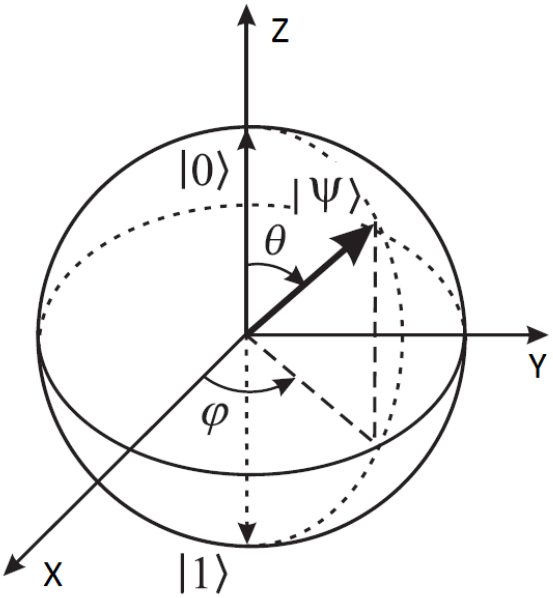
Федеральное государственное образовательное бюджетное учреждение
высшего профессионального образования.
Московский технический университет связи и информатики

Кафедра теории вероятностей и прикладной математики

Т.Э. Кренкель

ВВЕДЕНИЕ В КВАНТОВУЮ ТЕОРИЮ ИНФОРМАЦИИ

Учебное пособие



Москва 2015

Федеральное государственное образовательное бюджетное учреждение
высшего профессионального образования.
Московский технический университет связи и информатики

Кафедра теории вероятностей и прикладной математики
Кренкель Т.Э.

Допущено УМО по образованию в области
прикладной математики и управления
качеством в качестве учебного пособия
для студентов МТУСИ специальности 231300
.
Протокол №___от . . 2015 г.

ВВЕДЕНИЕ В КВАНТОВУЮ ТЕОРИЮ ИНФОРМАЦИИ

Учебное пособие

для направления подготовки

01.03.04 Прикладная математика

Москва 2016

УДК 535

Кренкель Т.Э. Введение в квантовую теорию информации: Учебное пособие/ МТУСИ.- М., 2015. – 52 с.

Квантовая теория информации (КТИ) – новый раздел науки, посвященный использованию квантовых объектов для обработки и передачи информации.

Собственно идея использования квантовых объектов для обработки и передачи информации была высказана в 80-х годах прошлого столетия Юрием Ивановичем Маниным и Ричардом Фейнманом. Далее последовал этап бурного становления и развития основных понятий теории квантовых вычислений.

Следует различать основы квантовой механики (раздела физики) и квантовой теории информации (раздела математики). Хотя основные идеи квантовой информатики повзаимствованы из квантовой механики, основное направление развития квантовой информатики связано с созданием и применением вероятностных квантовых алгоритмов.

Теория квантовой информатики является торжеством копенгагенской интерпретации квантовой механики Нильса Бора. Знаменитая дискуссия Эйнштейна-Бора 1935 года в течение почти тридцать лет служила предметом философских исследований, пока в 1965 году Джон Белл не обосновал теоретически понятие квантовой запутанности и не ввел четыре состояния Белла (первое из которых является знаменитым состоянием ЭПР (Эйнштейна-Подольского-Розена)).

Основными понятиями КТИ являются:

А) кубит – единица квантовой информации,

Б) квантовые гейты - матричные операторы, действующие на кубиты,

В) квантовая мера информации по фон Нейману, основанная на понятии матрицы плотности,

Г) запутывание кубитов и определение меры запутанности.

Из квантовой механики в КТИ перешло определение наблюдаемой как самосопряженного (эрмитова) оператора (матрицы) и обозначение Дирака состояний квантовой системы (бракет).

Из линейной алгебры в КТИ применяются такие понятия как вычислительный базис, кронекеровское (тензорное) произведение векторов и матриц и вычисление собственных чисел и векторов эрмитовых матриц.

Настоящее учебное пособие предназначено для чтения лекций по дисциплине «Теория информации» бакалаврам специальности Прикладная математика 231300.

Автор выражает благодарность Семину Е.А. и Неронову М.М., чьи бакалаврские работы легли в основу настоящего учебного пособия.

Список литературы 12 назв.

Издание утверждено Методическим советом ОТФ в качестве учебного пособия. Протокол № 4 от 5 мая 2015 г.

Рецензенты: А.В. Михалев, доктор физ.-мат.наук, профессор (МГУ)

А.Г. Кюркчан, доктор физ.-мат.наук, профессор (МТУСИ)

В.Г. Данилов, доктор физ.-мат.наук, профессор (НИУ ВШЭ)

Содержание

Часть четвертая **Квантовая запутанность.**

Введение

Современный мир сложно представить без информации. В том или ином представлении мы встречаемся с ней каждый день. Но что же конкретно такое, информация? Так, согласно теории цифровой физики, вся вселенная является информацией и может быть представлена аналогией на некоторое абстрактное вычислительное устройство[**1**]. Примерно той же концепции придерживается известный американский физик Джон Уилер, чья доктрина «всё из бита» гласит, что все физические сущности состоят из информации. А то, что мы называем реальностью, возникает из выяснения ответов на вопросы вида «да/нет»[**2**]. Как бы то ни было, наряду с материей и энергией, информация является первичным понятием нашего мира и не может быть определена в строгом смысле. Однако можно перечислить её свойства:

1) Информация приносит знания об окружающем мире, которых до её получения не было.
2) Информация нематериальна, но она проявляется в форме всевозможных материальных носителей: дискретных знаков, сигналов или даже функций времени.
3) Знаки и сигналы, являющиеся словами некоего алфавита, несут информацию только для получателя, способного распознать их.

Распознавание, в свою очередь, состоит в отождествлении сообщений с объектами и их отношениями в реальном мире. Так что информацию можно определить как результат моделирования исследуемой части реального мира.

Разделяют два наиболее распространённых вида информации:

1) Семантическая (она же смысловая) информация основана однозначной связи сигналов с объектами реального мира.
2) Синтактическая – информация, заключённая в порядке и взаимосвязи следования элементов в сообщении.

Также стоит отметить существование прагматического аспекта информации. В нём изучается практическое использование информации, её ценность для достижения поставленных целей. Однако теория меры прагматической информации пока что окончательно не разработана[**3**].

Отдельно отстоящим разделом, даже целой наукой, является квантовая теория информации. Несмотря на то, что квантовая теория информации на 21 год старше классической теории информации, серьёзное развитие этой науки началось гораздо позже. И только пару десятилетий тому назад для неё начали активно создавать экспериментальную и теоретическую основы. Благодаря развитию квантовой теории информации и квантовой физики могут быть получены эффективные способы управления и изучения различного рода микросистем на уровне их индивидуальных компонентов, невозможные для реализации на данный момент. Не исключено что, при таком накоплении знаний в этой области, в ближайшие годы произойдёт революция в квантовых технологиях, подарив нам такие вещи, как квантовый хронометр для сверхточного геопозиционирования квантовые датчики[**4**].

Часть первая. Классическая теория информации.

1.1 Мера количества информации.

Под теорией информации в математике подразумевается дисциплина, изучающая способы преобразования и передачи информации.

Впервые способ измерения информации был предложен Робертом Хартли в 1928 г.[**5**]. Эта мера была независима от способа передачи сигналов и их логического и психологического содержания. По Хартли количество информации – это неопределённость выбора, которая исчезает после

получения некоторого сообщения из множества m. Им была предложена логарифмическая мера неопределённости выбора:

$$H = k \log_a m, \tag{1.1}$$

где k – коэффициент пропорциональности, m – множество возможных сообщений, а a – константа, определяемая исходя из области применения формулы.

Идеи Хартли были пересмотрены и развиты Клодом Шенноном в работах «Математическая теория связи» и «Связь при наличии шума» в 1948, 1949гг.[**6**][**7**]. Предложенный им метод расчёта количества информации основывался на вероятности появления того или иного события из заранее заданного множества всех возможных исходов. Формула количества информации по Шеннону имеет вид:

$$I = -\sum_{i=1}^{M} P(i) \log P(i), \tag{1.2}$$

где $-P(i)\log P(i)$ – информация, приносимая i-ым случайным событием, используется в неизменном виде для большинства прикладных задач и по сей день.

Дополнительно накладываются ещё два условия:

$$\begin{cases} \sum_{i=1}^{M} P(i) = 1, 0 \le P(i) \le 1 \\ 0 \cdot \log 0 = 0 \end{cases} \tag{1.3}$$

В случае зависимости между n элементами формула приобретает общий вид:

$$I = \frac{-1}{n} \sum_{i,j,\dots,n} P(i,j,\dots,n) \log P(i,j,\dots,n) \tag{1.4}$$

Колмогоров выделял три различных подхода к введению базовых понятий информации: чисто комбинаторный, вероятностный, и алгоритмический[**8**]. Нам наиболее интересны именно вероятностные меры. К ним и относится описанная выше формула Клода Шеннона.

В математической статистике широко применяется другая вероятностная мера информации, введённая Рональдом Фишером для непрерывных распределений:

$$I=\int\left(\frac{\partial}{\partial\theta}\log f(x;\theta)\right)^2\cdot f(x;\theta)dx, \tag{1.5}$$

где θ – неизвестный параметр, от которого зависит вероятность x, а $f(x;\theta)$ – является функцией правдоподобия для θ и плотностью распределения для x.

1.2 Энтропия.

Одним из важнейших понятий теории информации является энтропия.

Остановимся подробнее на исследовании дискретных сообщений, так как именно они в основном используются в теории связи и многих других практических областях.

Дискретный источник информации характеризуется конечным множеством из M элементов с заданными для каждого элемента вероятностями его появления.

Чаще всего, при передаче обычных не зашифрованных сообщений, появление элемента x_i зависит от того, какие элементы в принятой последовательности ему предшествовали.

Так, для случая с зависимостью от одного предыдущего элемента, получаем матрицу, составленную из условных вероятностей:

$$P(x_i|x_j)=P(i|j)=\begin{Vmatrix} P(1|1) & P(1|2) & \dots & P(1|M) \\ P(2|1) & P(2|2) & \dots & P(2|M) \\ \dots & \dots & \dots & \dots \\ P(i\vee 1) & P(i\vee 2) & \dots & P(i\vee M) \\ \dots & \dots & \dots & \dots \\ P(M\vee 1) & P(M\vee 2) & \dots & P(M\vee M) \end{Vmatrix} \tag{1.6}$$

Из теории вероятностей известно что, если взаимосвязи между элементами нет, то

$$P(x_i|x_j)=P(i|j)=P(x_i)=P(i) \tag{1.7}$$

Неопределённость выбора элементов сообщения Шеннон назвал энтропией. Термин «Энтропия» был предложен Клоду Шеннону не менее знаменитым венгерским математиком Джоном фон Нейманом. Нейман предложил позаимствовать это определение из термодинамики, так как, по его мнению, никто не знает, что это на самом деле значит, и люди меньше будут критиковать его в спорах. Энтропия обозначается символом H и, для независимых элементов с заданными вероятностями при условии отсутствия помех, она равна количеству информации в сообщении:

$$H(x)=I=-\sum_{i=1}^{M} P(i)\log P(i) \tag{1.8}$$

При наличии зависимых элементов, необходимо сперва определить условную энтропию:

$$H(x\vee x_j)=-\sum_{i=1}^{M} P(i\vee j)\log P(i\vee j) \tag{1.9}$$

После чего, избавлением от случайной составляющей при помощи усреднения по вероятностям появления элементов, вычисляется безусловная энтропия:

$$H(x)=\sum_{j=1}^{M}\left[\sum_{i=1}^{M} P(i|j)\log P(i|j)\right]P(j) \tag{1.10}$$

В общем случае, количество информации выражается по формуле:

$$I=H-H_{апост} \tag{1.11}$$

Где H – энтропия до передачи данных (или теоретически рассчитанная по имеющимся данным энтропия), а $H_{апост}$ – так называемая апостериорная энтропия (полученная после передачи сообщения). В случае отсутствия помех $H_{апост}=0$. За единицу измерения количества информации и энтропии принят 1 бит. Иногда так же говорят о $\frac{бит}{символ}$ или $\frac{бит}{элемент}$

Свойства энтропии:

1) Неотрицательность:

$$H(X) \geq 0 \tag{1.12}$$

2) Ограниченность:

$$H(X) = \sum_{i=1}^{n} p_i \log \frac{1}{p_i} = \sum_{i=1}^{n} p_i f(g_i) \leq f\left(\sum_{i=1}^{n} p_i g_i \right) = \log n \tag{1.13}$$

3) Если X и Y независимы, то:

$$H(XY) = H(X) + H(Y) \tag{1.14}$$

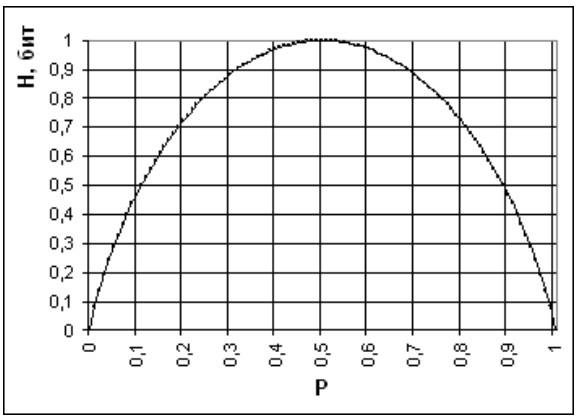
4) Энтропия – выпуклая вверх функция распределения вероятностей элементов.

