АЛИЕВ Физули Камилович — доктор физико-математических наук, ведущий советник Главного управления развития информационных и телекоммуникационных технологий Министерства обороны Российской Федерации (ГУРИТТ МО РФ) (Москва)

КОРОЛЬКОВ Андрей Вячеславович — кандидат технических наук, доцент, член-корреспондент Академии криптографии Российской Федерации (АК РФ), заведующий кафедрой ФГБУ ВО Московский технологический университет (МИРЭА), заведующий лабораторией АК РФ (Москва)

МАТВЕЕВ Евгений Анатольевич — директор научно-технического предприятия «Криптософт» (Пенза)

Посвящена разработке базовых элементов теории несепарабельных состояний многокубитных квантовых систем. Представленные результаты улучшают понимание несепарабельности – одного из основных ресурсов современных квантовых технологий хранения, обработки и передачи информации, не имеющего классических аналогов; расширяют возможности разработки квантовых алгоритмов и построения систем квантовой криптографии и связи. Приводится один из модельных вариантов технологии связи, основанной на использовании квантового физического ресурса – несепарабельности.

Ориентирована на широкий круг читателей, интересующихся новыми направлениями развития информационных и телекоммуникационных технологий

ISBN 978-5-93108-148-9

Ф. К. Алиев
А. В. Корольков
Е. А. Матвеев
НЕСЕПАРАБЕЛЬНЫЕ СОСТОЯНИЯ МНОГОКУБИТНЫХ КВАНТОВЫХ СИСТЕМ

Ф. К. Алиев
А. В. Корольков
Е. А. Матвеев

НЕСЕПАРАБЕЛЬНЫЕ СОСТОЯНИЯ МНОГОКУБИТНЫХ КВАНТОВЫХ СИСТЕМ

Под редакцией Ф. К. Алиева

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

$$\text{B: } |0\rangle$$

$$\text{BAC: } \frac{|000\rangle + |011\rangle}{\sqrt{2}} = |0\rangle \otimes \left(\frac{|00\rangle + |11\rangle}{\sqrt{2}}\right)$$

$$\text{ACB: } \frac{|000\rangle + |110\rangle}{\sqrt{2}} = \left(\frac{|00\rangle + |11\rangle}{\sqrt{2}}\right) \otimes |0\rangle$$

$$\text{ABC: } \frac{|000\rangle + |101\rangle}{\sqrt{2}} = ?$$

РАДИОТЕХНИКА

Ф. К. Алиев, А. В. Корольков, Е. А. Матвеев

НЕСЕПАРАБЕЛЬНЫЕ СОСТОЯНИЯ МНОГОКУБИТНЫХ КВАНТОВЫХ СИСТЕМ

Монография

Под редакцией Ф. К. Алиева

Москва
Радиотехника
2017

УДК 681.327+530.145
ББК 32.973.202
А 50

***Авторы*:**

Алиев Физули Камилович – доктор физико-математических наук, ведущий советник Главного управления развития информационных и телекоммуникационных технологий Министерства обороны Российской Федерации (ГУРИТТ МО РФ) (Москва);

Корольков Андрей Вячеславович – кандидат технических наук, доцент, член-корреспондент Академии криптографии Российской Федерации (АК РФ), заведующий кафедрой ФГБУ ВО Московский технологический университет (МИРЭА), заведующий лабораторией АК РФ (Москва);

Матвеев Евгений Анатольевич – директор научно-технического предприятия «Криптософт» (Пенза)

***Рецензенты*:**

Барковский С.С. – доктор технических наук, преподаватель кафедры государственного управления и национальной безопасности Военной академии Генерального штаба Вооруженных Сил РФ;

Рожков М.И. – доктор технических наук, профессор кафедры компьютерной безопасности Департамента прикладной математики Московского института электроники и математики Национального исследовательского университета «Высшая школа экономики»

Алиев Ф. К., Корольков А. В., Матвеев Е. А.

А50 Несепарабельные состояния многокубитных квантовых систем. Монография / Под ред. *Ф. К. Алиева*. – М.: Радиотехника. 2017. – 320 с.

ISBN 978-5-93108-148-9

Посвящена разработке базовых элементов теории несепарабельных состояний многокубитных квантовых систем. Представленные результаты улучшают понимание несепарабельности – одного из основных ресурсов современных квантовых технологий хранения, обработки и передачи информации, не имеющего классических аналогов; расширяют возможности разработки квантовых алгоритмов и построения систем квантовой криптографии и связи. Приводится один из модельных вариантов технологии связи, основанной на использовании квантового физического ресурса – несепарабельности.

Ориентирована на широкий круг читателей, интересующихся новыми направлениями развития информационных и телекоммуникационных технологий.

УДК 681.327+530.145
ББК 32.973.202

ISBN 978-5-93108-148-9

ОГЛАВЛЕНИЕ

Список используемых обозначений

$\in$	– знак принадлежности;
$\varnothing$	– пустое множество;
$\lvert M \rvert$	– мощность множества *M*, то есть количество элементов в множестве *M*;
$M_0 \cup M_1$	– объединение множеств M_0 и M_1;
$M_0 \cap M_1$	– пересечение множеств M_0 и M_1;
$M_0 \setminus M_1$	– разность множеств M_0 и M_1;
$\mathbb{N}$	– множество натуральных чисел;
$\mathbb{Z}$	– множество целых чисел;
$\mathbb{R}$	– множество (поле) действительных (вещественных) чисел;
$\mathbb{C}$	– множество (поле) комплексных чисел;
i	– мнимая единица, то есть $i^2 = -1$; $i \in \mathbb{C}$;
$\mathbb{R}^n$	– линейное *n*-мерное пространство вектор-столбцов с действительными координатами (линейное *n*-мерное пространство вектор-столбцов над полем действительных чисел $\mathbb{R}$);
$\mathbb{C}^n$	– линейное *n*-мерное пространство вектор-столбцов с комплексными координатами (конечномерное гильбертово пространство размерности *n* над полем комплексных чисел $\mathbb{C}$);
$\lvert\psi\rangle$	– вектор-столбец с комплексными координатами (кет-вектор);
$\langle\psi\rvert$	– вектор-строка, двойственная к вектор-столбцу $\lvert\psi\rangle$, то есть вектор-строка, получаемая из вектор-столбца $\lvert\psi\rangle$ путем замены всех его координат на комплексно сопряженные к ним и последующего применения операции транспонирования (бра-вектор);
$\langle\varphi\vert\psi\rangle$	– скалярное произведение векторов $\lvert\varphi\rangle$ и $\lvert\psi\rangle$;

$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \in \mathbb{C}^2$;

$|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \in \mathbb{C}^2$;

$A = A_{m,n} = (a_{ij})$ – матрица размера $m \times n$; a_{ij} – элемент матрицы A, стоящий на пересечении i-й строки и j-го столбца матрицы A;

A^{T} – матрица, транспонированная к матрице A;

$\otimes$ – знак операции тензорного произведения;

$A \otimes B$ – тензорное произведение матриц A и B; если $A = (a_{ij})$ – матрица размера $m \times n$, B – матрица размера $r \times s$, то тензорное произведение $A \otimes B$ матрицы A на матрицу B определяется как следующая матрица размера $(mr) \times (ns)$:

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ a_{21}B & a_{22}B & \cdots & a_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}B & a_{m2}B & \cdots & a_{mn}B \end{pmatrix};$$

$|\varphi_1\varphi_2\varphi_3\ldots\varphi_{k-1}\varphi_k\rangle$ – вектор-столбец, определяемый равенством

$$|\varphi_1\varphi_2\varphi_3\ldots\varphi_{k-1}\varphi_k\rangle = |\varphi_1\rangle \otimes |\varphi_2\rangle \otimes |\varphi_3\rangle \otimes \ldots \otimes |\varphi_{k-1}\rangle \otimes |\varphi_k\rangle,$$

где $\varphi_m \in \{0;1\}$, $m = \overline{1,k}$;

$|\varphi_1\rangle|\varphi_2\rangle|\varphi_3\rangle\ldots|\varphi_{k-1}\rangle|\varphi_k\rangle$ – еще одно обозначение вектора $|\varphi_1\varphi_2\varphi_3\ldots\varphi_{k-1}\varphi_k\rangle$, то есть

$$|\varphi_1\rangle|\varphi_2\rangle|\varphi_3\rangle\ldots|\varphi_{k-1}\rangle|\varphi_k\rangle = |\varphi_1\varphi_2\varphi_3\ldots\varphi_{k-1}\varphi_k\rangle;$$

$\mathcal{H}_1 \otimes \mathcal{H}_2$ – тензорное произведение пространств $\mathcal{H}_1$ и $\mathcal{H}_2$; если $\mathcal{H}_1 = \mathbb{C}^{d_1}$ и $\mathcal{H}_2 = \mathbb{C}^{d_2}$ – два конечномерных гильбертовых пространства размерностей d_1 и d_2 над полем комплексных чисел $\mathbb{C}$, то $\mathcal{H}_1 \otimes \mathcal{H}_2$ – конечномерное гильбертово пространство размерности $d_1 d_2$ над полем комплексных чисел $\mathbb{C}$;

$\mathbf{I}_n$ – единичный оператор в гильбертовом пространстве размерности n (через $\mathbf{I}_n$ обозначается также единичная матрица $n \times n$);

tr – матричная функция *след*, то есть $\mathrm{tr}(X)$ – это сумма диагональных элементов квадратной матрицы X;

$\rho^{(\mathrm{A})}\left(|\psi\rangle\right)$ – матрица плотности (то есть оператор плотности в матричном представлении) квантовой системы A, находящейся в чистом состоянии $|\psi\rangle$; $\rho^{(\mathrm{A})}\left(|\psi\rangle\right) = |\psi\rangle\langle\psi|$;

$\rho^{(\mathrm{A})} = \sum_{k=1}^{n} p_k |\psi_k\rangle\langle\psi_k|$ – матрица плотности (то есть оператор плотности в матричном представлении) квантовой системы A, находящейся в смешанном состоянии, характеризуемой вероятностной смесью чистых состояний $\left\{\left(p_1; |\psi_1\rangle\right), \left(p_2; |\psi_2\rangle\right), \ldots, \left(p_n; |\psi_n\rangle\right)\right\}$;

$\rho_{\mathrm{A}}^{(\mathrm{AB})}$ – редуцированная матрица плотности (то есть редуцированный оператор плотности в матричном представлении) для подсистемы A квантовой системы AB, состоящей из двух подсистем A и B;

$\sigma_0 = \mathbf{I}_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ – вентиль Паули $\mathbf{I}_2$;

$\sigma_1 = \sigma_{\mathbf{X}} = \mathbf{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ – вентиль Паули $\mathbf{X}$;

$\sigma_2 = \sigma_{\mathbf{Y}} = \mathbf{Y} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$ – вентиль Паули $\mathbf{Y}$;

$\sigma_3 = \sigma_{\mathbf{Z}} = \mathbf{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ – вентиль Паули $\mathbf{Z}$;

$\mathbf{P}(\theta) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}$ – фазовращающий вентиль (вентиль изменения фазы);

$\mathbf{H} = \dfrac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ – вентиль Адамара $\mathbf{H}$;

$\mathbf{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$ – квантовый логический элемент, действующий на состояния квантовой системы из двух кубитов;

$\mathbb{S}_n$ – симметрическая группа подстановок на множестве $\{1, 2, \ldots, n\}$;

$s(k)$ – образ элемента $k \in \{1, 2, \ldots, n\}$, определяемый подстановкой $s \in \mathbb{S}_n$;

$s = \begin{pmatrix} 1 & 2 & \ldots & n \\ s(1) & s(2) & \ldots & s(n) \end{pmatrix}$ – двустрочная запись подстановки $s \in \mathbb{S}_n$;

$(s(1), s(2), \ldots, s(n))$ – перестановка элементов 1, 2, …, n, определяемая подстановкой $s \in \mathbb{S}_n$;

s^{-1} – подстановка, обратная к подстановке $s \in \mathbb{S}_n$;

$M_n^{(t)}$ – множество разбиений натурального числа n на t слагаемых, где $t \in \{2, 3, \ldots, n\}$, то есть $M_n^{(t)}$ – множество упорядоченных наборов натуральных чисел $(k_1, k_2, \ldots, k_t)$, таких, что справедливо равенство

$k_1 + k_2 + \ldots + k_t = n$;

B_{ψ} – булева маска состояния $|\psi\rangle$;

$\mathrm{wt}(|\psi\rangle)$ – вес состояния $|\psi\rangle$;

$N_{|\psi\rangle}(x, y)$ – нумератор весов состояния $|\psi\rangle$;

$S(\rho)$ – энтропия фон Неймана;

$E(|\psi\rangle)$ – мера несепарабельности состояния $|\psi\rangle$, определенная через энтропию фон Неймана;

$H(x) = -x\log_2 x - (1-x)\log_2(1-x)$ – функция энтропии Шеннона;

$C_{\mathrm{A}}(\rho)$ – мера несепарабельности подсистемы A (любой размерности) со всем ее окружением (также любой размерности), когда исходная квантовая система с матрицей плотности ρ находится в состоянии, которое может быть как чистым, так и смешанным;

$C_{\mathrm{A}}(|\psi\rangle)$ – мера несепарабельности состояния $|\psi\rangle$ квантовой системы AB, состоящей из двух кубитов A и B;

$\mathrm{A}(s,\ k) = \mathrm{A}_{s(1)}\mathrm{A}_{s(2)}\ldots\mathrm{A}_{s(k)}$ – подсистема из k кубитов $\mathrm{A}_{s(1)}$, $\mathrm{A}_{s(2)}$, …, $\mathrm{A}_{s(k)}$ квантовой системы $\mathrm{A}_1\mathrm{A}_2\ldots\mathrm{A}_n$, состоящей из $n > 1$ кубитов A_1, A_2, …, A_n; $s \in \mathbb{S}_n$; k – натуральное число, $k \in \{1,\ 2,\ \ldots,\ n-1\}$;

$\mathrm{B}(s, n-k) = \mathrm{A}_{s(k+1)}\mathrm{A}_{s(k+2)}\ldots\mathrm{A}_{s(n)}$ – подсистема из $n - k$ кубитов $\mathrm{A}_{s(k+1)}$, $\mathrm{A}_{s(k+2)}$, …, $\mathrm{A}_{s(n)}$ квантовой системы $\mathrm{A}_1\mathrm{A}_2\ldots\mathrm{A}_n$, состоящей из $n > 1$ кубитов A_1, A_2, …, A_n; $s \in \mathbb{S}_n$; k – натуральное число, $k \in \{1,\ 2,\ \ldots,\ n-1\}$;

$|\psi^{(s)}\rangle$ – состояние квантовой системы $\mathrm{A}_{s(1)}\mathrm{A}_{s(2)}\ldots\mathrm{A}_{s(n)}$ при условии, что квантовая система $\mathrm{A}_1\mathrm{A}_2\ldots\mathrm{A}_n$, состоящая из $n > 1$ кубитов A_1, A_2, …, A_n, находится в состоянии $|\psi\rangle$; $s \in \mathbb{S}_n$;

$C_{\mathrm{A}(s,\, k)}\left(\rho(s)\right)$ – мера несепарабельности подсистемы $\mathrm{A}(s,\, k)$ с подсистемой $\mathrm{B}(s,\, n-k)$ квантовой системы $\mathrm{A}_{s(1)}\mathrm{A}_{s(2)}\ldots\mathrm{A}_{s(n)}$ с матрицей плотности $\rho(s)=\left|\psi^{(s)}\right\rangle\left\langle\psi^{(s)}\right|$; $s\in\mathbb{S}_n$; k – натуральное число, $k\in\{1,\ 2,\ \ldots,\ n-1\}$;

$V\left(|\psi\rangle\right)$ – **V-мера** несепарабельности состояния $|\psi\rangle$ квантовой системы $\mathrm{A}_1\mathrm{A}_2\ldots\mathrm{A}_n$, состоящей из $n>1$ кубитов $\mathrm{A}_1,\ \mathrm{A}_2,\ \ldots,\ \mathrm{A}_n$.

От авторов

Основной материал книги представляет собой результаты авторов по разработке и развитию элементов теории несепарабельных (синонимы: запутанных, перепутанных, сцепленных) состояний многокубитных квантовых систем и модельные приложения в области связи, базовым элементом которых служит ресурс несепарабельности. Исходной точкой исследования является уже известная часть теории несепарабельных состояний для двухсоставных квантовых систем, в частности, двухкубитных.

Несепарабельные состояния квантовых систем и их свойства представляют большой научный и практический интерес. Они относятся к ряду основных объектов и ресурсов современных квантовых технологий хранения, обработки и передачи информации, не имеющих классических аналогов. В первом приближении их можно описать следующим образом: возможно для двух или более разделённых пространством объектов образовывать в действительности единое целое в том смысле, что если мы потревожим один из этих объектов, то среагируют все остальные объекты. Состояние такой единой целой квантовой системы называется несепарабельным состоянием.

Теория несепарабельных состояний квантовых систем содержит в себе бурно развивающиеся составные части квантовой механики, теории квантовой информации и квантовых вычислений. Понятийный аппарат и методы исследования этого научного направления находятся на переднем крае современной науки.

Тематика данной книги актуальна прежде всего в связи с тем, что теоретические и экспериментальные достижения в области исследования несепарабельных состояний квантовых систем могут послужить основой предполагаемых в ближайшем будущем крупных инновационных достижений в области компьютерных, информационных и телекоммуникационных технологий. Ожидания чрезвычайно велики.

Материал книги ориентирован и рассчитан на понимание и восприятие читателями, обладающими знаниями по математике и физике в объёме соответствующих стандартных курсов любого из факультетов математического, физического и технического профилей высших учебных заведений. Но круг потенциальных читателей может быть и шире. Ведь интересно и стоит задуматься над тем, что в наше время и на наших глазах происходят зачастую непостижимые чудеса (аж «дух захватывает») – меняются основные парадигмы информационных и телекоммуникационных технологий. И эта книга указывает, пусть и в модельном варианте, на некоторые из них.

Книга в минимальном объёме содержит необходимые для понимания и освоения основного материала сведения из квантовой механики, теории квантовой информации и квантовых вычислений, что делает её чтение во многом автономным, без существенного привлечения и использования дополнительной литературы.

Введение

Одной из характерных особенностей научно-практической области под общим названием «квантовые вычисления и квантовая информация» является то, что в ней для решения вычислительных задач и задач связи используются принципиально новые типы ресурсов квантовой физики, которые не имеют аналогов как в классической физике, так и в традиционной сфере вычислений, информации и связи. По-видимому, среди этих ресурсов наиболее впечатляющим является ресурс несепарабельных состояний квантовых систем. В качестве синонима понятия «несепарабельность» используются также термины «запутанность», «сцепленность» и «перепутанность».

Несмотря на то, что несепарабельные квантовые состояния не имеют аналога в классической физике, установлено, что они не теоретическая абстракция, а объективный элемент окружающей действительности [34; 47]. Это то, что существует в природе независимо от наших представлений. Кратко это физическое явление известный физик Николя Жизан описал следующим образом:

«Грубо говоря, странная теория квантовой физики говорит нам, что вполне возможно и даже обычно для двух разделённых пространством объектов образовывать в действительности единое целое! Это и называется запутанностью. Если мы потревожим одну из двух частей, среагируют обе… Теоретически запутанным может быть любой объект, но на практике физики продемонстрировали запутанность атомов, фотонов и некоторых элементарных частиц. Самые большие объекты, которые удалось связать, – это кристаллы… Этот феномен проявляет себя примерно одинаково вне зависимости от того, какие объекты оказались запутанными» [33].

В связи с размерами объектов, которые удалось запутать, уместно сослаться, например, на сообщение, представленное в русскоязычном журнале New Scientist RU № 1–2 (14) январь–февраль 2012 г. (со ссылкой на Science, DOI: 10.1126/science.1211914), о том, что в одной из лабораторий Оксфордского университета удалось создать «**при комнатной температуре запутанное состояние пары трёхмиллиметровых алмазов**».

В настоящее время наиболее весомым известным достижением, полученным с использованием ресурса несепарабельных квантовых состояний, является технология квантовой телепортации, позволяющая передавать квантовые состояния между удалёнными друг от друга абонентами, обладающими подсистемами квантовой системы в несепарабельном состоянии [50].

Кроме технологии квантовой телепортации имеются и другие существенные продвижения в области информационных технологий, полученные путём использования новых квантовых ресурсов, например, квантовая криптография и сверхплотное кодирование [36; 37; 39; 50; 52; 83].

Следует отметить, что в вышеуказанных достижениях были использованы несепарабельные состояния двухсоставных квантовых систем.

Результаты, полученные на основе использования несепарабельных состояний многосоставных квантовых систем, менее впечатляющие. В этом направлении первым – пожалуй, прорывным – экспериментальным успехом можно считать реализацию запутанного состояния трёх фотонов, осуществлённую в 2000 г. группой во главе с австрийским физиком Антоном Цайлингером [85]. Реализовано было так называемое состояние Гринбергера–Хорна–Цайлингера (ГХЦ-состояние) [77].

В целом можно сказать, что изучение ресурса несепарабельных квантовых состояний находится в начальной стадии своего развития. Пока ещё рано ставить точку в исследованиях по поиску и разработке новых информационных технологий на основе данного ресурса. В подтверждение этого уместно процитировать следующий тезис из известной монографии [50]: «…пока изучение запутанности только начинается, и не совсем ясно, насколько улучшится наше понимание квантовых вычислений и квантовой информации в результате изучения количественных мер запутанности. Мы сносно понимаем свойства чистых состояний квантовых систем из двух компонент, но очень плохо разбираемся в системах, состоящих из трёх и более компонент… Улучшение понимания запутанности и распространение полученных результатов на квантовые алгоритмы, исправление квантовых ошибок и квантовую связь являются основными вопросами в области квантовых вычислений и квантовой информации».

В этой же работе [50], говоря о большом интересе к задаче создания и развития теории несепарабельных состояний многосоставных систем, авторы обращают внимание и на трудности, связанные с её решением: «Конечно, очень интересно разработать общую теорию запутанности для многокомпонентных систем, но как это сделать — непонятно».

Наша работа представляет собой в основном попытку движения в направлении разработки и развития элементов теории запутанности для многокубитных квантовых систем, где под кубитом понимается квантовая система, состояния которой принадлежат двумерному гильбертову пространству (понятие кубита имеет два смысла [50]: здесь кубит – физический объект; кубит как математический объект будет рассмотрен позднее). При этом исходной точкой является уже разработанная и известная часть теории запутанности для двухсоставных квантовых систем.

Следуя данному руслу, выполним, к примеру, описание нашего представления несепарабельности многосоставных систем, опираясь на вышеприведённое мнение Николя Жизана [33] об этом физическом явлении для двухсоставных систем и несколько его расширяя.

В соответствии с положениями квантовой физики вполне возможно и даже обычно для двух или более разделённых пространством объектов образовывать в действительности единое целое в том смысле, что если мы потревожим один из этих объектов, то среагируют <u>все</u>. Это и называется несепарабельностью. Состояние такой единой целой квантовой системы называется несепарабельным состоянием, а сама квантовая система называется несепарабельной квантовой системой.

Уместно сделать три уточняющих комментария к этому описанию физического явления несепарабельности многосоставных квантовых систем.

Во-первых, выражение «разделённых пространством» по отношению к объектам, составляющим квантовую систему, надо понимать прежде всего как **отсутствие между ними любого вида классической коммуникации**.

Во-вторых, подчёркнутое в описании слово «<u>все</u>» в определённом смысле является ключевым словом. А именно, если какой-то из объектов не среагирует, то и вся квантовая система не является несепарабельной. При этом не исключаются случаи, когда квантовая система, сама не являясь несепарабельной, содержит несепарабельные квантовые подсистемы.

В-третьих, имеются элементы теории несепарабельности двухсоставных систем, которые напрямую, без соответствующего анализа, изменения и развития, не переносятся на случаи трёх- и более составных квантовых систем.

Особенности описания несепарабельности многосоставных систем, затронутые в этих комментариях, носят принципиальный характер.

Данное утверждение по отношению к содержанию первого комментария представляется естественным, так как несепарабельность «вводит в физику нелокальные корреляции» [33], и этим она отличается от всех известных физических ресурсов.

Что же касается второго комментария, то он связан с необходимостью выполнения требования определённости в наличии и полноте указанных нелокальных корреляций.

Принципиальную особенность третьего уточняющего комментария проиллюстрируем указанием соответствующих конкретных элементов теории несепарабельности для двухсоставных квантовых систем, которые в прямом виде, без дополнений и изменений, не могут быть перенесены на многосоставные квантовые системы.

В качестве одного из таких элементов может служить, например, известное строгое математическое определение несепарабельности двухсоставных квантовых систем, заключающееся в невозможности разложения состояния исходной квантовой системы в тензорное произведение состояний двух составляющих её подсистем [56; 59]. Данное определение находится в полном и точном соответствии с вышеприведённым описанием Николя Жизана [33] явления несепарабельности для двухсоставных квантовых систем. Однако для квантовых систем, состоящих из трёх или более кубитов, указанное математическое определение приводит к ситуациям, противоречивым с вышеприведённым описанием несепарабельности для случая многосоставных квантовых систем. Таковым является случай, когда состояние многокубитной (трёх- или более) квантовой системы не разлагается в тензорное произведение векторов меньшей размерности, но в то же самое время в рассматриваемой квантовой системе в данном состоянии имеются кубиты, не реагирующие на воздействия, оказанные на другие кубиты. Пример соответствующего состояния для случая трёхкубитной квантовой системы будет приведён в параграфе 2.4 главы 2 данной работы.

Другим элементом теории несепарабельности двухсоставных систем является количественная характеристика (в различных известных своих определениях) ресурса несепарабельности двухсоставных квантовых систем, так называемая мера несепарабельности [24; 80; 86; 91]. Имеющиеся результаты непригодны для количественного выражения ресурса несепарабельности в многосоставных (трёх- и более) системах, как с теоретико-информационных, так и с физических позиций.

Далее остановимся на структуре и содержании работы более подробно.

Работа состоит из введения, шести глав, заключения и списка литературы. Каждая глава состоит из нескольких параграфов, снабжена отдельным введением и заканчивается выводами о результатах, представленных в ней.

В работе принята трёхпозиционная последовательная единая нумерация объектов (определений, утверждений, замечаний и формул) в каждом параграфе. В номере каждого объекта первая позиция соответствует номеру главы, вторая – номеру параграфа, третья – порядковому номеру объекта внутри параграфа.

Глава 1 состоит из пяти параграфов.

В параграфе 1.1 приводятся основные понятия и определения квантовой теории, очерчен круг инструментов исследования квантовых систем, используемых в работе.

В параграфе 1.2 представлены элементы раздела квантовой механики по квантовым измерениям. Особое внимание уделяется проективным измерениям. Они будут использованы по необходимости в дальнейшей части данной работы при решении задач определения состояний квантовых систем.

Параграф 1.3 посвящён квантовым вычислениям. Приводится описание некоторого набора квантовых логических элементов, достаточного для дальнейшего изложения материала данной работы. Показано, что квантовые вычисления нацелены на решение вычислительно сложных задач с помощью устройств, основанных на принципах и ресурсах квантовой механики.

В параграфе 1.4 достаточно подробно описывается один из основных ресурсов квантовой механики, широко востребованный для построения протоколов квантовой криптографии. Этот ресурс заключается «в невозможности клонирования неизвестных квантовых состояний и эквивалентной ей невозможности идеального различения неортогональных квантовых состояний» [39]. Он обеспечивает возможность защиты информации методами квантовой криптографии путём использования квантовых носителей [39]. Теоретическое описание обсуждаемого ресурса представлено в виде теоремы о невозможности клонирования [74; 90].

Параграф 1.5 посвящён кубитам, их реализациям в физических системах и измерениям в вычислительных базисах.

Глава 2 состоит из шести параграфов.

Параграф 2.1 посвящён теории несепарабельных состояний квантовых систем. Кратко, в самом общем плане описывается история её зарождения и развития. Обсуждаются вопросы технической реализации.

Результаты по исследованию несепарабельных состояний двухкубитных квантовых систем представлены в параграфе 2.2.

В параграфе 2.3 рассмотрены трёхкубитные квантовые системы. Сформулирован и доказан критерий разложимости состояния трёхкубитной квантовой системы в тензорное произведение состояний меньшей размерности.

В параграфе 2.4 сформулированы новые определения понятий сепарабельности и несепарабельности состояний квантовых систем, учитывающие сложную специфику связей составных компонент многокубитных квантовых систем. Эти определения позволяют получить содержательные результаты для трёхкубитных квантовых систем, изложенные в параграфе 2.5. Наиболее ярким из них является критерий несепарабельности состояний трёхкубитной квантовой системы, названный **критерий $\mathbf{K_3}$**, где **К** – первая буква имени **Константин**, а индекс **3** указывает на число кубитов в обсуждаемой квантовой системе.

В параграфе 2.6 представлены результаты исследования состояний четырёхкубитных квантовых систем. Основным результатом данного параграфа является **критерий $\mathbf{K_4}$**, где, как и выше, **К** – первая буква имени **Константин**, а индекс **4** указывает на число кубитов в обсуждаемой квантовой системе.

Глава 3 состоит из трёх параграфов.

В параграфе 3.1 вводятся в рассмотрение и исследуются такие объекты, как булевы маски состояний квантовых систем.

Параграф 3.2 посвящён нумераторам весов состояний квантовых систем. Представленный в параграфах 3.1 и 3.2 аналитический аппарат, использующий булевы маски и нумераторы весов состояний квантовых систем, служит эффективным инструментом для выявления некоторых общих достаточных признаков несепарабельности квантовых состояний.

В параграфе 3.3 приводится полное алгоритмическое решение задачи бинарной классификации состояний трёхкубитной квантовой системы (т. е. задачи определения, несепарабельно данное трёхкубитное состояние или нет). Соответствующий алгоритм называется **алгоритм** $\mathbf{K_3}$, где **К** – первая буква имени **Константин**, а индекс **3** связан с числом кубитов в трёхкубитной квантовой системе, состояния которой исследуются.

Глава 4 состоит из шести параграфов.

В параграфе 4.1 рассматривается мера несепарабельности состояний двухкубитных квантовых систем. Эта мера основана на энтропии фон Неймана. Приведены результаты исследования свойств этой меры. Доказано, что свойство однозначной определённости состояния одного из кубитов двухкубитной квантовой системы после измерения состояния другого кубита в соответствующем базисе не является специфическим свойством состояний Белла. Установлено, что данное свойство присуще любому состоянию двухкубитной квантовой системы с положительной мерой несепарабельности, и указаны подходящие для соответствующего измерения операторы измерения, определённые через базисы Шмидта подсистем двухкубитной квантовой системы. Результаты данного параграфа, по сути дела, можно трактовать как выявление бесконечного множества несепарабельных состояний двухкубитных квантовых систем, подобных в определённой степени состояниям Белла в плане возможности их использования в квантовых информационных технологиях.

В параграфе 4.2 для любых двух произвольным образом заданных ортонормированных базисов двухмерного гильбертова пространства над полем комплексных чисел построено множество всех возможных состояний двухкубитной квантовой системы с максимальной мерой несепарабельности (основанной на энтропии фон Неймана), подобных состояниям Белла при проективных измерениях, определённых исходными базисами.

В параграфе 4.3 рассматривается более общая мера несепарабельности двухсоставной (не обязательно двухкубитной) системы, называемая **согласованностью**.

В параграфе 4.4 на основе меры несепарабельности двухсоставной системы (согласованности) строится мера несепарабельности состояний многокубитных квантовых систем. Эта мера названа **мера Виолетта** (более кратко – **V-мера**).

V-мера даёт количественную характеристику ресурса несепарабельности состояний n-кубитной квантовой системы (где $n > 1$) с позиции «наименее надёжного» звена (подсистемы исходной системы) по несепарабельности во всей системе.

В параграфе 4.5 значение **V-меры** для произвольного состояния трёхкубитной квантовой системы выражается через координаты данного состояния в вычислительном базисе.

В параграфе 4.6 значение **V-меры** для произвольного состояния четырёхкубитной квантовой системы выражается через координаты данного состояния в вычислительном базисе.

Глава 5 состоит из трёх параграфов.

К естественным двухуровневым квантовым ячейкам – кубитам – относятся электронные, протонные, нейтронные, ядерные и другие спины со спиновым числом $^1/_2$. В данной главе рассматриваются двухкубитные, трёхкубитные и четырёхкубитные квантовые системы, состоящие соответственно из двух, трёх и четырёх кубитов-спинов-$^1/_2$ с одним и тем же гиромагнитным отношением и находящиеся в постоянном магнитном поле. На стационарных состояниях данных физических систем иллюстрируются теоретические положения, разработанные в предыдущих главах.

Параграф 5.1 посвящён исследованию несепарабельности стационарных состояний двухкубитной квантовой системы, состоящей из двух кубитов-спинов-$^1/_2$ с одним и тем же гиромагнитным отношением и находящейся в постоянном магнитном поле.

Параграф 5.2 посвящён исследованию несепарабельности стационарных состояний трёхкубитной квантовой системы, состоящей из трёх кубитов-спинов-$^1/_2$ с одним и тем же гиромагнитным отношением и находящейся в постоянном магнитном поле.

Параграф 5.3 посвящён исследованию несепарабельности стационарных состояний четырёхкубитной квантовой системы, состоящей из четырёх кубитов-спинов-$^1/_2$ с одним и тем же гиромагнитным отношением и находящейся в постоянном магнитном поле.

Для всех рассмотренных стационарных состояний вычислены значения их **V-меры**.

В главе 6 представлены протокол детерминированной квантовой связи и его научное обоснование. В данной работе для протокола детерминированной квантовой связи используется также название **ATF**-технология связи, где **ATF** – соответственно первые буквы имён **Александр**, **Татьяна** и **Физули** при их написании в латинском алфавите.

ATF-технология связи имеет основу, состоящую из трёх компонент:

- способа дистанционного изменения **меры несепарабельности** (**V-меры**) квантовых систем (способ представлен в виде алгоритма **A**);
- совокупности предположений (названной гипотезой **T**) относительно такого физического явления, как **квантовый фазовый переход**;
- метода передачи однобитовых сообщений между удалёнными друг от друга абонентами с использованием ресурса несепарабельных состояний трёхкубитных квантовых систем (название метода – метод **F**).

В работе приводятся определённые доводы в пользу справедливости гипотезы **T**, что не исключает необходимости её экспериментальной проверки.

Главным отличием **ATF**-технологии связи от известной технологии квантовой телепортации является отсутствие классического канала связи (то есть исключается составляющая в виде классического канала).

Глава 6 состоит из шести параграфов.

Параграф 6.1 посвящён формулировке и обоснованию **гипотезы Татьяна** (или, кратко, **гипотезы T**) о некоторых свойствах квантового фазового перехода, присущих состояниям двухспиновых квантовых систем. Выдвигается и обсуждается тезис о том, что квантовый фазовый переход обусловлен понижением меры несепарабельности кубитов до определённой границы, названной в данной работе **граница Ксения** или, кратко, **граница К**.

В параграфе 6.2 разработан и представлен способ изменения меры несепарабельности кубитов трёхкубитной квантовой системы. При этом для двух из трёх кубитов, составляющих квантовую систему, этот способ является дистанционным в силу их пространственной удалённости от места воздействия на однокубитную подсистему рассматриваемой трёхкубитной квантовой системы.

Параграф 6.3 посвящён доказательству соотношений, использованных в параграфе 6.2.

В параграфе 6.4 приводится общее описание **ATF**-технологии связи и детальное описание её составной компоненты – метода **F**, – позволяющей передавать однобитовые сообщениям между удалёнными друг от друга абонентами с использованием ресурса несепарабельных состояний трёхкубитных квантовых систем. В **ATF**-технологии связи предполагается справедливость **гипотезы Т**. Пока еще не получены в необходимом количестве убедительные экспериментальные подтверждения гипотезы **Т**. ПоэтомуATF-технология связи носит модельный характер.

В параграфе 6.5 проводится анализ значений модулей амплитуд состояний трёхкубитных квантовых систем, используемых в **ATF**-технологии связи.

В параграфе 6.6 приводится решение статистической задачи выбора из двух простых гипотез, возникающей в **ATF**-технологии связи. По заданным ошибкам первого и второго рода вычислены объём выборки и критическая граница.

В **заключении** в краткой форме изложены основные результаты данной работы.

ГЛАВА 1

Понятия и инструменты квантовой теории

Введение к главе 1

Глава 1 состоит из пяти параграфов.

В параграфе 1.1 изложены формулировки базовых понятий и определений квантовой теории в объеме, достаточном для целей данной работы. Особое внимание уделено таким понятиям, как чистые и смешанные состояния, эксперименты, измерения, кубиты и квантовые системы. Понятие квантовой системы введено не формально, а описательно: под квантовой системой понимается объект, изучаемый методами квантовой теории. Под состояниями квантовой системы понимаются нормированные векторы конечномерного гильбертова пространства над полем комплексных чисел. При этом различаются чистые и смешанные состояния, под первыми подразумеваются нормированные векторы, а под вторыми – ансамбли пар вероятностей и нормированных векторов.

Выделен и описан ряд общих составляющих, присущих всем типам квантово-механических экспериментов.

Изложены элементы квантовой информатики, в том числе описательно представлены понятие кубита и конструкции из совокупности кубитов. Указаны состояния вычислительного базиса.

Представлены основные инструменты исследования квантовых систем, такие, как матрицы плотности, редуцированные матрицы плотности, разложение Шмидта и расширение до чистого состояния. Они применяются в дальнейшем в других частях работы.

