов) является очень важным и позволяет использовать сингулярное разложение для многоих практических задач: сжатие изображений, латентный семантический анализ, латентный семантический анализ (метод, позволяющий сравнивать текстовые документы не просто по статистике вхождения слов, но и по семантике; активно используется в текстовых поисковых системах), анализ статистических данных и др.

3 Разложение Шмидта

Пусть имеется чистое двухчастичное квантовое состояние в пространстве $H_A \otimes H_B$, $d_A = dim(H_A)$, $d_A = dim(H_A)$, $d = min(d_A, d_B)$.

$$|\psi\rangle = \sum_{i=1}^{d_A} \sum_{j=1}^{d_B} a_{ij} |i\rangle_A |j\rangle_B.$$

Как мы знаем, конечномерное гильбертово пространство изоморфно своему сопряжению, и мы можем рассматривать одно вместо другого. Заменим пространство H_B на H_B^*.

Задача 3.1 *Докажите, что пространство* $H_A \otimes H_B$ *изоморфно* $H_A \otimes H_B^*$.

Таким образом мы перешли к пространству $H_A \otimes H_B^*$. В этом пространстве состояние $|\psi\rangle$ перейдет в

$$\sum_{i=1}^{d_A} \sum_{j=1}^{d_B} a_{ij} |i\rangle_A \langle j|_B.$$

Это будет линейный оператор, действующий из H_B в H_A, с матрицей $M = \{a_{ij}\}$. Рассмотрим SVD-разложение этой матрицы:

$$M = USV^* = U\Big(\sum_{i=1}^{d} s_i |i\rangle_A \langle i|_B\Big)V^* = \sum_{i=1}^{d} s_i |\widetilde{i}\rangle_A \langle\widetilde{i}|_B,$$

где $\widetilde{i}_A$ – базис пространства H_A в которой перейдет базис i_A под действием матрицы U, а $\widetilde{i}_B$ – базис пространства H_B в которой перейдет базис i_B под действием матрицы V.

Возвращаясь к пространству $H_A \otimes H_B$, получим:

$$|\psi\rangle = \sum_{i=1}^{d} s_i |\widetilde{i}\rangle_A |\widetilde{i}\rangle_B.$$

Такое представление двухчастичных квантовых состояний и называют *разложением Шмидта*. Сформулируем его в виде теоремы.

Теорема 3.2 *Имеется чистое двухчастичное состояние в пространстве* $H_A \otimes H_B$:

$$|\psi\rangle = \sum_{i=1}^{dim(H_A)} \sum_{j=1}^{dim(H_B)} a_{ij} |i\rangle_A |j\rangle_B,$$

$$\sum_{i=1}^{dim(H_A)} \sum_{j=1}^{dim(H_B)} |a_{ij}|^2 = 1.$$

Тогда существуют ортонормированные базисы $\widetilde{i}_A$ *и* $\widetilde{i}_B$ *пространств* H_A *и* H_B *соответственно, такие, что*

$$|\psi\rangle = \sum_{i=1}^{d} \lambda_i |\widetilde{i}\rangle_A |\widetilde{i}\rangle_B,$$

где $d = min(dim(H_A), dim(H_B))$, $\lambda_i \in \mathbb{R}$, $\lambda_i \geq 0$, $\sum\limits_{i=1}^{d} \lambda_i^2 = 1$.

Действительные амплитуды λ_i называются коэффициентами Шмидта, а число ненулевых коэффициентов Шмидта – рангом Шмидта состояния.

Задача 3.3 *Чистое двухчастичное состояние запутано тогда и только тогда, когда его ранг Шмидта больше единицы.*

Ранг Шмидта может являться *мерой запутанности* двухчастичных состояний. Т.е. чем больше ранг Шмидта, тем сильнее запутано состояние. Теория мер квантовой запутанности выходит за рамки данной книги и мы не будем разбирать подробно это утверждение.

4 Разложение Шмидта и редуцированные матрицы плотности

Разложение Шмидта тесно связано со спектром редуцированных матриц плотности состояния. Кроме того, благодаря разложению Шмидта, легко увидеть связь двух матриц плотности подсистем одного состояния.

Снова запишем двухчастичное состояние в виде разложения Шмидта:

$$|\psi\rangle = \sum_{i=1}^{d} \lambda_i |\widetilde{i}\rangle_A |\widetilde{i}\rangle_B.$$

Задача 4.1 *Вычислите редуцированные матрицы плотности* $\rho_A = Tr_B(|\psi\rangle\langle\psi|)$ *и* $\rho_B = Tr_B(|\psi\rangle\langle\psi|)$.