5) Если X и Y имеют одинаковое распределение вероятностей, то:

$$H(X) = H(Y) \tag{1.15}$$

Из свойства 2) находим, что своего максимума энтропия достигает в случае равновероятных событий, т. е. для равномерного распределения.

Это же можно увидеть, построив график энтропии, например, для множества их двух различных сообщений.



В случае если распределение элементов множества слов в алфавите начального множества возможных сообщений отличается от равномерного, то говорят об избыточности. Избыточность является очень важной характеристикой сообщения, так как на ней базируются сразу три теории: помехоустойчивое кодирование, сжатие информации и криптография.

1.3 Условная энтропия двумерного распределения.

В качестве примера рассмотрим систему из двух зависимых нормально распределённых случайных величин с функцией плотности вероятности:

$$P(x1,x2)=\frac{1}{2\pi\sigma_1\sigma_2\sqrt{1-\rho^2}}\exp\left(\frac{-z}{2(1-\rho^2)}\right), \tag{1.16}$$

где

$$z=\frac{(x_1-\mu_1)^2}{\sigma_1^2}-\frac{2\rho(x_1-\mu_1)(x_2-\mu_2)}{\sigma_1\sigma_2}+\frac{(x_2-\mu_2)^2}{\sigma_2^2} \tag{1.17}$$

и

$$\rho=cor(x1,x2)=\frac{V_{12}}{\sigma_1\sigma_2} \tag{1.18}$$

Пусть имеются две нормально распределённые случайные величины X_1 и X_2 со средним равным 0 и единичной дисперсией.

Тогда случайные величины

$$Y_1=\mu_1+\sigma_{11}X_1+\sigma_{12}X_2 \tag{1.19}$$
$$Y_2=\mu_2+\sigma_{21}X_1+\sigma_{22}X_2 \tag{1.20}$$

Будут распределены по нормальному закону с математическими ожиданиями μ_1 и μ_2 и дисперсиями

$$\sigma_1^2=\sigma_{11}^2+\sigma_{12}^2 \tag{1.21}$$
$$\sigma_2^2=\sigma_{21}^2+\sigma_{22}^2 \tag{1.22}$$

соответственно. Ковариация

$$V_{12}=\sigma_{11}\sigma_{21}+\sigma_{12}\sigma_{22} \tag{1.23}$$

Запишем матрицу ковариации:

$$V_{ij}=\begin{pmatrix}\sigma_1^2 & \rho\sigma_1\sigma_2\\ \rho\sigma_1\sigma_2 & \sigma_2^2\end{pmatrix} \tag{1.24}$$

$$\rho=\frac{V_{12}}{\sigma_1\sigma_2}=\frac{(\sigma_{11}\sigma_{21}+\sigma_{12}\sigma_{22})}{\sigma_1\sigma_2} \tag{1.25}$$

В результате, по полученным формулам можно сгенерировать некоторую выборку из двух массивов по N элементов. Если построить эту выборку на плоскости, взяв за x координату значения из первого массива, а за y –

соответствующее значение из второго массива, то мы получим так называемый эллипсоид рассеяния. Его вытянутость будет прямо пропорционально зависеть от коэффициента корреляции между заданными случайными величинами. Так, в случае отсутствия корреляции, он выродится в обычный круг.

Далее проквантуем эти выборки на восемь уровней. Тогда вероятность появления каждого уровня можно будет посчитать как количество элементов, попавших в границы этого уровня делённое на общее количество элементов в массиве:

$$P(i)=\frac{\sum_{n:a_i\le x_n\le a_{i+1}} \frac{x_n}{x_n}}{N}, \tag{1.26}$$

где a_i-¿нижняя граница $i-ого$ уровня.

В таком случае условные вероятности можно рассчитать аналогичным способом, как количество элементов, попавших в границы уровня i, при условии, что элемент с тем же номером из второго массива попал в границы уровня j.

$$P(i\vee j)=\frac{\sum_{\substack{n:a_i\le x_n\le a_{i+1}\\ m:b_j\le y_n\le b_{i+1}}} \left(\frac{x_n}{x_n}\right)}{N} \tag{1.27}$$

Отсюда построим матрицу условных вероятностей размерности 8x8.

Зная формулы безусловной и условной энтропий, можно найти среднее количество информации в нашей матрице:

$$I(x,y)=H(x)-H(x|y)=-\sum_{i=1}^{m} p(x_i)\log\left(p(x_i)\right)+\sum_{i}^{m}\sum_{j}^{n} p(x_i,y_j)\log\left(p(x_i¿y_j)\right)$$

$$I(x,y)=\sum_{i=1}^{m}\sum_{j=1}^{n} p(x_i y_j)\log\left(\frac{1}{p(x_i)}\right)+\sum_{i=1}^{m}\sum_{j=1}^{n} p(x_i,y_j)\log\left(p(x_i\vee y_j)\right)$$

$$I(x,y)=\sum_{i=1}^{m}\sum_{j=1}^{n} p(x_i y_j)\log\left(\frac{p(x_i y_j)}{p(x_i)\,p(y_j)}\right) \tag{1.28}$$

Отсюда видно, что при независимых x и y, среднее количество информации будет равно нулю.

Часть вторая. Кубит и два кубита. Квантовые гейты. ЭПР парадокс

2.1Кубит и однокубитовые квантовые гейты

Основным понятием КТИ является кубит. Термин введен Робертом Шумахером в 1982 году и происходит от «q-bit», сокращения от quatntum bit. Кубит – математическое представление двухуровневой квантовой системы. Состояние кубита – нормированный вектор в комплексном гильбертовом пространстве$H^2=C^2$ со стандартным скалярным произведением.

Кубит это наименьший квантовый разряд или наименьшая единица информации, которую можно хранить в квантовом компьютере. С точки зрения квантовой физики кубит является простейшей квантовомеханической системой, пространство которой двумерно. На практике кубиты представляются в виде бра или кет векторов, названных так Дираком от слова bracket.

Бра-вектор $\langle\cdot|$ *Кет-вектор* $|\cdot\rangle$

По аналогии с классической теорией информации, где один разряд хранит значения 0 или 1, кубит также может принимать значения $|0\rangle$ или $|1\rangle$. В векторном виде это записывается как

$$|0\rangle=\begin{bmatrix}1\\0\end{bmatrix} \qquad |1\rangle=\begin{bmatrix}0\\1\end{bmatrix} \qquad (2.1.1)$$

Главное отличие кубитов от битов заключается в том, что помимо этих «чистых» состояний, возможна их линейная комбинация, называемая состоянием суперпозиции **[2]**

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \qquad (2.1.2)$$

где α и β в общем случае могут быть комплексными числами, а $|\psi\rangle$ имеет вид вектора на комплексной плоскости.

В общем случае мы не можем поспользоваться аналогией битов в классической теории информации, т.к. результатом измерения кубитов вектора $|\psi\rangle$ будет не «промежуточное» состояние, а:

- $|0\rangle$ с вероятностью ¿$\alpha \vee$¿^{2}¿
- $|1\rangle$ с вероятностью $|\beta|^2$

То есть кубит может находиться в бесконечном множестве суперпозиций, но при этом информация, которую из него возможно почерпнуть, ограничена. В таком случае следует ввести условие нормировки:

$$¿\alpha \vee ¿^2 + |\beta|^2 = 1¿ \qquad (2.1.3)$$

Любая логическая операция с кубитами называется *квантовым гейтом* (*quantum gate*) или просто *гейтом.* Гейты, как оператор над кет- или бра-вектором, имеет матричное представление, которым мы и будем пользоваться в дальнейшем для удобства и наглядности.
Например, тождественный элемент для одного кубита, представляется единичной матрицей

$$\sigma_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad (2.1.4)$$

Соответственно, имея в наличии некоторые логические операторы, представляемые в виде матриц вида 2x2 мы имеем возможность записать аналог классического логического отрицания

Элемент **NOT** (*Элемент X*)

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad X\begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \beta \\ \alpha \end{bmatrix} \qquad (2.1.5)$$

(*оператор, переводящий* $|0\rangle$ *в* $|1\rangle$ *и* $|1\rangle$ *в* $|0\rangle$)

Элемент **Z**

$$Z=\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}\quad Z\begin{bmatrix}\alpha\\ \beta\end{bmatrix}=\begin{bmatrix}\alpha\\ -\beta\end{bmatrix} \qquad (2.1.6)$$

(оператор, переводящий $|1\rangle$ *в* $-|1\rangle$ *и оставляющий* $|0\rangle$ *без изменений)*

Элемент *Адамара* **H**

$$H=\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\qquad Z\begin{bmatrix}\alpha\\ \beta\end{bmatrix}=\frac{1}{\sqrt{2}}\begin{bmatrix}\alpha+\beta\\ \alpha-\beta\end{bmatrix} \qquad (2.1.7)$$

(*так называемый «квадратный корень из NOT», переводящий* $|0\rangle$ *в* $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$, *а* $|1\rangle$ *в* $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$)**[2]**

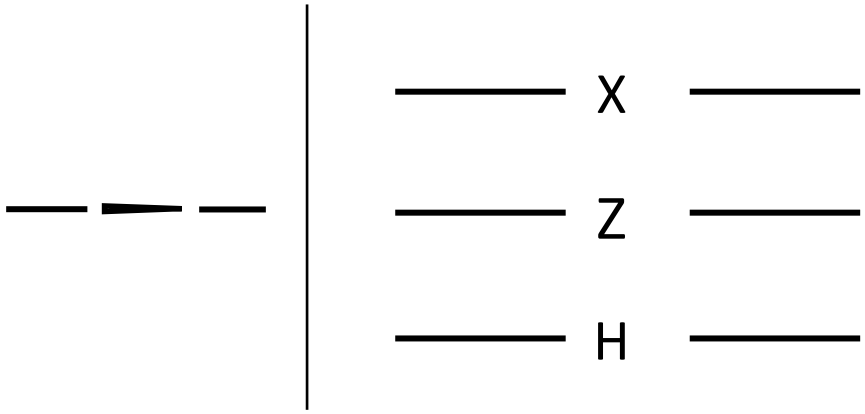


Рис. 1 – однобитовый элемент «не» слева и однокубитовые гейты справа.

Любая матрица представляет собой оператор. При этом матрица, описывающая однокубитовый гейт, должна быть унитарной, то есть квадратной матрицей 2 на 2 с комплексными элементами (в общем случае), результат умножения которой на эрмитово-сопряженную равен единичной матрице.

$$U\cdot U^{\dagger}=U^{\dagger}\cdot U=I \qquad (2.1.8)$$

Матрица *унитарна*, если её обратная матрица равна эрмитово-сопряжённой

$$U^{-1}=U^{\dagger} \qquad (2.1.9)$$

Эрмитово-сопряженная матрица – матрица $A^{\dagger}$, полученная путём транспонирования и замены каждого элемента на комплексно-сопряженный

Эрмитова матрица – квадратная матрица с комплексными числами, которая будучи транспонированной равна комплексно-сопряженной

$$A^{T}=A^{\dagger} \qquad (2.1.10)$$

Введём понятие *гильбертова пространства*.
Банахово пространство, норма которого порождена положительно определённым скалярным произведением называется гильбертовым пространством. Другими словами это обобщение евклидова пространства на размерность *n*, то есть полное, нормированное векторное пространство H^n над неким полем (в нашем случае полем комплексных чисел $\mathbb{C}$), удовлетворяющее аксиомам унитарного пространства, в котором для любого элемента *x, y*, принадлежащих пространству H^n определено скалярное произведение (*x, y*) Тогда произвольный кет-вектор $|\psi\rangle$, представляющий собой какое-либо состояние кубита, будет принадлежать гильбертову пространству размерности 2 с базисными векторами $|0\rangle$ и $|1\rangle$.