В параграфе 1.1 указано также, что на основе чисто математической процедуры, называемой расширением до чистого состояния, можно перейти от смешанных состояний к чистым состояниям и тем самым свести, в определенном смысле, ряд вопросов исследования смешанных состояний к вопросам исследования соответствующих чистых состояний.

В параграфе 1.2 внимание уделено такой неотъемлемой части квантово-механических экспериментов, как измерение. Описана общая модель квантовых измерений через линейные операторы, называемые операторами измерения. Выделены важные частные случаи квантовых измерений, такие, как различного рода проективные измерения.

Особое внимание уделено измерениям подсистем в составе квантовых систем. Говоря точнее, измерениям, проводимым над квантовой системой A как подсистемой составной квантовой системы AB, включающей в себя, наряду с подсистемой A, и квантовую подсистему B.

Измерения, проводимые только над подсистемой A квантовой системы AB, являются измерениями, проводимыми над всей квантовой системой AB, но с определенной спецификой, отличающей такие измерения как от измерений, проводимых собственно над подсистемой A (когда она представляет собой «изолированную» квантовую систему), так и от измерений над квантовой системой AB, когда измерительное устройство оказывает непосредственное локальное воздействие на обе подсистемы A и B квантовой системы AB.

То же самое и с симметричным случаем, то есть с измерениями над подсистемой B квантовой системы AB. Полученные результаты по описанию измерений подсистем в составе квантовых систем изложены в виде утверждения 1.2.24.

Вопросам квантовых вычислений посвящен параграф 1.3. Здесь обсуждается само понятие «квантовые вычисления» и приведены математические описания квантовых логических элементов, действующих на состояния однокубитных и многокубитных квантовых систем. Обращается внимание на применение квантовых логических элементов к квантовым системам, когда последние являются подсистемами других более крупных (составных) квантовых систем.

В параграфе 1.4 обсуждаются вопросы о возможности дублирования квантовой информации (в том числе и с помощью квантового логического элемента **CNOT**). Показано, что это возможно только при некоторых ограниченных условиях. А для общего случая сформулирована и доказана *теорема о невозможности клонирования* [74; 90], из которой следует невозможность дублирования произвольного неизвестного квантового состояния.

Параграф 1.5 посвящен обсуждению вопросов физической реализации кубитов. Описан простейший пример реализации кубита с использованием энергетических состояний электрона.

§ 1.1. Элементы квантовой теории

Под квантовыми системами (или квантовыми объектами) обычно подразумевают объекты микромира, например, электроны, протоны, ядра атомов, атомы, молекулы и их совокупности и т.д. [18; 38; 39; 42; 54; 57; 58; 89]. Принципиальной особенностью квантовых объектов является их статистический [28; 35; 43] характер в отношении результатов всевозможных измерений. Приготовленные тождественным образом квантовые объекты демонстрируют, в общем случае, различающиеся результаты измерений. Для описания этого факта в квантовой теории вводят понятие состояния квантовой системы.

Состояние квантовой системы – это список (каталог) возможных результатов измерений над этой системой [39].

В квантовой теории рассматривают два типа состояний квантовых систем: чистые и смешанные.

Чистые состояния описывают квантовые системы, которые независимы от всех остальных окружающих их квантовых объектов [39].

Смешанное состояние отдельной квантовой системы возникает, когда такая независимость отсутствует [39].

Пусть $\mathbb{C}^d$ – пространство вектор-столбцов размерности $d \in \mathbb{N}$ над полем комплексных чисел $\mathbb{C}$ со скалярным произведением [27; 43; 46], то есть **гильбертово пространство** размерности d, как принято говорить в квантовой механике [34; 50], где $\mathbb{N}$ – множество натуральных чисел.

В работах по квантовой механике для произвольного вектор-столбца $|\psi\rangle \in \mathbb{C}^d$ принято название *кет-вектор*, а для вектор-строки $\langle\psi|$, двойственной к $|\psi\rangle$, принято название *бра-вектор* [50]. Напомним, что двойственный к вектор-столбцу $|\psi\rangle$ вектор $\langle\psi|$ – это вектор-строка, получаемая из вектор-столбца $|\psi\rangle$ путем замены всех его координат на комплексно сопряженные к ним и последующего применения операции транспонирования [50]. Обозначения $|\psi\rangle$, $\langle\psi|$ и названия *кет-вектор* и *бра-вектор* введены известным физиком XX века П. А. М. Дираком [34]. В данной работе мы почти всегда вместо термина *кет-вектор* будем для простоты употреблять название «вектор».

С введением понятия гильбертова пространства конечной размерности (в данной работе только такие и будут рассматриваться) можно более строго описать состояния квантовых систем. Если состояние квантовой системы описывается некоторым нормированным вектором $|\psi\rangle$ гильбертова пространства $\mathbb{C}^d$, то говорят, что квантовая система находится в **чистом** состоянии [50].

Если квантовая система может находиться в состоянии, описываемом ансамблем пар

$$\left\{\left(p_1;\, |\psi_1\rangle\right), \left(p_2;\, |\psi_2\rangle\right),\, \ldots,\, \left(p_n;\, |\psi_n\rangle\right)\right\}$$

из вероятностей $p_k \geq 0$ и нормированных векторов $|\psi_k\rangle$ ($k = \overline{1,\, n}$; $p_1 + p_2 + \ldots + p_n = 1$) гильбертова пространства $\mathbb{C}^d$ (то есть квантовая система может находиться в состоянии, описываемом вектором $|\psi_k\rangle$, с вероятностью p_k), то говорят, что квантовая система находится в **смешанном** состоянии [50]. При этом ансамбль пар

$$\left\{\left(p_1;\, |\psi_1\rangle\right), \left(p_2; |\psi_2\rangle\right), \ldots, \left(p_n; |\psi_n\rangle\right)\right\}$$

из вероятностей $p_k \geq 0$ и нормированных векторов $|\psi_k\rangle$ называется **смесью чистых состояний** $|\psi_1\rangle$, $|\psi_2\rangle$, …, $|\psi_n\rangle$.

Замечание. В работах по квантовым компьютерам и вычислениям (например, в [24; 50]) встречается трактовка чистого состояния как частного случая смешанного состояния, когда $n = 1$.

Таким образом, математически, чистое состояние квантового объекта задается **вектором состояния** (по-другому называемым **волновой функцией** [34; 47]), который принято записывать в обозначениях Дирака [34] как кет-вектор $|\psi\rangle$. Этот вектор имеет норму 1 и является элементом гильбертова пространства $\mathbb{C}^d$ [50]. **Размерность** d гильбертова пространства задает важный параметр – число независимых состояний (**уровней**) квантового объекта. В принципе любой вектор $|\psi\rangle$ с нормой, равной единице, из гильбертова пространства размерности d, представляет собой возможное состояние d-уровневой квантовой системы. Используя в качестве базисных векторов взаимно ортогональные векторы $\{|k\rangle \,|\, k = 1, 2, \ldots, d\}$ с нормой, равной 1, образующие полный набор ($\sum_{k=1}^{d} |k\rangle\langle k| = \mathbf{I}_d$, где $\mathbf{I}_d$ – единичный оператор в гильбертовом пространстве размерности d, $\langle k|$ – вектор, двойственный к вектору $|k\rangle$), можно представить любой вектор в виде **суперпозиции** (**линейной комбинации**) базисных векторов:

$$|\psi\rangle = \sum_{k=1}^{d} c_k |k\rangle,\ c_k \in \mathbb{C},\ k = 1, 2, \ldots, d\,.$$

Совокупность $\{|k\rangle \,|\, k = 1,\ 2,\ \ldots,\ d\}$ таких базисных векторов называют также **ортонормированным** базисом гильбертова пространства. Существует бесконечное число ортонормированных базисов и, следовательно, бесконечное число различных представлений любого вектора состояний. Смысл выбора того или иного ортонормированного базиса $\{|k\rangle | k=1,2,\ldots,d\}$ и коэффициентов $\{c_k | k=1,2,\ldots,d\}$ разложения состояния $|\psi\rangle$, а вместе с тем и суть квантовой теории определяется в процедуре квантового эксперимента и его неотъемлемой части – измерении.

Следуя [39], поясним более подробно понятие эксперимента.

Если отвлечься от деталей, связанных с проведением квантово-механических экспериментов любой степени сложности, можно выделить ряд общих моментов, присущих всем таким экспериментам. Любой **эксперимент**, проводимый с квантовыми объектами, содержит следующие основные этапы:

А) выбор объекта и предполагаемого набора характеристик, которые будут измеряться;

Б) приготовление объекта в заданном состоянии $|\psi\rangle$;

В) взаимодействие или преобразование объекта в результате некоторых операций, приводящих объект в новое состояние $|\psi'\rangle$;

Г) измерение над объектом, находящимся в состоянии $|\psi'\rangle$.

Этап (А) заключается в выборе физической величины для измерения и выборе базиса для разложения векторов состояния.

Этап (Б) заключается в переводе исходного состояния с помощью унитарных преобразований в заданное начальное состояние.

Этап (В) заключается в изменении созданного состояния в результате взаимодействия с другими объектами.

Этап (Г) заключается в получении некоторой информации о состоянии квантовой системы.

В силу особой важности определенных частных форм этапа (Г) для данной работы, в параграфе 1.2 остановимся на нем более подробно.

Перейдем к изложению элементов квантовой информатики в объеме, достаточном для целей данной работы.

Кубит – это фундаментальное понятие в области квантовых вычислений и квантовой информации, имеющее смысл единицы квантовой информации. Этот смысл понятия представляет кубит как математический объект [50].

Кубиты в квантовой области являются «аналогами» таких классических объектов, как биты. Напомним, что **бит** – это фундаментальное понятие в области классических вычислений и классической информации, имеющее смысл единицы классической информации. Классический бит может находиться в состоянии 0 или 1. Состояниями кубита являются векторы двумерного гильбертова пространства $\mathbb{C}^2$ над полем комплексных чисел $\mathbb{C}$ вида $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, где $\alpha, \beta \in \mathbb{C}$, $|\alpha|^2 + |\beta|^2 = 1$; $\{|0\rangle, |1\rangle\}$ – ортонормированный базис пространства $\mathbb{C}^2$. И это главное различие между битами и кубитами.

Векторы $|0\rangle$ и $|1\rangle$ называются **состояниями вычислительного базиса** в случае одного кубита, и при этом вектор $|\psi\rangle$ является **суперпозицией** (линейной комбинацией) векторов $|0\rangle$ и $|1\rangle$. В качестве состояний вычислительного базиса может быть взята и любая другая ортонормированная система из двух векторов пространства $\mathbb{C}^2$. Для определенности положим

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

Если $\mathcal{H}_1 = \mathbb{C}^{d_1}$ и $\mathcal{H}_2 = \mathbb{C}^{d_2}$ – два конечномерных гильбертовых пространства размерностей d_1 и d_2 над полем комплексных чисел $\mathbb{C}$, то через $\mathcal{H}_1 \otimes \mathcal{H}_2$ обозначим конечномерное гильбертово пространство размерности $d_1 d_2$ над полем комплексных чисел $\mathbb{C}$, являющееся их тензорным произведением, а через $|\psi_1\rangle \otimes |\psi_2\rangle$ (или $|\psi_1 \psi_2\rangle$, или $|\psi_1\rangle|\psi_2\rangle$) обозначим тензорное произведение состояний $|\psi_1\rangle \in \mathcal{H}_1$ и $|\psi_2\rangle \in \mathcal{H}_2$, где $\otimes$ – знак операции тензорного произведения [50; 51].

Замечание. Из-за частой встречаемости в дальнейшем операции тензорного произведения, приведем ее определение. Пусть $A = \left(a_{ij}\right)$ – матрица размера $m \times n$, B – матрица размера $r \times s$. Тогда тензорное произведение $A \otimes B$ матрицы A на матрицу B определяется как следующая матрица размера $(mr) \times (ns)$:

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ a_{21}B & a_{22}B & \cdots & a_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}B & a_{m2}B & \cdots & a_{mn}B \end{pmatrix}.$$

Можно рассматривать квантовые конструкции и из более чем одного кубита. Состояниями системы из k ($k \geq 1$) кубитов являются нормированные векторы, принадлежащие k-той тензорной степени пространства $\mathbb{C}^2$, то есть 2^k-мерного гильбертова пространства $\mathbb{C}^{2^k} = \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \ldots \otimes \mathbb{C}^2$ над полем комплексных чисел $\mathbb{C}$. Эти векторы, называемые **суперпозициями** (**линейными комбинациями**), можно представить в следующем виде:

$$\alpha_0 \underbrace{\left|000\ldots00\right\rangle}_{k} + \alpha_1 \left|000\ldots01\right\rangle + \alpha_2 \left|000\ldots10\right\rangle + \ldots + \alpha_{2^k-1} \left|111\ldots11\right\rangle, \quad (1.1.1)$$

где

$$\alpha_0, \alpha_1, \alpha_2, \ldots \alpha_{2^k-1} \in \mathbb{C}, \ \left|\alpha_0\right|^2 + \left|\alpha_1\right|^2 + \ldots + \left|\alpha_{2^k-1}\right|^2 = 1, \quad (1.1.2)$$

$$\begin{gathered} \left|\varphi_1\varphi_2\varphi_3\ldots\varphi_{k-1}\varphi_k\right\rangle = \left|\varphi_1\right\rangle\left|\varphi_2\right\rangle\left|\varphi_3\right\rangle\ldots\left|\varphi_{k-1}\right\rangle\left|\varphi_k\right\rangle = \\ = \left|\varphi_1\right\rangle \otimes \left|\varphi_2\right\rangle \otimes \left|\varphi_3\right\rangle \otimes \ldots \otimes \left|\varphi_{k-1}\right\rangle \otimes \left|\varphi_k\right\rangle, \end{gathered} \quad (1.1.3)$$

$$\varphi_m \in \{0;1\}, \quad m = \overline{1,k}.$$

Состояния $\underbrace{\left|000\ldots00\right\rangle}_{k}$, $\left|000\ldots01\right\rangle$, …, $\left|111\ldots11\right\rangle$ называются **состояниями вычислительного базиса** в случае системы из k кубитов. Они составляют ортонормированный базис гильбертова пространства $\mathbb{C}^{2^k}$.

В квантовой теории имеется набор математических инструментов исследования квантовых систем. К ним относятся: операторы плотности, редуцированные операторы плотности, разложение Шмидта и расширение до чистого состояния [17; 34; 37; 50; 52]. Все они, в той или иной степени, будут востребованы и в данной работе. Особенно при исследовании составных квантовых систем, то есть квантовых систем, состоящих из нескольких подсистем, которые также являются квантовыми системами. Поэтому они будут описаны в этом параграфе на уровне, достаточном для понимания всего содержания данной работы.

Определение 1.1.4. Для квантовой системы A, находящейся в чистом состоянии $\left|\psi\right\rangle$, **матрицей плотности** (то есть **оператором плотности** в матричном представлении) называется матрица $\rho^{(\mathrm{A})}$, задаваемая равенством

$$\rho^{(\mathrm{A})}\left(\left|\psi\right\rangle\right)=\left|\psi\right\rangle\left\langle\psi\right|,$$

где $\left\langle\psi\right|$ – вектор, двойственный к вектору $\left|\psi\right\rangle$ [50].

Для квантовой системы A, находящейся в **смешанном состоянии**, характеризуемой вероятностной смесью чистых состояний $\left\{\left(p_1;\left|\psi_1\right\rangle\right),\left(p_2;\left|\psi_2\right\rangle\right),\ldots,\left(p_n;\left|\psi_n\right\rangle\right)\right\}$, **матрицей плотности** [50] (то есть **оператором плотности** в матричном представлении) называется матрица $\rho^{(\mathrm{A})}$, задаваемая равенством

$$\rho^{(\mathrm{A})}=\sum_{k=1}^{n}p_k\left|\psi_k\right\rangle\left\langle\psi_k\right|.$$

Очевидно, что справедливо равенство

$$\rho^{(\mathrm{A})}=\sum_{k=1}^{n}p_k\rho^{(\mathrm{A})}\left(\left|\psi_k\right\rangle\right),$$

(где $\rho^{(\mathrm{A})}\left(\left|\psi_k\right\rangle\right)=\left|\psi_k\right\rangle\left\langle\psi_k\right|$ – матрица плотности квантовой системы в чистом состоянии $\left|\psi_k\right\rangle$, или просто матрица плотности чистого состояния $\left|\psi_k\right\rangle$), то есть матрица плотности квантовой системы в смешанном состоянии равна взвешенной сумме матриц плотности чистых состояний, соответствующей вероятностной смеси чистых состояний.

Определение 1.1.5. Пусть $\rho^{(\mathrm{AB})}$ – матрица плотности квантовой системы AB, состоящей из двух подсистем A и B. **Редуцированной матрицей плотности** $\rho_{\mathrm{A}}^{(\mathrm{AB})}$ (то есть **редуцированным оператором плотности** в матричном представлении) для системы A называется матрица $\rho_{\mathrm{A}}^{(\mathrm{AB})}$, задаваемая равенством $\rho_{\mathrm{A}}^{(\mathrm{AB})}=\mathrm{tr}_{\mathrm{B}}\left(\rho^{(\mathrm{AB})}\right)$, где tr_{B} – линейное отображение, называемое **частичным следом** по системе B, удовлетворяющее равенству

$$\mathrm{tr}_{\mathrm{B}}\left(\left|a_1\right\rangle\left\langle a_2\right|\otimes\left|b_1\right\rangle\left\langle b_2\right|\right)=\left|a_1\right\rangle\left\langle a_2\right|\mathrm{tr}\left(\left|b_1\right\rangle\left\langle b_2\right|\right),$$

в котором $\left|a_1\right\rangle$ и $\left|a_2\right\rangle$ – два произвольных вектора состояния системы A, $\left|b_1\right\rangle$ и $\left|b_2\right\rangle$ – два произвольных вектора состояния системы B; tr – матричная функция **след**, то есть для произвольной квадратной матрицы X по определению $\mathrm{tr}(X)$ есть сумма диагональных элементов матрицы X.

Аналогично определяется редуцированная матрица плотности $\rho_{\mathrm{B}}^{(\mathrm{AB})}$ для системы B: $\rho_{\mathrm{B}}^{(\mathrm{AB})}=\mathrm{tr}_{\mathrm{A}}\left(\rho^{(\mathrm{AB})}\right)$, где tr_{A} – линейное отображение, называемое **частичным следом** по системе A, удовлетворяющее равенству

$$\mathrm{tr}_{\mathrm{A}}\left(\left|a_1\right\rangle\left\langle a_2\right|\otimes\left|b_1\right\rangle\left\langle b_2\right|\right)=\mathrm{tr}\left(\left|a_1\right\rangle\left\langle a_2\right|\right)\left|b_1\right\rangle\left\langle b_2\right|,$$

в котором $\left|a_1\right\rangle$ и $\left|a_2\right\rangle$ – два произвольных вектора состояния системы A, $\left|b_1\right\rangle$ и $\left|b_2\right\rangle$ – два произвольных вектора состояния системы B.

Известна (см., например, [24; 39; 50; 56]) следующая теорема.

Теорема 1.1.6. Пусть $|\psi\rangle$ – чистое состояние составной квантовой системы AB, состоящей из двух подсистем A и B. Тогда существуют такие ортонормированные состояния $\left|\psi_i^{(\mathrm{A})}\right\rangle$ системы A и ортонормированные состояния $\left|\psi_i^{(\mathrm{B})}\right\rangle$ системы B (где $i=\overline{1,d}$; $d=\min\left(d_1,d_2\right)$; d_1, d_2 – размерности пространств состояний подсистем A и B соответственно), что верно равенство

$$|\psi\rangle=\sum_{i=1}^{d}\lambda_i\left|\psi_i^{(\mathrm{A})}\right\rangle\left|\psi_i^{(\mathrm{B})}\right\rangle, \tag{1.1.7}$$

где λ_i ($i=\overline{1,d}$) – неотрицательные действительные числа, удовлетворяющие условию $\sum_{i=1}^{d}\lambda_i^2=1$.

Определение 1.1.8. Представление чистого состояния $|\psi\rangle$ составной квантовой системы AB в виде (1.1.7) называется **разложением Шмидта**; числа λ_i, где $i=\overline{1,d}$, называются **коэффициентами Шмидта**; количество ненулевых коэффициентов Шмидта называется **числом Шмидта**. В случае, когда размерности пространств состояний подсистем A и B одинаковы и равны d, то множества состояний $\left\{\left|\psi_i^{(\mathrm{A})}\right\rangle\middle|\, i=\overline{1,d}\right\}$ и $\left\{\left|\psi_i^{(\mathrm{B})}\right\rangle\middle|\, i=\overline{1,d}\right\}$ называются **базисами Шмидта** соответственно для систем A и B.

Рассмотрим еще один математический инструмент квантовой теории – расширение до чистого состояния. Предположим, что имеется квантовая система A с матрицей плотности $\rho^{(\mathrm{A})}$. Тогда можно ввести (см. [50]) квантовую систему R и определить чистое состояние $\left|\psi^{(\mathrm{AR})}\right\rangle$

для квантовой системы AR так, что $\rho^{(\mathrm{A})}$ совпадает с редуцированной матрицей плотности $\rho_{\mathrm{A}}^{(\mathrm{AR})}$ для системы A, то есть $\rho^{(\mathrm{A})} = \rho_{\mathrm{A}}^{(\mathrm{AR})} = \mathrm{tr}_{\mathrm{R}}\left(\rho^{(\mathrm{AR})}\right)$, где

$$\rho^{(\mathrm{AR})} = \left|\psi^{(\mathrm{AR})}\right\rangle\left\langle\psi^{(\mathrm{AR})}\right|$$

– матрица плотности квантовой системы AR. Изложенная процедура – это чисто математическая процедура, называемая **расширением до чистого состояния**. При этом квантовая система R – фиктивная система, не имеющая прямого физического смысла. Таким образом, расширение до чистого состояния – процедура, позволяющая связать чистые состояния со смешанными состояниями.

§ 1.2. Квантовые измерения

В моделях квантовых измерений рассматриваются типы измерений, которые можно провести для квантовых систем, а также способы определения вероятности того, что измерение дает ожидаемый результат. Кроме этого важен учет и того, какое влияние оказывает измерение на состояние квантовой системы. То есть важно выявление того, в каком состоянии находится квантовая система после измерения. Такие модели квантовых измерений описываются в виде постулата измерения [50], суть которого заключается в следующем. Процесс квантового измерения описывается набором $\left\{M_j \middle| j \in J\right\}$ линейных операторов, называемых операторами измерения. Здесь J – некоторый набор индексов, используемых для нумерации результатов измерения. Часто вместо выражения «результат с индексом j» используется выражение «результат j». Операторы измерения действуют на пространстве состояний системы, подлежащей измерению. Если непосредственно перед измерением квантовая система находилась в состоянии $|\psi\rangle$, то вероятность [22; 28] $p(j)$ того, что в результате измерения будет получен результат $j \in J$, задается выражением

$$p(j) = \langle \psi | M_j^* M_j | \psi \rangle, \tag{1.2.1}$$

где $\langle \psi | M_j^* M_j | \psi \rangle$ – скалярное произведение векторов $|\psi\rangle$ и $M_j^* M_j |\psi\rangle$, M_j^* – оператор (в матричном представлении), эрмитово-сопряженный с оператором M_j. А после измерения система будет находиться в состоянии

$$\frac{M_j |\psi\rangle}{\sqrt{\langle \psi | M_j^* M_j | \psi \rangle}}. \tag{1.2.2}$$

Операторы измерения удовлетворяют **условию полноты**

$$\sum_{j \in J} M_j^* M_j = \mathbf{I}_d, \tag{1.2.3}$$

где $\mathbf{I}_d$ – единичный оператор в гильбертовом пространстве размерности d.

Обратимся теперь к персонажам, являющимся традиционными героями некоторых текстов в области защиты информации и связи. Предположим, что Алиса управляет устройством, которое приготавливает квантовую систему, то есть выполняет этап (Б) (см. § 1.1) некоторого эксперимента над квантовой системой. А Боб проводит измерение, то есть выполняет этап (Г) (см. § 1.1) эксперимента над квантовой системой, и записывает результаты.

Устройство подготовки задает те состояния, в которых будет находиться квантовая система после этапа (Б). Событию подготовительного считывания с номером t (где $t \in T$) с подготовительного устройства ставится в соответствие линейный неотрицательно определенный оператор Λ_t, действующий в пространстве состояний квантовой системы. Операторы Λ_t, $t \in T$, в общем случае могут и не быть ортогональны друг другу.

Для устройства измерения происходит событие считывания с номером j, где $j \in J$ показывает результат измерения. Устройству измерения ставится, как указывается выше, оператор устройства измерения M_j, который также линеен.

Пусть

$$\Lambda = \sum_{t=1}^{T} \Lambda_t\,,\; M = \sum_{j \in J} M_j\,, \tag{1.2.4}$$

tr – матричная функция *след*, то есть для любой квадратной матрицы A значение $\mathrm{tr}(A)$ – это сумма диагональных элементов матрицы A. Тогда, следуя [56],

$$p(t,j) = \frac{\mathrm{tr}(\Lambda_t M_j)}{\mathrm{tr}(\Lambda M)} \tag{1.2.5}$$

задает совместное распределение вероятностей [14], сопоставленное отдельной точке (t, j) в пространстве выборок;

$$p(t) = \frac{\mathrm{tr}(\Lambda_t M)}{\mathrm{tr}(\Lambda M)} \tag{1.2.6}$$

– это безусловная вероятность [14] того, что в результате случайно выбранного эксперимента с зарегистрированным составным событием было подготовлено событие с номером t;

$$p(j) = \frac{\mathrm{tr}(\Lambda M_j)}{\mathrm{tr}(\Lambda M)} \tag{1.2.7}$$

– это вероятность получить результат измерения с номером j при заданном составном событии;

$$p(j\,|\,t) = \frac{\mathrm{tr}(\Lambda_t M_j)}{\mathrm{tr}(\Lambda_t M)} \tag{1.2.8}$$

– это вероятность получения Бобом результата измерения с номером j при условии, что Алисой подготовлено событие с номером t;

$$p(t \mid j) = \frac{\mathrm{tr}\left(\Lambda_t M_j\right)}{\mathrm{tr}\left(\Lambda M_j\right)} \tag{1.2.9}$$

– это вероятность того, что Алисой подготовлено состояние с номером t при условии, что Бобом зарегистрировано событие с номером j.

Рассмотрим один важный частный случай квантового измерения, называемый измерением фон Неймана, или проективным квантовым измерением, или просто проективным измерением. Для этого приведем определение понятия *наблюдаемая* (в литературе встречается и другое название этого понятия – *измеряемая*).

Наблюдаемой называется любое свойство квантовой системы, которое в принципе может быть измерено [52].

В квантовой механике наблюдаемая представляется эрмитовым оператором [37; 50]. И, наоборот, любой эрмитов оператор (эрмитова матрица), действующий в пространстве состояний изучаемой квантовой системы, является представлением некоторой наблюдаемой [37; 50]. Поэтому часто вместо выражения «наблюдаемая, представляемая эрмитовым оператором A» используется выражение «наблюдаемая A».

Пусть P – эрмитова матрица $d\times d$. В этом случае собственные значения λ_j, где $j \in J$, матрицы P являются действительными числами. Матрицу P можно представить в следующем виде (называемом *спектральным разложением*):

$$P = \sum_{j \in J} \lambda_j P_j\ , \tag{1.2.10}$$

где P_j – *проектор* (т.е. *проективный оператор*) на собственное подпространство оператора P, соответствующее значению λ_j, $j \in J$. Для проективных операторов имеет место равенство

$$P_j P_k = \delta_{jk} P_j\ . \tag{1.2.11}$$

Любая наблюдаемая P определяет *проективное измерение*. В этом случае, с учетом вышеприведенных обозначений, имеем $M_j = P_j$, где

$j \in J$. Возможные результаты измерения соответствуют собственным значениям $\left\{\lambda_j \middle| j \in J\right\}$.

При проективном измерении квантовой системы, находящейся в состоянии $|\psi\rangle$, получается результат λ_j с вероятностью

$$p(\lambda_j) = p(j) = \langle\psi|P_j|\psi\rangle. \quad (1.2.12)$$

А после проективного измерения сама квантовая система будет находиться в состоянии

$$\frac{P_j|\psi\rangle}{\sqrt{\langle\psi|P_j|\psi\rangle}}. \quad (1.2.13)$$

При этом если квантовая система подвергается тому же самому измерению сразу после проективного измерения, то однозначно можно сказать, что результат будет тем же.

Проективные измерения обладают рядом примечательных свойств. В частности, если выполняется большое количество экспериментов, в которых заранее подготавливается состояние $|\psi\rangle$, то несложно вычислить среднее значение $\langle P\rangle$ (то есть математическое ожидание $\mathbb{E}(P)$ [17]) таких измерений:

$$\langle P\rangle = \mathbb{E}(P) = \sum_{j\in J}\lambda_j p(j) = \sum_{j\in J}\lambda_j\langle\psi|P_j|\psi\rangle = \langle\psi|P|\psi\rangle. \quad (1.2.14)$$

А дисперсия [17] получаемых значений определяется формулой

$$(\Delta(P))^2 = \langle P^2\rangle - \langle P\rangle^2. \quad (1.2.15)$$

Существуют еще и другие подходы к определению проективных измерений, среди которых отметим следующий подход.

Часто вместо того, чтобы описывать проективные измерения с помощью наблюдаемых, выписывается полное множество ортогональных проекторов $\left\{P_j \middle| j \in J\right\}$ [52], удовлетворяющих соотношениям:

$$P_j P_k = \delta_{jk} P_j \quad (1.2.16)$$

и

$$\sum_{j \in J} P_j = \mathbf{I}_d \,. \tag{1.2.17}$$

В рамках данного подхода определения проективных измерений примечательным является способ, заключающийся в выборе некоторого ортонормированного базиса $\left\{ |k\rangle \middle| k = 1, 2, \ldots, d \right\}$ в пространстве состояний квантовой системы и выполнении проективных измерений с проекторами

$$P_k = |k\rangle\langle k|, \;\; k = 1, 2, \ldots, d. \tag{1.2.18}$$

Довольно часто встречаются ситуации, когда состояние системы после измерения не представляет никакого интереса. Например, это имеет место, когда исследователя интересуют только возможные результаты измерений, а само измерение над квантовой системой производится один раз – по окончании эксперимента. В таких случаях применяется *положительное операторнозначное измерение* (ПОЗИ) [56], по-английски называемое POVM-измерением (Positive Operator-Valued Measure) [50]. В этом случае берется множество $\left\{ E_j \middle| j \in J \right\}$ неотрицательно определенных операторов E_j, удовлетворяющих условию $\sum_{j \in J} E_j = \mathbf{I}_d$. Когда состояние $|\psi\rangle$ подвергается такому измерению, исход с номером j появляется с вероятностью

$$p(j) = \langle \psi | E_j | \psi \rangle \,. \tag{1.2.9}$$

В данной работе большое значение придается проективным измерениям. Для них вышеприведенные выражения (1.2.5) – (1.2.8) вероятностей

$$p(t,j), \; p(t), \; p(j), \; p(j\,|\,t)$$

примут следующий вид:

$$p(t,j) = \frac{\mathrm{tr}\left(\Lambda_t P_j\right)}{\mathrm{tr}(\Lambda)}, \tag{1.2.20}$$

$$p(t) = \frac{\mathrm{tr}(\Lambda_t)}{\mathrm{tr}(\Lambda)}, \tag{1.2.21}$$

$$p(j) = \frac{\mathrm{tr}(\Lambda P_j)}{\mathrm{tr}(\Lambda)}, \tag{1.2.22}$$

$$p(j \mid t) = \frac{\mathrm{tr}(\Lambda_t P_j)}{\mathrm{tr}(\Lambda_t)}. \tag{1.2.23}$$

Остановимся еще на одном аспекте квантовых измерений, а именно – на особенностях измерений, проводимых над квантовой системой A как подсистемой составной квантовой системы AB, включающей в себя, наряду с подсистемой A, и квантовую подсистему B.

Дело в том, что измерения, проводимые только над подсистемой A квантовой системы AB, по сути являются измерениями, проводимыми над всей квантовой системой AB, но с определенной спецификой, отличающей такие измерения как от измерений, проводимых собственно над A (когда она представляет собой «изолированную» квантовую систему), так и от измерений над квантовой системой AB, когда измерительное устройство оказывает непосредственное локальное воздействие на обе подсистемы A и B квантовой системы AB.

То же самое и с симметричным случаем, то есть с измерениями над подсистемой B квантовой системы AB. Эта специфика в рамках спектра задач, решаемых в данной работе, требует более подробного математического описания. Дальнейшую часть данного параграфа посвятим решению именно этой задачи. Начнем с уточнения условия задачи.

Условие задачи. Пусть $\{M_j \mid j \in J\}$ – полное множество ортогональных проекторов, определяющих некоторое проективное измерение над квантовой системой A, с множеством возможных результатов $\{\lambda_j \mid j \in J\}$; $\{N_k \mid k \in K\}$ – полное множество ортогональных проекторов, определяющих некоторое проективное измерение над квантовой системой B, с множеством возможных результатов $\{\mu_k \mid k \in K\}$. Требуется следующее:

1) Описать измерение над составной квантовой системой AB, такое, что для любых состояний $|\psi_1\rangle$ и $|\psi_2\rangle$ соответственно подсистем A и B результатами этого измерения над системой AB в состоянии $|\psi_1\rangle\otimes|\psi_2\rangle$ являются числа λ_j, $j \in J$, с теми же вероятностями, с какими они появляются при проведении измерения, определяемого множеством проекторов $\{M_j | j \in J\}$, над квантовой системой A в состоянии $|\psi_1\rangle$. И при этом после измерения состояние $|\psi_2\rangle$ подсистемы B не меняется, а подсистема A после измерения будет находиться в том же состоянии, в котором оказывается A при проведении над ней измерения (определяемого множеством проекторов $\{M_j | j \in J\}$) как над изолированной квантовой системой.

2) Описать измерение над составной квантовой системой AB, такое, чтодля любых состояний $|\psi_1\rangle$ и $|\psi_2\rangle$ соответственно подсистем A и B результатами этого измерения над системой AB в состоянии $|\psi_1\rangle\otimes|\psi_2\rangle$ являются числа μ_k, $k \in K$, с теми же вероятностями, с какими они появляются при проведении измерения, определяемого множеством проекторов $\{N_k | k \in K\}$, над квантовой системой B в состоянии $|\psi_2\rangle$. И при этом состояние $|\psi_1\rangle$ подсистемы A не меняется после измерения, а подсистема B после измерения будет находиться в том же состоянии, в котором оказывается B при проведении над ней измерения (определяемого множеством проекторов $\{N_k | k \in K\}$) как над изолированной квантовой системой.

Решение данной задачи вытекает из следующего утверждения.

Утверждение 1.2.24.

а) Первому пункту условия задачи удовлетворяет измерение над составной квантовой системой AB, определяемое множеством операторов

$$\left\{M_j \otimes \mathbf{I}_{d(\mathrm{B})} \middle| j \in J\right\},$$

где $\mathbf{I}_{d(\mathrm{B})}$ – единичная матрица $d(\mathrm{B})\times d(\mathrm{B})$, $d(\mathrm{B})$ – размерность пространства состояний подсистемы B.

б) Второму пункту условия задачи удовлетворяет измерение над составной квантовой системой AB, определяемое множеством операторов

$$\left\{\mathbf{I}_{d(\mathrm{A})}\otimes N_k \middle| k\in K\right\},$$

где $\mathbf{I}_{d(\mathrm{A})}$ – единичная матрица $d(\mathrm{A})\times d(\mathrm{A})$, $d(\mathrm{A})$ – размерность пространства состояний подсистемы A.

Доказательство. Доказательство пункта (б) данного утверждения аналогично доказательству пункта (а). Поэтому ограничимся доказательством пункта (а).

Выпишем сперва выражения для вероятностей, с какими появляются числа λ_j, $j\in J$, как результаты при проведении измерения, определяемого множеством проекторов $\left\{M_j \middle| j\in J\right\}$, над квантовой системой A в состоянии $|\psi_1\rangle$, а также выражения для состояния квантовой системы A после проведения измерения:

$$p(\lambda_j)=p(j)=\langle\psi_1|M_j|\psi_1\rangle,\ j\in J \tag{1.2.25}$$

– выражения для вероятностей;

$$\frac{M_j|\psi_1\rangle}{\sqrt{\langle\psi_1|M_j|\psi_1\rangle}} \tag{1.2.26}$$

– выражение для состояния после измерения.