Задача 4.2 *Убедитесь, что собственные значения матриц ρ_A и ρ_B совпадают и представляют собой квадраты коэффициентов Шмидта.*

Задача 4.3 *Убедитесь, что $|\widetilde{i}\rangle_A$ и $|\widetilde{i}\rangle_B$ являются собственными векторами ρ_A и ρ_B соответственно.*

Следствием приведенных выше свойств является важная связь понятий чистоты и незапутанности:

Задача 4.4 *Докажите, что двухчастичное состояние незапутано тогда и только тогда, когда матрицы плотности его подсистем являются чистыми.*

Кроме того, приведенные выше свойства дают алгоритм вычисления разложения Шмидта двухчастичного состояния $|\psi\rangle$ без использования SVD-разложения:

1. Вычислить редуцированные матрицы плотности $\rho_A = Tr_B(|\psi\rangle\langle\psi|)$ и $\rho_B = Tr_B(|\psi\rangle\langle\psi|)$.

2. Найти общие собственные значения a_i и соответствующие им собственные вектора $|\widetilde{i}\rangle_A$ и $|\widetilde{i}\rangle_B$ матриц ρ_A и ρ_B.

3. Разложение Шмидта будет иметь вид:

$$|\psi\rangle = \sum_{i=1}^{d} \sqrt{a_i}|\widetilde{i}\rangle_A|\widetilde{i}\rangle_B.$$

Задача 4.5 *Найти разложение Шмидта состояния* $1/5\sqrt{2}(5|00\rangle + 3|10\rangle - 4|11\rangle)$.

Задача 4.6 **(Расширение состояния до чистого) Доказать, что для любого смешанного состояния $\rho_A \in H_A \otimes H_A^*$ найдется чистое состояние $|\psi\rangle \in H_A \otimes H_B$, такое, что ρ_A является состоянием его подсистемы, т.е. $\rho_A = Tr_B(|\psi\rangle\langle\psi|)$.*

Указание. Использовать связь коэффициентов Шмидта **чистого** запутанного состояния со спектром его **смешанных** редуцированных матриц плотности.

Задача 4.7 **Какова минимальная возможная размерность пространства H_B из предыдущей задачи?*

Замечание 4.8 *Как и в случае с анализом двухчастичной запутанности, можно рассматривать разложение Шмидта многочастичной системы по двум подсистемам (разбиению множества частиц на два).*

Задача 4.9 *** На примере состояния $|W\rangle = 1/\sqrt{3}(|100\rangle + |010\rangle + |001\rangle)$ показать, что для трех кубитов не существует разложения Шмидта, т.е. $|W\rangle \neq \lambda_0|\tilde{0}\tilde{0}\tilde{0}\rangle + \lambda_1|\tilde{1}\tilde{1}\tilde{1}\rangle$. Или, что эквивалентно, не существует унитарных матриц U_1, U_2, U_3, таких, что $U_1 \otimes U_2 \otimes U_3|W\rangle = \lambda_0|000\rangle + \lambda_1|111\rangle$.*

Указание. Рассмотреть разложение Шмидта для первого кубита и двух оставшихся. Использовать его единственность.

5 Энтропия фон Неймана

Для матриц плотности важную роль играет аналог классической энтропии Шеннона - *энтропия фон Неймана*:

$$H_{vN}(\rho) = -tr(\rho \log \rho).$$

Как и в случае энтропии Шеннона, основание логарифма не играет существенной роли.

Задача 5.1 *Как вычислять энтропию фон Неймана?*

Указание. Вспомнить, как вычислять матричные функции от эрмитовых матриц.

Задача 5.2 *Вычислить энтропию фон Неймана матрицы плотности*

$$\rho = \begin{pmatrix} 2/3 & 1/3 \\ 1/3 & 1/3 \end{pmatrix}$$

Задача 5.3 *Доказать, что энтропии фон Неймана матриц плотности подсистем чистого двухчастичного состояния совпадают.*

Предыдущая задача дает возможность ввести следующие определение:

Определение 5.4 *Энтропия фон Неймана подсистем чистого двухчастичного состояния называется его* редуцированной энтропией фон Неймана.

Задача 5.5 *Доказать, что редуцированная энтропия фон Неймана состояния совпадает с энтропией Шеннона квадратов его коэффициентов Шмидта.*

Задача 5.6 *Доказать, что матрица плотности является чистой тогда и только тогда, когда $H_{vN}(\rho) = 0$. Или, что эквивалентно, двухчастичное состояние является незапутанным тогда и только тогда, когда его редуцированная энтропия фон Неймана равна нулю.*

Замечание 5.7 *Редуцированная энтропия фон Неймана, как и ранг Шмидта, может служить мерой двухчастичной запутанности.*

Литература

1. Винберг Э. Б. Курс алгебры. Факториал Пресс, 2002.

2. Деммель Д. Вычислительная линейная алгебра. МИР, 2001.

3. Колмогоров А.Н. Ф. С. Элементы теории функций и функционального анализа . Физматлит, 2006.

4. Нильсен М., Чанг И. Квантовые вычисления и квантовая информация:Пер с англ. МИР, 2006.

5. Ожигов Ю. И. Квантовые вычисления. Учебно-методическое пособие. 2003.

6. Preskill J. Lecture notes for physics 229: Quantum information and computation // California Institute of Technology. 1998.