Каждому векторному пространству V можно сопоставить дуальное пространство $V^¿$, элементы которого будут являться функционалами на V. В случае дуального пространства пространству кет-векторов любая функция $f ¿ \epsilon V^¿$ будет являться вектором $\langle\varphi|$, так же именуемым бра-вектором. А значение, принимаемое этой функцией при некотором $|\psi\rangle$, есть некоторое комплексное (в общем виде) число, которое обозначается $\langle\varphi|\psi\rangle$.

На практике же вектора $\langle\varphi|$ имеют представление в виде вектор-строки с некоторыми комплексными значениями

$$\langle\varphi| = (\varphi_1, \varphi_2, \ldots, \varphi_m) \qquad (2.1.11)$$

А пространство всех бра-векторов так же будет являться гильбертовым размерности *m*. В случае сопоставления дуального векторного пространства гильбертову их размерность совпадёт, более того они будут сопряженными, то есть:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \qquad (2.1.12)\langle\psi| = \alpha^¿\langle 0| + \beta^¿\langle 1|, \text{ откуда } |\psi\rangle = \langle\psi|^¿$$

Определим скалярное произведение для двух произвольных векторов $|\psi\rangle$ и $\langle\varphi|$. Пусть имеется гильбертово пространство H^n с ортонормированным базисом $|i\rangle$, тогда $|\psi\rangle = \sum_i \psi_i \cdot |i\rangle$ и $|\varphi\rangle = \sum_j \varphi_j \cdot |j\rangle$ – их пресдставления в базисе.

Положим $\langle i|j\rangle = \delta_{i,j}$, где $\delta_{i,j} = \begin{cases} 1, i = j \\ 0, i \neq j \end{cases}$, тогда

$$\langle\varphi|\psi\rangle = \left(\sum_j \varphi_j \cdot |j\rangle, \sum_i \psi_i \cdot |i\rangle\right) = \sum_{i,j} \varphi_i^¿ \cdot \psi_i \cdot \delta_{i,j} = \sum_i \varphi_i^¿ \cdot \psi_i = ¿¿¿ \begin{bmatrix} \varphi_1^¿ & \cdots & \varphi_n^¿ \end{bmatrix} \cdot \begin{bmatrix} \psi_1 \\ \vdots \\ \psi_n \end{bmatrix} = c \in C$$

(2.1.13)

Для представления линейных операторов с помощью скалярного произведения воспользуемся *представлением с помощью тензорного произведения*. Пусть имеются векторы $|v\rangle u|w\rangle$ в пространствах V и W соответственно со скалярным произведением. Определим $|w\rangle\langle v|$, как линейный оператор, отображающий V в W по следующему правилу:

$$(|w\rangle\langle v|)(|\psi\rangle)\equiv|w\rangle\langle v|\psi\rangle=\langle v|\psi\rangle|w\rangle \qquad (2.1.14)$$

То есть по сути мы умножаем вектор $|w\rangle$ на комплексное число $\langle v|\psi\rangle$

Вывод из этого представления, если $|i\rangle$ – ортонормированный базис в векторном пространстве V, тогда произвольный вектор $|v\rangle$ может быть записан в виде $|v\rangle=\sum_i v_i|i\rangle$, а путём небольших преобразований, можно получить следующее равенство, называемое *условием полноты*.

$$\sum_i |i\rangle\langle i|=E$$

2.2 Два кубита

Для работы с двумя кубитами воспользуемся тензорным произведением, результатом которого станет пространство бóльшей размерности.

Пусть V, W – конечномерные векторные пространства над полем K, размерности n и m соответственно, где v_i, $i=1..n$ – базис пространства V, а w_j, $j=1..m$ – базис пространства W, тогда *тензорным произведением* $V\otimes W$ будем называть такое векторное пространство размерности nm, порождённое элементами $v_i\otimes w_j$, называемыми тензорными произведениями базисных векторов **[2]**

Для двух вектор-столбцов тензорное произведение будет являться вектор-столбцом размерности $n\times m$.

$$a \otimes b = \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix} \cdot \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{bmatrix} = \begin{bmatrix} a_1 b_1 \\ a_1 b_2 \\ \vdots \\ a_1 b_m \\ \vdots \\ a_n b_1 \\ a_n b_2 \\ \vdots \\ a_n b_m \end{bmatrix} \quad (2.2.1)$$

Для линейных операторов A и B в пространствах V и W, линейный оператор $A \otimes B$ действующий в пространстве $V \otimes W$ задаётся следующим образом:

$$(A \otimes B)(|v\rangle \otimes |w\rangle) = A|v\rangle \otimes B|w\rangle \quad (2.2.2)$$

Частным случаем тензорного произведения будет являться операция *Кронекерова произведения матриц*. Пусть A – матрица размера $n \times m$, B – матрица $p \times q$, тогда имеется следующее матричное представление:

$$A \otimes B \equiv \begin{bmatrix} A_{11}B & A_{12}B & \cdots & A_{1m}B \\ A_{21}B & A_{22}B & \cdots & A_{2m}B \\ \vdots & \vdots & \ddots & \vdots \\ A_{n1}B & A_{n2}B & \cdots & A_{nm}B \end{bmatrix} (2.2.3)$$

Где через $A_{11}B$ обозначены подматрицы размера $p \times q$. Далее, для удобства, будем вместо $|\psi\rangle \otimes |\varphi\rangle$ употреблять запись вида $|\psi\rangle|\varphi\rangle$ или $|\psi\,\varphi\rangle$.

Теперь возьмём тензорное произведение двух однокубитовых пространств H^2 для получения одного двухкубитового пространства H^4. По определению вычислительный базис H^4 представляет собой тензорное произведение базисов H^2, то есть:

$$|0\rangle \otimes |0\rangle = |00\rangle = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \qquad |0\rangle \otimes |1\rangle = |01\rangle = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}$$

$$|1\rangle \otimes |0\rangle = |10\rangle = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} \qquad |1\rangle \otimes |1\rangle = |11\rangle = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

$\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ - ортонормированный базис в H^4. Произвольный вектор $|\psi\rangle$ из этого пространства (то есть просто состояние двух кубитов) будет выглядеть следующим образом:

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle \qquad (2.2.4)$$

Для коэффициентов α_i, $i = 1..n$, которые так же называются амплитудами, следует ввести нормировку, как и в случае однокубитового элемента.

$$|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1 \qquad (2.2.5)$$

А результат измерения $x (¿ 00, 01, 10 или 11)$ встречается с вероятностью $¿ \alpha_x \vee ¿^2 ¿$ и после измерения кубиты остаются в состоянии $|x\rangle$

Для такой системы, содержащей в себе два кубита, можно провести измерения некоторго подмножества, например только первого кубита. При его измерении получается 0 с вероятностью $¿ \alpha_{00} \vee ¿^2 + ¿ \alpha_{01} \vee ¿^2 ¿ ¿$, а система переходит в новое состояние

$|\psi'\rangle = \frac{\alpha_{00}|00\rangle + \alpha_{01}|01\rangle}{\sqrt{¿ \alpha_{00} \vee ¿^2 + ¿ \alpha_{01} \vee ¿^2 (2.2.6) ¿ ¿}}$ После измерения состояние перенормировывается на коэффициент $\sqrt{¿ \alpha_{00} \vee ¿^2 + ¿ \alpha_{01} \vee ¿^2 ¿ ¿}$, соблюдая условие нормировки.

Теперь, когда мы расписали необходимый математический аппарат для работы с двумя кубитами, можно перейти к обобщению гейтов (то есть логических операций) на случай нескольких кубитов.

Простешим элементом над двумя кубитами является гейт CNOT или Controlled-NOT. Как можно понять из названия, он имеет два входных кубита, - управляющий *(control)* и управляемый *(target)*. Его структурная схема выглядит следующим образом

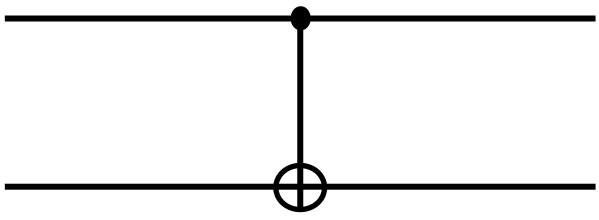


Рис. 2 – двухкубитовый элемент CNOT

Верхняя линия представляет собой управляющий кубит, в то время как нижняя – представляемый соответственно. Работу элемента можно описать так: Если $|A\rangle$ установлен в ноль, то $|B\rangle$ не меняется, если $|A\rangle$ установлен в единицу, то управляемый кубит изменится. Формальная запись:

$$|00\rangle \to |00\rangle \qquad |01\rangle \to |01\rangle \qquad |10\rangle \to |11\rangle \qquad |11\rangle \to |10\rangle$$

В матричном виде действие CNOT описать можно представлением.

$$U_{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

U_{CNOT} – унитарная матрица, т.е. $U_{CNOT}{}^{\dagger} U_{CNOT} = I$

Еще одним распространённым элементом над двумя кубитами является SWAP-гейт

$$S = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Таблица истинности этого элемента будет следующей

$$|00\rangle \to |00\rangle \qquad |01\rangle \to |10\rangle \qquad |10\rangle \to |01\rangle \qquad |11\rangle \to |11\rangle$$

То есть он меняет два элемента в середине, поэтому и называется гейтом-SWAP.

2.3 ЭПР-Парадокс

Парадокс Эйнштейна-Подольского-Розена (ЭПР-парадокс) – это *мысленный* эксперимент, который по замыслу авторов должен опровергать основы квантовой механиики, а именно её копенгагенскую (вероятностную) интерпретацию.

«Бог не играет в кости» – Альберт Эйнштейн

Согласно истории, в 1927 году, на Пятом Сольвеевском конгрессе, Эйнштейн решительно выступил против «копенгагенской интерпретации» Макса Борна и Нильса Бора, трактующей математическую модель квантовой механики как существенно вероятностную. Он заявил, что сторонники этой интерпретации «из нужды делают добродетель», а вероятностный характер свидетельствует лишь о том, что наше знание физической сущности микропроцессов неполно. Так зародился спор Бора — Эйнштейна о физическом смысле волновой функции. В 1935 году Альберт Эйнштейн вместе с Борисом Подольским и Натаном Розеном написал статью «Можно ли считать квантово-механическое описание физической реальности полным?», в которой описал мысленный эксперимент, так как технической возможности его осуществить в то время еще не было.

Суть парадокса такова: согласно принципу неопределённости Гейзенберга, нельзя одновременно точно определить координату частицы и её импульс. Предполагая, что причиной неопределённости является то, что измерение одной величины вносит принципиально неустранимые возмущения в состояние и производит искажение значения другой величины, можно предложить гипотетический способ, которым соотношение неопределённостей можно обойти. Проще говоря авторы хотели указать на то, что существуют некоторые элементы действительности, не включенные в квантовую механику, но оказывающие на неё влияние. Схема эксперимента следующая: берутся две элементарных частицы с суммарным нулевым импульсом, разнесенные на достаточное расстояние, так, чтобы они не могли взаимодействовать. Потом у одной частицы точно (т. е. с очень малой погрешностью) измеряется импульс, а у другой частицы после этого точно измеряется координата. Тогда у второй частицы будет точно измерен и импульс, и координата, что невозможно согласно соотношению Гейзенберга. Объяснение парадокса согласно современной интерпретации квантовой механики заключается в том, что измерение одной частицы меняет сразу состояние всей системы, состоящей из двух частиц. После измерения импульса у первой частицы, вторая частица перейдет также в состояние с определенным импульсом.

Антикорреляция в эксперименте Эйнштейна-Подольского-Розена. Пусть у нас есть состояние двух кубитов

$$|\psi\rangle=\frac{|01\rangle-|10\rangle}{\sqrt{2}}\quad(2.3.1)$$

Это состояние является запутанным состоянием системы из двух кубитов. Предположим так же, что мы измерили компоненты спина вдоль оси $\vec{v}$ для обоих кубитов, т.е. измерили наблюдаемую $\vec{v}\cdot\vec{\sigma}$, получив для

каждого из них ответ +1 или -1. Оказывается, что вне зависимости от выбора направления $\vec{v}$ результаты обоих этих измерений будут противоположными. Другими словами, если при измерении над первым кубитов получен ответ +1, то при измерении над вторым получено значение -1 и наоборот. Наши кубиты в конечном итогда оказались намного более коррелированны друг с другом, чем что-угодно в классической теории информации.

В споре о парадоксе Эйнштейна-Подольского-Розена последнее слово осталось за квантовомеханическими законами, которые были подтверждены экспериментальным путём спустя приблизительно тридцать лет после публикации статьи. Главным моментом в этом экспериментальном опровержении явился результат, известный под названием неравенства Белла. Утверждение, не относящееся непосредственно к квантовой механике. **[12]**

Часть третья Матрица плотности. Квантовая энтропия и мера квантовой информации по фон Нейману

3.1 Матрица плотности.