Теперь покажем, что множество матриц $\left\{M_j\otimes\mathbf{I}_{d(\mathrm{B})}\middle| j\in J\right\}$ определяет измерение. Для этого достаточно показать, что множество $\left\{M_j\otimes\mathbf{I}_{d(\mathrm{B})}\middle| j\in J\right\}$ удовлетворяет условию полноты. Выполнение этого условия вытекает из следующей цепочки равенств:

$$\sum_{j\in J}\left(M_j\otimes\mathbf{I}_{d(\text{B})}\right)^*\left(M_j\otimes\mathbf{I}_{d(\text{B})}\right)=\sum_{j\in J}\left(M_j^*M_j\right)\otimes\left(\mathbf{I}_{d(\text{B})}\mathbf{I}_{d(\text{B})}\right)=$$
$$=\left(\sum_{j\in J}M_j^*M_j\right)\otimes\mathbf{I}_{d(\text{B})}=\mathbf{I}_{d(\text{A})}\otimes\mathbf{I}_{d(\text{B})}=\mathbf{I}_{d(\text{A})d(\text{B})}.$$

Вычислим вероятность $p\left(\lambda_j\right)$ появления числа λ_j, $j\in J$, как результата при проведении измерения, определяемого множеством операторов (в матричном представлении) $\left\{M_j\otimes\mathbf{I}_{d(\text{B})}\middle|\, j\in J\right\}$, над квантовой системой AB в состоянии $|\psi_1\rangle\otimes|\psi_2\rangle$:

$$p\left(\lambda_j\right)=\langle\psi_1\psi_2|\left(M_j\otimes\mathbf{I}_{d(\text{B})}\right)^*\left(M_j\otimes\mathbf{I}_{d(\text{B})}\right)|\psi_1\psi_2\rangle=$$
$$=\langle\psi_1\psi_2|\left(M_j^*M_j\right)\otimes\left(\mathbf{I}_{d(\text{B})}\mathbf{I}_{d(\text{B})}\right)|\psi_1\psi_2\rangle=\langle\psi_1\psi_2|\left(M_j\otimes\mathbf{I}_{d(\text{B})}\right)|\psi_1\psi_2\rangle=$$
$$=\left\langle\psi_1\psi_2\middle|\left(M_j|\psi_1\rangle\otimes\mathbf{I}_{d(\text{B})}|\psi_2\rangle\right)\right\rangle=\langle\psi_1|M_j|\psi_1\rangle\otimes\langle\psi_2|\mathbf{I}_{d(\text{B})}|\psi_2\rangle=$$
$$=\langle\psi_1|M_j|\psi_1\rangle\otimes\langle\psi_2|\psi_2\rangle=\langle\psi_1|M_j|\psi_1\rangle\otimes\mathbf{1}=\langle\psi_1|M_j|\psi_1\rangle,\ j\in J,\quad(1.2.27)$$

что совпадает с (1.2.25).

Определим состояние, в котором будет находиться квантовая система AB после измерения:

$$\frac{M_j\otimes\mathbf{I}_{d(\text{B})}|\psi_1\psi_2\rangle}{\sqrt{\langle\psi_1|\left(M_j\otimes\mathbf{I}_{d(\text{B})}\right)^*\left(M_j\otimes\mathbf{I}_{d(\text{B})}\right)|\psi_1\psi_2\rangle}}=\frac{\left(M_j|\psi_1\rangle\right)\otimes\left(\mathbf{I}_{d(\text{B})}|\psi_2\rangle\right)}{\sqrt{\langle\psi_1|M_j^*M_j|\psi_1\rangle}}=$$
$$=\frac{\left(M_j|\psi_1\rangle\right)\otimes|\psi_2\rangle}{\sqrt{\langle\psi_1|M_j|\psi_1\rangle}}=\frac{M_j|\psi_1\rangle}{\sqrt{\langle\psi_1|M_j|\psi_1\rangle}}\otimes|\psi_2\rangle.\quad(1.2.28)$$

Отсюда и из (1.2.26) следует, что после измерения состояние $|\psi_2\rangle$ подсистемы B не меняется, а подсистема A после измерения будет находиться в том же состоянии, в котором оказывается A при проведении над ней измерения (определяемого множеством проекторов $\left\{M_j\middle|\, j\in J\right\}$) как над изолированной квантовой системой.

Пункт (а) утверждения доказан.

Замечание 1.2.29. При фиксированных базисах пространств состояний подсистем А и В квантовой системы АВ множества $\left\{M_j \otimes \mathbf{I}_{d(\mathrm{B})} \middle| j \in J\right\}$ и $\left\{\mathbf{I}_{d(\mathrm{A})} \otimes N_k \middle| k \in K\right\}$ определены однозначно. Это следует из того, что в базисе пространства состояний квантовой системы АВ, являющейся тензорным произведением базисов состояний подсистем А и В квантовой системы АВ, однозначно определяются матрицы соответствующих линейных операторов.

Замечание 1.2.30. В данной работе, как и во многих работах по квантовой информации и квантовым вычислениям (см., например, [50; 52]), могут встречаться не совсем «точные» выражения типа «измерим кубит А», или «измерим квантовую систему А в состоянии $|\psi\rangle$», или «измерим состояние $|\psi\rangle$ квантовой системы А», или «измерив квантовую систему А, получим состояние $|\psi\rangle$». Точные формулировки этих выражений соответственно следующие: первое выражение надо понимать в смысле «проведем измерение над кубитом А», следующие два выражения – в смысле «проведем измерение над квантовой системой А, находящейся в состоянии $|\psi\rangle$», а последнее выражение – в смысле «в результате проведения измерения над квантовой системой А она перешла в состояние $|\psi\rangle$». По мнению авторов данной работы, причиной использования «жаргонных» (если так можно выразиться) выражений является кажущееся понижение «тяжеловесности» текста за счет использования менее «точных» формулировок. Однако это не должно быть чрезмерным и не должно приводить к искажению смысловой части излагаемого материала.

§ 1.3. Квантовые вычисления

Изменения, происходящие с состояниями квантовых систем, можно описать на языке **квантовых вычислений**. Известно, что классический компьютер строится из электрических схем, содержащих логические элементы, позволяющие обрабатывать классическую информацию, преобразуя ее из одного вида в другой, и «провода» (кавычки здесь из-за того, что слово *провод* имеет обобщенный смысл, как канал передачи), позволяющие передавать классическую информацию. Точно также квантовый вычислитель состоит из квантовых «проводов» и элементарных квантовых логических элементов (вентилей), позволяющих передавать квантовую информацию[52; 59] и манипулировать ею [49; 50; 52], а также измерительных элементов, действие которых описывается операторами измерений (последние подробно были рассмотрены в параграфе 1.2).

Если взять состояние квантовой системы из n кубитов (где $n \in \mathbb{N}$) и применить к нему последовательность квантовых логических элементов и измерительных элементов, то получится квантовая цепь (или, подругому, квантовая схема). При этом упомянутое состояние n-кубитной квантовой системы называется начальным входным состоянием квантовой цепи.

Таким образом, квантовая цепь – это квантовое вычислительное устройство, состоящее из синхронизированных по времени квантовых логических элементов и измерительных элементов [51]. Выходы одних элементов связаны «проводами» с входами других. Несколько цепей могут быть соединены друг с другом квантовыми «проводами». Как уже говорилось, в цепях, кроме квантовых логических элементов и «проводов», могут быть использованы и измерительные элементы. Следует отметить, что всегда можно квантовую цепь составить так, чтобы все измерения выполнялись в конце, после применения всех необходимых квантовых логических элементов [51].

В отличие от классических цепей, которые могут содержать в себе циклы, квантовые цепи являются «однопроходными», т.е. исполняются один раз слева направо [51]. Более того, квантовые цепи являются специфическими, т.е. каждая цепь реализует только один квантовый алгоритм.

Действие каждого логического элемента на n-кубитное состояние в квантовой цепи можно представить в виде результата преобразования этого состояния с помощью унитарного оператора с матрицей размера $2^n \times 2^n$. То есть математически квантовые логические элементы представляются унитарными операторами, действующими в гильбертовых пространствах соответствующих размерностей. Таким образом, термин *квантовое вычисление* в данной работе понимается как выполнение последовательности унитарных операторов и операторов измерений, преобразующей начальное входное состояние в некоторое конечное выходное состояние квантовой цепи. Отметим, что квантовые вычисления нацелены на решение вычислительно сложных задач с помощью устройств, основанных на принципах и ресурсах квантовой механики.

Опишем некоторый набор квантовых логических элементов, достаточный для дальнейшего изложения материала данной работы. При этом матрицы унитарных операторов, соответствующих квантовым логическим элементам, будем обозначать так же, как и сами квантовые логические элементы.

Среди квантовых логических элементов, действующих на состояние квантовой системы из одного кубита, выделим следующие:

вентиль Паули $\mathbf{I}_2$; этот логический элемент представляет собой тождественное преобразование

$$\sigma_0 = \mathbf{I}_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

которое на однокубитное состояние $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ ($\alpha, \beta \in \mathbb{C}$, $|\alpha|^2 + |\beta|^2 = 1$) действует следующим образом

$$\sigma_0|\psi\rangle = \mathbf{I}_2|\psi\rangle = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}|\psi\rangle = |\psi\rangle;$$

вентиль Паули $\mathbf{X}$; этот квантовый логический элемент реализует унитарный оператор

$$\sigma_1 = \sigma_{\mathbf{X}} = \mathbf{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

и представляет собой квантовый аналог классического логического элемента NOT; действует следующим образом

$$\sigma_1 |\psi\rangle = \sigma_{\mathbf{X}} |\psi\rangle = \mathbf{X}|\psi\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} |\psi\rangle = \beta |0\rangle + \alpha |1\rangle ;$$

<u>вентиль Паули **Y**</u>; этот квантовый логический элемент реализует унитарный оператор

$$\sigma_2 = \sigma_{\mathbf{Y}} = \mathbf{Y} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

и действует следующим образом

$$\sigma_2 |\psi\rangle = \sigma_{\mathbf{Y}} |\psi\rangle = \mathbf{Y}|\psi\rangle = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} |\psi\rangle = -\beta i |0\rangle + \alpha i |1\rangle ,$$

где $i \in \mathbb{C}$, i – мнимая единица, то есть $i^2 = (-1)$;

<u>вентиль Паули **Z**</u>; этот квантовый логический элемент реализует унитарный оператор

$$\sigma_3 = \sigma_{\mathbf{Z}} = \mathbf{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

и действует следующим образом

$$\sigma_3 |\psi\rangle = \sigma_{\mathbf{Z}} |\psi\rangle = \mathbf{Z}|\psi\rangle = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} |\psi\rangle = \alpha |0\rangle - \beta |1\rangle ;$$

<u>фазовращающий вентиль (вентиль изменения фазы) **P**(θ)</u>; этот квантовый логический элемент реализует унитарный оператор

$$\mathbf{P}(\theta) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}$$

и действует следующим образом

$$\mathbf{P}(\theta)|\psi\rangle = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix} |\psi\rangle = \alpha |0\rangle + e^{i\theta} \beta |1\rangle ;$$

вентиль Адамара **H**; этот квантовый логический элемент реализует унитарный оператор

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

и действует следующим образом

$$\mathbf{H}|\psi\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}|\psi\rangle = \frac{\alpha+\beta}{\sqrt{2}}|0\rangle + \frac{\alpha-\beta}{\sqrt{2}}|1\rangle.$$

Выше было указано, что квантовые вычисления нацелены на решение вычислительно сложных задач с помощью устройств, основанных на принципах и ресурсах квантовой механики. Однако человеческие органы чувств настроены на классический мир, поэтому необходимы устройства сопряжения (интерфейсы) между пользователем и оборудованием. Интерфейс на выходе отвечает за то, как получить классическую информацию после выполнения квантового алгоритма. Он называется измерением, и, как было указано выше, всегда можно так построить соответствующую квантовую цепь, чтобы измерение реализовалось последним элементом квантовой цепи.

Так как интерфейс на выходе, т.е. квантовые измерения, нами были подробно рассмотрены ранее в параграфе 1.2, то имеет смысл сосредоточиться на простом примере входного интерфейса, а именно, на том, как начиная, например, с состояния $|0\rangle$ создать состояние $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ с определенными $\alpha, \beta \in \mathbb{C}$, где $|\alpha|^2 + |\beta|^2 = 1$, однокубитной квантовой системы на входе некоторой квантовой цепи для того, чтобы запустить эту цепь. Для решения такой задачи необходимо, в свою очередь, предложить другую подходящую квантовую цепь. Соответствующая последовательность квантовых логических элементов может быть построена с использованием приведенных выше однокубитных квантовых логических элементов.

Действительно, рассмотрим следующую последовательность квантовых логических элементов:

$$\mathbf{H},\ \mathbf{P}(\theta),\ \mathbf{H},\ \mathbf{P}\left(0{,}5\pi+\tau-\frac{\theta}{2}\right),\ \mathbf{X},\ \mathbf{P}\left(\gamma-\frac{\theta}{2}\right),\ \mathbf{X}, \tag{1.3.1}$$

где θ – минимальный неотрицательный угол, такой, что $\cos\frac{\theta}{2}=|\alpha|$ и $\sin\frac{\theta}{2}=|\beta|$; угол θ существует, так как справедливо равенство $|\alpha|^2+|\beta|^2=1$; $\gamma=\arg\alpha$, $\tau=\arg\beta$, $e^{i\gamma}\cos\frac{\theta}{2}=\alpha$, $e^{i\tau}\sin\frac{\theta}{2}=\beta$.

Выпишем по шагам квантовый алгоритм, реализуемый квантовой цепью, состоящей из последовательности квантовых логических элементов (1.3.1). Состояние на входе квантовой цепи

$$|\psi_0\rangle=|0\rangle.$$

Шаг 1. Пропускаем кубит через элемент **H**, что равносильно применению к состоянию $|\psi_0\rangle$ линейного преобразования с матрицей $\mathbf{H}=\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$. В результате кубит перейдет в состояние

$$|\psi_1\rangle=\mathbf{H}|\psi_0\rangle=\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}|\psi_0\rangle=\frac{|0\rangle+|1\rangle}{\sqrt{2}}.$$

Шаг 2. Пропускаем кубит через элемент **P**(θ), что равносильно применению к состоянию $|\psi_1\rangle$ линейного преобразования с матрицей $\mathbf{P}(\theta)=\begin{pmatrix}1 & 0\\ 0 & e^{i\theta}\end{pmatrix}$. В результате кубит перейдет в состояние

$$|\psi_2\rangle=\mathbf{P}(\theta)|\psi_1\rangle=\begin{pmatrix}1 & 0\\ 0 & e^{i\theta}\end{pmatrix}|\psi_1\rangle=\frac{1}{\sqrt{2}}|0\rangle+e^{i\theta}\frac{1}{\sqrt{2}}|1\rangle.$$

Шаг 3. Пропускаем кубит через элемент **H**, что равносильно применению к состоянию $|\psi_2\rangle$ линейного преобразования с матрицей $\mathbf{H}=\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$. В результате кубит перейдет в состояние

$$|\psi_3\rangle = \mathbf{H}|\psi_2\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}|\psi_2\rangle = \frac{1}{\sqrt{2}}\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}} + e^{i\theta}\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) =$$
$$= 0,5\left(1+e^{i\theta}\right)|0\rangle + 0,5\left(1-e^{i\theta}\right)|1\rangle.$$

Шаг 4. Пропускаем кубит через элемент $\mathbf{P}\left(0,5\pi+\tau-\frac{\theta}{2}\right)$, что равносильно применению к состоянию $|\psi_3\rangle$ линейного преобразования с матрицей $\mathbf{P}\left(0,5\pi+\tau-\frac{\theta}{2}\right)=\begin{pmatrix}1 & 0\\ 0 & e^{i(0,5\pi+\tau-0,5\theta)}\end{pmatrix}$. В результате кубит перейдет в состояние

$$|\psi_4\rangle = \mathbf{P}\left(0,5\pi+\tau-\frac{\theta}{2}\right)|\psi_3\rangle = \begin{pmatrix}1 & 0\\ 0 & e^{i(0,5\pi+\tau-0,5\theta)}\end{pmatrix}|\psi_3\rangle =$$
$$= 0,5\left(1+e^{i\theta}\right)|0\rangle + e^{i(0,5\pi+\tau-0,5\theta)}0,5\left(1-e^{i\theta}\right)|1\rangle =$$
$$= e^{i\frac{\theta}{2}}\cos\frac{\theta}{2}|0\rangle + e^{i\left(\tau-\frac{\theta}{2}\right)}e^{i\frac{\theta}{2}}\sin\frac{\theta}{2}|1\rangle = e^{i\left(\frac{\theta}{2}-\gamma\right)}e^{i\gamma}\cos\frac{\theta}{2}|0\rangle + e^{i\tau}\sin\frac{\theta}{2}|1\rangle =$$
$$= e^{i\left(\frac{\theta}{2}-\gamma\right)}\alpha|0\rangle + \beta|1\rangle.$$

Шаг 5. Пропускаем кубит через элемент **X**, что равносильно применению к состоянию $|\psi_4\rangle$ линейного преобразования с матрицей $\mathbf{X}=\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$. В результате кубит перейдет в состояние

$$|\psi_5\rangle = \mathbf{X}|\psi_4\rangle = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}|\psi_4\rangle = \beta|0\rangle + e^{i\left(\frac{\theta}{2}-\gamma\right)}\alpha|1\rangle.$$

Шаг 6. Пропускаем кубит через элемент $\mathbf{P}\left(\gamma-\frac{\theta}{2}\right)$, что равносильно применению к состоянию $|\psi_5\rangle$ линейного преобразования с матрицей $\mathbf{P}\left(\gamma-\frac{\theta}{2}\right)=\begin{pmatrix}1 & 0\\ 0 & e^{i(\gamma-0,5\theta)}\end{pmatrix}$. В результате кубит перейдет в состояние

$$\left|\psi_6\right\rangle = \mathbf{P}\left(\gamma - \frac{\theta}{2}\right)\left|\psi_5\right\rangle = \begin{pmatrix} 1 & 0 \\ 0 & e^{i(\gamma - 0{,}5\theta)} \end{pmatrix}\left|\psi_5\right\rangle =$$

$$= \beta\left|0\right\rangle + e^{i\left(\gamma - \frac{\theta}{2}\right)} e^{i\left(\frac{\theta}{2} - \gamma\right)} \alpha\left|1\right\rangle = \beta\left|0\right\rangle + \alpha\left|1\right\rangle.$$

Шаг 7. Пропускаем кубит через элемент **X**, что равносильно применению к состоянию $\left|\psi_6\right\rangle$ линейного преобразования с матрицей $\mathbf{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. В результате кубит перейдет в состояние

$$\left|\psi_7\right\rangle = \mathbf{X}\left|\psi_6\right\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\left|\psi_6\right\rangle = \alpha\left|0\right\rangle + \beta\left|1\right\rangle = \left|\psi\right\rangle.$$

Таким образом, удалось создать состояние $\left|\psi\right\rangle$ в виде состояния $\left|\psi_7\right\rangle$ после выполнения шага 7.

Отметим еще в виде замечания следующую связь вентилей Паули с процессами квантовых измерений.

Замечание 1.3.2. С вентилями Паули связано *измерение компоненты спина вдоль оси v*, где $v = (v_1, v_2, v_3)$ – единичный вектор (норма вектора равна единице) в трехмерном пространстве над полем действительных чисел $\mathbb{R}$. Под таким измерением понимается измерение наблюдаемой

$$v \cdot \sigma = v_1\sigma_1 + v_2\sigma_2 + v_3\sigma_3.$$

Перейдем теперь к квантовым логическим элементам, действующим на состояния квантовой системы из более чем одного кубита.

Возьмем двухкубитную квантовую систему и применим однокубитный элемент **X** только к первому кубиту. Тогда, как и в случае измерений (см. параграф 1.2), воздействию подвергается вся двухкубитная система, и ко второму кубиту будет применен тождественный оператор $\mathbf{I}_2$. В результате этого к двухкубитной квантовой системе будет применен квантовый логический элемент, которому отвечает унитарный оператор с матрицей

$$\mathbf{X}\otimes\mathbf{I}_2=\begin{pmatrix}0&1\\1&0\end{pmatrix}\otimes\begin{pmatrix}1&0\\0&1\end{pmatrix}=\begin{pmatrix}0&0&1&0\\0&0&0&1\\1&0&0&0\\0&1&0&0\end{pmatrix},$$

где $\otimes$ – знак операции тензорного произведения.

Если же элемент **X** применен только ко второму кубиту, то, опять же, воздействию подвергается вся двухкубитная система, и соответствующему унитарному оператору отвечает матрица

$$\mathbf{I}_2\otimes\mathbf{X}=\begin{pmatrix}1&0\\0&1\end{pmatrix}\otimes\begin{pmatrix}0&1\\1&0\end{pmatrix}=\begin{pmatrix}0&1&0&0\\1&0&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}.$$

Этот подход очевидным образом распространяется на описание квантовых логических элементов, применяемых к состояниям многокубитных систем путем задействования применения квантовых логических элементов к их подсистемам.

Однако имеются квантовые логические элементы для многокубитных систем, матрицы которых нельзя представить в виде тензорных произведений матриц квантовых логических элементов, применяемых к их подсистемам. Среди них для дальнейшего наибольший интерес представляет элемент **CNOT**. Так как это квантовый логический элемент, действующий на состояния квантовой системы из двух кубитов, ему соответствует унитарный оператор с матрицей 4×4

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

В вычислительном базисе элемент **CNOT** инвертирует второй кубит, если состояние первого кубита равно 1, а в противном случае оставляет его без изменений. Как и все унитарные операторы, элемент **CNOT** действует на суперпозиции линейно, то есть если двухкубитную квантовую систему в состоянии

$$|\psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle,$$

где $a, b, c, d \in \mathbb{C}$, $|a|^2 + |b|^2 + |c|^2 + |d|^2 = 1$, пропустить через элемент **CNOT**, то в результате эта система окажется в состоянии

$$|\varphi\rangle = a|00\rangle + b|01\rangle + c|11\rangle + d|10\rangle.$$

Кроме элемента **CNOT** имеется много других квантовых логических элементов, действующих на состояния многокубитных квантовых систем. Однако **CNOT** и однокубитные квантовые логические элементы в некотором смысле могут порождать все остальные многокубитные квантовые логические элементы в силу **теоремы полноты** [50]:

*любой многокубитный квантовый логический элемент может быть составлен из **CNOT** и однокубитных элементов.*

Кроме сказанного, квантовый логический элемент **CNOT** интересен как «копировальная машина» [36]. Однако его возможности ограничены. В каком случае возможно *копирование* (или, как часто говорят, *клонирование* [56]) неизвестного квантового состояния, а в каком случае – нет, будет обсуждаться в следующем параграфе 1.4.

§ 1.4. Клонирование

Информация – основное понятие научно-практических направлений, изучающих процессы передачи, обработки и хранения различных данных. Суть понятия информации обычно поясняется на примерах. Формальное определение не дается, поскольку понятие информации относится к фундаментальным понятиям [31]. Информацию в данном традиционном ее понимании принято называть *классической информацией* [50; 52; 59]. Помимо известных и широко распространенных способов ее передачи, она может быть также «записана» (закодирована) в состояниях квантовых систем, например, в поляризационных состояниях одиночных фотонов, и передана через соответствующий физический канал связи. Так, к примеру, происходит при распределении криптографических ключей методами квантовой криптографии [39].

Однако квантовое состояние (то есть состояние квантовой системы) и само по себе представляет особого рода информационный ресурс, содержащий сведения о статистике всевозможных измерений над данной квантовой системой [52]. И в этом смысле информация, содержащаяся в квантовом состоянии, имеет качественные отличия от классической информации, и поэтому для нее применяют специальный термин *квантовая информация* [50; 52]. Наиболее ярким отличием квантовой информации от классической информации является невозможность копирования произвольного неизвестного квантового состояния (no cloning [59]).

Нет никаких проблем при копировании классической информации. Этому яркое свидетельство – копировальные машины в различных своих формах и реализациях, широко используемые в повседневной деятельности людей во многих государственных и частных организациях, учреждениях и предприятиях.

Единицей классической информации является бит. Копирование классической информации – по сути дела, копирование конечной битовой последовательности. Поэтому решить задачу копирования классической информации можно, например, путем решения задачи копирования одного бита и повторения этого решения необходимое число раз по отношению ко всем битам, составляющим информацию.

Копирование одного бита можно осуществить, например, с помощью классического логического элемента **CNOT** [50], реализующего функцию

$$f(x,y)=\begin{pmatrix} x \\ x\oplus y \end{pmatrix}$$

(где x и y – двоичные переменные, $\oplus$ – знак операции сложения по модулю 2), подав на вход элемента **CNOT** копируемый бит (в неизвестном состоянии x, то есть неизвестно, $x = 0$ или $x = 1$) и бит-«заготовку», инициализированную нулем (то есть $y = 0$). На выходе классического логического элемента **CNOT** будут два бита, имеющие одинаковые значения x. Реализуя эту процедуру по отношению к каждому биту информации, создаем ее копию.

В случае квантовой информации ситуация более сложная. Как уже говорилось в предыдущем параграфе, в случае квантовой информации принято использовать вместо термина «копирование» термин «клонирование», подчеркивая тем самым физический характер квантовой информации [52; 59].

Клонирование – это копирование квантовой информации. Клонирование – обязательно физический процесс [56].

В некоторых случаях можно клонировать квантовую информацию, а в других – нет. Конечно, это можно сделать каждый раз специальным прибором для данного конкретного известного квантового состояния (и даже для фиксированного набора ортогональных квантовых состояний). Но не существует универсального прибора, который бы размножал (клонировал) произвольное неизвестное квантовое состояние.

Рассмотрим пример, когда квантовую информацию можно клонировать. Предположим, что квантовая информация представлена кубитами, состояние каждого из которых принадлежит множеству $\{|0\rangle, |1\rangle\}$.

Возьмем любой из этих кубитов и обозначим его состояние $|x\rangle = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$, где $x_1,\ x_2 \in \{0, 1\}$ и справедливы равенства:

$$x_1 \cdot x_2 = 0\,,\ x_1 + x_2 = 1\,.$$

Это состояние нам неизвестно. Мы знаем только то, что $|x\rangle \in \{|0\rangle, |1\rangle\}$. Далее мы хотим использовать двухкубитный квантовый логический элемент **CNOT**, который на множестве состояний квантовой системы из двух кубитов реализует унитарный оператор с матрицей 4×4

$$\mathbf{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \qquad (1.4.1)$$

Поэтому нам необходим еще второй «вспомогательный» кубит. Этот второй кубит инициализируем в состоянии $|0\rangle$. Таким образом, на вход квантового логического элемента **CNOT** подаем два кубита в общем состоянии

$$|x\rangle|0\rangle = |x\rangle \otimes |0\rangle = \begin{pmatrix} x_1 \\ 0 \\ x_2 \\ 0 \end{pmatrix} = \begin{pmatrix} x_1x_1 \\ x_1x_2 \\ x_2x_2 \\ x_1x_2 \end{pmatrix}.$$

Умножив матрицу (1.4.1) на это состояние, получаем для двух кубитов на выходе квантового логического элемента **CNOT** следующее общее состояние:

$$\mathbf{CNOT}|x\rangle|0\rangle = \mathbf{CNOT}|x\rangle \otimes |0\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} x_1x_1 \\ x_1x_2 \\ x_2x_2 \\ x_1x_2 \end{pmatrix} = \begin{pmatrix} x_1x_1 \\ x_1x_2 \\ x_2x_1 \\ x_2x_2 \end{pmatrix} =$$

$$= \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \otimes \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = |x\rangle \otimes |x\rangle = |x\rangle|x\rangle.$$

Таким образом, нам удалось с помощью квантового логического элемента **CNOT** получить два кубита в общем состоянии $|x\rangle|x\rangle$, то есть мы убедились в том, что с помощью квантового логического элемента **CNOT** можно успешно клонировать квантовую информацию, представленную кубитами, состояние каждого из которых принадлежит множеству $\{|0\rangle, |1\rangle\}$.

Теперь рассмотрим общий случай, когда кубит находится в неизвестном состоянии

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle,$$

где $\alpha, \beta \in \mathbb{C}$, $|\alpha|^2 + |\beta|^2 = 1$. Когда говорится, что состояние неизвестно, имеется в виду, что неизвестны значения комплексных чисел α и β. Точно также, как и выше, для клонирования кубита в состоянии $|\psi\rangle$ воспользуемся квантовым логическим элементом **CNOT** и вторым «вспомогательным» кубитом в состоянии $|0\rangle$. Таким образом, на вход квантового логического элемента **CNOT** подаем два кубита в общем состоянии

$$|\psi\rangle|0\rangle = |\psi\rangle \otimes |0\rangle = \alpha|00\rangle + \beta|10\rangle = \begin{pmatrix} \alpha \\ 0 \\ \beta \\ 0 \end{pmatrix}. \tag{1.4.2}$$

Умножив матрицу (1.4.1) на состояние (1.4.2), получаем для двух кубитов на выходе квантового логического элемента **CNOT** следующее общее состояние:

$$\mathbf{CNOT}|\psi\rangle|0\rangle = \mathbf{CNOT}|\psi\rangle \otimes |0\rangle =$$
$$= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha \\ 0 \\ \beta \\ 0 \end{pmatrix} = \begin{pmatrix} \alpha \\ 0 \\ 0 \\ \beta \end{pmatrix} = \alpha|00\rangle + \beta|11\rangle. \tag{1.4.3}$$

С другой стороны, для состояния $|\psi\rangle|\psi\rangle$ справедливо равенство

$$|\psi\rangle|\psi\rangle = \alpha^2|00\rangle + \alpha\beta|01\rangle + \alpha\beta|10\rangle + \beta^2|11\rangle. \tag{1.4.4}$$

Следовательно, состояния (1.4.3) и (1.4.4) совпадают тогда и только тогда, когда справедливы равенства:

$$\alpha^2 = \alpha,\ \beta^2 = \beta,\ \alpha\beta = 0. \tag{1.4.5}$$

Отсюда, с учетом условия $|\alpha|^2 + |\beta|^2 = 1$, следует, что клонирование квантовой информации с помощью квантового логического элемента

CNOT возможно лишь в том случае, когда оно представлено кубитами, состояние каждого из которых принадлежит множеству $\{|0\rangle, |1\rangle\}$. И эта возможность не зависит от того, известны состояния этих кубитов или нет.

Здесь уместно, хотя и отвлекаясь от основного русла изложения и обсуждаемых в этом параграфе вопросов, привести следующее замечание, справедливость которого следует из вышеприведенного равенства (1.4.3).

Замечание 1.4.6. Хотя квантовый логический элемент **CNOT** пригоден как инструмент клонирования квантовой информации только в определенных ограниченных условиях, он (т.е. **CNOT**), как следует из равенства (1.4.3), представляет собой эффективный инструмент для построения **запутанных состояний** квантовой системы из двух кубитов на основе кубита в произвольном состоянии $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ и кубита в состоянии $|0\rangle$ при условии, что $\alpha \cdot \beta \neq 0$. Квантовая запутанность, или, точнее, запутанность состояний квантовых систем из двух и более кубитов, является новым ресурсом квантовой механики, пригодным для применений в области информационных и телекоммуникационных технологий. Этот ресурс и его различные свойства будут предметами обсуждения в последующих главах данной работы.

Возвращаясь теперь к обсуждаемым в данном параграфе вопросам, отметим следующее: установлено, что клонирование кубита с помощью квантового логического элемента **CNOT** не всегда возможно. И оказывается, что это касается не только элемента **CNOT**. Это свойство (что кубиты в неизвестном состоянии нельзя клонировать) носит более общий характер и известно как теорема *о невозможности клонирования* [74; 90].

Прежде, чем сформулировать и доказать теорему *о невозможности клонирования*, имеет смысл на качественном уровне объяснить, что следует из этой теоремы.

Во-первых, физического прибора (инструмента) в самом широком смысле этого понятия, позволяющего осуществить клонирование кубита в произвольном неизвестном состоянии

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle,$$

где $\alpha, \beta \in \mathbb{C}$, $|\alpha|^2 + |\beta|^2 = 1$, **не существует**.

Более того, не существует физического прибора (инструмента), позволяющего клонировать кубит в неизвестном состоянии, принадлежащем известному множеству состояний, содержащему не менее чем два неортогональных состояния. Например, не существует физического прибора (инструмента), позволяющего клонировать кубит в неизвестном состоянии, который принадлежит множеству состояний $\left\{|0\rangle, \dfrac{|0\rangle + |1\rangle}{\sqrt{2}}\right\}$. Понимается последнее предложение в следующем смысле: пусть $|\psi_1\rangle, |\psi_2\rangle \in \left\{|0\rangle, \dfrac{|0\rangle + |1\rangle}{\sqrt{2}}\right\}$, $|\psi_1\rangle \neq |\psi_2\rangle$, $|s\rangle$ – произвольное однокубитное состояние; тогда не существует прибора (инструмента), позволяющего при подаче на свой вход двух кубитов в общем состоянии $|\psi_1\rangle \otimes |s\rangle$ на выходе получить два кубита в общем состоянии $|\psi_1\rangle \otimes |\psi_1\rangle$ и при подаче на свой вход двух кубитов в общем состоянии $|\psi_2\rangle \otimes |s\rangle$ на выходе получить два кубита в общем состоянии $|\psi_2\rangle \otimes |\psi_2\rangle$.

Во-вторых, для любых двух ортогональных состояний $|\psi_1\rangle$ и $|\psi_2\rangle$ **существует** физический прибор (инструмент), позволяющий осуществить клонирование кубита в неизвестном состоянии $|\psi\rangle \in \{|\psi_1\rangle, |\psi_2\rangle\}$. При этом, если состояния $|\psi_1\rangle$ и $|\psi_2\rangle$ известны, то **можно построить** квантовый логический элемент, позволяющий клонировать квантовую информацию, представленную кубитами, состояние каждого из которых неизвестно, но принадлежит множеству $\{|\psi_1\rangle, |\psi_2\rangle\}$.

В-третьих, свойство, установленное в теореме о *невозможности клонирования*, представляет собой одно из главных различий между квантовой и классической информацией [52]. Оно является новым квантовым ресурсом, эффективно применяемым, например, в квантовой криптографии при построении квантовых криптографических систем генерации и распределения ключей (квантовые криптографические протоколы BB84 [69], B92 [70] и др. [39; 50]).

В заключение данного параграфа приведем формулировку и доказательство теоремы о *невозможности клонирования* [74; 90].

Теорема 1.4.7. Пусть $|\psi\rangle$ и $|\varphi\rangle$ – произвольные состояния произвольной квантовой системы K, такие, что их скалярное произведение $\langle\psi|\varphi\rangle$ удовлетворяет условиям

$$\langle\psi|\varphi\rangle \neq 0,\ \langle\psi|\varphi\rangle \neq 1 \tag{1.4.8}$$

(то есть состояния $|\psi\rangle$ и $|\varphi\rangle$ не ортогональны и не совпадают).

Тогда для любого состояния $|s\rangle$ квантовой системы K не существует унитарной матрицы U, такой, что одновременно справедливы равенства

$$U\left(|\psi\rangle\otimes|s\rangle\right) = |\psi\rangle\otimes|\psi\rangle \tag{1.4.9}$$

и

$$U\left(|\varphi\rangle\otimes|s\rangle\right) = |\varphi\rangle\otimes|\varphi\rangle. \tag{1.4.10}$$

Доказательство. Докажем методом от противного. Допустим, что существует унитарная матрица U, такая, что одновременно справедливы равенства (1.4.9) и (1.4.10). Отсюда следует, что должны быть равны скалярное произведение левых частей равенств (1.4.9) и (1.4.10) и скалярное произведение правых частей равенств (1.4.9) и (1.4.10), то есть должно быть справедливо равенство

$$\left\langle U\left(|\psi\rangle\otimes|s\rangle\right) \middle| U\left(|\varphi\rangle\otimes|s\rangle\right)\right\rangle = \left\langle\left(|\psi\rangle\otimes|\psi\rangle\right) \middle| \left(|\varphi\rangle\otimes|\varphi\rangle\right)\right\rangle. \tag{1.4.11}$$

Для скалярного произведения левых частей равенств (1.4.9) и (1.4.10) в силу унитарности матрицы U и свойств тензорного произведения справедлива следующая цепочка равенств

$$\begin{gathered}\Big\langle U\big(|\psi\rangle\otimes|s\rangle\big)\Big|U\big(|\varphi\rangle\otimes|s\rangle\big)\Big\rangle=\Big\langle U^{*}U\big(|\psi\rangle\otimes|s\rangle\big)\Big|\big(|\varphi\rangle\otimes|s\rangle\big)\Big\rangle=\\=\Big\langle\big(|\psi\rangle\otimes|s\rangle\big)\Big|\big(|\varphi\rangle\otimes|s\rangle\big)\Big\rangle=\langle\psi|\varphi\rangle\cdot\langle s|s\rangle=\langle\psi|\varphi\rangle.\end{gathered}\tag{1.4.12}$$

Аналогично, для скалярного произведения правых частей равенств (1.4.9) и (1.4.10) из свойств тензорного произведения следует справедливость следующей цепочки равенств

$$\Big\langle\big(|\psi\rangle\otimes|\psi\rangle\big)\Big|\big(|\varphi\rangle\otimes|\varphi\rangle\big)\Big\rangle=\langle\psi|\varphi\rangle\cdot\langle\psi|\varphi\rangle=\langle\psi|\varphi\rangle^{2}.\tag{1.4.13}$$

Из равенств (1.4.11), (1.4.12) и (1.4.13) следует справедливость равенства

$$\langle\psi|\varphi\rangle=\langle\psi|\varphi\rangle^{2}.\tag{1.4.14}$$

Равенство (1.4.14) справедливо при $\langle\psi|\varphi\rangle=0$, что противоречит первому из условий (1.4.8), и при $\langle\psi|\varphi\rangle=1$, что противоречит второму из условий (1.4.8). Следовательно, допущение о существовании унитарной матрицы U, такой, что одновременно справедливы равенства (1.4.9) и (1.4.10), является неверным допущением. Теорема полностью доказана.

§ 1.5. Физическая реализация кубита

В этом параграфе обратим еще раз внимание на очень важное понятие квантовой информатики (раздела квантовой теории) – кубит (quantum bit = qubit). На этот раз нас будут интересовать вопросы физического воплощения кубитов в квантовых системах.

Выше в § 1.1 было отмечено, что кубит – это фундаментальное понятие в области квантовых вычислений и квантовой информации, имеющее смысл единицы квантовой информации. Таким образом, под кубитом понимается математический объект с некоторыми заданными свойствами. Однако кубиты, подобно битам, реализуются как физические системы. Существует достаточно много исследований, посвященных проблеме осуществления перехода от абстрактного математического представления к реальным системам. Соответствующие обзоры и описания конкретных примеров физической реализации кубитов можно найти, например, в работах [19; 21; 24; 29; 32; 39; 47; 50; 52; 53; 78; 79; 82] и др. Установлено, что для реализации кубита можно использовать различные физические системы. Но общее в них то, что все они имеют два независимых состояния. То есть кубит реализуется на основе **двухуровневых** квантовых систем, таких, как две разные поляризации фотона; направление ядерного спина в однородном магнитном поле; два состояния (основное и возбужденное) электрона в одиночном атоме и т.д.