Если у нас есть полная информация о квантовой системе, то её чистое состояние может быть описано волновой функцией $¿\psi\rangle$. Однако она применима только для не взаимодействующих с окружением замкнутых систем. Применение волновых функций к скоррелированным подсистемам приводило к различным парадоксам вроде знаменитого ЭПР парадокса. Матрица плотности (или оператор плотности) – другой широко распространённый в квантовой механике способ описания квантовой системы. Учитывая не только внутренние условия системы, но и внешние, в которых эта система находится, она позволяет описывать все, как чистые, так и смешанные состояния системы, что делает её особенно полезной. Матрица плотности впервые была описана фон Нейманом в 1927 году[**9**], однако её

существованию десятилетиями не уделяли должного внимания, ошибочно полагая, что любую систему можно описать при помощи волнового уравнения. Но если бы в квантовой теории не было матриц плотности, то вообще невозможно было бы описывать открытые системы и говорить о частях составной системы, когда они взаимодействуют друг с другом[**10**]. В том же году Лев Ландау начал писать свою новую работу «Проблема торможения в волновой механике». Анализируя механизмы торможения излучением, он, независимо от Неймана, также ввёл понятие матрицы плотности[**11**]. Именно в матрице плотности содержится информация о корреляциях с окружением — в векторе состояния (пси-функции) такой информации нет. Публикация рукописи Неймана в 1927г. также считается началом создания квантовой теории информации. Вектор состояния и матрица плотности могут применяться для квантового описания (в терминах состояний) и в более общем случае, когда мы имеем дело с текстовыми сообщениями (или любой другой информацией). Этот подход широко применяется сейчас в квантовой теории информации. Часто используется стандартный базис — из чисел в двоичной системе. Так делается в компьютерах, где любая информация записывается в двоичном базисе. Этот же базис применяется в физике: например, в случае спиновых степеней свободы каждая позиция соответствует двум возможным состояниям одного спина во внешнем магнитном поле (0-спин-вверх, 1-спин-вниз). Сумма диагональных элементов, то есть след матрицы плотности равен единице. В квантовой теории информации, когда пересылается какое-либо сообщение, возможны искажения, и получателю может прийти не то, что было послано: к примеру, вместо одной буквы — другая. Набор основных состояний системы (диагональные элементы матрицы плотности) характеризует все возможные варианты таких искажений (их вероятности), а «приемник» прочитает только один из них. То есть будет реализован один из искаженных вариантов с соответствующей вероятностью, а сумма вероятностей (след матрицы плотности) должен быть равен единице.

В случае, когда система находится в каждом из взаимно ортогональных состояний $¿\psi_j\rangle$ с вероятностью p_j, оператор плотности имеет вид:

$$\rho=\sum_j p_j ¿\psi_j\rangle\langle\psi_j\vee, \tag{3.1.1}$$

где

$$\begin{cases}\sum_j p_j=1\\ 0\le p_j\le 1\end{cases} \tag{3.1.2}$$

Причём, суперпозиция далеко не всегда будет являться смешанным состоянием, так как суперпозиция чистых состояний даст другое чистое состояние.

Свойства матрицы плотности:

1) Производная по времени от оператора плотности гамильтоновой квантовой системы выражается через коммутатор с гамильтонианом в виде уравнения:

$$\frac{\partial\rho}{\partial t}=\frac{1}{i\hbar}[H,\rho] \tag{3.1.3}$$

Это уравнение называется уравнением Лиувилля-фон Неймана и описывает эволюцию смешанных состояний квантовых гамильтоновых систем.

2) След матрицы плотности равен единице:

$$Tr(\rho)=1 \tag{3.1.4}$$

3) След квадрата матрицы плотности для чистых состояний равен единице и всегда меньше единицы для смешанных состояний:

$$Tr(\rho^2)\le 1 \tag{3.1.5}$$

$$Tr(\rho^2)=1\Leftrightarrow\exists\ ¿\psi\rangle:\rho=¿\psi\rangle¿ \tag{3.1.6}$$

4) Оператор ρ является эрмитовым, следовательно:

$$\rho=\rho^{\dagger} \tag{3.1.7}$$

Приведём простой пример матрицы плотности для одного кубита.

Имеется двухуровневая система в чистом состоянии, представленная волновой функцией $¿\psi\rangle=\alpha¿a\rangle+\beta¿b\rangle$

Тогда оператор плотности для этой системы будет иметь следующий вид:

$$\rho=¿\psi\rangle¿ \tag{3.1.8}$$

Элементы матрицы будут иметь вид:

$$\rho_{aa}=|\alpha|^2 \quad (3.1.9)$$
$$\rho_{ab}=\alpha\,\beta^{¿} \quad (3.1.10)$$
$$\rho_{ba}=\rho_{ab}^{¿} \quad (3.1.11)$$
$$\rho_{bb}=|\beta|^2 \quad (3.1.12)$$

В результате получим матрицу:

$$\rho=\begin{pmatrix}\rho_{aa} & \rho_{ab}\\ \rho_{ba} & \rho_{bb}\end{pmatrix} \quad (3.1.14)$$

Рассмотрим пример получения матрицы плотности для трех кубитов.

Три когерентных кубита представляют 2^3 различных чистых состояний.

Обозначим полученные восемь вычислительных базисов как $¿000\rangle$, $¿001\rangle$, $¿010\rangle$, $¿011\rangle$, $¿100\rangle$, $¿101\rangle$, $¿110\rangle$ и $¿111\rangle$.

Кубиты могут находиться в суперпозициях этих состояний, поэтому для описания квантового состояния такой системы потребуется следующий вектор:

$$¿\psi\rangle=\alpha_{000}¿000\rangle+\alpha_{001}¿001\rangle+\alpha_{010}¿010\rangle+\alpha_{011}¿011\rangle+\alpha_{100}¿100\rangle+\alpha_{101}¿101\rangle+\alpha_{110}¿11 \quad (3.1.15)$$

Для них матрица плотности будет выглядеть следующим образом

$$\rho=\begin{pmatrix}\alpha_{000}\alpha'_{000} & \alpha_{000}\alpha'_{001} & \dots & \alpha_{000}\alpha'_{110} & \alpha_{000}\alpha'_{111}\\ \alpha_{001}\alpha'_{000} & \alpha_{001}\alpha'_{001} & \dots & \alpha_{001}\alpha'_{110} & \alpha_{001}\alpha'_{111}\\ \vdots & \vdots & \ddots & \vdots & \vdots\\ \alpha_{110}\alpha'_{000} & \alpha_{110}\alpha'_{001} & \dots & \alpha_{110}\alpha'_{110} & \alpha_{110}\alpha'_{111}\\ \alpha_{111}\alpha'_{000} & \alpha_{111}\alpha'_{001} & \dots & \alpha_{111}\alpha'_{110} & \alpha_{111}\alpha'_{111}\end{pmatrix} \quad (3.1.16)$$

3.2 Квантовая энтропия. Мера квантовой информации по фон Нейману.

Прежде, чем вводить квантовую энтропию, определим функцию от оператора. Пусть $\hat{L}$ – линейный оператор, λ_k и $¿\psi_k\rangle$ – его собственные числа и вектора. Тогда этот оператор можно представить в виде:

$$\hat{L}=\sum_n \lambda_n ¿\psi_n\rangle¿ \quad (3.2.1)$$

Определим функцию от оператора соотношением:

$$f(\hat{L})=\sum_n f(\lambda_n)¿\psi_n\rangle¿ \quad (3.2.2)$$

Рассмотрим функцию:

$$f(x)=\begin{cases}-x\log_2 x, x>0\\ 0, x=0\end{cases} \quad (3.2.3)$$

Введём след матрицы оператора $\hat{A}$ соотношением:

$$Tr(\hat{A})=\sum_n ¿ ¿ \quad (3.2.4)$$

Пусть ρ – матрица плотности рассматриваемой системы. Квантовой энтропией или энтропией фон Неймана называется величина:

$$S(\hat{\rho})=Tr(f(\hat{\rho})) \quad (3.2.5)$$

Из заданных выше уравнений получаем:

$$\hat{\rho}=\sum_n \lambda_n ¿\psi_n\rangle\langle\psi_n\vee, \quad (3.2.6)$$

$$S(\hat{\rho})=Tr ¿ \quad (3.2.7)$$

или

$$S(\hat{\rho})=\sum_{n,k} f(\lambda_n)¿ \quad (3.2.8)$$

В результате, энтропия Неймана равна:

$$S(\hat{\rho})=\sum_n f(\lambda_n)=-\sum_n \lambda_n\log_2(\lambda_n) \quad (3.2.9)$$

Эта формула отчасти схожа с формулой энтропии Шеннона для классической теории информации. Разница состоит лишь в том, что логарифм берётся от матрицы, но, тем не менее, после диагонализации можно утверждать, что данная формула энтропии означает сумму произведений вероятностей нахождения квантовой системы во всех её чистых состояниях на логарифмы этих вероятностей.

В качестве примера возьмём систему из двух кубитов:

$$¿\psi\rangle=a¿0_A\rangle¿0_B\rangle+b¿0_A\rangle¿1_B\rangle+c¿1_A\rangle¿0_B\rangle+d¿1_A\rangle¿1_B\rangle \quad (3.2.10)$$

С условием нормировки:

$$|a|^2+|b|^2+|c|^2+|d|^2=1 \quad (3.2.11)$$

Соответствующая матрица плотности имеет вид:

$$\hat{\rho}_{AB}=¿\psi\rangle¿ \quad (3.2.12)$$

Построим теперь матрицу плотности подсистемы A, усреднив матрицу плотности системы AB по всем возможным состояниям подсистемы B:

$$\hat{\rho}_A=\langle 0_B|\hat{\rho}_{AB}|0_B\rangle+\langle 1_B|\hat{\rho}_{AB}|1_B\rangle \quad (3.2.13)$$

$$\hat{\rho}_A=\left(|a|^2+|b|^2\right)¿0_A\rangle\langle 0_A\vee+\left(ac^¿+bd^¿\right)¿0_A\rangle¿$$

(3.2.14)

Таким образом, матрица плотности имеет вид:

$$\hat{\rho}=\begin{pmatrix}|a|^2+|b|^2 & a\,c^¿+b\,d^¿\\ a^¿\,c+b^¿\,d & |c|^2+|d|^2\end{pmatrix} \quad (3.2.15)$$

Собственные числа матрицы плотности являются корнями уравнения:

$$\begin{vmatrix}|a|^2+|b|^2-\lambda & a\,c^¿+b\,d^¿\\ a^¿\,c+b^¿\,d & |c|^2+|d|^2-\lambda\end{vmatrix}=0 \quad (3.2.16)$$

или

$$\lambda^2-\lambda+|a|^2|d|^2+|b|^2|c|^2-a\,b^¿\,c^¿\,d-a^¿\,bc\,d^¿=0 \quad (3.2.17)$$

Тогда:

$$S\left(\hat{\rho}_A\right)=-\lambda_1\log_2\lambda_1-\lambda_2\log_2\lambda_2 \quad (3.2.18)$$

Значение квантовой энтропии $S\left(\hat{\rho}_A\right)$ можно использовать для того, чтобы охарактеризовать степень запутанности состояния AB. Однако, помимо этого, существует и другой, более прямой способ оценки степени запутанности двух кубитов[**12**]. Наряду с волновой функцией двухкубитового состояния рассмотрим прямое произведение двух кубитов:

$$¿\psi\rangle=a¿0_A\rangle¿0_B\rangle+b¿0_A\rangle¿1_B\rangle+c¿1_A\rangle¿0_B\rangle+d¿1_A\rangle¿1_B\rangle \quad (3.2.19)$$

$$¿\psi\rangle=\left(\alpha\vee 0\rangle+\beta\vee 1\rangle\right)\left(\gamma\vee 0\rangle+\delta\vee 1\rangle\right)=¿¿\alpha\gamma¿00\rangle+\alpha\delta¿01\rangle+\beta\gamma¿10\rangle+\beta\delta¿11\rangle \quad (3.2.20)$$

Приравнивая коэффициенты находим:

$$a=\alpha\gamma \quad (3.2.21)$$

$$b=\alpha\delta \quad (3.2.22)$$

$$c=\beta\gamma \quad (3.2.23)$$

$$d=\beta\delta \quad (3.2.24)$$

Отсюда получаем необходимое и достаточное условие на коэффициенты произвольного двухкубитового состояния, при выполнении которого двухкубитовое состояние является тензорным произведение однокубитовых.

$$ad-bc=0 \quad (3.2.25)$$

При выполнении этого условия двухкубитовое состояние является не запутанным. Следовательно, величину:

$$P=ad-bc \quad (3.2.26)$$

Можно рассматривать, как меру запутанности двухкубитового состояния.

Исходя из результатов исследований, проведённых с помощью приложения №2, можно сделать вывод, что энтропия Неймана характеризует степень смешанности описываемой матрицей плотности системы.

Любая матрица плотности, полученная из произведения волновых функций, будет иметь удовлетворяющие неравенству Шура собственные значения:

$$\lambda=(1,0,0,\ldots,0) \tag{3.2.27}$$

Покажем это

$$\begin{pmatrix} |a_1|^2 & \cdots & a_1 \acute{a}_2 \\ \vdots & \ddots & \vdots \\ \acute{a}_1 a_2 & \cdots & |a_n|^2 \end{pmatrix} = U \Lambda U^{\dagger}, \tag{3.2.28}$$

где

$$U=\begin{pmatrix} a_1 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ a_n & 0 & \cdots & 0 \end{pmatrix} \text{ – унитарная матрица} \tag{3.2.29}$$

$$U^{\dagger}=\begin{pmatrix} \acute{a}_1 & \cdots & \acute{a}_n \\ 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{pmatrix} \text{ – эрмитово сопряжённая к } U \tag{3.2.30}$$

диагональная матрица из собственных значений матрицы плотности:

$$\Lambda=\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix} \tag{3.2.31}$$

Для оператора плотности

$$\sum_{i=1}^{n}\sum_{j=1}^{n}|a_{ij}|^2=\left(|\alpha_1|^2+|\alpha_2|^2+\cdots+|\alpha_n|^2\right)^2=1, \tag{3.2.32}$$

и, согласно неравенству Шура,

$$\sum_{i=1}^{n}|\lambda_i|^2 \le \sum_{i,j=1}^{n}|a_{ij}|^2, \tag{3.2.33}$$

где a_{ij} - элементы некоторой матрицы A.

В нашем случае, для нормальной матрицы плотности данное неравенство переходит в строго равенство

$$\sum_{i=1}^{n} |\lambda_i|^2 = \sum_{i,j=1}^{n} |a_{ij}|^2 \quad (3.2.34)$$

Что и выполняется для собственных значений (3.27)

Энтропия фон Неймана в таком случае будет равна

$$S(\hat{\rho}) = 1 \cdot \log_2 1 + 0 \cdot \log_2 0 + \cdots + 0 \cdot \log_2 0 \quad (3.2.35)$$

$$S(\hat{\rho}) = 0 + 0 + \cdots + 0 = 0 \quad (3.2.36)$$

Отсюда видно, что энтропия фон Неймана для матриц плотности такого типа всегда будет равна 0. Это объясняется тем, что суперпозиция двух чистых состояний тоже является чистым состоянием и, как следствие, смешанности у таких операторов не будет, что и показывает энтропия фон Неймана.

Однако меру фон Неймана можно использовать для вычисления меры запутанности нескольких кубитов, находящихся в замкнутой системе. Обобщив формулу (3.13) всегда можно построить редуцированную матрицу плотности подсистемы из одного или нескольких кубитов и посчитать для неё энтропию Неймана. Такая матрица плотности уже будет описывать смешанную систему, что недоступно для обыкновенной волновой функции. Фактически она будет представлять собой открытую систему из взятой подсистемы, где внешней средой будет являться вся система. А мера смешанности данной системы будет одновременно являться мерой запутанности исходной системы

Часть четвертая Квантовая запутанность

4.1 Квантовая запутанность

Что такое квантовая запутанность? Говоря простым языком, квантовая запутанность – это такое состояние системы, при котором состояния двух или более объектов этой системы оказываются во взаимодействии. Причем это взаимодействие сохраняется, даже если эти объекты будут находиться в

самых крайних уголках вселенной, что, в общем, нарушает принцип локальности. Раньше, до появляения слова *entanglement (запутанность)* такие системы называли коррелированными. Причем корреляция эта намного сильнее любой классической корреляции. Как говорил Эшер Перес, – «Квантовая запутанность – это трюк, используемый квантовыми волшебниками для создания феноменов, которые не могут повторить классические волшебники».

Рассмотрим состояние $|\psi\rangle$ в гильбертовом пространстве $H_1^2 \otimes H_2^2$ и сформулируем критерий запутанности.

Запутанной двухкубитной системой называется состояние, для которого выполняется следующее условие:

$$|\psi\rangle \neq |\psi_1\rangle \otimes |\psi_2\rangle \quad |\psi\rangle \in H_1^2 \otimes H_2^2$$
$$|\psi_1\rangle \in H_1^2, \qquad |\psi_2\rangle \in H_2^2$$

То есть если оно может быть записано в виде тензорного произведения каждого кубита, в противном случае состояние называется *разложимым*.

Теперь проанализируем написанное выше. Если $|\psi_1\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$ и $|\psi_2\rangle = \alpha_2|0\rangle + \alpha_3|1\rangle$по определению, то

$$|\psi_1\rangle \otimes |\psi_2\rangle = (\alpha_0|0\rangle + \alpha_1|1\rangle) \otimes (\alpha_2|0\rangle + \alpha_3|1\rangle) = \begin{bmatrix} \alpha_0 \\ \alpha_1 \end{bmatrix} \otimes \begin{bmatrix} \alpha_2 \\ \alpha_3 \end{bmatrix} =$$

$$\begin{bmatrix} \alpha_0\alpha_2 \\ \alpha_0\alpha_3 \\ \alpha_1\alpha_2 \\ \alpha_1\alpha_3 \end{bmatrix} = |\psi\rangle = \alpha_0\alpha_2|00\rangle + \alpha_0\alpha_3|01\rangle + \alpha_1\alpha_2|10\rangle + \alpha_1\alpha_3|11\rangle,$$ перезапишем в более привычном виде $|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$. Для выполнения $|\psi\rangle \neq |\psi_1\rangle \otimes |\psi_2\rangle$ достаточно, чтобы определитель матрицы $\begin{bmatrix} \alpha_{00} & \alpha_{01} \\ \alpha_{10} & \alpha_{11} \end{bmatrix}$ не был равен нулю, то есть выполнялось неравенство

$$\alpha_{00}\alpha_{11} - \alpha_{10}\alpha_{01} \neq 0 \qquad (4.1.1)$$

Конечный упорядоченный набор из *n*-кубитов (изолированных или взаимодействующих) называют *n*-разрядным квантовым регистром, причем число его базисных состояний ($|0\rangle$ и $|1\rangle$ для одного кубита) равно 2^n.

Как мы выясним позже любое незапутанное состояние можно преобразовать в запутанное с помощью определённых логических элементов – гейтов.

Введём новое определение. *Ансамблем чистых состояний* называется множество элементов $\{p_i, |\psi_i\rangle\}, i \in N$, где $|\psi_i\rangle$ – возможное состояние квантовой системы, вероятность нахождения в которой равна p_i. Квантовая система, описываемая вектором $|\psi\rangle$ находится в *чистом* состоянии, если у нас есть о нём вся информация. То есть полностью задан вектор $|\psi\rangle$ с определёнными вероятностями нахождения в таких то состояниях. Только чистые состояния можно описать волновой функцией.
Оператор плотности такой системы будет определяться выражением
$$\rho \equiv \sum_i p_i |\psi_i\rangle\langle\psi_i| \quad (4.1.2)$$

Этот оператор также носит название *матрицы плотности*. По сути оператор плотности – другое представление систем смешанных состояний в терминах операторов гильбертова пространства. Представляет из себя матрицу размера $m \times m$, где $m = 2^n$, а n – количество кубитов в системе. То есть в общем виде для замкнутой системы (то есть системы в чистом состоянии), которая записывается в виде вектор состояния $|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$, матрица плотности будет выглядеть следующим образом:

$$\rho_\psi = |\psi\rangle\langle\psi| = \begin{bmatrix} |\alpha_{00}|^2 & 0 & 0 & 0 \\ 0 & |\alpha_{01}|^2 & 0 & 0 \\ 0 & 0 & |\alpha_{10}|^2 & 0 \\ 0 & 0 & 0 & |\alpha_{11}|^2 \end{bmatrix}, \quad (4.1.3)$$

а числа $|\alpha_{00}|^2, |\alpha_{01}|^2, |\alpha_{10}|^2, |\alpha_{11}|^2$ – вероятности нахождения системы в каждом из четырёх собственных состояний $|00\rangle, |01\rangle, |10\rangle, |11\rangle$.

А чтобы проверить, относится ли матрица плотности к чистому состоянию, достаточно умножить её на саму себя. Если полученная матрица совпадёт с исходной, то есть если выполнится равенство $\rho^2 = \rho$, то можно сказать, что ρ описывает чистое состояния и для него может быть записан вектор состояния. То есть матрица ρ должна быть идемпотентной.

Приведём пример, пусть эволюция замкнутой квантовой системы описывается унитарным оператором U (а эволюция замкнутой квантовой системы может описываться лишь *унитарным преобразованием*, о чём гласит один из постулатов квантовой механики). Если система сначала находилась в состоянии $|\psi_i\rangle$ с вероятностью p_i, то в результате эволюции она окажется в состоянии $U|\psi_i\rangle$ с вероятностью p_i. Таким образом эволюцию оператора

плотности можно описать уравнением

$$\rho \equiv \sum_i p_i \left|\psi_i\right\rangle \left\langle\psi_i\right| \underset{\rightarrow}{U} \sum_i p_i U \left|\psi_i\right\rangle \left\langle\psi_i\right| U^\dagger = U \cdot \rho \cdot U^\dagger \quad (4.1.4)$$

Постулат из квантовой физики: квантовые измерения описываются множеством $\{M_m\}$ операторов измерения, то есть операторами, действующими в пространстве состояний системы, которая подвергается измерения. Если квантовая система находилась в состоянии $\left|\psi\right\rangle$, то вероятность того, что в результате измерения будет получен результат *m,* задаётся выражением

$p(m) = \langle\psi| M_m^\dagger M_m |\psi\rangle$ а после измерения система перейдёт в состояние

$$\frac{M_m \left|\psi\right\rangle}{\sqrt{\langle\psi| M_m^\dagger M_m |\psi\rangle}}$$

Теперь попробуем описать измерения состояний систем на языке операторов плотности. Положим, что мы проводим измерение, описываемое операторами $\{M_m\}$. Если система задавалась вектором $\left|\psi_i\right\rangle$, то вероятность результата *m* определяется выражением

$$p(m \vee i) = \left\langle\psi_i\right| M_m^\dagger M_m \left|\psi_i\right\rangle = tr\left(M_m^\dagger M_m \left|\psi_i\right\rangle \left\langle\psi_i\right|\right) = tr(M_m^\dagger M_m \rho)$$

После получения результата *m* состояние будет иметь вид

$$\left|\psi_i^m\right\rangle = \frac{M_m \left|\psi\right\rangle}{\sqrt{\langle\psi| M_m^\dagger M_m |\psi\rangle}}$$

Оператор плотности для системы, находящейся в чистом состоянии выглядит в виде $\rho = \left|\psi\right\rangle \left\langle\psi\right|$, иначе будем говорить, что ρ описывает *смешанное состояние* (или смесь разных чистых состояний в ансамбле).

Для чистого состояние верно следующее условие: $tr\left(\rho^2\right) = 1$ Для смешанных состояний: $tr\left(\rho^2\right) < 1$

Оператор ρ является оператором плотности, связанным с ансамблем $\left\{p_i, \left|\psi_i\right\rangle\right\}$, тогда и только тогда, когда выполнены условия:

1. *Условие единичности следа* $- tr(\rho) = 1$
2. *Условие неотрицательности* $-$ *ρ должен быть неотрицательно определённым оператором*.

Возможно так же и наиболее содержательное применение оператора плотности – использование его, как средства для описания подсистем составных квантовых систем. Это возможно с помощью *редуцированного*

оператора плотности, а полезен он тем, что встречается почти везде в анализе составных систем.