Заметим, что если некоторая квантовая система имеет максимальное число n независимых состояний, то о ней говорят как об ***n*-уровневой** квантовой системе.

Естественными двухуровневыми квантовыми системами являются, например, фотоны, отдельные электроны в атомах, ядра атомов, протоны с абсолютным значением спина, равным 1/2, и др. Состояния всех этих систем описываются волновыми функциями, представляющими собой векторы состояния в двухмерном гильбертовом пространстве $\mathbb{C}^2$.

Казалось бы, возможность физического воплощения кубита и структура его состояний являются несовместимыми явлениями. Способность кубита находиться в состоянии суперпозиции $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ противоречит нашим обыденным представлениям об окружающем физическом мире. Классический бит подобен хорошо уравновешенной монете: либо орел, либо решка. Кубит, напротив, до момента измерения может находиться в целом континууме состояний между $|0\rangle$ и $|1\rangle$.

Чтобы получить конкретное представление о том, как это может существовать, полезно рассмотреть пример конкретной физической реализации кубита [50]. С этой целью рассмотрим два состояния электрона в одиночном атоме. В достаточно «огрубленной» модели электрон в атоме может существовать либо в так называемом основном, либо в возбужденном состояниях, которые обозначим $|0\rangle$ и $|1\rangle$ соответственно. Облучая атом в течение некоторого времени светом с подходящей энергией, можно перевести электрон из состояния $|0\rangle$ в состояние $|1\rangle$ и наоборот. Но более интересно то, что, сокращая время облучения, можно оставить электрон, первоначально находившийся в состоянии $|0\rangle$, на полпути между $|0\rangle$ и $|1\rangle$ в состоянии

$$|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right).$$

Это состояние является частным примером проявления одного общего принципа квантовой механики – принципа суперпозиции квантовых состояний, который формулируется следующим образом:

Если частица может находиться в нескольких квантовых состояниях, то она может находиться и в квантовом состоянии, представляющем собой линейную комбинацию (нормированную) исходных квантовых состояний [17; 30; 47].

В связи с суперпозицией квантовых состояний обратим внимание на еще одно очень существенное отличие кубита от бита, связанное с выявлением их состояний путем измерения.

Мы можем измерить бит, чтобы определить, находится ли он в состоянии 0 или 1. Например, компьютеры делают это каждый раз, когда считывают содержимое своей памяти.

Совершенно иная ситуация в случае измерения кубита в состоянии суперпозиции $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, где $\alpha, \beta \in \mathbb{C}$, $|\alpha|^2 + |\beta|^2 = 1$; $\{|0\rangle, |1\rangle\}$ – ортонормированный базис пространства $\mathbb{C}^2$. Из квантовой механики следует, что само состояние $|\psi\rangle$ кубита не наблюдаемо, то есть путем измерения невозможно определить состояние $|\psi\rangle$. Путем измерения можно получить гораздо более ограниченную информацию: при измерении кубита, находящегося в состоянии $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, мы получаем либо результат $|0\rangle$ с вероятностью $|\alpha|^2$, либо $|1\rangle$ с вероятностью $|\beta|^2$. Этот разрыв между ненаблюдаемым состоянием кубита и доступными нам наблюдениями, то есть отсутствие между ними привычного прямого соответствия, затрудняет интуитивное понимание поведения квантовых систем. Однако существует непрямое соответствие: состояния кубита можно менять тем или иным способом, в результате чего данные измерения будут существенно зависеть от различных свойств исходного состояния. Можно сказать, что в состоянии кубита ПРИРОДА прячет массу скрытой информации [50]. Но, несмотря на это, измерение кубита всегда дает только $|0\rangle$ или $|1\rangle$ с некоторой вероятностью. Например, кубит может находиться в состоянии $|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$, измерение которого дает $|0\rangle$ с вероятностью $\left|\frac{1}{\sqrt{2}}\right|^2 = 0,5$ или $|1\rangle$ с той же вероятностью $\left|\frac{1}{\sqrt{2}}\right|^2 = 0,5$.

Заметим, что состояния $|0\rangle$ и $|1\rangle$ представляют лишь один из многих возможных наборов базисных состояний кубита [52]. Другим возможным вариантом является, например, набор $|+\rangle$ и $|-\rangle$, где

$$|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \text{ и } |-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle.$$

В этом случае состояние $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ можно выразить через состояния $|+\rangle$ и $|-\rangle$:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \frac{1}{\sqrt{2}}\alpha\big(|+\rangle + |-\rangle\big) + \frac{1}{\sqrt{2}}\beta\big(|+\rangle - |-\rangle\big) =$$
$$= \frac{1}{\sqrt{2}}(\alpha + \beta)|+\rangle + \frac{1}{\sqrt{2}}(\alpha - \beta)|-\rangle.$$

При этом состояния $|+\rangle$ и $|-\rangle$ можно рассматривать так, как если бы они были состояниями вычислительного базиса, и выполнять измерения относительно этого нового базиса. Измерение относительно базиса из состояний $|+\rangle$ и $|-\rangle$ дает результат $|+\rangle$ с вероятностью $\left|\frac{1}{\sqrt{2}}(\alpha+\beta)\right|^2$ и результат $|-\rangle$ с вероятностью $\left|\frac{1}{\sqrt{2}}(\alpha-\beta)\right|^2$ соответственно. Состояниями кубита после измерения будут $|+\rangle$ и $|-\rangle$ соответственно.

Таким образом, выбор вычислительного базиса равносилен, в известном смысле, выбору устройства измерения. После проведения измерения результат на выходе устройства указывает на состояние из вычислительного базиса, соответствующего этому устройству. Непосредственно после проведения измерения сам кубит оказывается в состоянии, указанном в определенном смысле результатом измерения. Вычислительный базис и устройство измерения как бы «жестко связаны». Тогда возникает вопрос: что же в результате, который выдает измерительное устройство, определяется состоянием кубита, подвергающегося измерению? Ответ таков: состоянием кубита, подвергающегося измерению, определяется вероятность появления того или иного результата измерения и, следовательно, вероятность попадания кубита после проведения измерения в то или иное состояние вычислительного базиса, отвечающего данному устройству измерения. Для любого конкретного состояния из вычислительного базиса эта вероятность равна квадрату модуля коэффициента, с каким данное состояние вычислительного базиса входит в разложение по вычислительному базису состояния кубита, подвергающегося измерению.

Заметим, что измерение кубита в состоянии $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ меняет состояние кубита. Кубит «коллапсирует» из суперпозиции $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ в одно из состояний $|0\rangle$ или $|1\rangle$, соответствующее результату измерения. На вопрос, почему происходит такой «коллапс», квантовая механика не дает ответ. Однако такое поведение квантовых систем согласуется с соответствующим постулатом (из совокупности фундаментальных постулатов квантовой механики) о воздействии измерений на квантовые системы [20; 50; 60; 61].

Выводы по главе 1

1. Операторы плотности, редуцированные операторы плотности, разложение Шмидта и расширение до чистого состояния входят в арсенал основных инструментов исследования квантовых систем.

2. Ряд вопросов исследования смешанных состояний квантовых систем может быть сведен к вопросам исследования чистых состояний квантовых систем на основе применения математической процедуры расширения до чистого состояния.

3. Измерения, проводимые над подсистемами в составе квантовых систем, являются частными случаями измерений в целом над квантовой системой. Эти измерения определяются матрицами измерений, явно описываемыми через операторы измерений подсистем, рассматриваемых изолированно вне составной квантовой системы.

4. Квантовая цепь (схема) – это квантовое вычислительное устройство, состоящее из синхронизированных по времени квантовых логических элементов, измерительных элементов и квантовых «проводов», соединяющих выходы одних элементов с входами других.

5. Любой многокубитный квантовый логический элемент может быть составлен из **CNOT** и однокубитных квантовых логических элементов. Таким образом, набор из квантового логического элемента

CNOT и однокубитных квантовых логических элементов, а также операторов измерительных элементов, достаточен для построения любой квантовой цепи (схемы).

6. Под термином *квантовые вычисления* понимается применение последовательности унитарных операторов и операторов измерений, преобразующей начальное входное состояние в некоторое конечное выходное состояние квантовой цепи.

7. Состояние квантовой системы само по себе представляет особого рода информационный ресурс, содержащий сведения о статистике всевозможных измерений над данной квантовой системой. Для обозначения этого информационного ресурса применяется специальный термин *квантовая информация*.

8. В некоторых случаях можно клонировать квантовую информацию, а в других – нет. Это можно сделать каждый раз специальным прибором для данного конкретного известного квантового состояния (и даже для фиксированного набора ортогональных квантовых состояний). Но не существует универсального прибора, который бы размножал (клонировал) произвольное неизвестное квантовое состояние.

9. Квантовая информация имеет качественные отличия от классической информации. Наиболее ярким отличием квантовой информации от классической информации является невозможность клонирования произвольного неизвестного квантового состояния.

10. Для физической реализации единицы квантовой информации кубита можно использовать любую двухуровневую квантовую систему.

ГЛАВА 2

Состояния многокубитных квантовых систем

Введение к главе 2

Глава 2 состоит из шести параграфов.

В параграфе 2.1 осуществлено неформальное введение в теорию несепарабельных состояний квантовых систем. Рассмотрены исторические аспекты данного научного направления, указаны современные технологии физической реализации несепарабельных квантовых состояний.

Параграф 2.2. посвящен в основном исследованию состояний двухкубитных квантовых систем. Рассмотрены задачи бинарной классификации квантовых состояний. Двумя классами, на которые делятся множества квантовых состояний, являются классы сепарабельных и несепарабельных состояний. При этом предполагается, что состояния представлены в виде разложений в произвольном вычислительном базисе.

Для решения задачи бинарной классификации состояний двухкубитных квантовых систем привлекается известное в специальной литературе свойство несепарабельных квантовых состояний о неравенстве нулю разности произведений крайних (нулевого и третьего) и произведения средних (первого и второго) коэффициентов (concurrence [24]) разложения, представляющего состояние при определенном вычислительном базисе, с нумерацией каждого коэффициента числом, определяемым двоичным содержанием записи соответствующего вектора из вычислительного базиса. Это свойство формулируется в виде утверждения 2.2.8.

Приведены два доказательства утверждения 2.2.8, каждое из которых, кроме своего основного предназначения, предоставляет еще некоторые довольно эффективные средства исследования квантовых состояний.

Так, если состояние двухкубитной квантовой системы является сепарабельным состоянием, то, используя соотношения, полученные в первом доказательстве, относительно коэффициентов его разложения в вычислительном базисе, можно вычислить коэффициенты разложений сомножителей тензорного произведения, результат которого совпадает с исходным сепарабельным состоянием.

Второе доказательство иллюстрирует возможности инструментария квантовой теории и может служить наиболее доступной для понимания версией иллюстрации основных идей доказательств утверждений, получаемых в рамках решения задачи бинарной классификации состояний многокубитных квантовых систем, способствует установлению некоторого общего подхода в рамках соответствующих исследований.

Исследованию вопроса разложимости в тензорные произведения применительно к состояниям трехкубитных квантовых систем посвящен параграф 2.3.

В начале параграфа на примере трехкубитных состояний иллюстрируется наличие определенной ограниченности возможности представления состояний многокубитных квантовых систем в виде тензорных произведений состояний меньшей размерности.

Далее в виде утверждения 2.3.4 формулируется критерий разложимости трехкубитного состояния в тензорное произведение состояний меньшей размерности. Утверждение 2.3.4 состоит из двух пунктов: (а) и (б).

В первом пункте (а) утверждения 2.3.4 трехкубитная квантовая система ABC рассматривается как двухсоставная квантовая система в составе однокубитной подсистемы A и двухкубитной подсистемы BC. Указаны необходимые и достаточные условия, которым должны удовлетворять амплитуды состояния квантовой системы ABC, при выполнении которых данное состояние представимо в виде тензорного произведения состояний подсистемы A и подсистемы BC.

Во втором пункте (б) утверждения 2.3.4 трехкубитная квантовая система ABC рассматривается как двухсоставная квантовая система в составе двухкубитной подсистемы AB и однокубитной подсистемы C.

Указаны необходимые и достаточные условия, которым должны удовлетворять амплитуды состояния квантовой системы ABC, при выполнении которых данное состояние представимо в виде тензорного произведения состояний подсистемы AB и подсистемы C.

Путем отрицания условий, представленных в пунктах (а) и (б) утверждения 2.3.4, формулируется следствие 2.3.5, в котором также в виде двух пунктов (а) и (б) изложены необходимые и достаточные условия невозможности представления состояния трехкубитной квантовой системы ABC в виде тензорного произведения подсистем A и BC (пункт (а)) или AB и C (пункт (б)).

Однако утверждение 2.3.4 и следствие 2.3.5 не дают возможности для полного решения задачи бинарной классификации состояний трехкубитных квантовых систем на сепарабельные и несепарабельные в смысле известных определений этих понятий [56; 59] в силу определенной ограниченности представления состояний квантовых систем векторами конечномерных гильбертовых пространств над полем комплексных чисел и их тензорных произведений, на которую было обращено внимание в начале параграфа 2.3.

Параграф 2.3 завершается доказательством утверждения 2.3.4.

Доказательство обоих пунктов утверждения 2.3.4 осуществляется по одинаковой схеме с применением инструментов квантовой теории. А именно, вычисляется матрица плотности состояния трехкубитной квантовой системы. На основе этой матрицы вычисляется редуцированная матрица плотности состояния «меньшей», то есть однокубитной, квантовой подсистемы. Показывается, что чистое состояние однокубитной подсистемы влечет сепарабельность состояния исходной трехкубитной квантовой системы. Далее выписываются условия, при которых редуцированная матрица плотности является матрицей плотности квантовой системы, находящейся в чистом состоянии.

Затруднения, возникающие при исследовании состояний многокубитной квантовой системы в связи с определенными ограничениями возможности их представления в виде тензорных произведений состояний меньшей размерности для всех возможных конфигураций связи между составными компонентами системы, можно преодолеть путем введения новых понятий сепарабельности и несепарабельности по отношению к состояниям многокубитных систем. Этому посвящен параграф 2.4. Показано, что для двухкубитных систем введенные понятия совпадают с ранее известными [56; 59].

Всюду далее в данной работе начиная с параграфа 2.5 понятия, где используются слова *сепарабельность* и *несепарабельность*, по смыслу совпадают с понятиями, введенными в параграфе 2.4 через определения 2.4.4, 2.4.8 – 2.4.12.

В параграфе 2.5 сформулированы утверждение 2.5.21 и следствия из него. Пункт (б) следствия 2.5.27 представляет собой несложный для практических применений **критерий $\mathbf{K_3}$** несепарабельности состояний трехкубитных квантовых систем, где **К** – первая буква имени **Константин**, а индекс **3** связан с числом кубитов в трехкубитной квантовой системе. Разобран пример 2.5.28, иллюстрирующий полученные результаты. В завершение параграфа приводится доказательство основного в этом параграфе утверждения 2.5.21.

В параграфе 2.6 для четырехкубитных квантовых систем приводятся результаты, аналогичные результатам из параграфа 2.5 для состояний трехкубитных квантовых систем. Сформулированы утверждения 2.6.3 и 2.6.4. Утверждение 2.6.3 представляет собой критерий неразложимости состояния четырехкубитной квантовой системы в тензорное произведение состояний меньшей размерности. А утверждение 2.6.4 представляет собой **критерий $\mathbf{K_4}$** несепарабельности состояний четырехкубитных квантовых систем.

§ 2.1. Несепарабельные состояния квантовых систем

Несепарабельные состояния (по-другому, запутанные состояния) квантовых систем и их свойства представляют большой научный и практический интерес. Они относятся к ряду основных объектов и ресурсов современных квантовых технологий хранения, обработки и передачи информации, не имеющих классических аналогов. Теория несепарабельных состояний квантовых систем является бурно развивающейся составной частью квантовой механики. Понятийный аппарат и методы исследования этого научного направления являются новыми, можно сказать, что они, в определенном смысле, находятся на переднем крае современной физики. Теоретические и экспериментальные достижения в области исследования несепарабельных состояний квантовых систем являются основой предполагаемых в ближайшем будущем крупных инновационных достижений в области компьютерных и информационных технологий.

В качестве синонима для термина **несепарабельность** в квантовой теории информации используются также термины: **запутанность**, **перепутанность**, **сцепленность** [24; 50; 52; 59].

Несмотря на то, что в данной работе нас будут интересовать решения чисто прикладных задач связи на основе применения результатов теории несепарабельных состояний квантовых систем, представляется полезным предварительное ознакомление с историей возникновения, становления и современным содержанием теории несепарабельных состояний квантовых систем, не претендуя при этом на исчерпывающий охват всей информации в этой области. Это само по себе не только захватывающе интересно, но и необходимо с позиции облегчения понимания дальнейшей части данной работы.

Сразу после возникновения квантовой механики было обнаружено, что она содержит новые, противоречащие привычной интуиции черты. Попытки их описания, толкования и объяснения повлекли за собой споры и дискуссии ученых-физиков. Вследствие этого был сформулирован ряд так называемых концептуальных проблем [29; 33; 47], от разрешения которых зависело дальнейшее существование и направление развития самой квантовой механики как науки. Среди них, прежде всего, укажем на проблему полноты описания мира квантовой механикой [29; 33; 47]. При попытках разрешения этой проблемы в свое время физики XX века столкнулись с таким явлением, как несепарабельные (запутанные) состояния (entangled states) квантовой системы, характеризующимся наличием нелокальных корреляций частиц, составляющих квантовую систему.

Несепарабельные квантовые состояния не имеют аналога в классической физике. Но в то же самое время установлено [33; 34; 47; 66; 67; 71; 73; 78; 79; 82; 83; 88], что они – не теоретическая абстракция, которую ввели физики-теоретики, а объективный факт окружающей действительности. Это то, что существует в природе независимо от наших представлений. Напомним (см. введение) описание этого явления природы.

В соответствии с положениями квантовой физики вполне возможно и даже обычно для двух или более разделенных пространством объектов образовывать в действительности единое целое в том смысле, что если мы потревожим один из этих объектов, то среагируют <u>все</u>. Это и называется несепарабельностью. Состояние такой единой целой квантовой системы называется несепарабельным состоянием, а сама квантовая система называется несепарабельной квантовой системой.

Здесь выражение «разделенных пространством» по отношению к объектам, составляющим квантовую систему, понимается прежде всего как **отсутствие между ними любого вида классической коммуникации**.

Первые попытки исследования свойств несепарабельных состояний были предприняты Альбертом Эйнштейном [76] и Эрвином Шредингером [88] еще в 30-х годах XX века. Это было время, когда квантовая теория находилась в стадии становления и, как было указано выше, необычные свойства ее новых объектов являлись поводом для сомнений в адекватности описания мира квантовой механикой. Следствием чего и является концептуальная проблема квантовой механики – проблема полноты описания мира квантовой механикой [47].

В частности, знаменитая статья Эйнштейна, Подольского и Розена [76] имела своей целью доказать на примере несепарабельных квантовых состояний неполноту описания мира квантовой механикой, то есть отрицательное решение соответствующей концептуальной проблемы квантовой механики. С тех пор впервые рассмотренная в работе [76] квантовая система из двух частиц, находящаяся в несепарабельном квантовом состоянии, называется ЭПР-парой в честь тех людей, которые первыми указали на странные свойства таких систем – Эйнштейна, Подольского и Розена.

Эйнштейну казалась противоестественной возможность существования мгновенного действия на расстоянии. Он исходил из привычных представлений, и ему казалось правильным считать, что если квантовая система состоит из двух пространственно разделенных подсистем A и B, то при полном описании физической реальности действия, выполненные над подсистемой A, не должны изменять свойства подсистемы B. Этот принцип принято в физике называть *принципом локальности Эйнштейна* [47].

Своим примером с ЭПР-парой Эйнштейн пытался доказать, что квантовая механика «ущербна», что она не способна полностью и однозначно описать реальный мир в принципе. Отсюда возникло предположение о скрытых локальных параметрах (якобы реально существующих, но пока еще не выявленных), которые могут помочь вернуться к привычному, локальному описанию объектов и, в частности, объяснить странное поведение ЭПР-пары [47].

Однако конечный результат исследования проблемы полноты описания мира квантовой механикой оказался противоположным тому, что пытался доказать Эйнштейн [76]. В итоге оказалось, что правильным является именно квантовомеханический подход при описании реального мира [47].

Первый шаг к такому выводу сделал Белл в 1964 году [68]. В настоящее время имеются разные и иногда противоположные оценки и интерпретации достижений Белла: [24; 29; 34; 36; 47; 50; 52; 60] и др. До сих пор не иссякает поток публикаций. В нашей работе по отношению к этому вопросу мы придерживаемся классического учебного пособия для вузов по атомной физике [47].

Белл [68] уточнил и формализовал «объективную локальную теорию», которой придерживались Эйнштейн и его сторонники. Основные положения этой теории в формулировке Белла выглядят следующим образом [47; 68]:

- физические системы существуют сами по себе, они объективны и не зависят от измерения;
- измерение одной системы не влияет на результат измерения другой системы;
- поведение системы зависит лишь от условий в более ранние моменты времени.

Далее Белл сформулировал и доказал теорему [68], откуда следует, что «объективная локальная теория» и квантовая механика дают разные несовпадающие предсказания для результатов измерений коэффициента корреляции в ЭПР-паре. Это был ошеломляющий теоретический результат, полученный в буквальном смысле «на кончике пера», но, несомненно, логически истинный. Он произвел эффект разорвавшейся бомбы в науке спустя почти 30 лет после начала споров о полноте описания квантовой механикой реального мира. Разные численные значения коэффициента корреляции в ЭПР-паре, представленные в теореме Белла на основе «объективной локальной теории» и на основе квантовой механики, больше не оставляли ни малейшей возможности параллельному существованию этих двух научных направлений. Одно из них, чье предсказание коэффициента корреляции в ЭПР-паре согласуется с экспериментальными результатами, должно было быть принято, а другое, не прошедшее экспериментального теста, – отвергнуто. Поэтому вопрос, что же верно – «объективная локальная теория» или квантовая механика, – перешедший после теоремы Белла в экспериментальную плоскость, еще более остро начал привлекать внимание ученых-физиков.

Ответ на этот вопрос можно было получить только путем проведения конкретных экспериментальных измерений коэффициента корреляции в ЭПР-парах и сравнительного анализа результатов экспериментов с теми значениями, которые были предсказаны теоремой Белла.

Необходимые эксперименты впервые были проведены Аленом Аспе (AlainAspect) в 80-х годах XX века [66; 67], примерно через полвека после публикации известной статьи Эйнштейна, Подольского и Розена [76].

Эксперименты Аспе и ряд других изящных экспериментов с использованием фотонов (т. е. частиц света) [47] убедительно показали истинность значения корреляции в ЭПР-паре, предсказанного квантовой механикой. То есть экспериментально было установлено, что наш реальный мир является в своей основе квантовым, описывается законами квантовой механики. И все предположения «объективной локальной теории», приведенные выше, в общем случае несправедливы.

Здесь уместна ссылка на мнение известного швейцарского физика и специалиста в области квантовых технологий Николя Жизана [33] о том, что физика почти всегда давала нелокальное описание мироздания. Человечество существовало с ньютоновской нелокальностью (*закон всемирного тяготения Ньютона, в соответствии с которым гравитационное взаимодействие осуществляется нелокально, то есть мгновенно между двумя пространственно удаленными телами*) вплоть до 1915 года (*до времени появления общей теории относительности Эйнштейна, в соответствии с которой взаимодействие распространяется в пространстве локально, то есть непрерывно от точки к точке с ограниченной скоростью*) – и с квантовой нелокальностью начиная с 1927 года. Следовательно, делает заключение Жизан, «**физика всегда была нелокальной, за исключением этого небольшого отрезка в 12 лет**».

Таким образом, Эйнштейн и его сторонники спустя многие годы после начала инициированных ими научных диспутов по поводу полноты квантового описания реального мира окончательно проиграли, что само по себе не так важно с общецивилизационных позиций.

Для человеческой цивилизации на данном этапе ее развития чрезвычайно важно другое – уяснение научной истины: несомненности полноты описания реального мира квантовой механикой. Сегодня квантовая механика «утвердилась в самом центре современной физики» [33]. Возможно, пройдут годы и будут другие мнения, основанные на новых теориях описания мироздания. Но это неопределенное будущее, и когда оно станет реальностью? Невозможно сейчас ответить на этот вопрос. Положительно хотя бы то, что человечество в настоящем обладает достаточно точным инструментальным и аналитическим аппаратом квантовой механики, позволяющим ему делать успешные шаги на путях прогрессивного научно-технического развития. Хотелось бы надеяться, что в дальнейшей перспективе положение дел в этой сфере будет только улучшаться.

Что же касается Эйнштейна, то, наверное, он не был бы сильно огорчен опровержением его точки зрения на квантовую механику, так как, будучи великим ученым, он на первое место в науке ставил необходимость достижения истины. Кроме того, для нас Эйнштейн попрежнему остается гением науки. Его заслуги перед человечеством безмерно велики в силу того, что он, помимо многих разнообразных блестящих научных достижений, является автором теории относительности, являющейся составной частью современной физики и не теряющей своей научной содержательности и в наше время.

Гениальность Эйнштейна сказалась и на его заблуждениях. Заблуждения гения – также гениальны. Они сыграли гигантскую положительную роль в развитии науки. Благодаря его спорам по вопросам квантовой механики, наука в общем и квантовая механика в частности получили сильный импульс развития и в теоретических, и в прикладных направлениях. Одним из результатов данного развития является и описываемое ниже крупное достижение, позволяющее надеяться на существенные технологические прорывы в ближайшем будущем, появление значимых инноваций.

В процессе разрешения проблемы полноты описания мира квантовой механикой, что само по себе является выдающимся теоретическим результатом в общенаучном смысле, произошло и нечто другое, не менее грандиозное для практических приложений в различных направлениях информационных технологий, что фундаментальным образом изменило отношение научного сообщества к явлению квантовых запутанных состояний. Это нечто представляет собой осознание того, что несепарабельность (запутанность) состояний квантовых систем – это новый, не имеющий классических аналогов, реализуемый на практике (экспериментально) физический ресурс. Такое осознание произошло в 80-х – 90-х годах XX века. С этого времени акценты как экспериментаторов, так и теоретиков сместились в сторону прикладных исследований и технического применения несепарабельных квантовых состояний. Большие усилия были направлены на то, чтобы понять роль несепарабельных состояний в природе, найти возможность их практического применения в качестве принципиально нового нелокального ресурса в технических устройствах в области создания квантовых криптографических систем и квантовых компьютеров [19; 21; 24; 33; 36; 39; 50; 51; 52; 59; 69; 70].

Говоря о современных результатах исследования свойств несепарабельных квантовых состояний, коснемся также и темы технической реализации, имеющей первостепенное значение для практических применений.

Традиционными источниками запутанных квантовых состояний являются процессы каскадного распада атомных возбуждений и спонтанного параметрического рассеяния света в нелинейных кристаллах [19; 21; 39; 40; 41; 47; 53; 63]. С помощью этих процессов в лабораторных и промышленных условиях создают фотонные пары с несепарабельными состояниями поляризации, которыми затем управляют при помощи зеркал и поляризаторов. Однако подобные источники несепарабельных состояний обладают рядом недостатков.

С одной стороны, процессы распада высокочастотного фотона на фотонную пару и релаксационного распада атомных возбуждений являются случайными, так как они обусловлены квантовыми флуктуациями в рассматриваемой среде [40; 41; 53; 63].

С другой стороны, созданные фотонные пары распространяются со скоростью света, так что их трудно локализовать и сохранить для последующего использования [39; 41; 53; 63].

Именно эти причины и привели к необходимости уделить внимание в плане практических реализаций несепарабельных квантовых состояний еще и разработке и применению *детерминистских* (в противоположность случайным) методов создания несепарабельных квантовых состояний *массивных* частиц (в противоположность фотонам) – прежде всего отдельных атомов и ионов, захваченных в ловушках соответствующих типов [23; 24; 63]. Здесь под детерминизмом понимается возможность создавать нужное несепарабельное квантовое состояние данных частиц в любой заданный момент времени и сохранять это состояние длительно, то есть в течение временных отрезков, обусловленных потребностями конкретных практических приложений.

Было уяснено, что два указанных вида «носителей» несепарабельных квантовых состояний – фотоны и атомы (или ионы) – в принципе дополняют друг друга [23; 24; 39; 50; 63]. Аргументируется это следующим образом. Если удастся создать надежные устройства для генерации и манипулирования несепарабельными квантовыми состояниями массивных частиц (атомов или ионов), а также управления взаимодействием этих массивных частиц со светом (фотонами), то в результате появится идеальная практическая база для всех необходимых технических решений. При этом атомы (или их составные частицы типа электронов, ядер и протонов) предоставят возможность долговременного хранения специфической квантовой информации, а фотоны обеспечат ее считывание с атомов, а также возможность ее передачи практически на любые расстояния.

В настоящее время уже выполнен целый ряд практических работ, которые подтвердили возможности искусственного создания и сохранения несепарабельных квантовых состояний в формах, пригодных для технического воплощения [24; 39; 50; 63; 78; 79; 82]. Перечислим основные технологические направления, используемые в этих работах:

- технологии, основанные на использовании оптических фотонов в качестве носителей несепарабельных квантовых состояний;
- различного рода технические методы квантовой электродинамики резонаторов;

- технологии, основанные на использовании ионов в ловушках;
- технологии, основанные на использовании нейтральных атомов в ловушках;
- технологии и технические методы ядерного магнитного резонанса;
- технологии, основанные на использовании носителей зарядов в сверхпроводниках;
- технологии, основанные на использовании квантовых точек, изготовленных из полупроводников;
- технологии, основанные на использовании дефектов в полупроводниках, и др.

Выполненные исследования показали, в частности, что большая часть трудностей, с которыми сталкиваются экспериментаторы при технических реализациях «долгоживущих» несепарабельных квантовых состояний, связана с необходимостью технического решения задачи исключения декогеренции [21]. Здесь под *декогеренцией* понимается физический процесс, при котором происходит потеря когерентности квантового состояния, то есть в результате декогеренции квантовое состояние перестает быть чистым. Уменьшается или полностью исчезает квантовая несепарабельность между составными частями квантовой системы в результате ее взаимодействия с окружением.

Использование выражения «уменьшается квантовая несепарабельность (запутанность)» является корректным и не должно вызывать удивление. Ведь несепарабельность (запутанность) квантовых состояний – это физический ресурс, хотя и принципиально нового типа. Несмотря на свою новизну, этот ресурс, как и любой другой физический ресурс (например, масса, энергия, скорость и т.д.), предполагает свое количественное описание путем использования подходящей меры. В качестве такой меры можно взять, например, меру несепарабельности для двухкубитных квантовых систем в чистом состоянии, предложенную в работе [72]. Эта мера определяется через энтропию фон Неймана [50; 52], и численные значения количества несепарабельности могут меняться от 0 до 1 по непрерывной шкале. При этом значение 0 характеризует полную независимость состояний подсистем квантовой системы, минимальную несепарабельность, то есть отсутствие несепарабельности (нелокальной связи); а значение 1 характеризует максимальную несепарабельность состояний подсистем квантовой системы [72]. Более широкие возможности представляет другая мера несепарабельности под названием **согласованность**, дающая более общую количественную характеристику запутанности двухсоставной квантовой системы (не обязательно двухкубитной). Она предложена в работе [86].

Возвращаясь к обсуждению задачи исключения декогеренции, можно отметить следующее. Эта задача решается путем улучшения изолированности квантовой системы от окружающей среды, то есть: чем лучше изолирована квантовая система, находящаяся в запутанном квантовом состоянии, тем меньше она подвержена декогеренции. К счастью, исключение декогеренции относится к числу тех задач, для которых продолжающееся совершенствование в искусстве проведения физических экспериментов способно произвести существенные изменения в сторону улучшения ситуации.

В плане решения задачи обеспечения «длительности жизни» несепарабельных квантовых состояний наилучшим обнадеживающим ориентиром является следующий теоретический результат: теоретические расчеты «времени жизни» несепарабельных квантовых состояний, реализованных с использованием спинов ядер атомов некоторых химических элементов, дают результат – около 3 000 000 лет [50].

§ 2.2. Состояния двухкубитных квантовых систем

Приведем известные определения понятий *сепарабельное* (незапутанное) состояние и *несепарабельное* (запутанное) состояние для двухкубитных квантовых систем [56; 59].

Определение 2.2.1. Пусть вектор $|\psi\rangle \in \mathbb{C}^4 = \mathbb{C}^2 \otimes \mathbb{C}^2$ является состоянием двухкубитной квантовой системы AB, состоящей из кубитов A и B. Состояние $|\psi\rangle$ называется **сепарабельным состоянием** (**незапутанным состоянием**) двухкубитной квантовой системы AB, если существуют состояние $|\psi_1\rangle \in \mathbb{C}^2$ кубита A и состояние $|\psi_2\rangle \in \mathbb{C}^2$ кубита B, такие, что справедливо равенство

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle.$$

Состояние $|\psi\rangle \in \mathbb{C}^4$ двухкубитной квантовой системы AB называется **несепарабельным состоянием** (**запутанным состоянием**), если оно не является сепарабельным состоянием.

Напомним, что в качестве синонима для термина **несепарабельность** в квантовой теории информации используются также термины: **запутанность**, **перепутанность**, **сцепленность**.

Определение 2.2.2. Состояниями Белла, или **ЭПР-состояниями** (состояниями Эйнштейна – Подольского – Розена), или состояниями **ЭПР-пары** называются состояния $|\psi_{00}\rangle$, $|\psi_{01}\rangle$, $|\psi_{10}\rangle$, $|\psi_{11}\rangle \in \mathbb{C}^4$, где

$$|\psi_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}; \quad |\psi_{01}\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}};$$

$$|\psi_{10}\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}}; \quad |\psi_{11}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}. \qquad (2.2.3)$$

Утверждение 2.2.4. Состояния Белла являются несепарабельными состояниями.

Доказательство данного утверждения можно найти, например, в работе [50]. Кроме того, можно отметить, что оно является следствием нижеприведенного утверждения 2.2.8.

Более сложные несепарабельные состояния могут образовываться как суперпозиции многокубитных состояний. Они будут подробно рассмотрены позже. Здесь же укажем, что примером такого несепарабельного состояния служит известное состояние Гринбергера – Хорна – Цайлингера (называемое ГХЦ-состоянием) [19; 24; 29; 36; 52]. Это состояние квантовой системы из трех кубитов принадлежит гильбертову пространству $\mathbb{C}^8$ и определяется равенством:

$$\left|\psi_{\mathrm{GHZ}}\right\rangle = \frac{|000\rangle + |111\rangle}{\sqrt{2}}. \qquad (2.2.5)$$

Другим трехкубитным несепарабельным состоянием является W-состояние [75]

$$\left|\psi_{\mathrm{W}}\right\rangle = \frac{|001\rangle + |010\rangle + |100\rangle}{\sqrt{3}}. \qquad (2.2.6)$$

Существуют и другие многокубитные несепарабельные состояния [19; 21; 50; 75].

Принципиально важным является вопрос о возможности эффективного выявления несепарабельных состояний.

Для случая двухкубитных состояний ответ на поставленный вопрос является довольно простым и может быть сформулирован в виде утверждения, приведенного в работе [24] без доказательства. Сформулируем и, для полноты картины, докажем это утверждение. При этом представим два разных доказательства этого утверждения, каждое из которых, кроме своего основного функционального назначения, несет еще дополнительную нагрузку по представлению возможностей решения некоторых смежных задач. В русле этого, в частности, имеет место следующее.

Первое доказательство является, грубо говоря, «лобовым», без привлечения инструментов квантовой теории. Несомненным достоинством данного доказательства является то, что если рассматриваемое состояние двухкубитной квантовой системы является сепарабельным состоянием, то можно, используя нижеприведенные соотношения (2.2.12), (2.2.13), (2.2.14) и (2.2.15), полученные по ходу первого доказательства, выписать сомножители тензорного произведения, представляющего данное двухкубитное состояние.

Второе доказательство существенным образом использует аналитические инструменты квантовой теории, такие, как матрица плотности и редуцированная матрица плотности. Это обстоятельство иллюстрирует возможность существования некоторого общего подхода к решению задачи выявления несепарабельных квантовых состояний, что достаточно убедительно подтверждается ниже в § 2.3, при рассмотрении трехкубитных квантовых систем.

Кроме этого, прежде чем сформулировать утверждение, заметим, что в вычислительном базисе из векторов $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$ произвольное двухкубитное состояние $|\psi\rangle$ можно представить в следующем общем виде:

$$|\psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle, \tag{2.2.7}$$

где $a, b, c, d \in \mathbb{C}$, $|a|^2 + |b|^2 + |c|^2 + |d|^2 = 1$.

А теперь сформулируем и само утверждение.

Утверждение 2.2.8. Двухкубитное состояние $|\psi\rangle$, представленное равенством (2.2.7), является несепарабельным состоянием тогда и только тогда, когда выполняется неравенство $ad - bc \neq 0$.

Первое доказательство. Данное утверждение равносильно утверждению о том, что состояние $|\psi\rangle$ является сепарабельным состоянием тогда и только тогда, когда выполняется равенство $ad - bc = 0$. Поэтому достаточно доказать последнее утверждение.

Пусть $|\psi\rangle$ является сепарабельным состоянием. Тогда из определения 2.2.1 следует, что

$$|\psi\rangle = \left(\alpha|0\rangle + \beta|1\rangle\right) \otimes \left(\gamma|0\rangle + \tau|1\rangle\right) \tag{2.2.9}$$

для некоторых $\alpha, \beta, \gamma, \tau \in \mathbb{C}$, таких, что

$$|\alpha|^2 + |\beta|^2 = 1, \quad |\gamma|^2 + |\tau|^2 = 1.$$

Раскрыв скобки в правой части равенства (2.2.9), имеем

$$|\psi\rangle = \alpha\gamma|00\rangle + \alpha\tau|01\rangle + \beta\gamma|10\rangle + \beta\tau|11\rangle. \tag{2.2.10}$$

В силу однозначности разложения вектора по базису линейного векторного пространства [27; 43; 45; 46], из равенств (2.2.7) и (2.2.10) вытекает справедливость следующих равенств:

$$a = \alpha\gamma,\ b = \alpha\tau,\ c = \beta\gamma,\ d = \beta\tau. \qquad (2.2.11)$$

Отсюда, в силу свойства коммутативности произведения комплексных чисел, имеем

$$ad = \alpha\gamma\beta\tau = \alpha\tau\beta\gamma = bc.$$

Теперь проведем доказательство в обратную сторону. Пусть $ad = bc$. Из равенства $|a|^2 + |b|^2 + |c|^2 + |d|^2 = 1$ следует, что хотя бы одно число из комплексных чисел a, b, c и d не равно нулю. Рассмотрим все возможные случаи.

Если $a \neq 0$, то равенство $ad = bc$ равносильно равенству $d = bc/a$ и, положив

$$m = \sqrt{|a|^2 + |c|^2},\ \alpha = a/m,\ \beta = c/m,\ \gamma = m,\ \tau = bm/a, \qquad (2.2.12)$$

получаем для состояния $|\psi\rangle$ представление (2.2.9). Действительно, имеет место цепочка равенств

$$\left(\alpha|0\rangle + \beta|1\rangle\right) \otimes \left(\gamma|0\rangle + \tau|1\rangle\right) = \left(\frac{a}{m}|0\rangle + \frac{c}{m}|1\rangle\right) \otimes \left(m|0\rangle + \frac{bm}{a}|1\rangle\right) =$$

$$= a|00\rangle + b|01\rangle + c|10\rangle + \frac{bc}{a}|11\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle = |\psi\rangle.$$

Кроме этого выполняются также и соотношения для α, β, γ, τ из (2.2.9):

$$|\alpha|^2 + |\beta|^2 = \frac{|a|^2}{m^2} + \frac{|c|^2}{m^2} = \frac{|a|^2 + |c|^2}{m^2} = \frac{|a|^2 + |c|^2}{|a|^2 + |c|^2} = 1,$$

$$|\gamma|^2 + |\tau|^2 = m^2 + \left|\frac{bm}{a}\right|^2 = m^2 + \frac{|b|^2}{|a|^2}m^2 = \left(|a|^2 + |c|^2\right) + \frac{|b|^2}{|a|^2}\left(|a|^2 + |c|^2\right) =$$

$$= |a|^2 + |c|^2 + |b|^2 + \frac{|b|^2|c|^2}{|a|^2} = |a|^2 + |c|^2 + |b|^2 + |d|^2 = 1.$$

Аналогично, с точностью до равенств для $m,\ \alpha,\ \beta,\ \gamma,\ \tau$, все повторяется и в остальных случаях. Для полноты доказательства выпишем соответствующие равенства для $m,\ \alpha,\ \beta,\ \gamma,\ \tau$.

Если $b \neq 0$, то $c = ad/b$ и, положив

$$m = \sqrt{|b|^2 + |d|^2}\,,\ \alpha = b/m\,,\ \beta = d/m\,,\ \gamma = am/b\,,\ \tau = m\,, \qquad (2.2.13)$$

получаем для состояния $|\psi\rangle$ представление (2.2.9).

Если $c \neq 0$, то $b = ad/c$ и, положив

$$m = \sqrt{|c|^2 + |d|^2}\,,\ \alpha = am/c\,,\ \beta = m\,,\ \gamma = c/m\,,\ \tau = d/m\,, \qquad (2.2.14)$$

получаем для состояния $|\psi\rangle$ представление (2.2.9).

Если $d \neq 0$, то $a = bc/d$ и, положив

$$m = \sqrt{|c|^2 + |d|^2}\,,\ \alpha = bm/d\,,\ \beta = m\,,\ \gamma = c/m\,,\ \tau = d/m\,, \qquad (2.2.15)$$

получаем для состояния $|\psi\rangle$ представление (2.2.9).

Если более одного числа из комплексных чисел a, b, c и d не равны нулю, то такая ситуация исчерпывается хотя бы одним из вышерассмотренных случаев. Поэтому и здесь получаем для состояния $|\psi\rangle$ представление (2.2.9).

Таким образом, если выполняется равенство $ad = bc$, то для состояния $|\psi\rangle$ имеем представление (2.2.9), то есть $|\psi\rangle$ – сепарабельное состояние. Первое доказательство утверждения 2.2.8 завершено.

Второе доказательство. Так же, как и в первом доказательстве, ограничимся доказательством следующего утверждения: состояние $|\psi\rangle$ является сепарабельным состоянием тогда и только тогда, когда выполняется равенство $ad - bc = 0$.

Пусть $|\psi\rangle$ является сепарабельным состоянием квантовой системы AB. Это условие равносильно тому, что существуют чистые состояния

$|\psi_1\rangle$ и $|\psi_2\rangle$ соответственно подсистем A и B квантовой системы AB, такие, что

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle.$$

Отсюда в соответствии с [50] следует, что редуцированная матрица плотности $\rho_{\mathrm{A}}^{(\mathrm{AB})}$ подсистемы A совпадает с матрицей плотности $\rho^{(\mathrm{A})}$ подсистемы A и при этом выполняется равенство

$$\mathrm{tr}\left(\left(\rho^{(\mathrm{A})}\right)^2\right) = 1. \tag{2.2.16}$$

Вычислим матрицу $\rho^{(\mathrm{A})}$ путем использования представления (2.2.7) и с учетом ее совпадения с матрицей $\rho_{\mathrm{A}}^{(\mathrm{AB})}$.

Для матрицы $\rho^{(\mathrm{A})}$ справедлива следующая цепочка равенств:

$$\rho^{(\mathrm{A})} = \rho_{\mathrm{A}}^{(\mathrm{AB})} = \mathrm{tr}_{\mathrm{B}}\left(\rho^{(\mathrm{AB})}\right), \tag{2.2.17}$$

где, в соответствии с определением 1.1.5, отображение tr_{B} – это линейное по аргументу отображение, называемое частичным следом по системе B, удовлетворяющее равенству

$$\mathrm{tr}_{\mathrm{B}}\left(|a_1\rangle\langle a_2| \otimes |b_1\rangle\langle b_2|\right) = |a_1\rangle\langle a_2| \,\mathrm{tr}\left(|b_1\rangle\langle b_2|\right), \tag{2.2.18}$$

в котором $|a_1\rangle$ и $|a_2\rangle$ – два произвольных состояния системы A, $|b_1\rangle$ и $|b_2\rangle$ – два произвольных состояния системы B.

Для матрицы плотности $\rho^{(\mathrm{AB})}$ с учетом (2.2.7) по определению 1.1.4 имеем:

$$\begin{gathered}
\rho^{(\mathrm{AB})} = |\psi\rangle\langle\psi| = \\
= \left(a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle\right)\left(\tilde{a}\langle 00| + \tilde{b}\langle 01| + \tilde{c}\langle 10| + \tilde{d}\langle 11|\right) = \\
= a\tilde{a}|00\rangle\langle 00| + a\tilde{b}|00\rangle\langle 01| + a\tilde{c}|00\rangle\langle 10| + a\tilde{d}|00\rangle\langle 11| + \\
+ b\tilde{a}|01\rangle\langle 00| + b\tilde{b}|01\rangle\langle 01| + b\tilde{c}|01\rangle\langle 10| + b\tilde{d}|01\rangle\langle 11| +
\end{gathered}$$

$$+c\tilde{a}|10\rangle\langle 00|+c\tilde{b}|10\rangle\langle 01|+c\tilde{c}|10\rangle\langle 10|+c\tilde{d}|10\rangle\langle 11|+$$
$$+d\tilde{a}|11\rangle\langle 00|+d\tilde{b}|11\rangle\langle 01|+d\tilde{c}|11\rangle\langle 10|+d\tilde{d}|11\rangle\langle 11|=$$
$$=a\tilde{a}|0\rangle\langle 0|\otimes|0\rangle\langle 0|+a\tilde{b}|0\rangle\langle 0|\otimes|0\rangle\langle 1|+$$
$$+a\tilde{c}|0\rangle\langle 1|\otimes|0\rangle\langle 0|+a\tilde{d}|0\rangle\langle 1|\otimes|0\rangle\langle 1|+$$
$$+b\tilde{a}|0\rangle\langle 0|\otimes|1\rangle\langle 0|+b\tilde{b}|0\rangle\langle 0|\otimes|1\rangle\langle 1|+$$
$$+b\tilde{c}|0\rangle\langle 1|\otimes|1\rangle\langle 0|+b\tilde{d}|0\rangle\langle 1|\otimes|1\rangle\langle 1|+$$
$$+c\tilde{a}|1\rangle\langle 0|\otimes|0\rangle\langle 0|+c\tilde{b}|1\rangle\langle 0|\otimes|0\rangle\langle 1|+$$
$$+c\tilde{c}|1\rangle\langle 1|\otimes|0\rangle\langle 0|+c\tilde{d}|1\rangle\langle 1|\otimes|0\rangle\langle 1|+$$
$$+d\tilde{a}|1\rangle\langle 0|\otimes|1\rangle\langle 0|+d\tilde{b}|1\rangle\langle 0|\otimes|1\rangle\langle 1|+$$
$$+d\tilde{c}|1\rangle\langle 1|\otimes|1\rangle\langle 0|+d\tilde{d}|1\rangle\langle 1|\otimes|1\rangle\langle 1|, \qquad (2.2.19)$$

где $\tilde{x}$ – комплексное число, сопряженное к комплексному числу x.

Из (2.2.19), учитывая свойство линейности отображения $\mathrm{tr_B}$, получаем

$$\mathrm{tr_B}\left(\rho^{(\mathrm{AB})}\right)=$$
$$=\mathrm{tr_B}\Big(a\tilde{a}|0\rangle\langle 0|\otimes|0\rangle\langle 0|+a\tilde{b}|0\rangle\langle 0|\otimes|0\rangle\langle 1|+$$
$$+a\tilde{c}|0\rangle\langle 1|\otimes|0\rangle\langle 0|+a\tilde{d}|0\rangle\langle 1|\otimes|0\rangle\langle 1|+$$
$$+b\tilde{a}|0\rangle\langle 0|\otimes|1\rangle\langle 0|+b\tilde{b}|0\rangle\langle 0|\otimes|1\rangle\langle 1|+$$
$$+b\tilde{c}|0\rangle\langle 1|\otimes|1\rangle\langle 0|+b\tilde{d}|0\rangle\langle 1|\otimes|1\rangle\langle 1|+$$
$$+c\tilde{a}|1\rangle\langle 0|\otimes|0\rangle\langle 0|+c\tilde{b}|1\rangle\langle 0|\otimes|0\rangle\langle 1|+$$
$$+c\tilde{c}|1\rangle\langle 1|\otimes|0\rangle\langle 0|+c\tilde{d}|1\rangle\langle 1|\otimes|0\rangle\langle 1|+$$
$$+d\tilde{a}|1\rangle\langle 0|\otimes|1\rangle\langle 0|+d\tilde{b}|1\rangle\langle 0|\otimes|1\rangle\langle 1|+$$
$$+d\tilde{c}|1\rangle\langle 1|\otimes|1\rangle\langle 0|+d\tilde{d}|1\rangle\langle 1|\otimes|1\rangle\langle 1|\Big)=$$
$$=a\tilde{a}\,\mathrm{tr_B}\left(|0\rangle\langle 0|\otimes|0\rangle\langle 0|\right)+a\tilde{b}\,\mathrm{tr_B}\left(|0\rangle\langle 0|\otimes|0\rangle\langle 1|\right)+$$
$$+a\tilde{c}\,\mathrm{tr_B}\left(|0\rangle\langle 1|\otimes|0\rangle\langle 0|\right)+a\tilde{d}\,\mathrm{tr_B}\left(|0\rangle\langle 1|\otimes|0\rangle\langle 1|\right)+$$
$$+b\tilde{a}\,\mathrm{tr_B}\left(|0\rangle\langle 0|\otimes|1\rangle\langle 0|\right)+b\tilde{b}\,\mathrm{tr_B}\left(|0\rangle\langle 0|\otimes|1\rangle\langle 1|\right)+$$

$$
\begin{gathered}
+b\tilde{c}\mathrm{tr}_{\mathrm{B}}\left(|0\rangle\langle 1|\otimes|1\rangle\langle 0|\right)+b\tilde{d}\mathrm{tr}_{\mathrm{B}}\left(|0\rangle\langle 1|\otimes|1\rangle\langle 1|\right)+\\
+c\tilde{a}\mathrm{tr}_{\mathrm{B}}\left(|1\rangle\langle 0|\otimes|0\rangle\langle 0|\right)+c\tilde{b}\mathrm{tr}_{\mathrm{B}}\left(|1\rangle\langle 0|\otimes|0\rangle\langle 1|\right)+\\
+c\tilde{c}\mathrm{tr}_{\mathrm{B}}\left(|1\rangle\langle 1|\otimes|0\rangle\langle 0|\right)+c\tilde{d}\mathrm{tr}_{\mathrm{B}}\left(|1\rangle\langle 1|\otimes|0\rangle\langle 1|\right)+\\
+d\tilde{a}\mathrm{tr}_{\mathrm{B}}\left(|1\rangle\langle 0|\otimes|1\rangle\langle 0|\right)+d\tilde{b}\mathrm{tr}_{\mathrm{B}}\left(|1\rangle\langle 0|\otimes|1\rangle\langle 1|\right)+\\
+d\tilde{c}\mathrm{tr}_{\mathrm{B}}\left(|1\rangle\langle 1|\otimes|1\rangle\langle 0|\right)+d\tilde{d}\mathrm{tr}_{\mathrm{B}}\left(|1\rangle\langle 1|\otimes|1\rangle\langle 1|\right).
\end{gathered}
\tag{2.2.20}
$$

Из равенств (2.2.18) и (2.2.20) следует, что

$$
\begin{gathered}
\mathrm{tr}_{\mathrm{B}}\left(\rho^{(\mathrm{AB})}\right)=\\
=a\tilde{a}|0\rangle\langle 0|\,\mathrm{tr}\left(|0\rangle\langle 0|\right)+a\tilde{b}|0\rangle\langle 0|\,\mathrm{tr}\left(|0\rangle\langle 1|\right)+\\
+a\tilde{c}|0\rangle\langle 1|\,\mathrm{tr}\left(|0\rangle\langle 0|\right)+a\tilde{d}|0\rangle\langle 1|\,\mathrm{tr}\left(|0\rangle\langle 1|\right)+\\
+b\tilde{a}|0\rangle\langle 0|\,\mathrm{tr}\left(|1\rangle\langle 0|\right)+b\tilde{b}|0\rangle\langle 0|\,\mathrm{tr}\left(|1\rangle\langle 1|\right)+\\
+b\tilde{c}|0\rangle\langle 1|\,\mathrm{tr}\left(|1\rangle\langle 0|\right)+b\tilde{d}|0\rangle\langle 1|\,\mathrm{tr}\left(|1\rangle\langle 1|\right)+\\
+c\tilde{a}|1\rangle\langle 0|\,\mathrm{tr}\left(|0\rangle\langle 0|\right)+c\tilde{b}|1\rangle\langle 0|\,\mathrm{tr}\left(|0\rangle\langle 1|\right)+\\
+c\tilde{c}|1\rangle\langle 1|\,\mathrm{tr}\left(|0\rangle\langle 0|\right)+c\tilde{d}|1\rangle\langle 1|\,\mathrm{tr}\left(|0\rangle\langle 1|\right)+\\
+d\tilde{a}|1\rangle\langle 0|\,\mathrm{tr}\left(|1\rangle\langle 0|\right)+d\tilde{b}|1\rangle\langle 0|\,\mathrm{tr}\left(|1\rangle\langle 1|\right)+\\
+d\tilde{c}|1\rangle\langle 1|\,\mathrm{tr}\left(|1\rangle\langle 0|\right)+d\tilde{d}|1\rangle\langle 1|\,\mathrm{tr}\left(|1\rangle\langle 1|\right)=\\
=a\tilde{a}|0\rangle\langle 0|\,\mathrm{tr}\left(|0\rangle\langle 0|\right)+a\tilde{c}|0\rangle\langle 1|\,\mathrm{tr}\left(|0\rangle\langle 0|\right)+\\
+b\tilde{b}|0\rangle\langle 0|\,\mathrm{tr}\left(|1\rangle\langle 1|\right)+b\tilde{d}|0\rangle\langle 1|\,\mathrm{tr}\left(|1\rangle\langle 1|\right)+\\
+c\tilde{a}|1\rangle\langle 0|\,\mathrm{tr}\left(|0\rangle\langle 0|\right)+c\tilde{c}|1\rangle\langle 1|\,\mathrm{tr}\left(|0\rangle\langle 0|\right)+\\
+d\tilde{b}|1\rangle\langle 0|\,\mathrm{tr}\left(|1\rangle\langle 1|\right)+d\tilde{d}|1\rangle\langle 1|\,\mathrm{tr}\left(|1\rangle\langle 1|\right)=\\
=a\tilde{a}|0\rangle\langle 0|+a\tilde{c}|0\rangle\langle 1|+b\tilde{b}|0\rangle\langle 0|+b\tilde{d}|0\rangle\langle 1|+\\
+c\tilde{a}|1\rangle\langle 0|+c\tilde{c}|1\rangle\langle 1|+d\tilde{b}|1\rangle\langle 0|+d\tilde{d}|1\rangle\langle 1|=\\
=\begin{pmatrix} |a|^2+|b|^2 & a\tilde{c}+b\tilde{d}\\ c\tilde{a}+d\tilde{b} & |c|^2+|d|^2 \end{pmatrix}.
\end{gathered}
\tag{2.2.21}
$$

Из (2.2.17) и (2.2.21) следует, что

$$\rho^{(\mathrm{A})} = \rho_{\mathrm{A}}^{(\mathrm{AB})} = \mathrm{tr}_{\mathrm{B}}\left(\rho^{(\mathrm{AB})}\right) = \begin{pmatrix} |a|^2 + |b|^2 & a\tilde{c} + b\tilde{d} \\ c\tilde{a} + d\tilde{b} & |c|^2 + |d|^2 \end{pmatrix}. \qquad (2.2.22)$$

Из (2.2.22) и равенства (2.2.16) следует, что

$$1 = \mathrm{tr}\left(\left(\rho^{(\mathrm{A})}\right)^2\right) =$$
$$= \left(\left(|a|^2 + |b|^2\right)^2 + \left(a\tilde{c} + b\tilde{d}\right)\left(c\tilde{a} + d\tilde{b}\right)\right) +$$
$$+ \left(\left(c\tilde{a} + d\tilde{b}\right)\left(a\tilde{c} + b\tilde{d}\right) + \left(|c|^2 + |d|^2\right)^2\right) =$$
$$= |a|^4 + |b|^4 + |c|^4 + |d|^4 +$$
$$+2\left(|a|^2|b|^2 + |c|^2|d|^2 + |a|^2|c|^2 + |b|^2|d|^2 + a\tilde{b}\tilde{c}d + \tilde{a}bc\tilde{d}\right) =$$
$$= \left(|a|^2 + |b|^2 + |c|^2 + |d|^2\right)^2 - 2\left(|a|^2|d|^2 + |b|^2|c|^2 - a\tilde{b}\tilde{c}d - \tilde{a}bc\tilde{d}\right) =$$
$$= 1 - 2\left(|a|^2|d|^2 + |b|^2|c|^2 - a\tilde{b}\tilde{c}d - \tilde{a}bc\tilde{d}\right). \qquad (2.2.23)$$

Удалив слагаемые, равные 1, из первой и последней частей цепочки равенств (2.2.23), получаем

$$0 = -2\left(|a|^2|d|^2 + |b|^2|c|^2 - a\tilde{b}\tilde{c}d - \tilde{a}bc\tilde{d}\right).$$

Поделив обе части последнего равенства на число (–2), получаем

$$|a|^2|d|^2 + |b|^2|c|^2 - a\tilde{b}\tilde{c}d - \tilde{a}bc\tilde{d} = 0.$$

Группируя в левой части данного равенства первый член с последним членом, а второй член – с предпоследним и вынося общие сомножители за скобки, имеем

$$\tilde{a}\tilde{d}(ad - bc) + \tilde{b}\tilde{c}(bc - ad) = 0.$$

Отсюда следует, что $(ad - bc)\left(\tilde{a}\tilde{d} - \tilde{b}\tilde{c}\right) = 0$. Заметив, что значение выражения $\tilde{a}\tilde{d} - \tilde{b}\tilde{c}$ является комплексным числом, сопряженным к значению выражения $ad - bc$, из последнего равенства получаем $|ad - bc|^2 = 0$, что равносильно равенству

$$ad - bc = 0.$$

Утверждение в одну сторону доказано.

Обратно, пусть $ad - bc = 0$. Тогда $|ad - bc|^2 = 0$, что равносильно равенству $(ad - bc)(\tilde{a}\tilde{d} - \tilde{b}\tilde{c}) = 0$. Раскрыв скобки в левой части последнего равенства, получаем

$$|a|^2 |d|^2 + |b|^2 |c|^2 - a\tilde{b}\tilde{c}d - \tilde{a}bc\tilde{d} = 0$$

Помножив на (–2) обе части последнего равенства и к обеим частям получившегося равенства прибавив по 1, имеем

$$1 - 2\left(|a|^2 |d|^2 + |b|^2 |c|^2 - a\tilde{b}\tilde{c}d - \tilde{a}bc\tilde{d}\right) = 1 .$$

Отсюда, учитывая, что

$$|a|^2 + |b|^2 + |c|^2 + |d|^2 = 1 ,$$

получаем

$$\left(|a|^2 + |b|^2 + |c|^2 + |d|^2\right)^2 - 2\left(|a|^2 |d|^2 + |b|^2 |c|^2 - a\tilde{b}\tilde{c}d - \tilde{a}bc\tilde{d}\right) = 1. \quad (2.2.24)$$

Далее, проводя вычисления, аналогичные вычислениям в равенствах (2.2.20) – (2.2.22), из равенства (2.2.19) получаем редуцированную матрицу плотности подсистемы A квантовой системы AB:

$$\rho_{\mathrm{A}}^{(\mathrm{AB})} = \mathrm{tr}_{\mathrm{B}}\left(\rho^{(\mathrm{AB})}\right) = \begin{pmatrix} |a|^2 + |b|^2 & a\tilde{c} + b\tilde{d} \\ c\tilde{a} + d\tilde{b} & |c|^2 + |d|^2 \end{pmatrix}, \quad (2.2.25)$$

Теперь вычислим след от квадрата матрицы $\rho_{\mathrm{A}}^{(\mathrm{AB})}$:

$$\mathrm{tr}\left(\left(\rho_{\mathrm{A}}^{(\mathrm{AB})}\right)^2\right) =$$

$$= \left(\left(|a|^2 + |b|^2\right)^2 + \left(a\tilde{c} + b\tilde{d}\right)\left(c\tilde{a} + d\tilde{b}\right)\right) + \left(\left(c\tilde{a} + d\tilde{b}\right)\left(a\tilde{c} + b\tilde{d}\right) + \left(|c|^2 + |d|^2\right)^2\right) =$$

$$= |a|^4 + |b|^4 + |c|^4 + |d|^4 +$$

$$+ 2\left(|a|^2 |b|^2 + |c|^2 |d|^2 + |a|^2 |c|^2 + |b|^2 |d|^2 + a\tilde{b}\tilde{c}d + \tilde{a}bc\tilde{d}\right) =$$

$$= \left(|a|^2 + |b|^2 + |c|^2 + |d|^2\right)^2 - 2\left(|a|^2 |d|^2 + |b|^2 |c|^2 - a\tilde{b}\tilde{c}d - \tilde{a}bc\tilde{d}\right). \quad (2.2.26)$$

Из равенств (2.2.24) и (2.2.26) следует справедливость равенства $\operatorname{tr}\left(\left(\rho_{\mathrm{A}}^{(\mathrm{AB})}\right)^2\right)=1$, которое в соответствии с результатами, представленными в работе [50], равносильно тому, что состояние подсистемы A квантовой системы AB является чистым состоянием. Тогда в силу того, что состояние $|\psi\rangle$ квантовой системы AB является чистым состоянием, имеем, что состояние подсистемы B также является чистым. Следовательно, состояние $|\psi\rangle$ квантовой системы AB является сепарабельным состоянием, так как состояния ее подсистем A и B являются чистыми состояниями и, следовательно, они описываются некоторыми нормированными векторами, тензорное произведение которых совпадает с вектором $|\psi\rangle$.

<u>Второе доказательство утверждения 2.2.8 завершено</u>.

Замечание 2.2.27. Позднее в данной работе удвоенный модуль $2|ad-bc|$ величины, определяемой выражением $ad-bc$ для состояния

$$|\psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle,$$

будет рассматриваться как мера несепарабельности состояния $|\psi\rangle$, называемая **согласованностью** (concurrence) двухкубитного состояния $|\psi\rangle$ [72; 73]. В данном контексте согласованность состояния $|\psi\rangle$ отражает величину ресурса несепарабельности в двухкубитном состоянии $|\psi\rangle$. Таким образом, из утверждения 2.2.8 следует, что двухкубитное состояние $|\psi\rangle$ сепарабельно тогда и только тогда, когда его согласованность равна 0.

Завершая обсуждение двухкубитных квантовых состояний в этом параграфе, отметим, что, по сути дела, утверждение 2.2.8 представляет собой весьма несложный в вычислительном плане и удобный для практического применения критерий проверки и выявления несепарабельных двухкубитных квантовых состояний.

§ 2.3. Состояния трехкубитных квантовых систем и операция тензорного произведения

В вычислительном базисе из векторов

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

произвольное трехкубитное состояние можно представить в следующем общем виде:

$$\begin{gathered} |\psi\rangle = a_0|000\rangle + a_1|001\rangle + a_2|010\rangle + a_3|011\rangle + \\ + a_4|100\rangle + a_5|101\rangle + a_6|110\rangle + a_7|111\rangle, \end{gathered} \tag{2.3.1}$$

где $a_0,\ a_1,\ a_2,\ a_3,\ a_4,\ a_5,\ a_6,\ a_7 \in \mathbb{C}$,

$$|a_0|^2 + |a_1|^2 + |a_2|^2 + |a_3|^2 + |a_4|^2 + |a_5|^2 + |a_6|^2 + |a_7|^2 = 1. \tag{2.3.2}$$

Из (2.3.1) и (2.3.2) следует, что любой нормированный вектор восьмимерного гильбертова пространства $\mathbb{C}^8$ над полем комплексных чисел $\mathbb{C}$ может служить состоянием трехкубитной квантовой системы. Поэтому нормированные векторы гильбертова пространства $\mathbb{C}^8$ будем также называть состояниями трехкубитных квантовых систем или трехкубитными состояниями.

Для гильбертова пространства $\mathbb{C}^8$ возможны только следующие три представления в виде тензорного произведения гильбертовых пространств (над полем комплексных чисел $\mathbb{C}$) размерностей, равных натуральным степеням числа 2:

$$\mathbb{C}^8 = \mathbb{C}^2 \otimes \mathbb{C}^4,\ \mathbb{C}^8 = \mathbb{C}^4 \otimes \mathbb{C}^2,\ \mathbb{C}^8 = \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2.$$

Следовательно, если состояние $|\psi\rangle \in \mathbb{C}^8$ представляется в виде тензорного произведения состояний меньших размерностей, то это можно записать в виде лишь одного из следующих равенств:

1) $|\psi\rangle = |\psi_1\rangle \otimes |\psi_{23}\rangle$,

где $|\psi_1\rangle \in \mathbb{C}^2$, $|\psi_1\rangle$ – однокубитное состояние, $|\psi_{23}\rangle \in \mathbb{C}^4$, $|\psi_{23}\rangle$ – двухкубитное состояние, не представимое в виде тензорного произведения состояний меньших размерностей;

2) $|\psi\rangle = |\psi_{12}\rangle \otimes |\psi_3\rangle$,

где $|\psi_{12}\rangle \in \mathbb{C}^4, |\psi_{12}\rangle$ – двухкубитное состояние, не представимое в виде тензорного произведения состояний меньших размерностей, $|\psi_3\rangle \in \mathbb{C}^2$, $|\psi_3\rangle$ – однокубитное состояние;

3) $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \otimes |\psi_3\rangle$,

где $|\psi_1\rangle \in \mathbb{C}^2$, $|\psi_2\rangle \in \mathbb{C}^2$, $|\psi_3\rangle \in \mathbb{C}^2$; $|\psi_1\rangle$, $|\psi_2\rangle$, $|\psi_3\rangle$ – однокубитные состояния.

Напомним [50], что в соответствии с постулатами квантовой механики пространство состояний составной системы представляет собой тензорное произведение пространств состояний входящих в нее подсистем. Более того, если указаны состояния подсистем и определен порядок (нумерация) на множестве подсистем, то состояние квантовой системы является тензорным произведением состояний ее подсистем, и сомножители в тензорном произведении имеют тот же порядок, какой определен на множестве подсистем.

Тогда, если считать $|\psi\rangle \in \mathbb{C}^8$ состоянием трехкубитной квантовой системы ABC в порядке следования составляющих ее кубитов в соответствии с записью ABC (то есть первый кубит – A, второй кубит – B и третий кубит – C), то имеет место быть следующее.

Первое равенство соответствует ситуации, когда состояние $|\psi_1\rangle \in \mathbb{C}^2$ однокубитной подсистемы A является чистым состоянием, а двухкубитная подсистема BC находится в чистом несепарабельном состоянии $|\psi_{23}\rangle \in \mathbb{C}^4$.

Второе равенство соответствует ситуации, когда двухкубитная подсистема AB находится в чистом несепарабельном состоянии $|\psi_{12}\rangle \in \mathbb{C}^4$, а однокубитная подсистема C находится в чистом состоянии $|\psi_3\rangle \in \mathbb{C}^2$.

Третье равенство соответствует ситуации, когда однокубитные подсистемы A, B и C исходной трехкубитной квантовой системы ABC находятся соответственно в чистых состояниях $|\psi_1\rangle \in \mathbb{C}^2$, $|\psi_2\rangle \in \mathbb{C}^2$, $|\psi_3\rangle \in \mathbb{C}^2$.

Однако, как следует из вышеизложенного, для ситуации, когда в квантовой системе ABC кубит B находится в чистом состоянии, а двухкубитная подсистема AC находится в чистом несепарабельном состоянии, не существует равенства, выражающего состояние $|\psi\rangle \in \mathbb{C}^8$ через тензорное произведение состояний меньших размерностей. Пример такого состояния будет разобран в параграфе 2.4 (пример 2.4.3). И это обстоятельство влечет существенные отличия между двухкубитными состояниями и трехкубитными состояниями в связи с понятием несепарабельности. В трехкубитном случае все намного сложнее, чем в двухкубитном. Поэтому для случая трехкубитной квантовой системы ABC сначала разберемся с вопросом о возможности представления ее состояний в виде тензорного произведения. Для решения данного вопроса ниже будет сформулировано и доказано утверждение 2.3.4.

Для состояния $|\psi\rangle \in \mathbb{C}^8$, заданного равенством (2.3.1), определим величины $V_1, V_2, V_3, V_4, V_5, V_6$ и $Y_1, Y_2, Y_3, Y_4, Y_5, Y_6$, положив

$$\begin{gathered} V_1 = a_0a_5 - a_1a_4\,,\ V_2 = a_0a_6 - a_2a_4\,,\ V_3 = a_0a_7 - a_3a_4\,, \\ V_4 = a_1a_6 - a_2a_5\,,\ V_5 = a_1a_7 - a_3a_5\,,\ V_6 = a_2a_7 - a_3a_6\,, \\ Y_1 = a_0a_3 - a_1a_2\,,\ Y_2 = a_0a_5 - a_1a_4\,,\ Y_3 = a_0a_7 - a_1a_6\,, \\ Y_4 = a_2a_5 - a_3a_4\,,\ Y_5 = a_2a_7 - a_3a_6\,,\ Y_6 = a_4a_7 - a_5a_6\,. \end{gathered} \tag{2.3.3}$$

Имеет место следующее утверждение.

Утверждение 2.3.4.

а) Для чистого состояния $|\psi\rangle$ трехкубитной квантовой системы ABC равенство

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_{23}\rangle,$$

где $|\psi_1\rangle \in \mathbb{C}^2$, $|\psi_{23}\rangle \in \mathbb{C}^4$, $|\psi_1\rangle$ – чистое состояние однокубитной квантовой системы A, $|\psi_{23}\rangle$ – чистое состояние двухкубитной квантовой системы BC, справедливо тогда и только тогда, когда справедлива цепочка равенств

$$V_1 = V_2 = V_3 = V_4 = V_5 = V_6 = 0\,.$$

б) Для чистого состояния $|\psi\rangle$ трехкубитной квантовой системы ABC равенство

$$|\psi\rangle = |\psi_{12}\rangle \otimes |\psi_3\rangle,$$

где $|\psi_{12}\rangle \in \mathbb{C}^4$, $|\psi_3\rangle \in \mathbb{C}^2$, $|\psi_{12}\rangle$ – чистое состояние двухкубитной квантовой системы AB, $|\psi_3\rangle$ – чистое состояние однокубитной квантовой системы C, справедливо тогда и только тогда, когда справедлива цепочка равенств

$$Y_1 = Y_2 = Y_3 = Y_4 = Y_5 = Y_6 = 0\,.$$

Непосредственно из утверждения 2.3.4 вытекает

Следствие 2.3.5.

а) Чистое состояние $|\psi\rangle$ трехкубитной квантовой системы ABC не представимо в виде тензорного произведения $|\psi_1\rangle \otimes |\psi_{23}\rangle$, где $|\psi_1\rangle$ – чистое состояние однокубитной квантовой подсистемы A, $|\psi_{23}\rangle$ – чистое состояние двухкубитной квантовой подсистемы BC, тогда и только тогда, когда отлична от нуля хотя бы одна из величин V_1, V_2, V_3, V_4, V_5, V_6.

б) Чистое состояние $|\psi\rangle$ трехкубитной квантовой системы ABC не представимо в виде тензорного произведения $|\psi_{12}\rangle \otimes |\psi_3\rangle$, где $|\psi_{12}\rangle$ – чистое состояние двухкубитной квантовой подсистемы AB, $|\psi_3\rangle$ – чистое состояние однокубитной квантовой подсистемы C, тогда и только тогда, когда отлична от нуля хотя бы одна из величин $Y_1,\ Y_2,\ Y_3,\ Y_4,\ Y_5,\ Y_6$.

в) Чистое состояние $|\psi\rangle$ трехкубитной квантовой системы ABC не представимо в виде тензорного произведения состояний меньших размерностей тогда и только тогда, когда в каждом из наборов величин $\{V_1,\ V_2,\ V_3,\ V_4,\ V_5,\ V_6\}$ и $\{Y_1,\ Y_2,\ Y_3,\ Y_4,\ Y_5,\ Y_6\}$ имеется величина, не равная нулю.

Замечание. В формулировках утверждения 2.3.4 и следствия 2.3.5 отсутствует требование несепарабельности двухкубитных состояний $|\psi_{12}\rangle \in \mathbb{C}^4$ и $|\psi_{23}\rangle \in \mathbb{C}^4$.

Дальнейшую часть данного параграфа отведем доказательству утверждения 2.3.4 с использованием инструментов аналитического аппарата квантовой механики.

Доказательство утверждения 2.3.4.

Докажем пункт (а).

Пусть $|\psi\rangle$ – чистое состояние трехкубитной квантовой системы ABC и

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_{23}\rangle,$$

где $|\psi_1\rangle$ – чистое состояние однокубитной квантовой системы A, $|\psi_{23}\rangle$ – чистое состояние двухкубитной квантовой системы BC. Отсюда в соответствии с [50] следует, что редуцированная матрица плотности $\rho_{\mathrm{A}}^{(\mathrm{ABC})}$ подсистемы A совпадает с матрицей плотности $\rho^{(\mathrm{A})}$ подсистемы A и при этом выполняется равенство

$$\mathrm{tr}\left(\left(\rho^{(\mathrm{A})}\right)^2\right)=1. \tag{2.3.6}$$

Вычислим матрицу $\rho^{(\mathrm{A})}$ путем использования представления (2.3.1) и с учетом ее совпадения с редуцированной матрицей плотности $\rho_{\mathrm{A}}^{(\mathrm{ABC})}$.