Положим, что у нас есть две квантовые системы A и B, а состояние составной системы описывается оператором ρ^{AB}. Тогда редуцированный оператор плотности для системы A определяется соотношением

$$\rho^A \equiv tr_B(\rho^{AB}) \quad (4.1.5)$$

где tr_B – отображение операторов, называемое частичным следом по системе B. Частичный след определяется следующим образом:

$$tr_B(|a_1\rangle\langle a_2| \otimes |b_1\rangle\langle b_2|) \equiv |a_1\rangle\langle a_2| tr(|b_1\rangle\langle b_2|), \quad (4.1.6)$$

$$|a_1\rangle,\ |a_2\rangle \epsilon A \qquad |b_1\rangle,\ |b_2\rangle \epsilon B$$

$$tr(|b_1\rangle\langle b_2|) = \langle b_2|b_1\rangle \qquad (4.1.7)$$

Рассмотрим небольшие примеры, чтобы получше понять написанное. Пусть квантовая система находится в состоянии, описываемом тензорным произведением $\rho^{AB} \equiv \rho \otimes \sigma$, где ρ и σ – операторы плотности для систем A и B, соответственно. Тогда

$$\rho^A = tr_B(\rho \otimes \sigma) = \rho\, tr(\sigma) = \rho \qquad (4.1.8)$$

Что и следовало ожидать исходя из интуитивных представлений. Аналогично для $\rho^B = \sigma$ **[7]**

Теперь взглянем на одно из состояний Белла:

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

Его оператор плотности равен:

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

Возьмём след по второму кубиту и найдём редуцированный оператор плотности для первого кубита:

$$\rho^1 = tr_2(\rho) = \frac{tr_2(|00\rangle\langle 00|) + tr_2(|11\rangle\langle 00|) + tr_2(|00\rangle\langle 11|) + tr_2(|11\rangle\langle 11|)}{\sqrt{2}} = \frac{|0\rangle\langle 0|\langle 0|0\rangle + |1\rangle\langle 0|\langle 0|1\rangle + |0\rangle\langle 1|\langle 1|0}{\sqrt{2}}$$

При этом полученное состояние является смешанным, т.к. $tr\left(\left(\frac{E}{2}\right)^2\right)=\frac{1}{2}<1$. Это интересный результат, потому что состояние системы, содержащей оба кубита, является чистым, т.е. известно точно, однако первый кубит находится в смешанном состоянии, о котором мы не можем получить полную информацию. Это необычное свойство – отличительный признак квантовой запутанности, по полному и известному состоянию всей системы мы, в общем случае, не можем определить её составные части.

4.2 Запутывание кубитов

Как говорилось ранее, из пары чистых кубитов можно получить пару запутанных с помощью некоторого преобразования, то есть двухкубитового гейта (в случае двух кубитов).

Двухкубитовый квантовый гейт G является линейным унитарным преобразованием $G: V \otimes V \to V \otimes V$, где V – векторное пространство размерности 2 над полем комплексных чисел $\mathbb{C}$

Гейт G называется универсальным, если он совместно с локальными унитарными преобразованиями H, S, и T (однокубитовыми гейтами) является образующим для всех унитарных линейных преобразований комплексного гильбертова пространства размерности 2^n. Проще говоря – некий набор элементов является универсальным для квантовых вычислений, если любая унитарная операция может быть сколь угодно точно аппроксимирована квантовой схемой, содержащей элементы только этого набора. Например для классических вычислений универсальным набором, создающим базис булевых функций, является And, Or, Not или, что используют чаще – базис из стрелки Пирса или штриха Шеффера. Опуская сложные доказательства, скажем, что универсальным семейством для квантовых вычислений служат CNOT и однокубитовые унитарные операторы.

Теорема *Брылинских* и матрица $\check{G}$:
Если имеется двухкубитовый гейт $G: V \otimes V \to V \otimes V,$ то он называется запутывающим в том случае, если существует вектор

$$|\alpha\beta\rangle = |\alpha\rangle \otimes |\beta\rangle \in V \otimes V \qquad (4.2.1)$$

такой что $G|\alpha\beta\rangle$ будет неразложимым на тензорное произведение двух кубитов. Только при выполнении этого условия $G|\alpha\beta\rangle$ будет запутан.

Так же братья Брылинские ввели критерий *универсальности* гейта G. В их учебнике было доказано, что двухкубитовый гейт G универсален тогда и только тогда, когда он запутывающий.

$$(\check{G}\otimes E)(E\otimes\check{G})(\check{G}\otimes E)=(E\otimes\check{G})(\check{G}\otimes E)(E\otimes\check{G}) \qquad (4.2.2)$$

Формула (2.3.2) является уравнением Янга-Бакстера, а гейт, $\check{G}$, который удовлетворяет этому равенству является *запутывающим* и называется $\check{R}$-матрицей.

Квадратная матрица $\check{G}$ является $\check{R}$-матрицей тогда и только тогда, когда выполняются следующие условия:

$$\check{G}=\begin{bmatrix} p & 0 & 0 & 0 \\ 0 & a & b & 0 \\ 0 & c & d & 0 \\ 0 & 0 & 0 & q \end{bmatrix}$$

1. $q^2a=qa^2+abc$
2. $p^2a=pa^2+abc$
3. $p^2d=pd^2+dbc$
4. $q^2d=qd^2+dbc$
5. $adb=adc=ad(a-b)=0$

Приведём пример $\check{G}$ – матрицы, которую мы исследуем.

$$\check{G}=\begin{bmatrix} a & 0 & 0 & 0 \\ 0 & 0 & d & 0 \\ 0 & c & 0 & 0 \\ 0 & 0 & 0 & b \end{bmatrix},$$

Для которой все условия 1-5 будут выполняться в следствии того, что $a=d=0$

где $ab\neq cd$. В таком случае матрица $\check{G}$ унитарна и является решением уравнения Янга-Бакстера.

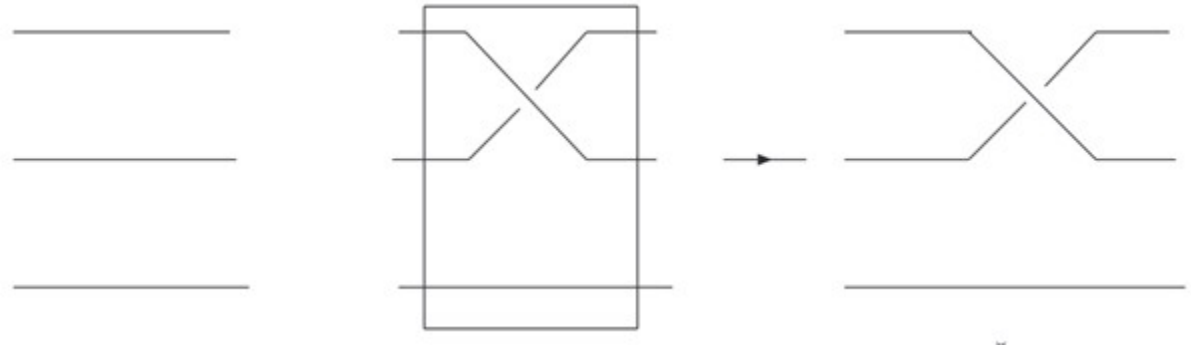


рис 3: оператор $\check{R} \otimes E$, который создаёт косу для трёх прямых

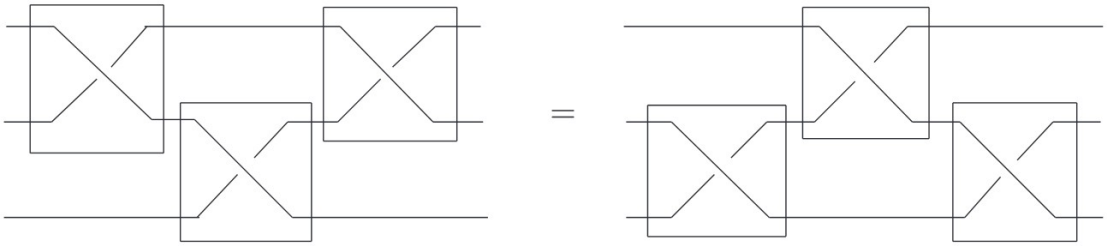
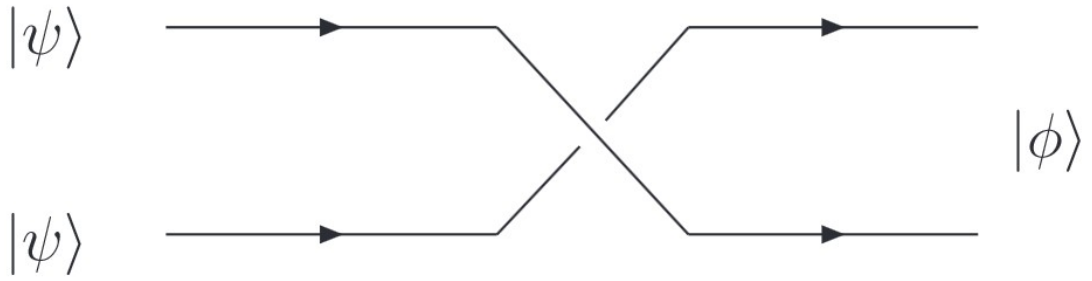


рис 4: Графическая иллюстрация уравнения Янга-Бакстера (отношения Янга-Бакстера)



$\check{R}(|\psi\rangle \otimes |\psi\rangle) = |\phi\rangle$

рис 5: «Вяжущий» оператор $\check{R}$ в виде запутывающего оператора

Приведём пример, иллюстрирующий запутывание двух кубитов с помощью $\check{R}$-матрицы. Пусть имеются два кубита

$$|\psi_1\rangle = |\psi_2\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle,$$

Определим $\check{R}$-матрицу следующим образом:

$$\check{R} = 2\begin{bmatrix} a & 0 & 0 & 0 \\ 0 & 0 & d & 0 \\ 0 & c & 0 & 0 \\ 0 & 0 & 0 & b \end{bmatrix},$$

где $ab \neq cd$ и $|a|^2+|b|^2+|c|^2+|d|^2=1$

Тогда воздействуя на тензорное произведение кубитов $|\psi_1\rangle$ и $|\psi_2\rangle$ получим следующее состояние

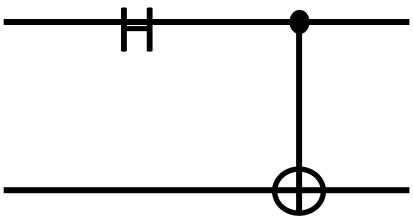
$\check{R}\left(|\psi_1\rangle \otimes |\psi_2\rangle\right)=a|00\rangle+c|01\rangle+d|10\rangle+b|11\rangle=|\psi\rangle$

Очевидно, что $|\psi\rangle$ является неразложимым на тензорное произведение двух кубитов и, следовательно, запутанным.

4.3 Состояния и неравенство Белла

В первой главе мы уже рассматривали состояние Белла $|\psi\rangle=\frac{|01\rangle-|10\rangle}{\sqrt{2}}$ и рассказали об удивительном результате запутанности двух кубитов, в котором при измерении одного из них в любом вычислительном базисе имеется возможность достоверно предсказать результат измерения второго.

Получаются состояния Белла простым способом, показанном на



рисунке ниже

рис 6: Квантовая схема, создающее состояния Белла

Результаты, получаемые при использовании этой схемы с различными кубитами на входе будут выглядеть следующим образом:

$\|00\rangle$	$\frac{\|00\rangle+\|11\rangle}{\sqrt{2}} \equiv \|\beta_{00}\rangle$
$\|01\rangle$	$\frac{\|01\rangle+\|10\rangle}{\sqrt{2}} \equiv \|\beta_{01}\rangle$
$\|10\rangle$	$\frac{\|00\rangle-\|11\rangle}{\sqrt{2}} \equiv \|\beta_{10}\rangle$

$\|11\rangle$	$\frac{\|01\rangle - \|10\rangle}{\sqrt{2}} \equiv \|\beta_{11}\rangle$

таблица 1: таблица значения дла произвольного входного и выходного состояний

Перейдём от обычных состояний Белла и ЭПР-эксперимента к принципу неравенства Белла.

Представим, что мы готовимся к эксперименту, который описывался в главе 1.3 и исходное состояние двух частиц лишь в процессе приготовления. При этом нам совершенно неважно, каким именно состояние окажется, существеннно лишь то, что подготовка может происходит сколько угодно раз. По её окончании одна частица отправляется Алисе, а вторая – Бобу. Когда Алиса получит свою частицу, она должна будет выполнить её измерение. Предположим, что в её распоряжении имеются два разных прибора, то есть она может выбрать, какое из двух измерений P_Q и P_R ей провести. Так же Алиса не знает, что она выберет, это определяется случайным образом, – броском монетки или чётностью количества прохожих за окном. Для простоты будем считать, что каждое из измерений имеет лишь два возможных исхода: +1 и -1. Предположим, Алиса в результате измерения P_Q для своей частицы получила значение Q, тогда полагается, что Q – объективная характеристика частицы, находящейся у Алисы, которая была просто обнаружена в результате измерения (Которая существовала до измерения и была у частницы НЕ зависимо от того, что она оказалась у бедной Алисы с её измерениями). Аналогичным образом поступим с измерением P_R и R назовём характеристикой, полученной в результате другого процесса.

Так же положим, что Боб находится в такой же ситуацией с характеристиками P_S и P_T, объективно определяя существующие значения величины S или T, каждая из которых принимает или +1 или -1. Боб так же не знает, что именно будет измерять, определяя свой выбор лишь после получения частицы. А временные рамки эксперимента подобраны таким образом, что Алиса и Боб проводят измерения в одно и то же время, то есть провоизводимое Алисой действие не может повлять на результат Боба и наоборот, так как физическое воздействие не может распространяться со скоростью, превышающей скорость света.