Для матрицы $\rho^{(\mathrm{A})}$ справедлива следующая цепочка равенств:

$$\rho^{(\mathrm{A})}=\rho_{\mathrm{A}}^{(\mathrm{ABC})}=\mathrm{tr}_{\mathrm{BC}}\left(\rho^{(\mathrm{ABC})}\right). \tag{2.3.7}$$

Напомним, $\tilde{x}$ – комплексное число, сопряженное к комплексному числу x. Тогда для матрицы плотности $\rho^{(\mathrm{ABC})}$ с учетом (2.3.1) по определению 1.1.4 имеем:

$$\begin{gathered}
\rho^{(\mathrm{ABC})}=|\psi\rangle\langle\psi|= \\
=\left(a_0|000\rangle+a_1|001\rangle+a_2|010\rangle+a_3|011\rangle+\right. \\
\left.+a_4|100\rangle+a_5|101\rangle+a_6|110\rangle+a_7|111\rangle\right) \\
\left(\tilde{a}_0\langle 000|+\tilde{a}_1\langle 001|+\tilde{a}_2\langle 010|+\tilde{a}_3\langle 011|+\right. \\
\left.+\tilde{a}_4\langle 100|+\tilde{a}_5\langle 101|+\tilde{a}_6\langle 110|+\tilde{a}_7\langle 111|\right)=
\end{gathered}$$

$$\begin{gathered}
=\left(a_0\tilde{a}_0|000\rangle\langle 000|+a_0\tilde{a}_1|000\rangle\langle 001|+a_0\tilde{a}_2|000\rangle\langle 010|+a_0\tilde{a}_3|000\rangle\langle 011|+\right. \\
\left.+a_0\tilde{a}_4|000\rangle\langle 100|+a_0\tilde{a}_5|000\rangle\langle 101|+a_0\tilde{a}_6|000\rangle\langle 110|+a_0\tilde{a}_7|000\rangle\langle 111|\right)+ \\
+\left(a_1\tilde{a}_0|001\rangle\langle 000|+a_1\tilde{a}_1|001\rangle\langle 001|+a_1\tilde{a}_2|001\rangle\langle 010|+a_1\tilde{a}_3|001\rangle\langle 011|+\right. \\
\left.+a_1\tilde{a}_4|001\rangle\langle 100|+a_1\tilde{a}_5|001\rangle\langle 101|+a_1\tilde{a}_6|001\rangle\langle 110|+a_1\tilde{a}_7|001\rangle\langle 111|\right)+ \\
+\left(a_2\tilde{a}_0|010\rangle\langle 000|+a_2\tilde{a}_1|010\rangle\langle 001|+a_2\tilde{a}_2|010\rangle\langle 010|+a_2\tilde{a}_3|010\rangle\langle 011|+\right. \\
\left.+a_2\tilde{a}_4|010\rangle\langle 100|+a_2\tilde{a}_5|010\rangle\langle 101|+a_2\tilde{a}_6|010\rangle\langle 110|+a_2\tilde{a}_7|010\rangle\langle 111|\right)+ \\
+\left(a_3\tilde{a}_0|011\rangle\langle 000|+a_3\tilde{a}_1|011\rangle\langle 001|+a_3\tilde{a}_2|011\rangle\langle 010|+a_3\tilde{a}_3|011\rangle\langle 011|+\right. \\
\left.+a_3\tilde{a}_4|011\rangle\langle 100|+a_3\tilde{a}_5|011\rangle\langle 101|+a_3\tilde{a}_6|011\rangle\langle 110|+a_3\tilde{a}_7|011\rangle\langle 111|\right)+ \\
+\left(a_4\tilde{a}_0|100\rangle\langle 000|+a_4\tilde{a}_1|100\rangle\langle 001|+a_4\tilde{a}_2|100\rangle\langle 010|+a_4\tilde{a}_3|100\rangle\langle 011|+\right. \\
\left.+a_4\tilde{a}_4|100\rangle\langle 100|+a_4\tilde{a}_5|100\rangle\langle 101|+a_4\tilde{a}_6|100\rangle\langle 110|+a_4\tilde{a}_7|100\rangle\langle 111|\right)+ \\
+\left(a_5\tilde{a}_0|101\rangle\langle 000|+a_5\tilde{a}_1|101\rangle\langle 001|+a_5\tilde{a}_2|101\rangle\langle 010|+a_5\tilde{a}_3|101\rangle\langle 011|+\right.
\end{gathered}$$

$$
\begin{gathered}
+a_5\tilde{a}_4|101\rangle\langle 100|+a_5\tilde{a}_5|101\rangle\langle 101|+a_5\tilde{a}_6|101\rangle\langle 110|+a_5\tilde{a}_7|101\rangle\langle 111|\big)+\\
+\big(a_6\tilde{a}_0|110\rangle\langle 000|+a_6\tilde{a}_1|110\rangle\langle 001|+a_6\tilde{a}_2|110\rangle\langle 010|+a_6\tilde{a}_3|110\rangle\langle 011|+\\
+a_6\tilde{a}_4|110\rangle\langle 100|+a_6\tilde{a}_5|110\rangle\langle 101|+a_6\tilde{a}_6|110\rangle\langle 110|+a_6\tilde{a}_7|110\rangle\langle 111|\big)+\\
+\big(a_7\tilde{a}_0|111\rangle\langle 000|+a_7\tilde{a}_1|111\rangle\langle 001|+a_7\tilde{a}_2|111\rangle\langle 010|+a_7\tilde{a}_3|111\rangle\langle 011|+\\
+a_7\tilde{a}_4|111\rangle\langle 100|+a_7\tilde{a}_5|111\rangle\langle 101|+a_7\tilde{a}_6|111\rangle\langle 110|+a_7\tilde{a}_7|111\rangle\langle 111|\big)=\\
=\big(a_0\tilde{a}_0|0\rangle\langle 0|\otimes|00\rangle\langle 00|+a_0\tilde{a}_1|0\rangle\langle 0|\otimes|00\rangle\langle 01|+a_0\tilde{a}_2|0\rangle\langle 0|\otimes|00\rangle\langle 10|+\\
+a_0\tilde{a}_3|0\rangle\langle 0|\otimes|00\rangle\langle 11|+a_0\tilde{a}_4|0\rangle\langle 1|\otimes|00\rangle\langle 00|+a_0\tilde{a}_5|0\rangle\langle 1|\otimes|00\rangle\langle 01|+\\
+a_0\tilde{a}_6|0\rangle\langle 1|\otimes|00\rangle\langle 10|+a_0\tilde{a}_7|0\rangle\langle 1|\otimes|00\rangle\langle 11|\big)+\\
+\big(a_1\tilde{a}_0|0\rangle\langle 0|\otimes|01\rangle\langle 00|+a_1\tilde{a}_1|0\rangle\langle 0|\otimes|01\rangle\langle 01|+a_1\tilde{a}_2|0\rangle\langle 0|\otimes|01\rangle\langle 10|+\\
+a_1\tilde{a}_3|0\rangle\langle 0|\otimes|01\rangle\langle 11|+a_1\tilde{a}_4|0\rangle\langle 1|\otimes|01\rangle\langle 00|+a_1\tilde{a}_5|0\rangle\langle 1|\otimes|01\rangle\langle 01|+\\
+a_1\tilde{a}_6|0\rangle\langle 1|\otimes|01\rangle\langle 10|+a_1\tilde{a}_7|0\rangle\langle 1|\otimes|01\rangle\langle 11|\big)+\\
+\big(a_2\tilde{a}_0|0\rangle\langle 0|\otimes|10\rangle\langle 00|+a_2\tilde{a}_1|0\rangle\langle 0|\otimes|10\rangle\langle 01|+a_2\tilde{a}_2|0\rangle\langle 0|\otimes|10\rangle\langle 10|+\\
+a_2\tilde{a}_3|0\rangle\langle 0|\otimes|10\rangle\langle 11|+a_2\tilde{a}_4|0\rangle\langle 1|\otimes|10\rangle\langle 00|+a_2\tilde{a}_5|0\rangle\langle 1|\otimes|10\rangle\langle 01|+\\
+a_2\tilde{a}_6|0\rangle\langle 1|\otimes|10\rangle\langle 10|+a_2\tilde{a}_7|0\rangle\langle 1|\otimes|10\rangle\langle 11|\big)+\\
+\big(a_3\tilde{a}_0|0\rangle\langle 0|\otimes|11\rangle\langle 00|+a_3\tilde{a}_1|0\rangle\langle 0|\otimes|11\rangle\langle 01|+a_3\tilde{a}_2|0\rangle\langle 0|\otimes|11\rangle\langle 10|+\\
+a_3\tilde{a}_3|0\rangle\langle 0|\otimes|11\rangle\langle 11|+a_3\tilde{a}_4|0\rangle\langle 1|\otimes|11\rangle\langle 00|+a_3\tilde{a}_5|0\rangle\langle 1|\otimes|11\rangle\langle 01|+\\
+a_3\tilde{a}_6|0\rangle\langle 1|\otimes|11\rangle\langle 10|+a_3\tilde{a}_7|0\rangle\langle 1|\otimes|11\rangle\langle 11|\big)+\\
+\big(a_4\tilde{a}_0|1\rangle\langle 0|\otimes|00\rangle\langle 00|+a_4\tilde{a}_1|1\rangle\langle 0|\otimes|00\rangle\langle 01|+a_4\tilde{a}_2|1\rangle\langle 0|\otimes|00\rangle\langle 10|+\\
+a_4\tilde{a}_3|1\rangle\langle 0|\otimes|00\rangle\langle 11|+a_4\tilde{a}_4|1\rangle\langle 1|\otimes|00\rangle\langle 00|+a_4\tilde{a}_5|1\rangle\langle 1|\otimes|00\rangle\langle 01|+\\
+a_4\tilde{a}_6|1\rangle\langle 1|\otimes|00\rangle\langle 10|+a_4\tilde{a}_7|1\rangle\langle 1|\otimes|00\rangle\langle 11|\big)+\\
+\big(a_5\tilde{a}_0|1\rangle\langle 0|\otimes|01\rangle\langle 00|+a_5\tilde{a}_1|1\rangle\langle 0|\otimes|01\rangle\langle 01|+a_5\tilde{a}_2|1\rangle\langle 0|\otimes|01\rangle\langle 10|+\\
+a_5\tilde{a}_3|1\rangle\langle 0|\otimes|01\rangle\langle 11|+a_5\tilde{a}_4|1\rangle\langle 1|\otimes|01\rangle\langle 00|+a_5\tilde{a}_5|1\rangle\langle 1|\otimes|01\rangle\langle 01|+\\
+a_5\tilde{a}_6|1\rangle\langle 1|\otimes|01\rangle\langle 10|+a_5\tilde{a}_7|1\rangle\langle 1|\otimes|01\rangle\langle 11|\big)+\\
+\big(a_6\tilde{a}_0|1\rangle\langle 0|\otimes|10\rangle\langle 00|+a_6\tilde{a}_1|1\rangle\langle 0|\otimes|10\rangle\langle 01|+a_6\tilde{a}_2|1\rangle\langle 0|\otimes|10\rangle\langle 10|+\\
+a_6\tilde{a}_3|1\rangle\langle 0|\otimes|10\rangle\langle 11|+a_6\tilde{a}_4|1\rangle\langle 1|\otimes|10\rangle\langle 00|+a_6\tilde{a}_5|1\rangle\langle 1|\otimes|10\rangle\langle 01|+
\end{gathered}
$$

$$+a_6\tilde{a}_6\left|1\right\rangle\left\langle1\right|\otimes\left|10\right\rangle\left\langle10\right|+a_6\tilde{a}_7\left|1\right\rangle\left\langle1\right|\otimes\left|10\right\rangle\left\langle11\right|\Big)+$$
$$+\Big(a_7\tilde{a}_0\left|1\right\rangle\left\langle0\right|\otimes\left|11\right\rangle\left\langle00\right|+a_7\tilde{a}_1\left|1\right\rangle\left\langle0\right|\otimes\left|11\right\rangle\left\langle01\right|+a_7\tilde{a}_2\left|1\right\rangle\left\langle0\right|\otimes\left|11\right\rangle\left\langle10\right|+$$
$$+a_7\tilde{a}_3\left|1\right\rangle\left\langle0\right|\otimes\left|11\right\rangle\left\langle11\right|+a_7\tilde{a}_4\left|1\right\rangle\left\langle1\right|\otimes\left|11\right\rangle\left\langle00\right|+a_7\tilde{a}_5\left|1\right\rangle\left\langle1\right|\otimes\left|11\right\rangle\left\langle01\right|+$$
$$+a_7\tilde{a}_6\left|1\right\rangle\left\langle1\right|\otimes\left|11\right\rangle\left\langle10\right|+a_7\tilde{a}_7\left|1\right\rangle\left\langle1\right|\otimes\left|11\right\rangle\left\langle11\right|\Big). \qquad (2.3.8)$$

Из (2.3.8), учитывая свойство линейности отображения $\mathrm{tr}_{\mathrm{BC}}$, получаем

$$\mathrm{tr}_{\mathrm{BC}}\left(\rho^{(\mathrm{ABC})}\right)=$$
$$=a_0\tilde{a}_0\mathrm{tr}_{\mathrm{BC}}\left(\left|0\right\rangle\left\langle0\right|\otimes\left|00\right\rangle\left\langle00\right|\right)+a_0\tilde{a}_1\mathrm{tr}_{\mathrm{BC}}\left(\left|0\right\rangle\left\langle0\right|\otimes\left|00\right\rangle\left\langle01\right|\right)+$$
$$+a_0\tilde{a}_2\mathrm{tr}_{\mathrm{BC}}\left(\left|0\right\rangle\left\langle0\right|\otimes\left|00\right\rangle\left\langle10\right|\right)+a_0\tilde{a}_3\mathrm{tr}_{\mathrm{BC}}\left(\left|0\right\rangle\left\langle0\right|\otimes\left|00\right\rangle\left\langle11\right|\right)+$$
$$+a_0\tilde{a}_4\mathrm{tr}_{\mathrm{BC}}\left(\left|0\right\rangle\left\langle1\right|\otimes\left|00\right\rangle\left\langle00\right|\right)+a_0\tilde{a}_5\mathrm{tr}_{\mathrm{BC}}\left(\left|0\right\rangle\left\langle1\right|\otimes\left|00\right\rangle\left\langle01\right|\right)+$$
$$+a_0\tilde{a}_6\mathrm{tr}_{\mathrm{BC}}\left(\left|0\right\rangle\left\langle1\right|\otimes\left|00\right\rangle\left\langle10\right|\right)+a_0\tilde{a}_7\mathrm{tr}_{\mathrm{BC}}\left(\left|0\right\rangle\left\langle1\right|\otimes\left|00\right\rangle\left\langle11\right|\right)+$$
$$+a_1\tilde{a}_0\mathrm{tr}_{\mathrm{BC}}\left(\left|0\right\rangle\left\langle0\right|\otimes\left|01\right\rangle\left\langle00\right|\right)+a_1\tilde{a}_1\mathrm{tr}_{\mathrm{BC}}\left(\left|0\right\rangle\left\langle0\right|\otimes\left|01\right\rangle\left\langle01\right|\right)+$$
$$+a_1\tilde{a}_2\mathrm{tr}_{\mathrm{BC}}\left(\left|0\right\rangle\left\langle0\right|\otimes\left|01\right\rangle\left\langle10\right|\right)+a_1\tilde{a}_3\mathrm{tr}_{\mathrm{BC}}\left(\left|0\right\rangle\left\langle0\right|\otimes\left|01\right\rangle\left\langle11\right|\right)+$$
$$+a_1\tilde{a}_4\mathrm{tr}_{\mathrm{BC}}\left(\left|0\right\rangle\left\langle1\right|\otimes\left|01\right\rangle\left\langle00\right|\right)+a_1\tilde{a}_5\mathrm{tr}_{\mathrm{BC}}\left(\left|0\right\rangle\left\langle1\right|\otimes\left|01\right\rangle\left\langle01\right|\right)+$$
$$+a_1\tilde{a}_6\mathrm{tr}_{\mathrm{BC}}\left(\left|0\right\rangle\left\langle1\right|\otimes\left|01\right\rangle\left\langle10\right|\right)+a_1\tilde{a}_7\mathrm{tr}_{\mathrm{BC}}\left(\left|0\right\rangle\left\langle1\right|\otimes\left|01\right\rangle\left\langle11\right|\right)+$$
$$+a_2\tilde{a}_0\mathrm{tr}_{\mathrm{BC}}\left(\left|0\right\rangle\left\langle0\right|\otimes\left|10\right\rangle\left\langle00\right|\right)+a_2\tilde{a}_1\mathrm{tr}_{\mathrm{BC}}\left(\left|0\right\rangle\left\langle0\right|\otimes\left|10\right\rangle\left\langle01\right|\right)+$$
$$+a_2\tilde{a}_2\mathrm{tr}_{\mathrm{BC}}\left(\left|0\right\rangle\left\langle0\right|\otimes\left|10\right\rangle\left\langle10\right|\right)+a_2\tilde{a}_3\mathrm{tr}_{\mathrm{BC}}\left(\left|0\right\rangle\left\langle0\right|\otimes\left|10\right\rangle\left\langle11\right|\right)+$$
$$+a_2\tilde{a}_4\mathrm{tr}_{\mathrm{BC}}\left(\left|0\right\rangle\left\langle1\right|\otimes\left|10\right\rangle\left\langle00\right|\right)+a_2\tilde{a}_5\mathrm{tr}_{\mathrm{BC}}\left(\left|0\right\rangle\left\langle1\right|\otimes\left|10\right\rangle\left\langle01\right|\right)+$$
$$+a_2\tilde{a}_6\mathrm{tr}_{\mathrm{BC}}\left(\left|0\right\rangle\left\langle1\right|\otimes\left|10\right\rangle\left\langle10\right|\right)+a_2\tilde{a}_7\mathrm{tr}_{\mathrm{BC}}\left(\left|0\right\rangle\left\langle1\right|\otimes\left|10\right\rangle\left\langle11\right|\right)+$$
$$+a_3\tilde{a}_0\mathrm{tr}_{\mathrm{BC}}\left(\left|0\right\rangle\left\langle0\right|\otimes\left|11\right\rangle\left\langle00\right|\right)+a_3\tilde{a}_1\mathrm{tr}_{\mathrm{BC}}\left(\left|0\right\rangle\left\langle0\right|\otimes\left|11\right\rangle\left\langle01\right|\right)+$$
$$+a_3\tilde{a}_2\mathrm{tr}_{\mathrm{BC}}\left(\left|0\right\rangle\left\langle0\right|\otimes\left|11\right\rangle\left\langle10\right|\right)+a_3\tilde{a}_3\mathrm{tr}_{\mathrm{BC}}\left(\left|0\right\rangle\left\langle0\right|\otimes\left|11\right\rangle\left\langle11\right|\right)+$$
$$+a_3\tilde{a}_4\mathrm{tr}_{\mathrm{BC}}\left(\left|0\right\rangle\left\langle1\right|\otimes\left|11\right\rangle\left\langle00\right|\right)+a_3\tilde{a}_5\mathrm{tr}_{\mathrm{BC}}\left(\left|0\right\rangle\left\langle1\right|\otimes\left|11\right\rangle\left\langle01\right|\right)+$$
$$+a_3\tilde{a}_6\mathrm{tr}_{\mathrm{BC}}\left(\left|0\right\rangle\left\langle1\right|\otimes\left|11\right\rangle\left\langle10\right|\right)+a_3\tilde{a}_7\mathrm{tr}_{\mathrm{BC}}\left(\left|0\right\rangle\left\langle1\right|\otimes\left|11\right\rangle\left\langle11\right|\right)+$$
$$+a_4\tilde{a}_0\mathrm{tr}_{\mathrm{BC}}\left(\left|1\right\rangle\left\langle0\right|\otimes\left|00\right\rangle\left\langle00\right|\right)+a_4\tilde{a}_1\mathrm{tr}_{\mathrm{BC}}\left(\left|1\right\rangle\left\langle0\right|\otimes\left|00\right\rangle\left\langle01\right|\right)+$$
$$+a_4\tilde{a}_2\mathrm{tr}_{\mathrm{BC}}\left(\left|1\right\rangle\left\langle0\right|\otimes\left|00\right\rangle\left\langle10\right|\right)+a_4\tilde{a}_3\mathrm{tr}_{\mathrm{BC}}\left(\left|1\right\rangle\left\langle0\right|\otimes\left|00\right\rangle\left\langle11\right|\right)+$$

$$+a_4\tilde{a}_4\mathrm{tr}_{\mathrm{BC}}\left(|1\rangle\langle 1|\otimes|00\rangle\langle 00|\right)+a_4\tilde{a}_5\mathrm{tr}_{\mathrm{BC}}\left(|1\rangle\langle 1|\otimes|00\rangle\langle 01|\right)+$$
$$+a_4\tilde{a}_6\mathrm{tr}_{\mathrm{BC}}\left(|1\rangle\langle 1|\otimes|00\rangle\langle 10|\right)+a_4\tilde{a}_7\mathrm{tr}_{\mathrm{BC}}\left(|1\rangle\langle 1|\otimes|00\rangle\langle 11|\right)+$$
$$+a_5\tilde{a}_0\mathrm{tr}_{\mathrm{BC}}\left(|1\rangle\langle 0|\otimes|01\rangle\langle 00|\right)+a_5\tilde{a}_1\mathrm{tr}_{\mathrm{BC}}\left(|1\rangle\langle 0|\otimes|01\rangle\langle 01|\right)+$$
$$+a_5\tilde{a}_2\mathrm{tr}_{\mathrm{BC}}\left(|1\rangle\langle 0|\otimes|01\rangle\langle 10|\right)+a_5\tilde{a}_3\mathrm{tr}_{\mathrm{BC}}\left(|1\rangle\langle 0|\otimes|01\rangle\langle 11|\right)+$$
$$+a_5\tilde{a}_4\mathrm{tr}_{\mathrm{BC}}\left(|1\rangle\langle 1|\otimes|01\rangle\langle 00|\right)+a_5\tilde{a}_5\mathrm{tr}_{\mathrm{BC}}\left(|1\rangle\langle 1|\otimes|01\rangle\langle 01|\right)+$$
$$+a_5\tilde{a}_6\mathrm{tr}_{\mathrm{BC}}\left(|1\rangle\langle 1|\otimes|01\rangle\langle 10|\right)+a_5\tilde{a}_7\mathrm{tr}_{\mathrm{BC}}\left(|1\rangle\langle 1|\otimes|01\rangle\langle 11|\right)+$$
$$+a_6\tilde{a}_0\mathrm{tr}_{\mathrm{BC}}\left(|1\rangle\langle 0|\otimes|10\rangle\langle 00|\right)+a_6\tilde{a}_1\mathrm{tr}_{\mathrm{BC}}\left(|1\rangle\langle 0|\otimes|10\rangle\langle 01|\right)+$$
$$+a_6\tilde{a}_2\mathrm{tr}_{\mathrm{BC}}\left(|1\rangle\langle 0|\otimes|10\rangle\langle 10|\right)+a_6\tilde{a}_3\mathrm{tr}_{\mathrm{BC}}\left(|1\rangle\langle 0|\otimes|10\rangle\langle 11|\right)+$$
$$+a_6\tilde{a}_4\mathrm{tr}_{\mathrm{BC}}\left(|1\rangle\langle 1|\otimes|10\rangle\langle 00|\right)+a_6\tilde{a}_5\mathrm{tr}_{\mathrm{BC}}\left(|1\rangle\langle 1|\otimes|10\rangle\langle 01|\right)+$$
$$+a_6\tilde{a}_6\mathrm{tr}_{\mathrm{BC}}\left(|1\rangle\langle 1|\otimes|10\rangle\langle 10|\right)+a_6\tilde{a}_7\mathrm{tr}_{\mathrm{BC}}\left(|1\rangle\langle 1|\otimes|10\rangle\langle 11|\right)+$$
$$+a_7\tilde{a}_0\mathrm{tr}_{\mathrm{BC}}\left(|1\rangle\langle 0|\otimes|11\rangle\langle 00|\right)+a_7\tilde{a}_1\mathrm{tr}_{\mathrm{BC}}\left(|1\rangle\langle 0|\otimes|11\rangle\langle 01|\right)+$$
$$+a_7\tilde{a}_2\mathrm{tr}_{\mathrm{BC}}\left(|1\rangle\langle 0|\otimes|11\rangle\langle 10|\right)+a_7\tilde{a}_3\mathrm{tr}_{\mathrm{BC}}\left(|1\rangle\langle 0|\otimes|11\rangle\langle 11|\right)+$$
$$+a_7\tilde{a}_4\mathrm{tr}_{\mathrm{BC}}\left(|1\rangle\langle 1|\otimes|11\rangle\langle 00|\right)+a_7\tilde{a}_5\mathrm{tr}_{\mathrm{BC}}\left(|1\rangle\langle 1|\otimes|11\rangle\langle 01|\right)+$$
$$+a_7\tilde{a}_6\mathrm{tr}_{\mathrm{BC}}\left(|1\rangle\langle 1|\otimes|11\rangle\langle 10|\right)+a_7\tilde{a}_7\mathrm{tr}_{\mathrm{BC}}\left(|1\rangle\langle 1|\otimes|11\rangle\langle 11|\right). \qquad (2.3.9)$$

Из равенств (2.2.18) и (2.3.9) следует, что

$$\mathrm{tr}_{\mathrm{BC}}\left(\rho^{(\mathrm{ABC})}\right)=$$
$$=a_0\tilde{a}_0|0\rangle\langle 0|\,\mathrm{tr}\left(|00\rangle\langle 00|\right)+a_0\tilde{a}_1|0\rangle\langle 0|\,\mathrm{tr}\left(|00\rangle\langle 01|\right)+$$
$$+a_0\tilde{a}_2|0\rangle\langle 0|\,\mathrm{tr}\left(|00\rangle\langle 10|\right)+a_0\tilde{a}_3|0\rangle\langle 0|\,\mathrm{tr}\left(|00\rangle\langle 11|\right)+$$
$$+a_0\tilde{a}_4|0\rangle\langle 1|\,\mathrm{tr}\left(|00\rangle\langle 00|\right)+a_0\tilde{a}_5|0\rangle\langle 1|\,\mathrm{tr}\left(|00\rangle\langle 01|\right)+$$
$$+a_0\tilde{a}_6|0\rangle\langle 1|\,\mathrm{tr}\left(|00\rangle\langle 10|\right)+a_0\tilde{a}_7|0\rangle\langle 1|\,\mathrm{tr}\left(|00\rangle\langle 11|\right)+$$
$$+a_1\tilde{a}_0|0\rangle\langle 0|\,\mathrm{tr}\left(|01\rangle\langle 00|\right)+a_1\tilde{a}_1|0\rangle\langle 0|\,\mathrm{tr}\left(|01\rangle\langle 01|\right)+$$
$$+a_1\tilde{a}_2|0\rangle\langle 0|\,\mathrm{tr}\left(|01\rangle\langle 10|\right)+a_1\tilde{a}_3|0\rangle\langle 0|\,\mathrm{tr}\left(|01\rangle\langle 11|\right)+$$
$$+a_1\tilde{a}_4|0\rangle\langle 1|\,\mathrm{tr}\left(|01\rangle\langle 00|\right)+a_1\tilde{a}_5|0\rangle\langle 1|\,\mathrm{tr}\left(|01\rangle\langle 01|\right)+$$
$$+a_1\tilde{a}_6|0\rangle\langle 1|\,\mathrm{tr}\left(|01\rangle\langle 10|\right)+a_1\tilde{a}_7|0\rangle\langle 1|\,\mathrm{tr}\left(|01\rangle\langle 11|\right)+$$

$$
\begin{aligned}
&+a_2\tilde{a}_0\,|0\rangle\langle 0|\operatorname{tr}\big(|10\rangle\langle 00|\big)+a_2\tilde{a}_1\,|0\rangle\langle 0|\operatorname{tr}\big(|10\rangle\langle 01|\big)+\\
&+a_2\tilde{a}_2\,|0\rangle\langle 0|\operatorname{tr}\big(|10\rangle\langle 10|\big)+a_2\tilde{a}_3\,|0\rangle\langle 0|\operatorname{tr}\big(|10\rangle\langle 11|\big)+\\
&+a_2\tilde{a}_4\,|0\rangle\langle 1|\operatorname{tr}\big(|10\rangle\langle 00|\big)+a_2\tilde{a}_5\,|0\rangle\langle 1|\operatorname{tr}\big(|10\rangle\langle 01|\big)+\\
&+a_2\tilde{a}_6\,|0\rangle\langle 1|\operatorname{tr}\big(|10\rangle\langle 10|\big)+a_2\tilde{a}_7\,|0\rangle\langle 1|\operatorname{tr}\big(|10\rangle\langle 11|\big)+\\
&+a_3\tilde{a}_0\,|0\rangle\langle 0|\operatorname{tr}\big(|11\rangle\langle 00|\big)+a_3\tilde{a}_1\,|0\rangle\langle 0|\operatorname{tr}\big(|11\rangle\langle 01|\big)+\\
&+a_3\tilde{a}_2\,|0\rangle\langle 0|\operatorname{tr}\big(|11\rangle\langle 10|\big)+a_3\tilde{a}_3\,|0\rangle\langle 0|\operatorname{tr}\big(|11\rangle\langle 11|\big)+\\
&+a_3\tilde{a}_4\,|0\rangle\langle 1|\operatorname{tr}\big(|11\rangle\langle 00|\big)+a_3\tilde{a}_5\,|0\rangle\langle 1|\operatorname{tr}\big(|11\rangle\langle 01|\big)+\\
&+a_3\tilde{a}_6\,|0\rangle\langle 1|\operatorname{tr}\big(|11\rangle\langle 10|\big)+a_3\tilde{a}_7\,|0\rangle\langle 1|\operatorname{tr}\big(|11\rangle\langle 11|\big)+\\
&+a_4\tilde{a}_0\,|1\rangle\langle 0|\operatorname{tr}\big(|00\rangle\langle 00|\big)+a_4\tilde{a}_1\,|1\rangle\langle 0|\operatorname{tr}\big(|00\rangle\langle 01|\big)+\\
&+a_4\tilde{a}_2\,|1\rangle\langle 0|\operatorname{tr}\big(|00\rangle\langle 10|\big)+a_4\tilde{a}_3\,|1\rangle\langle 0|\operatorname{tr}\big(|00\rangle\langle 11|\big)+\\
&+a_4\tilde{a}_4\,|1\rangle\langle 1|\operatorname{tr}\big(|00\rangle\langle 00|\big)+a_4\tilde{a}_5\,|1\rangle\langle 1|\operatorname{tr}\big(|00\rangle\langle 01|\big)+\\
&+a_4\tilde{a}_6\,|1\rangle\langle 1|\operatorname{tr}\big(|00\rangle\langle 10|\big)+a_4\tilde{a}_7\,|1\rangle\langle 1|\operatorname{tr}\big(|00\rangle\langle 11|\big)+\\
&+a_5\tilde{a}_0\,|1\rangle\langle 0|\operatorname{tr}\big(|01\rangle\langle 00|\big)+a_5\tilde{a}_1\,|1\rangle\langle 0|\operatorname{tr}\big(|01\rangle\langle 01|\big)+\\
&+a_5\tilde{a}_2\,|1\rangle\langle 0|\operatorname{tr}\big(|01\rangle\langle 10|\big)+a_5\tilde{a}_3\,|1\rangle\langle 0|\operatorname{tr}\big(|01\rangle\langle 11|\big)+\\
&+a_5\tilde{a}_4\,|1\rangle\langle 1|\operatorname{tr}\big(|01\rangle\langle 00|\big)+a_5\tilde{a}_5\,|1\rangle\langle 1|\operatorname{tr}\big(|01\rangle\langle 01|\big)+\\
&+a_5\tilde{a}_6\,|1\rangle\langle 1|\operatorname{tr}\big(|01\rangle\langle 10|\big)+a_5\tilde{a}_7\,|1\rangle\langle 1|\operatorname{tr}\big(|01\rangle\langle 11|\big)+\\
&+a_6\tilde{a}_0\,|1\rangle\langle 0|\operatorname{tr}\big(|10\rangle\langle 00|\big)+a_6\tilde{a}_1\,|1\rangle\langle 0|\operatorname{tr}\big(|10\rangle\langle 01|\big)+\\
&+a_6\tilde{a}_2\,|1\rangle\langle 0|\operatorname{tr}\big(|10\rangle\langle 10|\big)+a_6\tilde{a}_3\,|1\rangle\langle 0|\operatorname{tr}\big(|10\rangle\langle 11|\big)+\\
&+a_6\tilde{a}_4\,|1\rangle\langle 1|\operatorname{tr}\big(|10\rangle\langle 00|\big)+a_6\tilde{a}_5\,|1\rangle\langle 1|\operatorname{tr}\big(|10\rangle\langle 01|\big)+\\
&+a_6\tilde{a}_6\,|1\rangle\langle 1|\operatorname{tr}\big(|10\rangle\langle 10|\big)+a_6\tilde{a}_7\,|1\rangle\langle 1|\operatorname{tr}\big(|10\rangle\langle 11|\big)+\\
&+a_7\tilde{a}_0\,|1\rangle\langle 0|\operatorname{tr}\big(|11\rangle\langle 00|\big)+a_7\tilde{a}_1\,|1\rangle\langle 0|\operatorname{tr}\big(|11\rangle\langle 01|\big)+\\
&+a_7\tilde{a}_2\,|1\rangle\langle 0|\operatorname{tr}\big(|11\rangle\langle 10|\big)+a_7\tilde{a}_3\,|1\rangle\langle 0|\operatorname{tr}\big(|11\rangle\langle 11|\big)+\\
&+a_7\tilde{a}_4\,|1\rangle\langle 1|\operatorname{tr}\big(|11\rangle\langle 00|\big)+a_7\tilde{a}_5\,|1\rangle\langle 1|\operatorname{tr}\big(|11\rangle\langle 01|\big)+\\
&+a_7\tilde{a}_6\,|1\rangle\langle 1|\operatorname{tr}\big(|11\rangle\langle 10|\big)+a_7\tilde{a}_7\,|1\rangle\langle 1|\operatorname{tr}\big(|11\rangle\langle 11|\big).
\end{aligned}
\tag{2.3.10}
$$

Учитывая, что при условии $b_1 \neq b_2$ справедливо равенство

$$\mathrm{tr}\left(|b_1\rangle\langle b_2|\right) = 0$$

(где $b_1,\ b_2 \in \{00,\ 01,\ 10,\ 11\}$), из (2.3.10) получаем

$$\begin{aligned}
&\mathrm{tr}_{\mathrm{BC}}\left(\rho^{(\mathrm{ABC})}\right) = \\
&= a_0\tilde{a}_0\,|0\rangle\langle 0|\,\mathrm{tr}\left(|00\rangle\langle 00|\right) + a_0\tilde{a}_4\,|0\rangle\langle 1|\,\mathrm{tr}\left(|00\rangle\langle 00|\right) + \\
&+ a_1\tilde{a}_1\,|0\rangle\langle 0|\,\mathrm{tr}\left(|01\rangle\langle 01|\right) + a_1\tilde{a}_5\,|0\rangle\langle 1|\,\mathrm{tr}\left(|01\rangle\langle 01|\right) + \\
&+ a_2\tilde{a}_2\,|0\rangle\langle 0|\,\mathrm{tr}\left(|10\rangle\langle 10|\right) + a_2\tilde{a}_6\,|0\rangle\langle 1|\,\mathrm{tr}\left(|10\rangle\langle 10|\right) + \\
&+ a_3\tilde{a}_3\,|0\rangle\langle 0|\,\mathrm{tr}\left(|11\rangle\langle 11|\right) + a_3\tilde{a}_7\,|0\rangle\langle 1|\,\mathrm{tr}\left(|11\rangle\langle 11|\right) + \\
&+ a_4\tilde{a}_0\,|1\rangle\langle 0|\,\mathrm{tr}\left(|00\rangle\langle 00|\right) + a_4\tilde{a}_4\,|1\rangle\langle 1|\,\mathrm{tr}\left(|00\rangle\langle 00|\right) + \\
&+ a_5\tilde{a}_1\,|1\rangle\langle 0|\,\mathrm{tr}\left(|01\rangle\langle 01|\right) + a_5\tilde{a}_5\,|1\rangle\langle 1|\,\mathrm{tr}\left(|01\rangle\langle 01|\right) + \\
&+ a_6\tilde{a}_2\,|1\rangle\langle 0|\,\mathrm{tr}\left(|10\rangle\langle 10|\right) + a_6\tilde{a}_6\,|1\rangle\langle 1|\,\mathrm{tr}\left(|10\rangle\langle 10|\right) + \\
&+ a_7\tilde{a}_3\,|1\rangle\langle 0|\,\mathrm{tr}\left(|11\rangle\langle 11|\right) + a_7\tilde{a}_7\,|1\rangle\langle 1|\,\mathrm{tr}\left(|11\rangle\langle 11|\right).
\end{aligned} \tag{2.3.11}$$

В силу того, что

$$\mathrm{tr}\left(|00\rangle\langle 00|\right) = \mathrm{tr}\left(|01\rangle\langle 01|\right) = \mathrm{tr}\left(|10\rangle\langle 10|\right) = \mathrm{tr}\left(|11\rangle\langle 11|\right) = 1,$$

из (2.3.11) получаем

$$\begin{aligned}
&\mathrm{tr}_{\mathrm{BC}}\left(\rho^{(\mathrm{ABC})}\right) = \\
&= a_0\tilde{a}_0\,|0\rangle\langle 0| + a_0\tilde{a}_4\,|0\rangle\langle 1| + a_1\tilde{a}_1\,|0\rangle\langle 0| + a_1\tilde{a}_5\,|0\rangle\langle 1| + \\
&+ a_2\tilde{a}_2\,|0\rangle\langle 0| + a_2\tilde{a}_6\,|0\rangle\langle 1| + a_3\tilde{a}_3\,|0\rangle\langle 0| + a_3\tilde{a}_7\,|0\rangle\langle 1| + \\
&+ a_4\tilde{a}_0\,|1\rangle\langle 0| + a_4\tilde{a}_4\,|1\rangle\langle 1| + a_5\tilde{a}_1\,|1\rangle\langle 0| + a_5\tilde{a}_5\,|1\rangle\langle 1| + \\
&+ a_6\tilde{a}_2\,|1\rangle\langle 0| + a_6\tilde{a}_6\,|1\rangle\langle 1| + a_7\tilde{a}_3\,|1\rangle\langle 0| + a_7\tilde{a}_7\,|1\rangle\langle 1| = \\
&= \begin{pmatrix} |a_0|^2 + |a_1|^2 + |a_2|^2 + |a_3|^2 & a_0\tilde{a}_4 + a_1\tilde{a}_5 + a_2\tilde{a}_6 + a_3\tilde{a}_7 \\ a_4\tilde{a}_0 + a_5\tilde{a}_1 + a_6\tilde{a}_2 + a_7\tilde{a}_3 & |a_4|^2 + |a_5|^2 + |a_6|^2 + |a_7|^2 \end{pmatrix}.
\end{aligned} \tag{2.3.12}$$