Теперь проведёт некоторые преобразования выражения $QS+RS+RT-QT$:

$$QS+RS+RT-QT=(Q+R)S+(R-Q)T \qquad (4.3.1)$$

Так как $R=Q=\pm 1$, то либо $(Q+R)S=\pm 2$, а $(R-Q)T=0$, либо наоборот, - $(Q+R)S=0$ и $(R-Q)T=\pm 2$. В обоих случаях из этого следует $QR+RS+RT-QT=\pm 2$. Обозначит через $p(q,r,s,t)$ вероятность того, что перед измерением система находится в таком состоянии, где $Q=q$, $R=r$, $S=s$,$T=t$. Эти вероятности могут зависить от того, как именно Чарли подготавливает исходное состояние, а так же от экспериментального шума. Обозначим через $M(\cdot)$ математическое ожидание, тогда получим

$$M(QS+RS+RT-QT)=\sum_{q,r,s,t} p(q,r,s,t)(qs+rs+rt-qt)\le \sum_{q,r,s,t} p(q,r,s,t)\times 2=2 (4.3.2)$$

Кроме того, полчим следующее соотношение:

$$M(QS+RS+RT-QT)=\sum_{q,r,s,t} p(q,r,s,t)qs+\sum_{q,r,s,t} p(q,r,s,t)rs+\sum_{q,r,s,t} p(q,r,s,t)rt-\sum_{q,r,s,t} p(q,r,s,t)qt=$$

Сравнив последние два равенства можно записать ключевое *неравенство Белла*:

M ¿

Которое также носит название *CHSH-неравенства* (в честь Clauser, Horn, Shimony, Holt – его первооткрывателей).

Многократно повторяя эксперимент Алиса и Боб могут определить каждую из величит, находящихся в левой части неравенства. Пусть после некоторой серии экспериментов Алиса и Боб встретятся и проанализируют полученные данные. Они возьмут результаты, где Алиса определяла P_Q, а Боб - P_S. Перемножив результаты, они найдут экспериментальное значение QS, а усреднив полученные величины, можно вычислить $M(QS)$ с точностью, ограничиваемой только числом проведённых измерений. Аналогичным образом можно определить все остальные необходимые величины, входящие в левую часть неравенство Белла, тем самым проверив, выполняется ли оно.

Посмотрим теперь на эксперимент с точки зрения механизма квантовой механики. Чарли подготавливает ту же самую систему в начальном состоянии

$$|\psi\rangle=\frac{|01\rangle-|10\rangle}{\sqrt{2}}$$

после чего первый кубит отдаётся Алисе, а второй – Бобу. Они выполняют свои измерения на следующих наблюдаемых

$$Q=Z_1, \qquad S=\frac{-Z_2-X_2}{\sqrt{2}}, \qquad R=X_1, \qquad T=\frac{Z_2-X_2}{\sqrt{2}}$$

Простые вычисления дадут нам средние значения с применением обозначений $\langle\cdot\rangle$, которые имеют вид:

$$\langle QS\rangle=\frac{1}{\sqrt{2}}, \qquad \langle RS\rangle=\frac{1}{\sqrt{2}}, \qquad \langle RT\rangle=\frac{1}{\sqrt{2}}, \qquad \langle QT\rangle=\frac{1}{\sqrt{2}},$$

$$\langle QS\rangle+\langle RS\rangle+\langle RT\rangle-\langle QT\rangle=\frac{2}{\sqrt{2}}$$

что противоречит исходному неравенству Белла.

Из этого следует, что некоторые предположения, которые были сделаны, неверны, а именно:

1. P_Q, P_R, P_S, P_T могут не существовать. Один из постулатов квантовой механики говорит, что они *определяются* лишь в момент измерения.
2. Выполнения измерения своего элемента Алисой может повлиять на результат Боба, что называется предположением *локальности.* [8]

4.4 Мера запутанности чистых систем

Мера квантовой запутанности - это количественная характеристика несепарабельности, числовое значение величины квантовых корреляций и степени нелокальности объекта. И когда речь заходит о количественном описании квантовой запутанности, то обращаться стоит к матрицам плотности. Вспомним одно из состояний Белла, а именно

$$|\psi\rangle=\frac{|01\rangle-|10\rangle}{\sqrt{2}}$$

Это суперпозиций состояний, которые не могут быть реализованы одновременно. Спины не могут быть одновременно направлены «вверх» и «вниз», но согласно этому выражению они с равной вероятностью (1/2) находятся в положении «вверх» и «вниз». При этом их нельзя считать независимыми, так как они связаны нелокальными квантовыми корреляциями или, как уже говорилось ранее, запутаны. Однако теперь стоит сказать, что все те состояния Белла, которые мы показывали, то есть:

$$|\psi\rangle=\frac{|01\rangle\mp|10\rangle}{\sqrt{2}} \text{ и } |\psi\rangle=\frac{|00\rangle\mp|11\rangle}{\sqrt{2}}$$

являются не просто запутанными, а максимально запутанными.

По определению: максимально запутанным состоянием двухсоставной квантовой системы Q (состоящей из подсистем A и B) называются чистые состояния, для которых частичные матрицы плотности пропорциональны единичной матрице

Введём количественную характеристику запутанности. В терминах энтропии фон-Неймана в 1996 году Чарльзом Беннеттом была предложена следующая мера, которая представляет собой аналог энтропии Шеннона, но для квантовой информации.

$$E(\psi)=S(\rho_A)=S(\rho_B) \qquad (4.4.1)$$

В свою очередь $S(\rho_{A(B)})=-Tr\{\rho_{A(B)}\log_2\rho_{A(B)}\}$

Рассмотрим чистое состояние (1.1.2)

$$|\psi\rangle=\alpha|00\rangle+\beta|11\rangle\ |\alpha|^2+|\beta|^2=1,$$

тогда по определению (2.1.2)

$\rho=|\psi\rangle\langle\psi|=(\alpha|00\rangle+\beta|11\rangle)(\alpha^{¿}\langle 00|+\beta^{¿}\langle 11|)=¿$
$¿|\alpha|^2|00\rangle\langle 00|+\alpha\beta^{¿}|00\rangle\langle 11|+\beta\alpha^{¿}|11\rangle\langle 00|+|\beta|^2|11\rangle\langle 11|$

$$|00\rangle\langle 00|=\begin{bmatrix}1&0&0&0\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{bmatrix} \qquad |00\rangle\langle 11|=\begin{bmatrix}0&0&0&1\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{bmatrix}$$

$$|11\rangle\langle 00|=\begin{bmatrix}0&0&0&0\\0&0&0&0\\0&0&0&0\\1&0&0&0\end{bmatrix} \qquad |11\rangle\langle 11|=\begin{bmatrix}0&0&0&0\\0&0&0&0\\0&0&0&0\\0&0&0&1\end{bmatrix}$$

$$\rho=\begin{bmatrix}|\alpha|^2&0&0&\alpha\beta^{¿}\\0&0&0&0\\0&0&0&0\\\beta\alpha^{¿}&0&0&|\beta|^2\end{bmatrix},$$

а редуцированный оператор плотности $\rho_A=\rho_B=|\alpha|^2|0\rangle\langle 0|+|\beta|^2|1\rangle\langle 1|$

$$\rho_A=\rho_B=\begin{bmatrix}|\alpha|^2&0\\0&|\beta|^2\end{bmatrix}$$

Теперь найдём собственные числа матрицы плотности, то есть решим уравнение $det(\rho-\lambda E)=0$. Поверим автору, который опустил некоторые томные вычисления, что $\lambda_1=1$, а $\lambda_2=\lambda_3=\lambda_4=0$. То есть матрица имеет одно ненулевое собственное значение равное единице. Это свойство являет собой характерную черту любого чистого состояния, т.е. матрица плотности произвольного чистого состояния имеет только одно, равное единице, собственное значение.

$$\log_2\rho=\begin{bmatrix}\log_2 1 & 0 & 0 & 0\\ 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0\end{bmatrix}=0$$

То есть энтропия чистого состояния $S(\rho)=-Tr\{\rho\log_2\rho\}$ для $|\psi\rangle=\alpha|00\rangle+\beta|11\rangle$ равна нулю, что не удивительно, ведь никакой информации о чистом состоянии то и нет.

Теперь перейдём к энтропии частичных матриц плотности ρ_A и ρ_B.

$\rho_A=\rho_B=\begin{bmatrix}|\alpha|^2 & 0\\ 0 & |\beta|^2\end{bmatrix}$, то есть $\lambda_1=|\alpha|^2$, а $\lambda_2=|\beta|^2$

$$\log_2\rho_A=\log_2\rho_B=\begin{bmatrix}\log_2|\alpha|^2 & 0\\ 0 & \log_2|\beta|^2\end{bmatrix}$$

$$\rho_A\log_2\rho_A=\begin{bmatrix}|\alpha|^2 & 0\\ 0 & |\beta|^2\end{bmatrix}\begin{bmatrix}\log_2|\alpha|^2 & 0\\ 0 & \log_2|\beta|^2\end{bmatrix}=\begin{bmatrix}|\alpha|^2\log_2|\alpha|^2 & 0\\ 0 & |\beta|^2\log_2|\beta|^2\end{bmatrix}$$

$$\rho_A\log_2\rho_A=\begin{bmatrix}\lambda_1\log_2\lambda_1 & 0\\ 0 & \lambda_2\log_2\lambda_2\end{bmatrix}$$

откуда получим, что

$$E(\psi)=S(\rho_A)=S(\rho_B)=-Tr\{\rho_{A(B)}\log_2\rho_{A(B)}\}=¿-|\alpha|^2\log_2|\alpha|^2-|\beta|^2\log_2|\beta|^2 \quad (4.4.2)$$

Не проводя лишних вычислений можно сразу сказать, что энтропия, а значит и мера запутанности этого состояния, больше или равна нулю, ведь коэффициенты $|\alpha|^2$ и $|\beta|^2$ в сумме должны равняться единице. А равенство достигается лишь в одном из двух случаев, когда $|\alpha|^2=0$ и $|\beta|^2=1$, либо наоборот, $|\beta|^2=0$, $|\alpha|^2=1$

При этом несложно показать, что при наличии $|\alpha|^2=|\beta|^2=\frac{1}{2}$, то $E(\psi)$ будет равна максимальна и равняться единице.

В самом деле, $E(\psi)=S(\rho_A)=-\left(\frac{1}{2}\log_2\left(\frac{1}{2}\right)+\frac{1}{2}\log_2\left(\frac{1}{2}\right)\right)=-\left(\frac{-1-1}{2}\right)=1$

Следует еще раз акцентировать внимание на том, что количественная характеристика, то есть мера, запутанности двухсоставной системы является энропия частичных, редуцированных матриц плотности. Энтропия с окружением же определяется энтропией Фон Неймана от оператора плотности и в нашем случае равна нулю, из-за того, что запутанности с окружением чистого состояния просто напросто нет.

Выведем теперь конечные формулы для чистого состояния

$$|\psi\rangle=a|00\rangle+b|01\rangle+c|10\rangle+d|11\rangle \quad (4.4.3)$$

Матрица плотности в данном случае будет выглядеть следующим образом

$$\rho=|\psi\rangle\langle\psi|=\left(a|00\rangle+b|01\rangle+c|10\rangle+d|11\rangle\right)*\left(a^{¿}\langle 00|+b^{¿}\langle 01|+c^{¿}\langle 10|+d^{¿}\langle 11|\right)=¿$$

$$\rho=\begin{bmatrix} |a|^2 & a\cdot b^{¿} & a\cdot c^{¿} & a\cdot d^{¿} \\ b\cdot a^{¿} & |b|^2 & b\cdot c^{¿} & b\cdot d^{¿} \\ c\cdot a^{¿} & c\cdot b^{¿} & |c|^2 & c\cdot d^{¿} \\ d\cdot a^{¿} & d\cdot b^{¿} & d\cdot c^{¿} & |d|^2 \end{bmatrix} \quad (4.4.4)$$

Далее вычислим редуцированный оператор плотности $\rho_A=tr_B(\rho^{AB})$, где $tr_B(|a_1a_2\rangle\otimes\langle b_1b_2|)\equiv|a_1\rangle\langle b_1|tr(|a_2\rangle\langle b_2|)$, если в более удобном виде переписать формулу (2.1.5), тогда $tr\left(|a_2\rangle\langle b_2|\right)=\langle b_2|a_2\rangle$

Нетрудно заметить, что $tr(|a_2\rangle\langle b_2|)$ будет нулевым в случае, $a_2=|0\rangle$, $\langle b_2|=\langle 1|$ и $a_2=|1\rangle$, $\langle b_2|=\langle 0|$, потому что $|0\rangle\langle 1|=\begin{bmatrix}0 & 1\\ 0 & 0\end{bmatrix}$ и $tr\begin{bmatrix}0 & 1\\ 0 & 0\end{bmatrix}=0$, а так же $tr\left(|1\rangle\langle 0|\right)=tr\begin{bmatrix}0 & 0\\ 1 & 0\end{bmatrix}=0$. Грубо говоря для двухкубитового состояния частичный след будет нулевым, если значения в последних разрядах соппадают, то есть выполняется следующее равенство

$$tr_B\left(|a_1a_2\rangle\otimes\langle b_1b_2|\right)=0 \text{ тогда и только тогда, когда } a_2\neq b_2$$

$$\rho_A=tr_B\left(a|00\rangle+b|01\rangle+c|10\rangle+d|11\rangle\right)\left(a^{¿}\langle 00|+b^{¿}\langle 01|+c^{¿}\langle 10|+d^{¿}\langle 11|\right)$$

Из этого выражения у нас в итоге останется только перемножение коэффициентов перед векторами, умноженных на произведение векторов из однокубитового базиса.

$\rho_A = a a^{¿} |0\rangle\langle 0| + a c^{¿} |0\rangle\langle 1| + b b^{¿} |0\rangle\langle 0| + b d^{¿} |0\rangle\langle 1| + c a^{¿} |1\rangle\langle 0| + c c^{¿} |1\rangle\langle 1| + ¿$

$+ d b^{¿} |1\rangle\langle 0| + d d^{¿} |1\rangle\langle 1|$, сгруппировав коэффициенты, получим

$$\rho_A = \left(|a|^2 + |b|^2\right)|0\rangle\langle 0| + \left(a c^{¿} + b d^{¿}\right)|0\rangle\langle 1| + \left(c a^{¿} + d b^{¿}\right)|1\rangle\langle 0| + \left(|c|^2 + |d|^2\right)|1\rangle\langle 0| = \begin{bmatrix} |a|^2 + |b|^2 & a c^{¿} + b d^{¿} \\ c a^{¿} + d b^{¿} & |c|^2 + |d|^2 \end{bmatrix} \quad (4.4.5)$$

Дальше попробуем найти собственные числа этой матрицы, решив следующее уравнение

$$\begin{bmatrix} |a|^2 + |b|^2 - \lambda & a c^{¿} + b d^{¿} \\ c a^{¿} + d b^{¿} & |c|^2 + |d|^2 - \lambda \end{bmatrix} = 0$$

$$\lambda^2 - \lambda\left(|a|^2 + |b|^2 + |c|^2 + |d|^2\right) + |a|^2|c|^2 + |a|^2|d|^2 + |b|^2|c|^2 + |b|^2|d|^2 - |a|^2|c|^2 - |b|^2|d|^2 - a b^{¿} c^{¿} d - a^{¿} b c d^{¿}$$

$$\lambda^2 - \lambda + \left(|a|^2|d|^2 + |b|^2|c|^2 - a b^{¿} c^{¿} d - a^{¿} b c d^{¿}\right) = 0$$

Тогда корни этого уравнения будут равняться

$$\lambda_1 = \frac{1}{2}\left(1 + \sqrt{1 - 4\left(|a|^2|d|^2 + |b|^2|c|^2 - a b^{¿} c^{¿} d - a^{¿} b c d^{¿}\right)}\right)$$

$$\lambda_2 = \frac{1}{2}\left(1 - \sqrt{1 - 4\left(|a|^2|d|^2 + |b|^2|c|^2 - a b^{¿} c^{¿} d - a^{¿} b c d^{¿}\right)}\right)$$

Подставив всё это в исходную формулу 3.1.1 получим, что

$$E(\psi) = S(\rho_A) = -Tr\{\rho \log_2 \rho\} = -\lambda_1 \log_2 \lambda_1 - \lambda_2 \log_2 \lambda_2 \quad (4.4.6)$$

(в целом формула не изменилась, но теперь у нас есть выведенные λ_1 и λ_2 для общего вектора $|\psi\rangle$.

Ранее в формуле 2.1.1 мы говорили, что состояния запутаны тогда и только тогда, когда выполняется неравенство $a d - bc \neq 0$ или $a d \neq bc$, теперь мы можем проверить это.

Допустим мы выберем $a d = bc$, тогда будет выполняться $a^{¿} d^{¿} = b^{¿} c^{¿}$, перепишем собственные числа λ_1 и λ_2

$$|a|^2|d|^2 + |b|^2|c|^2 - a b^{¿} c^{¿} d - a^{¿} b c d^{¿} = 2|b|^2|c|^2 - b b^{¿} c^{¿} c - b^{¿} b c c^{¿} = ¿¿ 2|b|^2|c|^2 - |b|^2|c|^2 - |b|^2|c|^2 = 0$$

Тогда

$$\lambda_1=\frac{1}{2}\left(1+\sqrt{1-4\left(|a|^2|d|^2+|b|^2|c|^2-a\,b\,c\,d-a\,bc\,d\right)}\right)=\frac{1}{2}(1+1)=1$$

$$\lambda_2=\frac{1}{2}\left(1-\sqrt{1-4\left(|a|^2|d|^2+|b|^2|c|^2-a\,b\,c\,d-a\,bc\,d\right)}\right)=\frac{1}{2}(1-1)=0$$

Подставим полученные результаты в формулу 3.1.6

$$E(\psi)=S(\rho_A)=-Tr\{\rho\log_2\rho\}=-\lambda_1\log_2\lambda_1-\lambda_2\log_2\lambda_2=0-0\log_2 0=0$$

То есть мера запутанности *произвольной* двухкубитовой система равна нулю, что и требовалось доказать.

4.5 Согласованность, как характеристика запутанности

Согласованность, описанная Чарльзом Беннеттом и Вуттерсом в 1996-1997 годах, является еще одной количественной характеристикой запутанности и определяется, как

$$C(\psi)=\left|\sum_i \alpha_i{}^2\right| (4.5.1)$$

где α_i – коэффициенты разложения произвольного вектора двухкубитовой системы

$$|\psi\rangle=\sum_{i=1}^{4}\alpha_i|\beta_i\rangle$$

в базисе Белла, состоящего из:

$$\frac{|00\rangle+|11\rangle}{\sqrt{2}}\equiv|\beta_1\rangle \qquad i\frac{|01\rangle+|10\rangle}{\sqrt{2}}\equiv|\beta_3\rangle$$

$$i\frac{|00\rangle-|11\rangle}{\sqrt{2}}\equiv|\beta_2\rangle \qquad \frac{|01\rangle-|10\rangle}{\sqrt{2}}\equiv|\beta_4\rangle$$

Запутанность состояния $|\psi\rangle$ выражается через $C(\psi)$, как

$$E(\psi)=H\left[\frac{1}{2}(1+\sqrt{1-C^2})\right], (4.5.2)$$

где $H(x)$ – бинарная функция энтропии:

$$H(x)=-x\log_2(x)-(1-x)\log_2(1-x) \qquad (4.5.3)$$

В целом согласованность характеризует, насколько близко наш вектор состояния $|\psi\rangle$ разбивается на линейную комбинацию максимально запутанных состояний.

Рассмотрим аналитический метод вычисления согласованности, основанный на матрице перевёрнутых спинов, - приёме, называемом в зарубежной литературе, как «Spin-flip»

$$\tilde{\rho}=(\sigma_y\otimes\sigma_y)\rho^{*}(\sigma_y\otimes\sigma_y) \qquad (4.5.4)$$

$$\sigma_y=\begin{bmatrix}0 & -i\\ i & 0\end{bmatrix} \text{ – матрица Паули}$$

После нахождения $\tilde{\rho}$, необходимо вычислить $\rho\tilde{\rho}$ – неэрмитову матрицу с вещественными, неотрицательными собственными значениями. В таком случае согласованность может быть найдена, как

$$C=max\left\{\sqrt{\lambda_1}-\sqrt{\lambda_2}-\sqrt{\lambda_3}-\sqrt{\lambda_4},0\right\}, \qquad (4.5.5)$$

где λ_i- собственные значения $\rho\tilde{\rho}$. Если ненулевых собственных значения два, то:

$$C=\left|\sqrt{\lambda_1}-\sqrt{\lambda_2}\right| \qquad (4.5.6)$$

Снова приведём пример с состоянием $|\psi\rangle=\alpha|00\rangle+\beta|11\rangle$, матрица плотности этого состояния имеет вид

$$\rho=\begin{bmatrix}|\alpha|^2 & 0 & 0 & \alpha\beta^{*}\\ 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0\\ \beta\alpha^{*} & 0 & 0 & |\beta|^2\end{bmatrix}, \text{ а комплексно-сопряжённая } \rho^{*}=\begin{bmatrix}|\alpha|^2 & 0 & 0 & \alpha^{*}\beta\\ 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0\\ \beta^{*}\alpha & 0 & 0 & |\beta|^2\end{bmatrix}$$

$$\sigma_y\otimes\sigma_y=\begin{bmatrix}0 & -i\\ i & 0\end{bmatrix}\otimes\begin{bmatrix}0 & -i\\ i & 0\end{bmatrix}=\begin{bmatrix}0 & 0 & 0 & -1\\ 0 & 0 & 1 & 0\\ 0 & 1 & 0 & 0\\ -1 & 0 & 0 & 0\end{bmatrix}$$

$$\tilde{\rho}=\begin{bmatrix}0 & 0 & 0 & -1\\ 0 & 0 & 1 & 0\\ 0 & 1 & 0 & 0\\ -1 & 0 & 0 & 0\end{bmatrix}\begin{bmatrix}|\alpha|^2 & 0 & 0 & \alpha^{*}\beta\\ 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0\\ \beta^{*}\alpha & 0 & 0 & |\beta|^2\end{bmatrix}\begin{bmatrix}0 & 0 & 0 & -1\\ 0 & 0 & 1 & 0\\ 0 & 1 & 0 & 0\\ -1 & 0 & 0 & 0\end{bmatrix}$$

$$\tilde{\rho}=\begin{bmatrix} |\beta|^2 & 0 & 0 & \beta^{¿}\alpha \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \alpha^{¿}\beta & 0 & 0 & |\alpha|^2 \end{bmatrix}$$

$$\rho\tilde{\rho}=\begin{bmatrix} |\alpha|^2 & 0 & 0 & \alpha\beta^{¿} \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \beta\alpha^{¿} & 0 & 0 & |\beta|^2 \end{bmatrix}\begin{bmatrix} |\beta|^2 & 0 & 0 & \beta^{¿}\alpha \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \alpha^{¿}\beta & 0 & 0 & |\alpha|^2 \end{bmatrix}$$

$$\rho\tilde{\rho}=\begin{bmatrix} 2|\alpha|^2|\beta|^2 & 0 & 0 & 2|\alpha|^2\alpha\beta^{¿} \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 2|\beta|^2\beta\alpha^{¿} & 0 & 0 & 2|\alpha|^2|\beta|^2 \end{bmatrix}$$

Избегая лишних подробностей, сразу скажем ответ. Эта матрица имеет только одно ненулевое собственное значение $\lambda=4|\alpha|^2|\beta|^2$, тогда

$$C=2|\alpha||\beta| \qquad\qquad C^2=4|\alpha|^2|\beta|^2$$

Посчитаем теперь запутанность, через полученную согласованность элементов.

$$E(\psi)=H\left[\frac{1}{2}(1+\sqrt{1-C^2})\right]=H\left[\frac{1}{2}(|\alpha|^2+|\beta|^2\pm(|\alpha|^2-|\beta|^2))\right],$$

Это выражение разбивается на два

$$E_1(\psi)=H\left[|\alpha|^2\right] \qquad\qquad E_2(\psi)=H\left[|\beta|^2\right],$$

а в конечном результате получим, что

$$E_1(\psi)=E_2(\psi)=-|\alpha|^2\log_2|\alpha|^2-|\beta|^2\log_2|\beta|^2,$$

результат, который совпал с ранее найденным (3.1.2), что не вызывает никаких вопросов. **[9]**

Список литературы

[1] Jaynes, E. T., «Information Theory and Statistical Mechanics», 1957

[2] John A. Wheeler, «Information, physics, quantum: The search for links», 1990

[3] В. А. Орлов, Л. И. Филиппов, «Теория информации в упражнениях и задачах», 1976

[4] Александр Львовский, «Квантовые технологии», http://postnauka.ru/faq/24983, 2014

[5] А. М. Яглом, И. М. Яглом, «Вероятность и информация», 1973

[6] Claude E. Shannon, «A mathematical theory of communication», 1948

[7] Claude E. Shannon, «Communication in the presence of noise», 1949

[8] А. Н. Колмогоров, «Теория информации и теория алгоритмов», 1987

[9] Neumann J. von, Gött. Nach, 1927

[10] С. Доронин, «Квантовая магия», 2007

[11] Майя Бессараб, «Страницы жизни Ландау», 1971

[12] С. А. Чивилихин, «Квантовая информатика», Учебное пособие, СпБ. 2009.- 80 с.