Из (2.3.7) и (2.3.12) следует, что

$$\rho^{(\mathrm{A})} = \rho_{\mathrm{A}}^{(\mathrm{ABC})} = \mathrm{tr}_{\mathrm{BC}}\left(\rho^{(\mathrm{ABC})}\right) =$$
$$= \begin{pmatrix} |a_0|^2 + |a_1|^2 + |a_2|^2 + |a_3|^2 & a_0\tilde{a}_4 + a_1\tilde{a}_5 + a_2\tilde{a}_6 + a_3\tilde{a}_7 \\ a_4\tilde{a}_0 + a_5\tilde{a}_1 + a_6\tilde{a}_2 + a_7\tilde{a}_3 & |a_4|^2 + |a_5|^2 + |a_6|^2 + |a_7|^2 \end{pmatrix}. \qquad (2.3.13)$$

Из (2.3.13) и равенства (2.3.6) следует, что

$$1 = \mathrm{tr}\left(\left(\rho^{(\mathrm{A})}\right)^2\right) =$$
$$= \left[\left(|a_0|^2 + |a_1|^2 + |a_2|^2 + |a_3|^2\right)^2 +\right.$$
$$+\left(a_0\tilde{a}_4 + a_1\tilde{a}_5 + a_2\tilde{a}_6 + a_3\tilde{a}_7\right)\left(a_4\tilde{a}_0 + a_5\tilde{a}_1 + a_6\tilde{a}_2 + a_7\tilde{a}_3\right)] +$$
$$+[\left(a_4\tilde{a}_0 + a_5\tilde{a}_1 + a_6\tilde{a}_2 + a_7\tilde{a}_3\right)\left(a_0\tilde{a}_4 + a_1\tilde{a}_5 + a_2\tilde{a}_6 + a_3\tilde{a}_7\right) +$$
$$\left.+\left(|a_4|^2 + |a_5|^2 + |a_6|^2 + |a_7|^2\right)^2\right] =$$
$$= |a_0|^4 + |a_1|^4 + |a_2|^4 + |a_3|^4 + |a_4|^4 + |a_5|^4 + |a_6|^4 + |a_7|^4 +$$
$$+2(|a_0|^2|a_4|^2 + \tilde{a}_0a_1a_4\tilde{a}_5 + \tilde{a}_0a_2a_4\tilde{a}_6 + \tilde{a}_0a_3a_4\tilde{a}_7 +$$
$$+a_0\tilde{a}_1\tilde{a}_4a_5 + |a_1|^2|a_5|^2 + \tilde{a}_1a_2a_5\tilde{a}_6 + \tilde{a}_1a_3a_5\tilde{a}_7 +$$
$$+a_0\tilde{a}_2\tilde{a}_4a_6 + a_1\tilde{a}_2\tilde{a}_5a_6 + |a_2|^2|a_6|^2 + \tilde{a}_2a_3a_6\tilde{a}_7 +$$
$$+a_0\tilde{a}_3\tilde{a}_4a_7 + a_1\tilde{a}_3\tilde{a}_5a_7 + a_2\tilde{a}_3\tilde{a}_6a_7 + |a_3|^2|a_7|^2 +$$
$$+|a_0|^2|a_1|^2 + |a_0|^2|a_2|^2 + |a_0|^2|a_3|^2 + |a_1|^2|a_2|^2 + |a_1|^2|a_3|^2 + |a_2|^2|a_3|^2 +$$
$$+|a_4|^2|a_5|^2 + |a_4|^2|a_6|^2 + |a_4|^2|a_7|^2 + |a_5|^2|a_6|^2 + |a_5|^2|a_7|^2 + |a_6|^2|a_7|^2) =$$
$$= \left(|a_0|^2 + |a_1|^2 + |a_2|^2 + |a_3|^2 + |a_4|^2 + |a_5|^2 + |a_6|^2 + |a_7|^2\right)^2 +$$
$$+2(\tilde{a}_0a_1a_4\tilde{a}_5 + \tilde{a}_0a_2a_4\tilde{a}_6 + \tilde{a}_0a_3a_4\tilde{a}_7 + a_0\tilde{a}_1\tilde{a}_4a_5 + \tilde{a}_1a_2a_5\tilde{a}_6 + \tilde{a}_1a_3a_5\tilde{a}_7 +$$
$$+a_0\tilde{a}_2\tilde{a}_4a_6 + a_1\tilde{a}_2\tilde{a}_5a_6 + \tilde{a}_2a_3a_6\tilde{a}_7 + a_0\tilde{a}_3\tilde{a}_4a_7 + a_1\tilde{a}_3\tilde{a}_5a_7 + a_2\tilde{a}_3\tilde{a}_6a_7 -$$
$$-|a_0|^2|a_5|^2 - |a_0|^2|a_6|^2 - |a_0|^2|a_7|^2 - |a_1|^2|a_4|^2 - |a_1|^2|a_6|^2 - |a_1|^2|a_7|^2 -$$
$$-|a_2|^2|a_4|^2 - |a_2|^2|a_5|^2 - |a_2|^2|a_7|^2 - |a_3|^2|a_4|^2 - |a_3|^2|a_5|^2 - |a_3|^2|a_6|^2) =$$
$$= 1 + 2(\tilde{a}_0a_1a_4\tilde{a}_5 + \tilde{a}_0a_2a_4\tilde{a}_6 + \tilde{a}_0a_3a_4\tilde{a}_7 + a_0\tilde{a}_1\tilde{a}_4a_5 + \tilde{a}_1a_2a_5\tilde{a}_6 + \tilde{a}_1a_3a_5\tilde{a}_7 +$$
$$+a_0\tilde{a}_2\tilde{a}_4a_6 + a_1\tilde{a}_2\tilde{a}_5a_6 + \tilde{a}_2a_3a_6\tilde{a}_7 + a_0\tilde{a}_3\tilde{a}_4a_7 + a_1\tilde{a}_3\tilde{a}_5a_7 + a_2\tilde{a}_3\tilde{a}_6a_7 -$$

$$-|a_0|^2|a_5|^2-|a_0|^2|a_6|^2-|a_0|^2|a_7|^2-|a_1|^2|a_4|^2-|a_1|^2|a_6|^2-|a_1|^2|a_7|^2-$$
$$-|a_2|^2|a_4|^2-|a_2|^2|a_5|^2-|a_2|^2|a_7|^2-|a_3|^2|a_4|^2-|a_3|^2|a_5|^2-|a_3|^2|a_6|^2\Big). \tag{2.3.14}$$

Удалив слагаемые, равные 1, из первой и последней частей цепочки равенств (2.3.14), получаем

$$0=2(\tilde{a}_0a_1a_4\tilde{a}_5+\tilde{a}_0a_2a_4\tilde{a}_6+\tilde{a}_0a_3a_4\tilde{a}_7+a_0\tilde{a}_1\tilde{a}_4a_5+\tilde{a}_1a_2a_5\tilde{a}_6+\tilde{a}_1a_3a_5\tilde{a}_7+$$
$$+a_0\tilde{a}_2\tilde{a}_4a_6+a_1\tilde{a}_2\tilde{a}_5a_6+\tilde{a}_2a_3a_6\tilde{a}_7+a_0\tilde{a}_3\tilde{a}_4a_7+a_1\tilde{a}_3\tilde{a}_5a_7+a_2\tilde{a}_3\tilde{a}_6a_7-$$
$$-|a_0|^2|a_5|^2-|a_0|^2|a_6|^2-|a_0|^2|a_7|^2-|a_1|^2|a_4|^2-|a_1|^2|a_6|^2-|a_1|^2|a_7|^2-$$
$$-|a_2|^2|a_4|^2-|a_2|^2|a_5|^2-|a_2|^2|a_7|^2-|a_3|^2|a_4|^2-|a_3|^2|a_5|^2-|a_3|^2|a_6|^2).$$

Поделив обе части последнего равенства на число (–2), получаем

$$|a_0|^2|a_5|^2+|a_0|^2|a_6|^2+|a_0|^2|a_7|^2+|a_1|^2|a_4|^2+|a_1|^2|a_6|^2+|a_1|^2|a_7|^2+$$
$$+|a_2|^2|a_4|^2+|a_2|^2|a_5|^2+|a_2|^2|a_7|^2+|a_3|^2|a_4|^2+|a_3|^2|a_5|^2+|a_3|^2|a_6|^2-$$
$$-\tilde{a}_0a_1a_4\tilde{a}_5-\tilde{a}_0a_2a_4\tilde{a}_6-\tilde{a}_0a_3a_4\tilde{a}_7-a_0\tilde{a}_1\tilde{a}_4a_5-\tilde{a}_1a_2a_5\tilde{a}_6-\tilde{a}_1a_3a_5\tilde{a}_7-$$
$$-a_0\tilde{a}_2\tilde{a}_4a_6-a_1\tilde{a}_2\tilde{a}_5a_6-\tilde{a}_2a_3a_6\tilde{a}_7-a_0\tilde{a}_3\tilde{a}_4a_7-a_1\tilde{a}_3\tilde{a}_5a_7-a_2\tilde{a}_3\tilde{a}_6a_7.$$

Группируя слагаемые и вычитаемые в левой части данного равенства и вынося общие сомножители за скобки, имеем

$$\left(a_0a_5-a_1a_4\right)\left(\tilde{a}_0\tilde{a}_5-\tilde{a}_1\tilde{a}_4\right)+\left(a_0a_6-a_2a_4\right)\left(\tilde{a}_0\tilde{a}_6-\tilde{a}_2\tilde{a}_4\right)+$$
$$+\left(a_0a_7-a_3a_4\right)\left(\tilde{a}_0\tilde{a}_7-\tilde{a}_3\tilde{a}_4\right)+\left(a_1a_6-a_2a_5\right)\left(\tilde{a}_1\tilde{a}_6-\tilde{a}_2\tilde{a}_5\right)+$$
$$+\left(a_1a_7-a_3a_5\right)\left(\tilde{a}_1\tilde{a}_7-\tilde{a}_3\tilde{a}_5\right)+\left(a_2a_7-a_3a_6\right)\left(\tilde{a}_2\tilde{a}_7-\tilde{a}_3\tilde{a}_6\right)=0.$$

Заметив, что пара сомножителей в каждом из шести слагаемых левой части данного равенства являются взаимно сопряженными комплексными числами, получаем

$$|a_0a_5-a_1a_4|^2+|a_0a_6-a_2a_4|^2+|a_0a_7-a_3a_4|^2+$$
$$+|a_1a_6-a_2a_5|^2+|a_1a_7-a_3a_5|^2+|a_2a_7-a_3a_6|^2=0.$$

Отсюда, с учетом (2.3.3), имеем

$$|V_1|^2+|V_2|^2+|V_3|^2+|V_4|^2+|V_5|^2+|V_6|^2=0\,,$$

что равносильно выполнению цепочки равенств

$$V_1=V_2=V_3=V_4=V_5=V_6=0\,.$$

Пункт (а) утверждения 2.3.4 в одну сторону доказан.

Обратно, пусть

$$V_1=V_2=V_3=V_4=V_5=V_6=0\,.$$

Тогда

$$|V_1|^2+|V_2|^2+|V_3|^2+|V_4|^2+|V_5|^2+|V_6|^2=0\,,$$

что, учитывая (2.3.3), равносильно равенству

$$\begin{aligned}
&(a_0a_5-a_1a_4)(\tilde a_0\tilde a_5-\tilde a_1\tilde a_4)+(a_0a_6-a_2a_4)(\tilde a_0\tilde a_6-\tilde a_2\tilde a_4)+\\
&+(a_0a_7-a_3a_4)(\tilde a_0\tilde a_7-\tilde a_3\tilde a_4)+(a_1a_6-a_2a_5)(\tilde a_1\tilde a_6-\tilde a_2\tilde a_5)+\\
&+(a_1a_7-a_3a_5)(\tilde a_1\tilde a_7-\tilde a_3\tilde a_5)+(a_2a_7-a_3a_6)(\tilde a_2\tilde a_7-\tilde a_3\tilde a_6)=0.
\end{aligned}$$

Раскрыв скобки в левой части последнего равенства, получаем

$$\begin{aligned}
&|a_0|^2|a_5|^2+|a_0|^2|a_6|^2+|a_0|^2|a_7|^2+|a_1|^2|a_4|^2+|a_1|^2|a_6|^2+|a_1|^2|a_7|^2+\\
&+|a_2|^2|a_4|^2+|a_2|^2|a_5|^2+|a_2|^2|a_7|^2+|a_3|^2|a_4|^2+|a_3|^2|a_5|^2+|a_3|^2|a_6|^2-\\
&-\tilde a_0a_1a_4\tilde a_5-\tilde a_0a_2a_4\tilde a_6-\tilde a_0a_3a_4\tilde a_7-a_0\tilde a_1\tilde a_4a_5-\tilde a_1a_2a_5\tilde a_6-\tilde a_1a_3a_5\tilde a_7-\\
&-a_0\tilde a_2\tilde a_4a_6-a_1\tilde a_2\tilde a_5a_6-\tilde a_2a_3a_6\tilde a_7-a_0\tilde a_3\tilde a_4a_7-a_1\tilde a_3\tilde a_5a_7-a_2\tilde a_3\tilde a_6a_7=0.
\end{aligned}$$

Помножив на (–2) обе части последнего равенства и к обеим частям получившегося равенства прибавив по 1, имеем

$$\begin{aligned}
&1+2(\tilde a_0a_1a_4\tilde a_5+\tilde a_0a_2a_4\tilde a_6+\tilde a_0a_3a_4\tilde a_7+a_0\tilde a_1\tilde a_4a_5+\tilde a_1a_2a_5\tilde a_6+\tilde a_1a_3a_5\tilde a_7+\\
&+a_0\tilde a_2\tilde a_4a_6+a_1\tilde a_2\tilde a_5a_6+\tilde a_2a_3a_6\tilde a_7+a_0\tilde a_3\tilde a_4a_7+a_1\tilde a_3\tilde a_5a_7+a_2\tilde a_3\tilde a_6a_7-\\
&-|a_0|^2|a_5|^2-|a_0|^2|a_6|^2-|a_0|^2|a_7|^2-|a_1|^2|a_4|^2-|a_1|^2|a_6|^2-|a_1|^2|a_7|^2-\\
&-|a_2|^2|a_4|^2-|a_2|^2|a_5|^2-|a_2|^2|a_7|^2-|a_3|^2|a_4|^2-|a_3|^2|a_5|^2-|a_3|^2|a_6|^2)=1.
\end{aligned}$$

Отсюда, учитывая (2.3.2), получаем

$$\left(|a_0|^2+|a_1|^2+|a_2|^2+|a_3|^2+|a_4|^2+|a_5|^2+|a_6|^2+|a_7|^2\right)^2+$$
$$+2(\tilde a_0 a_1 a_4 \tilde a_5+\tilde a_0 a_2 a_4 \tilde a_6+\tilde a_0 a_3 a_4 \tilde a_7+a_0 \tilde a_1 \tilde a_4 a_5+\tilde a_1 a_2 a_5 \tilde a_6+\tilde a_1 a_3 a_5 \tilde a_7+$$
$$+a_0 \tilde a_2 \tilde a_4 a_6+a_1 \tilde a_2 \tilde a_5 a_6+\tilde a_2 a_3 a_6 \tilde a_7+a_0 \tilde a_3 \tilde a_4 a_7+a_1 \tilde a_3 \tilde a_5 a_7+a_2 \tilde a_3 \tilde a_6 a_7-$$
$$-|a_0|^2|a_5|^2-|a_0|^2|a_6|^2-|a_0|^2|a_7|^2-|a_1|^2|a_4|^2-|a_1|^2|a_6|^2-|a_1|^2|a_7|^2-$$
$$-|a_2|^2|a_4|^2-|a_2|^2|a_5|^2-|a_2|^2|a_7|^2-|a_3|^2|a_4|^2-|a_3|^2|a_5|^2-|a_3|^2|a_6|^2)=1. \tag{2.3.15}$$

Далее, проводя вычисления, аналогичные вычислениям в равенствах (2.3.9) – (2.3.12), из равенства (2.3.8) получаем редуцированную матрицу плотности подсистемы A квантовой системы ABC:

$$\rho_{\mathrm{A}}^{(\mathrm{ABC})}=\mathrm{tr}_{\mathrm{BC}}\left(\rho^{(\mathrm{ABC})}\right)=$$
$$=\begin{pmatrix} |a_0|^2+|a_1|^2+|a_2|^2+|a_3|^2 & a_0\tilde a_4+a_1\tilde a_5+a_2\tilde a_6+a_3\tilde a_7 \\ a_4\tilde a_0+a_5\tilde a_1+a_6\tilde a_2+a_7\tilde a_3 & |a_4|^2+|a_5|^2+|a_6|^2+|a_7|^2 \end{pmatrix}.$$

Теперь вычислим след от квадрата матрицы $\rho_{\mathrm{A}}^{(\mathrm{ABC})}$:

$$\mathrm{tr}\left(\left(\rho_{\mathrm{A}}^{(\mathrm{ABC})}\right)^2\right)=$$
$$=\Big[\left(|a_0|^2+|a_1|^2+|a_2|^2+|a_3|^2\right)^2+$$
$$+\left(a_0\tilde a_4+a_1\tilde a_5+a_2\tilde a_6+a_3\tilde a_7\right)\left(a_4\tilde a_0+a_5\tilde a_1+a_6\tilde a_2+a_7\tilde a_3\right)\Big]+$$
$$+\Big[\left(a_4\tilde a_0+a_5\tilde a_1+a_6\tilde a_2+a_7\tilde a_3\right)\left(a_0\tilde a_4+a_1\tilde a_5+a_2\tilde a_6+a_3\tilde a_7\right)+$$
$$+\left(|a_4|^2+|a_5|^2+|a_6|^2+|a_7|^2\right)^2\Big]=$$
$$=\left(|a_0|^2+|a_1|^2+|a_2|^2+|a_3|^2+|a_4|^2+|a_5|^2+|a_6|^2+|a_7|^2\right)^2+$$
$$+2(\tilde a_0 a_1 a_4 \tilde a_5+\tilde a_0 a_2 a_4 \tilde a_6+\tilde a_0 a_3 a_4 \tilde a_7+a_0 \tilde a_1 \tilde a_4 a_5+\tilde a_1 a_2 a_5 \tilde a_6+\tilde a_1 a_3 a_5 \tilde a_7+$$
$$+a_0 \tilde a_2 \tilde a_4 a_6+a_1 \tilde a_2 \tilde a_5 a_6+\tilde a_2 a_3 a_6 \tilde a_7+a_0 \tilde a_3 \tilde a_4 a_7+a_1 \tilde a_3 \tilde a_5 a_7+a_2 \tilde a_3 \tilde a_6 a_7-$$
$$-|a_0|^2|a_5|^2-|a_0|^2|a_6|^2-|a_0|^2|a_7|^2-|a_1|^2|a_4|^2-|a_1|^2|a_6|^2-|a_1|^2|a_7|^2-$$
$$-|a_2|^2|a_4|^2-|a_2|^2|a_5|^2-|a_2|^2|a_7|^2-|a_3|^2|a_4|^2-|a_3|^2|a_5|^2-|a_3|^2|a_6|^2). \tag{2.3.16}$$

Из равенств (2.3.15) и (2.3.16) следует справедливость равенства

$$\mathrm{tr}\left(\left(\rho_{\mathrm{A}}^{(\mathrm{ABC})}\right)^2\right)=1,$$

которое в соответствии с результатами, представленными в работе [50], равносильно тому, что состояние подсистемы A квантовой системы ABC является чистым состоянием. Тогда в силу того, что состояние $|\psi\rangle$ квантовой системы ABC является чистым состоянием, имеем, что состояние подсистемы BC также является чистым. Следовательно, состояние $|\psi\rangle$ квантовой системы ABC представляется в виде тензорного произведения, так как соответствующие состояния $|\psi_1\rangle$ и $|\psi_{23}\rangle$ ее подсистем A и BC являются чистыми состояниями и, следовательно, они описываются некоторыми нормированными векторами $|\psi_1\rangle$ и $|\psi_{23}\rangle$, тензорное произведение $|\psi_1\rangle\otimes|\psi_{23}\rangle$ которых совпадает с вектором $|\psi\rangle$.

Доказательство пункта (а) утверждения 2.3.4 завершено.

Докажем теперь пункт (б) утверждения 2.3.4.

Пусть $|\psi\rangle$ – чистое состояние трехкубитной квантовой системы ABC и

$$|\psi\rangle=|\psi_{12}\rangle\otimes|\psi_3\rangle,$$

где $|\psi_{12}\rangle$ – чистое состояние двухкубитной квантовой системы AB, $|\psi_3\rangle$ – чистое состояние однокубитной квантовой системы C. Отсюда в соответствии с [50] следует, что редуцированная матрица плотности $\rho_{\mathrm{C}}^{(\mathrm{ABC})}$ подсистемы C совпадает с матрицей плотности $\rho^{(\mathrm{C})}$ подсистемы C и при этом выполняется равенство

$$\mathrm{tr}\left(\left(\rho^{(\mathrm{C})}\right)^2\right)=1. \qquad (2.3.17)$$

Вычислим матрицу $\rho^{(\mathrm{C})}$ путем использования представления (2.3.1) и с учетом ее совпадения с редуцированной матрицей плотности $\rho_{\mathrm{C}}^{(\mathrm{ABC})}$.

Для матрицы $\rho^{(\mathrm{C})}$ справедлива следующая цепочка равенств:

$$\rho^{(\mathrm{C})} = \rho_{\mathrm{C}}^{(\mathrm{ABC})} = \mathrm{tr}_{\mathrm{AB}}\left(\rho^{(\mathrm{ABC})}\right). \tag{2.3.18}$$

Для матрицы плотности $\rho^{(\mathrm{ABC})}$ справедлива следующая цепочка равенств, во многом аналогичная цепочке равенств (2.3.8):

$$\rho^{(\mathrm{ABC})} = |\psi\rangle\langle\psi| =$$

$$= \left(a_0\tilde{a}_0|00\rangle\langle 00|\otimes|0\rangle\langle 0| + a_0\tilde{a}_1|00\rangle\langle 00|\otimes|0\rangle\langle 1| + a_0\tilde{a}_2|00\rangle\langle 01|\otimes|0\rangle\langle 0| +\right.$$
$$+ a_0\tilde{a}_3|00\rangle\langle 01|\otimes|0\rangle\langle 1| + a_0\tilde{a}_4|00\rangle\langle 10|\otimes|0\rangle\langle 0| + a_0\tilde{a}_5|00\rangle\langle 10|\otimes|0\rangle\langle 1| +$$
$$\left. + a_0\tilde{a}_6|00\rangle\langle 11|\otimes|0\rangle\langle 0| + a_0\tilde{a}_7|00\rangle\langle 11|\otimes|0\rangle\langle 1|\right) +$$
$$+ \left(a_1\tilde{a}_0|00\rangle\langle 00|\otimes|1\rangle\langle 0| + a_1\tilde{a}_1|00\rangle\langle 00|\otimes|1\rangle\langle 1| + a_1\tilde{a}_2|00\rangle\langle 01|\otimes|1\rangle\langle 0| +\right.$$
$$+ a_1\tilde{a}_3|00\rangle\langle 01|\otimes|1\rangle\langle 1| + a_1\tilde{a}_4|00\rangle\langle 10|\otimes|1\rangle\langle 0| + a_1\tilde{a}_5|00\rangle\langle 10|\otimes|1\rangle\langle 1| +$$
$$\left. + a_1\tilde{a}_6|00\rangle\langle 11|\otimes|1\rangle\langle 0| + a_1\tilde{a}_7|00\rangle\langle 11|\otimes|1\rangle\langle 1|\right) +$$
$$+ \left(a_2\tilde{a}_0|01\rangle\langle 00|\otimes|0\rangle\langle 0| + a_2\tilde{a}_1|01\rangle\langle 00|\otimes|0\rangle\langle 1| + a_2\tilde{a}_2|01\rangle\langle 01|\otimes|0\rangle\langle 0| +\right.$$
$$+ a_2\tilde{a}_3|01\rangle\langle 01|\otimes|0\rangle\langle 1| + a_2\tilde{a}_4|01\rangle\langle 10|\otimes|0\rangle\langle 0| + a_2\tilde{a}_5|01\rangle\langle 10|\otimes|0\rangle\langle 1| +$$
$$\left. + a_2\tilde{a}_6|01\rangle\langle 11|\otimes|0\rangle\langle 0| + a_2\tilde{a}_7|01\rangle\langle 11|\otimes|0\rangle\langle 1|\right) +$$
$$+ \left(a_3\tilde{a}_0|01\rangle\langle 00|\otimes|1\rangle\langle 0| + a_3\tilde{a}_1|01\rangle\langle 00|\otimes|1\rangle\langle 1| + a_3\tilde{a}_2|01\rangle\langle 01|\otimes|1\rangle\langle 0| +\right.$$
$$+ a_3\tilde{a}_3|01\rangle\langle 01|\otimes|1\rangle\langle 1| + a_3\tilde{a}_4|01\rangle\langle 10|\otimes|1\rangle\langle 0| + a_3\tilde{a}_5|01\rangle\langle 10|\otimes|1\rangle\langle 1| +$$
$$\left. + a_3\tilde{a}_6|01\rangle\langle 11|\otimes|1\rangle\langle 0| + a_3\tilde{a}_7|01\rangle\langle 11|\otimes|1\rangle\langle 1|\right) +$$
$$+ \left(a_4\tilde{a}_0|10\rangle\langle 00|\otimes|0\rangle\langle 0| + a_4\tilde{a}_1|10\rangle\langle 00|\otimes|0\rangle\langle 1| + a_4\tilde{a}_2|10\rangle\langle 01|\otimes|0\rangle\langle 0| +\right.$$
$$+ a_4\tilde{a}_3|10\rangle\langle 01|\otimes|0\rangle\langle 1| + a_4\tilde{a}_4|10\rangle\langle 10|\otimes|0\rangle\langle 0| + a_4\tilde{a}_5|10\rangle\langle 10|\otimes|0\rangle\langle 1| +$$
$$\left. + a_4\tilde{a}_6|10\rangle\langle 11|\otimes|0\rangle\langle 0| + a_4\tilde{a}_7|10\rangle\langle 11|\otimes|0\rangle\langle 1|\right) +$$
$$+ \left(a_5\tilde{a}_0|10\rangle\langle 00|\otimes|1\rangle\langle 0| + a_5\tilde{a}_1|10\rangle\langle 00|\otimes|1\rangle\langle 1| + a_5\tilde{a}_2|10\rangle\langle 01|\otimes|1\rangle\langle 0| +\right.$$
$$+ a_5\tilde{a}_3|10\rangle\langle 01|\otimes|1\rangle\langle 1| + a_5\tilde{a}_4|10\rangle\langle 10|\otimes|1\rangle\langle 0| + a_5\tilde{a}_5|10\rangle\langle 10|\otimes|1\rangle\langle 1| +$$
$$\left. + a_5\tilde{a}_6|10\rangle\langle 11|\otimes|1\rangle\langle 0| + a_5\tilde{a}_7|10\rangle\langle 11|\otimes|1\rangle\langle 1|\right) +$$
$$+ \left(a_6\tilde{a}_0|11\rangle\langle 00|\otimes|0\rangle\langle 0| + a_6\tilde{a}_1|11\rangle\langle 00|\otimes|0\rangle\langle 1| + a_6\tilde{a}_2|11\rangle\langle 01|\otimes|0\rangle\langle 0| +\right.$$
$$+ a_6\tilde{a}_3|11\rangle\langle 01|\otimes|0\rangle\langle 1| + a_6\tilde{a}_4|11\rangle\langle 10|\otimes|0\rangle\langle 0| + a_6\tilde{a}_5|11\rangle\langle 10|\otimes|0\rangle\langle 1| +$$

$$+a_6\tilde{a}_6|11\rangle\langle 11|\otimes|0\rangle\langle 0|+a_6\tilde{a}_7|11\rangle\langle 11|\otimes|0\rangle\langle 1|)+$$
$$+\big(a_7\tilde{a}_0|11\rangle\langle 00|\otimes|1\rangle\langle 0|+a_7\tilde{a}_1|11\rangle\langle 00|\otimes|1\rangle\langle 1|+a_7\tilde{a}_2|11\rangle\langle 01|\otimes|1\rangle\langle 0|+$$
$$+a_7\tilde{a}_3|11\rangle\langle 01|\otimes|1\rangle\langle 1|+a_7\tilde{a}_4|11\rangle\langle 10|\otimes|1\rangle\langle 0|+a_7\tilde{a}_5|11\rangle\langle 10|\otimes|1\rangle\langle 1|+$$
$$+a_7\tilde{a}_6|11\rangle\langle 11|\otimes|1\rangle\langle 0|+a_7\tilde{a}_7|11\rangle\langle 11|\otimes|1\rangle\langle 1|\big). \qquad (2.3.19)$$

Из (2.3.19), учитывая свойство линейности отображения $\mathrm{tr}_{\mathrm{AB}}$, получаем

$$\mathrm{tr}_{\mathrm{AB}}\left(\rho^{(\mathrm{ABC})}\right)=$$
$$=a_0\tilde{a}_0\mathrm{tr}_{\mathrm{AB}}\left(|00\rangle\langle 00|\otimes|0\rangle\langle 0|\right)+a_0\tilde{a}_1\mathrm{tr}_{\mathrm{AB}}\left(|00\rangle\langle 00|\otimes|0\rangle\langle 1|\right)+$$
$$+a_0\tilde{a}_2\mathrm{tr}_{\mathrm{AB}}\left(|00\rangle\langle 01|\otimes|0\rangle\langle 0|\right)+a_0\tilde{a}_3\mathrm{tr}_{\mathrm{AB}}\left(|00\rangle\langle 01|\otimes|0\rangle\langle 1|\right)+$$
$$+a_0\tilde{a}_4\mathrm{tr}_{\mathrm{AB}}\left(|00\rangle\langle 10|\otimes|0\rangle\langle 0|\right)+a_0\tilde{a}_5\mathrm{tr}_{\mathrm{AB}}\left(|00\rangle\langle 10|\otimes|0\rangle\langle 1|\right)+$$
$$+a_0\tilde{a}_6\mathrm{tr}_{\mathrm{AB}}\left(|00\rangle\langle 11|\otimes|0\rangle\langle 0|\right)+a_0\tilde{a}_7\mathrm{tr}_{\mathrm{AB}}\left(|00\rangle\langle 11|\otimes|0\rangle\langle 1|\right)+$$
$$+a_1\tilde{a}_0\mathrm{tr}_{\mathrm{AB}}\left(|00\rangle\langle 00|\otimes|1\rangle\langle 0|\right)+a_1\tilde{a}_1\mathrm{tr}_{\mathrm{AB}}\left(|00\rangle\langle 00|\otimes|1\rangle\langle 1|\right)+$$
$$+a_1\tilde{a}_2\mathrm{tr}_{\mathrm{AB}}\left(|00\rangle\langle 01|\otimes|1\rangle\langle 0|\right)+a_1\tilde{a}_3\mathrm{tr}_{\mathrm{AB}}\left(|00\rangle\langle 01|\otimes|1\rangle\langle 1|\right)+$$
$$+a_1\tilde{a}_4\mathrm{tr}_{\mathrm{AB}}\left(|00\rangle\langle 10|\otimes|1\rangle\langle 0|\right)+a_1\tilde{a}_5\mathrm{tr}_{\mathrm{AB}}\left(|00\rangle\langle 10|\otimes|1\rangle\langle 1|\right)+$$
$$+a_1\tilde{a}_6\mathrm{tr}_{\mathrm{AB}}\left(|00\rangle\langle 11|\otimes|1\rangle\langle 0|\right)+a_1\tilde{a}_7\mathrm{tr}_{\mathrm{AB}}\left(|00\rangle\langle 11|\otimes|1\rangle\langle 1|\right)+$$
$$+a_2\tilde{a}_0\mathrm{tr}_{\mathrm{AB}}\left(|01\rangle\langle 00|\otimes|0\rangle\langle 0|\right)+a_2\tilde{a}_1\mathrm{tr}_{\mathrm{AB}}\left(|01\rangle\langle 00|\otimes|0\rangle\langle 1|\right)+$$
$$+a_2\tilde{a}_2\mathrm{tr}_{\mathrm{AB}}\left(|01\rangle\langle 01|\otimes|0\rangle\langle 0|\right)+a_2\tilde{a}_3\mathrm{tr}_{\mathrm{AB}}\left(|01\rangle\langle 01|\otimes|0\rangle\langle 1|\right)+$$
$$+a_2\tilde{a}_4\mathrm{tr}_{\mathrm{AB}}\left(|01\rangle\langle 10|\otimes|0\rangle\langle 0|\right)+a_2\tilde{a}_5\mathrm{tr}_{\mathrm{AB}}\left(|01\rangle\langle 10|\otimes|0\rangle\langle 1|\right)+$$
$$+a_2\tilde{a}_6\mathrm{tr}_{\mathrm{AB}}\left(|01\rangle\langle 11|\otimes|0\rangle\langle 0|\right)+a_2\tilde{a}_7\mathrm{tr}_{\mathrm{AB}}\left(|01\rangle\langle 11|\otimes|0\rangle\langle 1|\right)+$$
$$+a_3\tilde{a}_0\mathrm{tr}_{\mathrm{AB}}\left(|01\rangle\langle 00|\otimes|1\rangle\langle 0|\right)+a_3\tilde{a}_1\mathrm{tr}_{\mathrm{AB}}\left(|01\rangle\langle 00|\otimes|1\rangle\langle 1|\right)+$$
$$+a_3\tilde{a}_2\mathrm{tr}_{\mathrm{AB}}\left(|01\rangle\langle 01|\otimes|1\rangle\langle 0|\right)+a_3\tilde{a}_3\mathrm{tr}_{\mathrm{AB}}\left(|01\rangle\langle 01|\otimes|1\rangle\langle 1|\right)+$$
$$+a_3\tilde{a}_4\mathrm{tr}_{\mathrm{AB}}\left(|01\rangle\langle 10|\otimes|1\rangle\langle 0|\right)+a_3\tilde{a}_5\mathrm{tr}_{\mathrm{AB}}\left(|01\rangle\langle 10|\otimes|1\rangle\langle 1|\right)+$$
$$+a_3\tilde{a}_6\mathrm{tr}_{\mathrm{AB}}\left(|01\rangle\langle 11|\otimes|1\rangle\langle 0|\right)+a_3\tilde{a}_7\mathrm{tr}_{\mathrm{AB}}\left(|01\rangle\langle 11|\otimes|1\rangle\langle 1|\right)+$$
$$+a_4\tilde{a}_0\mathrm{tr}_{\mathrm{AB}}\left(|10\rangle\langle 00|\otimes|0\rangle\langle 0|\right)+a_4\tilde{a}_1\mathrm{tr}_{\mathrm{AB}}\left(|10\rangle\langle 00|\otimes|0\rangle\langle 1|\right)+$$
$$+a_4\tilde{a}_2\mathrm{tr}_{\mathrm{AB}}\left(|10\rangle\langle 01|\otimes|0\rangle\langle 0|\right)+a_4\tilde{a}_3\mathrm{tr}_{\mathrm{AB}}\left(|10\rangle\langle 01|\otimes|0\rangle\langle 1|\right)+$$

$$+a_4\tilde{a}_4\mathrm{tr}_{\mathrm{AB}}\left(|10\rangle\langle10|\otimes|0\rangle\langle0|\right)+a_4\tilde{a}_5\mathrm{tr}_{\mathrm{AB}}\left(|10\rangle\langle10|\otimes|0\rangle\langle1|\right)+$$
$$+a_4\tilde{a}_6\mathrm{tr}_{\mathrm{AB}}\left(|10\rangle\langle11|\otimes|0\rangle\langle0|\right)+a_4\tilde{a}_7\mathrm{tr}_{\mathrm{AB}}\left(|10\rangle\langle11|\otimes|0\rangle\langle1|\right)+$$
$$+a_5\tilde{a}_0\mathrm{tr}_{\mathrm{AB}}\left(|10\rangle\langle00|\otimes|1\rangle\langle0|\right)+a_5\tilde{a}_1\mathrm{tr}_{\mathrm{AB}}\left(|10\rangle\langle00|\otimes|1\rangle\langle1|\right)+$$
$$+a_5\tilde{a}_2\mathrm{tr}_{\mathrm{AB}}\left(|10\rangle\langle01|\otimes|1\rangle\langle0|\right)+a_5\tilde{a}_3\mathrm{tr}_{\mathrm{AB}}\left(|10\rangle\langle01|\otimes|1\rangle\langle1|\right)+$$
$$+a_5\tilde{a}_4\mathrm{tr}_{\mathrm{AB}}\left(|10\rangle\langle10|\otimes|1\rangle\langle0|\right)+a_5\tilde{a}_5\mathrm{tr}_{\mathrm{AB}}\left(|10\rangle\langle10|\otimes|1\rangle\langle1|\right)+$$
$$+a_5\tilde{a}_6\mathrm{tr}_{\mathrm{AB}}\left(|10\rangle\langle11|\otimes|1\rangle\langle0|\right)+a_5\tilde{a}_7\mathrm{tr}_{\mathrm{AB}}\left(|10\rangle\langle11|\otimes|1\rangle\langle1|\right)+$$
$$+a_6\tilde{a}_0\mathrm{tr}_{\mathrm{AB}}\left(|11\rangle\langle00|\otimes|0\rangle\langle0|\right)+a_6\tilde{a}_1\mathrm{tr}_{\mathrm{AB}}\left(|11\rangle\langle00|\otimes|0\rangle\langle1|\right)+$$
$$+a_6\tilde{a}_2\mathrm{tr}_{\mathrm{AB}}\left(|11\rangle\langle01|\otimes|0\rangle\langle0|\right)+a_6\tilde{a}_3\mathrm{tr}_{\mathrm{AB}}\left(|11\rangle\langle01|\otimes|0\rangle\langle1|\right)+$$
$$+a_6\tilde{a}_4\mathrm{tr}_{\mathrm{AB}}\left(|11\rangle\langle10|\otimes|0\rangle\langle0|\right)+a_6\tilde{a}_5\mathrm{tr}_{\mathrm{AB}}\left(|11\rangle\langle10|\otimes|0\rangle\langle1|\right)+$$
$$+a_6\tilde{a}_6\mathrm{tr}_{\mathrm{AB}}\left(|11\rangle\langle11|\otimes|0\rangle\langle0|\right)+a_6\tilde{a}_7\mathrm{tr}_{\mathrm{AB}}\left(|11\rangle\langle11|\otimes|0\rangle\langle1|\right)+$$
$$+a_7\tilde{a}_0\mathrm{tr}_{\mathrm{AB}}\left(|11\rangle\langle00|\otimes|1\rangle\langle0|\right)+a_7\tilde{a}_1\mathrm{tr}_{\mathrm{AB}}\left(|11\rangle\langle00|\otimes|1\rangle\langle1|\right)+$$
$$+a_7\tilde{a}_2\mathrm{tr}_{\mathrm{AB}}\left(|11\rangle\langle01|\otimes|1\rangle\langle0|\right)+a_7\tilde{a}_3\mathrm{tr}_{\mathrm{AB}}\left(|11\rangle\langle01|\otimes|1\rangle\langle1|\right)+$$
$$+a_7\tilde{a}_4\mathrm{tr}_{\mathrm{AB}}\left(|11\rangle\langle10|\otimes|1\rangle\langle0|\right)+a_7\tilde{a}_5\mathrm{tr}_{\mathrm{AB}}\left(|11\rangle\langle10|\otimes|1\rangle\langle1|\right)+$$
$$+a_7\tilde{a}_6\mathrm{tr}_{\mathrm{AB}}\left(|11\rangle\langle11|\otimes|1\rangle\langle0|\right)+a_7\tilde{a}_7\mathrm{tr}_{\mathrm{AB}}\left(|11\rangle\langle11|\otimes|1\rangle\langle1|\right). \qquad (2.3.20)$$

Из равенств (2.2.19) и (2.3.20) следует, что

$$\mathrm{tr}_{\mathrm{AB}}\left(\rho^{(\mathrm{ABC})}\right)=$$
$$=a_0\tilde{a}_0\mathrm{tr}\left(|00\rangle\langle00|\right)|0\rangle\langle0|+a_0\tilde{a}_1\mathrm{tr}\left(|00\rangle\langle00|\right)|0\rangle\langle1|+$$
$$+a_0\tilde{a}_2\mathrm{tr}\left(|00\rangle\langle01|\right)|0\rangle\langle0|+a_0\tilde{a}_3\mathrm{tr}\left(|00\rangle\langle01|\right)|0\rangle\langle1|+$$
$$+a_0\tilde{a}_4\mathrm{tr}\left(|00\rangle\langle10|\right)|0\rangle\langle0|+a_0\tilde{a}_5\mathrm{tr}\left(|00\rangle\langle10|\right)|0\rangle\langle1|+$$
$$+a_0\tilde{a}_6\mathrm{tr}\left(|00\rangle\langle11|\right)|0\rangle\langle0|+a_0\tilde{a}_7\mathrm{tr}\left(|00\rangle\langle11|\right)|0\rangle\langle1|+$$
$$+a_1\tilde{a}_0\mathrm{tr}\left(|00\rangle\langle00|\right)|1\rangle\langle0|+a_1\tilde{a}_1\mathrm{tr}\left(|00\rangle\langle00|\right)|1\rangle\langle1|+$$
$$+a_1\tilde{a}_2\mathrm{tr}\left(|00\rangle\langle01|\right)|1\rangle\langle0|+a_1\tilde{a}_3\mathrm{tr}\left(|00\rangle\langle01|\right)|1\rangle\langle1|+$$
$$+a_1\tilde{a}_4\mathrm{tr}\left(|00\rangle\langle10|\right)|1\rangle\langle0|+a_1\tilde{a}_5\mathrm{tr}\left(|00\rangle\langle10|\right)|1\rangle\langle1|+$$
$$+a_1\tilde{a}_6\mathrm{tr}\left(|00\rangle\langle11|\right)|1\rangle\langle0|+a_1\tilde{a}_7\mathrm{tr}\left(|00\rangle\langle11|\right)|1\rangle\langle1|+$$

$$
\begin{aligned}
&+a_2\tilde{a}_0\mathrm{tr}\left(|01\rangle\langle 00|\right)|0\rangle\langle 0|+a_2\tilde{a}_1\mathrm{tr}\left(|01\rangle\langle 00|\right)|0\rangle\langle 1|+\\
&+a_2\tilde{a}_2\mathrm{tr}\left(|01\rangle\langle 01|\right)|0\rangle\langle 0|+a_2\tilde{a}_3\mathrm{tr}\left(|01\rangle\langle 01|\right)|0\rangle\langle 1|+\\
&+a_2\tilde{a}_4\mathrm{tr}\left(|01\rangle\langle 10|\right)|0\rangle\langle 0|+a_2\tilde{a}_5\mathrm{tr}\left(|01\rangle\langle 10|\right)|0\rangle\langle 1|+\\
&+a_2\tilde{a}_6\mathrm{tr}\left(|01\rangle\langle 11|\right)|0\rangle\langle 0|+a_2\tilde{a}_7\mathrm{tr}\left(|01\rangle\langle 11|\right)|0\rangle\langle 1|+\\
&+a_3\tilde{a}_0\mathrm{tr}\left(|01\rangle\langle 00|\right)|1\rangle\langle 0|+a_3\tilde{a}_1\mathrm{tr}\left(|01\rangle\langle 00|\right)|1\rangle\langle 1|+\\
&+a_3\tilde{a}_2\mathrm{tr}\left(|01\rangle\langle 01|\right)|1\rangle\langle 0|+a_3\tilde{a}_3\mathrm{tr}\left(|01\rangle\langle 01|\right)|1\rangle\langle 1|+\\
&+a_3\tilde{a}_4\mathrm{tr}\left(|01\rangle\langle 10|\right)|1\rangle\langle 0|+a_3\tilde{a}_5\mathrm{tr}\left(|01\rangle\langle 10|\right)|1\rangle\langle 1|+\\
&+a_3\tilde{a}_6\mathrm{tr}\left(|01\rangle\langle 11|\right)|1\rangle\langle 0|+a_3\tilde{a}_7\mathrm{tr}\left(|01\rangle\langle 11|\right)|1\rangle\langle 1|+\\
&+a_4\tilde{a}_0\mathrm{tr}\left(|10\rangle\langle 00|\right)|0\rangle\langle 0|+a_4\tilde{a}_1\mathrm{tr}\left(|10\rangle\langle 00|\right)|0\rangle\langle 1|+\\
&+a_4\tilde{a}_2\mathrm{tr}\left(|10\rangle\langle 01|\right)|0\rangle\langle 0|+a_4\tilde{a}_3\mathrm{tr}\left(|10\rangle\langle 01|\right)|0\rangle\langle 1|+\\
&+a_4\tilde{a}_4\mathrm{tr}\left(|10\rangle\langle 10|\right)|0\rangle\langle 0|+a_4\tilde{a}_5\mathrm{tr}\left(|10\rangle\langle 10|\right)|0\rangle\langle 1|+\\
&+a_4\tilde{a}_6\mathrm{tr}\left(|10\rangle\langle 11|\right)|0\rangle\langle 0|+a_4\tilde{a}_7\mathrm{tr}\left(|10\rangle\langle 11|\right)|0\rangle\langle 1|+\\
&+a_5\tilde{a}_0\mathrm{tr}\left(|10\rangle\langle 00|\right)|1\rangle\langle 0|+a_5\tilde{a}_1\mathrm{tr}\left(|10\rangle\langle 00|\right)|1\rangle\langle 1|+\\
&+a_5\tilde{a}_2\mathrm{tr}\left(|10\rangle\langle 01|\right)|1\rangle\langle 0|+a_5\tilde{a}_3\mathrm{tr}\left(|10\rangle\langle 01|\right)|1\rangle\langle 1|+\\
&+a_5\tilde{a}_4\mathrm{tr}\left(|10\rangle\langle 10|\right)|1\rangle\langle 0|+a_5\tilde{a}_5\mathrm{tr}\left(|10\rangle\langle 10|\right)|1\rangle\langle 1|+\\
&+a_5\tilde{a}_6\mathrm{tr}\left(|10\rangle\langle 11|\right)|1\rangle\langle 0|+a_5\tilde{a}_7\mathrm{tr}\left(|10\rangle\langle 11|\right)|1\rangle\langle 1|+\\
&+a_6\tilde{a}_0\mathrm{tr}\left(|11\rangle\langle 00|\right)|0\rangle\langle 0|+a_6\tilde{a}_1\mathrm{tr}\left(|11\rangle\langle 00|\right)|0\rangle\langle 1|+\\
&+a_6\tilde{a}_2\mathrm{tr}\left(|11\rangle\langle 01|\right)|0\rangle\langle 0|+a_6\tilde{a}_3\mathrm{tr}\left(|11\rangle\langle 01|\right)|0\rangle\langle 1|+\\
&+a_6\tilde{a}_4\mathrm{tr}\left(|11\rangle\langle 10|\right)|0\rangle\langle 0|+a_6\tilde{a}_5\mathrm{tr}\left(|11\rangle\langle 10|\right)|0\rangle\langle 1|+\\
&+a_6\tilde{a}_6\mathrm{tr}\left(|11\rangle\langle 11|\right)|0\rangle\langle 0|+a_6\tilde{a}_7\mathrm{tr}\left(|11\rangle\langle 11|\right)|0\rangle\langle 1|+\\
&+a_7\tilde{a}_0\mathrm{tr}\left(|11\rangle\langle 00|\right)|1\rangle\langle 0|+a_7\tilde{a}_1\mathrm{tr}\left(|11\rangle\langle 00|\right)|1\rangle\langle 1|+\\
&+a_7\tilde{a}_2\mathrm{tr}\left(|11\rangle\langle 01|\right)|1\rangle\langle 0|+a_7\tilde{a}_3\mathrm{tr}\left(|11\rangle\langle 01|\right)|1\rangle\langle 1|+\\
&+a_7\tilde{a}_4\mathrm{tr}\left(|11\rangle\langle 10|\right)|1\rangle\langle 0|+a_7\tilde{a}_5\mathrm{tr}\left(|11\rangle\langle 10|\right)|1\rangle\langle 1|+\\
&+a_7\tilde{a}_6\mathrm{tr}\left(|11\rangle\langle 11|\right)|1\rangle\langle 0|+a_7\tilde{a}_7\mathrm{tr}\left(|11\rangle\langle 11|\right)|1\rangle\langle 1|.
\end{aligned}
\tag{2.3.21}
$$

Учитывая, что при условии $b_1 \neq b_2$ справедливо равенство

$$\operatorname{tr}\left(\left|b_1\right\rangle\left\langle b_2\right|\right)=0$$

(где $b_1,\ b_2 \in \{00,\ 01,\ 10,\ 11\}$), из (2.3.21) получаем

$$\begin{aligned}
&\operatorname{tr}_{\mathrm{AB}}\left(\rho^{(\mathrm{ABC})}\right)= \\
&=a_0\tilde{a}_0\operatorname{tr}\left(|00\rangle\langle 00|\right)|0\rangle\langle 0|+a_0\tilde{a}_1\operatorname{tr}\left(|00\rangle\langle 00|\right)|0\rangle\langle 1|+ \\
&+a_1\tilde{a}_0\operatorname{tr}\left(|00\rangle\langle 00|\right)|1\rangle\langle 0|+a_1\tilde{a}_1\operatorname{tr}\left(|00\rangle\langle 00|\right)|1\rangle\langle 1|+ \\
&+a_2\tilde{a}_2\operatorname{tr}\left(|01\rangle\langle 01|\right)|0\rangle\langle 0|+a_2\tilde{a}_3\operatorname{tr}\left(|01\rangle\langle 01|\right)|0\rangle\langle 1|+ \\
&+a_3\tilde{a}_2\operatorname{tr}\left(|01\rangle\langle 01|\right)|1\rangle\langle 0|+a_3\tilde{a}_3\operatorname{tr}\left(|01\rangle\langle 01|\right)|1\rangle\langle 1|+ \\
&+a_4\tilde{a}_4\operatorname{tr}\left(|10\rangle\langle 10|\right)|0\rangle\langle 0|+a_4\tilde{a}_5\operatorname{tr}\left(|10\rangle\langle 10|\right)|0\rangle\langle 1|+ \\
&+a_5\tilde{a}_4\operatorname{tr}\left(|10\rangle\langle 10|\right)|1\rangle\langle 0|+a_5\tilde{a}_5\operatorname{tr}\left(|10\rangle\langle 10|\right)|1\rangle\langle 1|+ \\
&+a_6\tilde{a}_6\operatorname{tr}\left(|11\rangle\langle 11|\right)|0\rangle\langle 0|+a_6\tilde{a}_7\operatorname{tr}\left(|11\rangle\langle 11|\right)|0\rangle\langle 1|+ \\
&+a_7\tilde{a}_6\operatorname{tr}\left(|11\rangle\langle 11|\right)|1\rangle\langle 0|+a_7\tilde{a}_7\operatorname{tr}\left(|11\rangle\langle 11|\right)|1\rangle\langle 1|.
\end{aligned} \tag{2.3.22}$$

В силу того, что

$$\operatorname{tr}\left(|00\rangle\langle 00|\right)=\operatorname{tr}\left(|01\rangle\langle 01|\right)=\operatorname{tr}\left(|10\rangle\langle 10|\right)=\operatorname{tr}\left(|11\rangle\langle 11|\right)=1,$$

из (2.3.22) получаем

$$\begin{aligned}
&\operatorname{tr}_{\mathrm{AB}}\left(\rho^{(\mathrm{ABC})}\right)= \\
&=a_0\tilde{a}_0|0\rangle\langle 0|+a_0\tilde{a}_1|0\rangle\langle 1|+a_1\tilde{a}_0|1\rangle\langle 0|+a_1\tilde{a}_1|1\rangle\langle 1|+ \\
&+a_2\tilde{a}_2|0\rangle\langle 0|+a_2\tilde{a}_3|0\rangle\langle 1|+a_3\tilde{a}_2|1\rangle\langle 0|+a_3\tilde{a}_3|1\rangle\langle 1|+ \\
&+a_4\tilde{a}_4|0\rangle\langle 0|+a_4\tilde{a}_5|0\rangle\langle 1|+a_5\tilde{a}_4|1\rangle\langle 0|+a_5\tilde{a}_5|1\rangle\langle 1|+ \\
&+a_6\tilde{a}_6|0\rangle\langle 0|+a_6\tilde{a}_7|0\rangle\langle 1|+a_7\tilde{a}_6|1\rangle\langle 0|+a_7\tilde{a}_7|1\rangle\langle 1|= \\
&=\begin{pmatrix} |a_0|^2+|a_2|^2+|a_4|^2+|a_6|^2 & a_0\tilde{a}_1+a_2\tilde{a}_3+a_4\tilde{a}_5+a_6\tilde{a}_7 \\ a_1\tilde{a}_0+a_3\tilde{a}_2+a_5\tilde{a}_4+a_7\tilde{a}_6 & |a_1|^2+|a_3|^2+|a_5|^2+|a_7|^2 \end{pmatrix}.
\end{aligned} \tag{2.3.23}$$

Из (2.3.18) и (2.3.23) следует, что

$$\rho^{(\mathrm{C})} = \rho_{\mathrm{C}}^{(\mathrm{ABC})} = \mathrm{tr}_{\mathrm{AB}}\left(\rho^{(\mathrm{ABC})}\right) =$$

$$= \begin{pmatrix} |a_0|^2 + |a_2|^2 + |a_4|^2 + |a_6|^2 & a_0\tilde{a}_1 + a_2\tilde{a}_3 + a_4\tilde{a}_5 + a_6\tilde{a}_7 \\ a_1\tilde{a}_0 + a_3\tilde{a}_2 + a_5\tilde{a}_4 + a_7\tilde{a}_6 & |a_1|^2 + |a_3|^2 + |a_5|^2 + |a_7|^2 \end{pmatrix}. \qquad (2.3.24)$$

Из (2.3.24) и равенства (2.3.17) следует, что

$$1 = \mathrm{tr}\left(\left(\rho^{(\mathrm{C})}\right)^2\right) =$$

$$= \Big[\left(|a_0|^2 + |a_2|^2 + |a_4|^2 + |a_6|^2\right)^2 +$$

$$+\left(a_0\tilde{a}_1 + a_2\tilde{a}_3 + a_4\tilde{a}_5 + a_6\tilde{a}_7\right)\left(a_1\tilde{a}_0 + a_3\tilde{a}_2 + a_5\tilde{a}_4 + a_7\tilde{a}_6\right)\Big] +$$

$$+\Big[\left(a_1\tilde{a}_0 + a_3\tilde{a}_2 + a_5\tilde{a}_4 + a_7\tilde{a}_6\right)\left(a_0\tilde{a}_1 + a_2\tilde{a}_3 + a_4\tilde{a}_5 + a_6\tilde{a}_7\right) +$$

$$+\left(|a_1|^2 + |a_3|^2 + |a_5|^2 + |a_7|^2\right)^2\Big] =$$

$$= |a_0|^4 + |a_1|^4 + |a_2|^4 + |a_3|^4 + |a_4|^4 + |a_5|^4 + |a_6|^4 + |a_7|^4 +$$

$$+2(|a_0|^2|a_1|^2 + a_0\tilde{a}_1\tilde{a}_2a_3 + a_0\tilde{a}_1\tilde{a}_4a_5 + a_0\tilde{a}_1\tilde{a}_6a_7 +$$

$$+\tilde{a}_0a_1a_2\tilde{a}_3 + |a_2|^2|a_3|^2 + a_2\tilde{a}_3\tilde{a}_4a_5 + a_2\tilde{a}_3\tilde{a}_6a_7 +$$

$$+\tilde{a}_0a_1a_4\tilde{a}_5 + \tilde{a}_2a_3a_4\tilde{a}_5 + |a_4|^2|a_5|^2 + a_4\tilde{a}_5\tilde{a}_6a_7 +$$

$$+\tilde{a}_0a_1a_6\tilde{a}_7 + \tilde{a}_2a_3a_6\tilde{a}_7 + \tilde{a}_4a_5a_6\tilde{a}_7 + |a_6|^2|a_7|^2 +$$

$$+|a_0|^2|a_2|^2 + |a_0|^2|a_4|^2 + |a_0|^2|a_6|^2 + |a_2|^2|a_4|^2 + |a_2|^2|a_6|^2 + |a_4|^2|a_6|^2 +$$

$$+|a_1|^2|a_3|^2 + |a_1|^2|a_5|^2 + |a_1|^2|a_7|^2 + |a_3|^2|a_5|^2 + |a_3|^2|a_7|^2 + |a_5|^2|a_7|^2) =$$

$$= \left(|a_0|^2 + |a_1|^2 + |a_2|^2 + |a_3|^2 + |a_4|^2 + |a_5|^2 + |a_6|^2 + |a_7|^2\right)^2 +$$

$$+2(a_0\tilde{a}_1\tilde{a}_2a_3 + a_0\tilde{a}_1\tilde{a}_4a_5 + a_0\tilde{a}_1\tilde{a}_6a_7 + \tilde{a}_0a_1a_2\tilde{a}_3 + a_2\tilde{a}_3\tilde{a}_4a_5 + a_2\tilde{a}_3\tilde{a}_6a_7 +$$

$$+\tilde{a}_0a_1a_4\tilde{a}_5 + \tilde{a}_2a_3a_4\tilde{a}_5 + a_4\tilde{a}_5\tilde{a}_6a_7 + \tilde{a}_0a_1a_6\tilde{a}_7 + \tilde{a}_2a_3a_6\tilde{a}_7 + \tilde{a}_4a_5a_6\tilde{a}_7 -$$

$$-|a_0|^2|a_3|^2 - |a_0|^2|a_5|^2 - |a_0|^2|a_7|^2 - |a_2|^2|a_1|^2 - |a_2|^2|a_5|^2 - |a_2|^2|a_7|^2 -$$

$$-|a_4|^2|a_1|^2 - |a_4|^2|a_3|^2 - |a_4|^2|a_7|^2 - |a_6|^2|a_1|^2 - |a_6|^2|a_3|^2 - |a_6|^2|a_5|^2) =$$

$$= 1 + 2(a_0\tilde{a}_1\tilde{a}_2a_3 + a_0\tilde{a}_1\tilde{a}_4a_5 + a_0\tilde{a}_1\tilde{a}_6a_7 + \tilde{a}_0a_1a_2\tilde{a}_3 + a_2\tilde{a}_3\tilde{a}_4a_5 + a_2\tilde{a}_3\tilde{a}_6a_7 +$$

$$+\tilde{a}_0 a_1 a_4 \tilde{a}_5 + \tilde{a}_2 a_3 a_4 \tilde{a}_5 + a_4 \tilde{a}_5 \tilde{a}_6 a_7 + \tilde{a}_0 a_1 a_6 \tilde{a}_7 + \tilde{a}_2 a_3 a_6 \tilde{a}_7 + \tilde{a}_4 a_5 a_6 \tilde{a}_7 -$$
$$-|a_0|^2|a_3|^2 - |a_0|^2|a_5|^2 - |a_0|^2|a_7|^2 - |a_2|^2|a_1|^2 - |a_2|^2|a_5|^2 - |a_2|^2|a_7|^2 -$$
$$-|a_4|^2|a_1|^2 - |a_4|^2|a_3|^2 - |a_4|^2|a_7|^2 - |a_6|^2|a_1|^2 -$$
$$-|a_6|^2|a_3|^2 - |a_6|^2|a_5|^2). \tag{2.3.25}$$

Удалив слагаемые, равные 1, из первой и последней частей цепочки равенств (2.3.25), получаем

$$0 = 2(a_0\tilde{a}_1\tilde{a}_2 a_3 + a_0\tilde{a}_1\tilde{a}_4 a_5 + a_0\tilde{a}_1\tilde{a}_6 a_7 + \tilde{a}_0 a_1 a_2 \tilde{a}_3 + a_2\tilde{a}_3\tilde{a}_4 a_5 + a_2\tilde{a}_3\tilde{a}_6 a_7 +$$
$$+\tilde{a}_0 a_1 a_4 \tilde{a}_5 + \tilde{a}_2 a_3 a_4 \tilde{a}_5 + a_4 \tilde{a}_5 \tilde{a}_6 a_7 + \tilde{a}_0 a_1 a_6 \tilde{a}_7 + \tilde{a}_2 a_3 a_6 \tilde{a}_7 + \tilde{a}_4 a_5 a_6 \tilde{a}_7 -$$
$$-|a_0|^2|a_3|^2 - |a_0|^2|a_5|^2 - |a_0|^2|a_7|^2 - |a_2|^2|a_1|^2 - |a_2|^2|a_5|^2 - |a_2|^2|a_7|^2 -$$
$$-|a_4|^2|a_1|^2 - |a_4|^2|a_3|^2 - |a_4|^2|a_7|^2 - |a_6|^2|a_1|^2 - |a_6|^2|a_3|^2 - |a_6|^2|a_5|^2).$$

Поделив обе части последнего равенства на число (–2), получаем

$$|a_0|^2|a_3|^2 + |a_0|^2|a_5|^2 + |a_0|^2|a_7|^2 + |a_2|^2|a_1|^2 + |a_2|^2|a_5|^2 + |a_2|^2|a_7|^2 +$$
$$+|a_4|^2|a_1|^2 + |a_4|^2|a_3|^2 + |a_4|^2|a_7|^2 + |a_6|^2|a_1|^2 + |a_6|^2|a_3|^2 + |a_6|^2|a_5|^2 -$$
$$-a_0\tilde{a}_1\tilde{a}_2 a_3 - a_0\tilde{a}_1\tilde{a}_4 a_5 - a_0\tilde{a}_1\tilde{a}_6 a_7 - \tilde{a}_0 a_1 a_2 \tilde{a}_3 - a_2\tilde{a}_3\tilde{a}_4 a_5 - a_2\tilde{a}_3\tilde{a}_6 a_7 -$$
$$-\tilde{a}_0 a_1 a_4 \tilde{a}_5 - \tilde{a}_2 a_3 a_4 \tilde{a}_5 - a_4 \tilde{a}_5 \tilde{a}_6 a_7 - \tilde{a}_0 a_1 a_6 \tilde{a}_7 - \tilde{a}_2 a_3 a_6 \tilde{a}_7 - \tilde{a}_4 a_5 a_6 \tilde{a}_7 = 0.$$

Группируя слагаемые и вычитаемые в левой части данного равенства и вынося общие сомножители за скобки, имеем

$$(a_0a_3 - a_1a_2)(\tilde{a}_0\tilde{a}_3 - \tilde{a}_1\tilde{a}_2) + (a_0a_5 - a_1a_4)(\tilde{a}_0\tilde{a}_5 - \tilde{a}_1\tilde{a}_4) +$$
$$+(a_0a_7 - a_1a_6)(\tilde{a}_0\tilde{a}_7 - \tilde{a}_1\tilde{a}_6) + (a_2a_5 - a_3a_4)(\tilde{a}_2\tilde{a}_5 - \tilde{a}_3\tilde{a}_4) +$$
$$+(a_2a_7 - a_3a_6)(\tilde{a}_2\tilde{a}_7 - \tilde{a}_3\tilde{a}_6) + (a_4a_7 - a_5a_6)(\tilde{a}_4\tilde{a}_7 - \tilde{a}_5\tilde{a}_6) = 0.$$

Заметив, что пара сомножителей в каждом из шести слагаемых левой части данного равенства являются взаимно сопряженными комплексными числами, получаем

$$|a_0a_3 - a_1a_2|^2 + |a_0a_5 - a_1a_4|^2 + |a_0a_7 - a_1a_6|^2 +$$
$$+|a_2a_5 - a_3a_4|^2 + |a_2a_7 - a_3a_6|^2 + |a_4a_7 - a_5a_6|^2 = 0.$$

Отсюда, с учетом (2.3.3), имеем

$$|Y_1|^2 = |Y_2|^2 = |Y_3|^2 = |Y_4|^2 = |Y_5|^2 = |Y_6|^2 = 0\,,$$

что равносильно выполнению цепочки равенств

$$Y_1 = Y_2 = Y_3 = Y_4 = Y_5 = Y_6 = 0\,.$$

Пункт (б) утверждения 2.3.4 в одну сторону доказан.

Обратно, пусть

$$Y_1 = Y_2 = Y_3 = Y_4 = Y_5 = Y_6 = 0\,.$$

Тогда

$$|Y_1|^2 = |Y_2|^2 = |Y_3|^2 = |Y_4|^2 = |Y_5|^2 = |Y_6|^2 = 0\,,$$

что, учитывая (2.3.3), равносильно равенству

$$\begin{gathered}\left(a_0a_3 - a_1a_2\right)\left(\tilde{a}_0\tilde{a}_3 - \tilde{a}_1\tilde{a}_2\right) + \left(a_0a_5 - a_1a_4\right)\left(\tilde{a}_0\tilde{a}_5 - \tilde{a}_1\tilde{a}_4\right) + \\ + \left(a_0a_7 - a_1a_6\right)\left(\tilde{a}_0\tilde{a}_7 - \tilde{a}_1\tilde{a}_6\right) + \left(a_2a_5 - a_3a_4\right)\left(\tilde{a}_2\tilde{a}_5 - \tilde{a}_3\tilde{a}_4\right) + \\ + \left(a_2a_7 - a_3a_6\right)\left(\tilde{a}_2\tilde{a}_7 - \tilde{a}_3\tilde{a}_6\right) + \left(a_4a_7 - a_5a_6\right)\left(\tilde{a}_4\tilde{a}_7 - \tilde{a}_5\tilde{a}_6\right) = 0.\end{gathered}$$

Раскрыв скобки в левой части последнего равенства, получаем

$$\begin{gathered}|a_0|^2|a_3|^2 + |a_0|^2|a_5|^2 + |a_0|^2|a_7|^2 + |a_2|^2|a_1|^2 + |a_2|^2|a_5|^2 + |a_2|^2|a_7|^2 + \\ + |a_4|^2|a_1|^2 + |a_4|^2|a_3|^2 + |a_4|^2|a_7|^2 + |a_6|^2|a_1|^2 + |a_6|^2|a_3|^2 + |a_6|^2|a_5|^2 - \\ - a_0\tilde{a}_1\tilde{a}_2a_3 - a_0\tilde{a}_1\tilde{a}_4a_5 - a_0\tilde{a}_1\tilde{a}_6a_7 - \tilde{a}_0a_1a_2\tilde{a}_3 - a_2\tilde{a}_3\tilde{a}_4a_5 - a_2\tilde{a}_3\tilde{a}_6a_7 - \\ - \tilde{a}_0a_1a_4\tilde{a}_5 - \tilde{a}_2a_3a_4\tilde{a}_5 - a_4\tilde{a}_5\tilde{a}_6a_7 - \tilde{a}_0a_1a_6\tilde{a}_7 - \tilde{a}_2a_3a_6\tilde{a}_7 - \tilde{a}_4a_5a_6\tilde{a}_7 = 0.\end{gathered}$$

Помножив на (−2) обе части последнего равенства и к обеим частям получившегося равенства прибавив по 1, имеем

$$\begin{gathered}1 + 2(a_0\tilde{a}_1\tilde{a}_2a_3 + a_0\tilde{a}_1\tilde{a}_4a_5 + a_0\tilde{a}_1\tilde{a}_6a_7 + \tilde{a}_0a_1a_2\tilde{a}_3 + a_2\tilde{a}_3\tilde{a}_4a_5 + a_2\tilde{a}_3\tilde{a}_6a_7 + \\ + \tilde{a}_0a_1a_4\tilde{a}_5 + \tilde{a}_2a_3a_4\tilde{a}_5 + a_4\tilde{a}_5\tilde{a}_6a_7 + \tilde{a}_0a_1a_6\tilde{a}_7 + \tilde{a}_2a_3a_6\tilde{a}_7 + \tilde{a}_4a_5a_6\tilde{a}_7 - \\ - |a_0|^2|a_3|^2 - |a_0|^2|a_5|^2 - |a_0|^2|a_7|^2 - |a_2|^2|a_1|^2 - |a_2|^2|a_5|^2 - |a_2|^2|a_7|^2 - \\ - |a_4|^2|a_1|^2 - |a_4|^2|a_3|^2 - |a_4|^2|a_7|^2 - |a_6|^2|a_1|^2 - |a_6|^2|a_3|^2 - |a_6|^2|a_5|^2) = 1.\end{gathered}$$

Отсюда, учитывая (2.3.2), получаем

$$\left(|a_0|^2+|a_1|^2+|a_2|^2+|a_3|^2+|a_4|^2+|a_5|^2+|a_6|^2+|a_7|^2\right)^2+$$
$$+2(a_0\tilde{a}_1\tilde{a}_2a_3+a_0\tilde{a}_1\tilde{a}_4a_5+a_0\tilde{a}_1\tilde{a}_6a_7+\tilde{a}_0a_1a_2\tilde{a}_3+a_2\tilde{a}_3\tilde{a}_4a_5+a_2\tilde{a}_3\tilde{a}_6a_7+$$
$$+\tilde{a}_0a_1a_4\tilde{a}_5+\tilde{a}_2a_3a_4\tilde{a}_5+a_4\tilde{a}_5\tilde{a}_6a_7+\tilde{a}_0a_1a_6\tilde{a}_7+\tilde{a}_2a_3a_6\tilde{a}_7+\tilde{a}_4a_5a_6\tilde{a}_7-$$
$$-|a_0|^2|a_3|^2-|a_0|^2|a_5|^2-|a_0|^2|a_7|^2-|a_2|^2|a_1|^2-|a_2|^2|a_5|^2-|a_2|^2|a_7|^2-$$
$$-|a_4|^2|a_1|^2-|a_4|^2|a_3|^2-|a_4|^2|a_7|^2-$$
$$-|a_6|^2|a_1|^2-|a_6|^2|a_3|^2-|a_6|^2|a_5|^2)=1\,. \tag{2.3.26}$$

Далее, проводя вычисления, аналогичные вычислениям в равенствах (2.3.20) – (2.3.23), из равенства (2.3.19) получаем редуцированную матрицу плотности подсистемы C квантовой системы ABC:

$$\rho_{\mathrm{C}}^{(\mathrm{ABC})}=\mathrm{tr}_{\mathrm{AB}}\left(\rho^{(\mathrm{ABC})}\right)=$$
$$=\begin{pmatrix}|a_0|^2+|a_2|^2+|a_4|^2+|a_6|^2 & a_0\tilde{a}_1+a_2\tilde{a}_3+a_4\tilde{a}_5+a_6\tilde{a}_7\\ a_1\tilde{a}_0+a_3\tilde{a}_2+a_5\tilde{a}_4+a_7\tilde{a}_6 & |a_1|^2+|a_3|^2+|a_5|^2+|a_7|^2\end{pmatrix}.$$

Теперь вычислим след от квадрата матрицы $\rho_{\mathrm{C}}^{(\mathrm{ABC})}$:

$$\mathrm{tr}\left(\left(\rho_{\mathrm{C}}^{(\mathrm{ABC})}\right)^2\right)=$$
$$=\Big[\left(|a_0|^2+|a_2|^2+|a_4|^2+|a_6|^2\right)^2+$$
$$+\left(a_0\tilde{a}_1+a_2\tilde{a}_3+a_4\tilde{a}_5+a_6\tilde{a}_7\right)\left(a_1\tilde{a}_0+a_3\tilde{a}_2+a_5\tilde{a}_4+a_7\tilde{a}_6\right)]+$$
$$+[\left(a_1\tilde{a}_0+a_3\tilde{a}_2+a_5\tilde{a}_4+a_7\tilde{a}_6\right)\left(a_0\tilde{a}_1+a_2\tilde{a}_3+a_4\tilde{a}_5+a_6\tilde{a}_7\right)+$$
$$+\left(|a_1|^2+|a_3|^2+|a_5|^2+|a_7|^2\right)^2\Big]=$$
$$\left(|a_0|^2+|a_1|^2+|a_2|^2+|a_3|^2+|a_4|^2+|a_5|^2+|a_6|^2+|a_7|^2\right)^2+$$
$$+2(a_0\tilde{a}_1\tilde{a}_2a_3+a_0\tilde{a}_1\tilde{a}_4a_5+a_0\tilde{a}_1\tilde{a}_6a_7+\tilde{a}_0a_1a_2\tilde{a}_3+a_2\tilde{a}_3\tilde{a}_4a_5+a_2\tilde{a}_3\tilde{a}_6a_7+$$
$$+\tilde{a}_0a_1a_4\tilde{a}_5+\tilde{a}_2a_3a_4\tilde{a}_5+a_4\tilde{a}_5\tilde{a}_6a_7+\tilde{a}_0a_1a_6\tilde{a}_7+\tilde{a}_2a_3a_6\tilde{a}_7+\tilde{a}_4a_5a_6\tilde{a}_7-$$
$$-|a_0|^2|a_3|^2-|a_0|^2|a_5|^2-|a_0|^2|a_7|^2-|a_2|^2|a_1|^2-|a_2|^2|a_5|^2-|a_2|^2|a_7|^2-$$

$$-|a_4|^2|a_1|^2-|a_4|^2|a_3|^2-|a_4|^2|a_7|^2-$$
$$-|a_6|^2|a_1|^2-|a_6|^2|a_3|^2-|a_6|^2|a_5|^2). \tag{2.3.27}$$

Из равенств (2.3.26) и (2.3.27) следует справедливость равенства

$$\mathrm{tr}\left(\left(\rho_{\mathrm{C}}^{(\mathrm{ABC})}\right)^2\right)=1,$$

которое в соответствии с результатами, представленными в работе [50], равносильно тому, что состояние подсистемы C квантовой системы ABC является чистым состоянием. Тогда в силу того, что состояние $|\psi\rangle$ квантовой системы ABC является чистым состоянием, имеем, что состояние подсистемы AB также является чистым. Следовательно, состояние $|\psi\rangle$ квантовой системы ABC представляется в виде тензорного произведения, так как состояния ее подсистем AB и C являются чистыми состояниями и, следовательно, они описываются некоторыми нормированными векторами $|\psi_{12}\rangle$ и $|\psi_3\rangle$, тензорное произведение $|\psi_{12}\rangle\otimes|\psi_3\rangle$ которых совпадает с вектором $|\psi\rangle$.

Доказательство пункта (б) утверждения 2.3.4 завершено и, тем самым, утверждение 2.3.4 **полностью доказано**.

§ 2.4. Понятие несепарабельности относительно состояний многокубитных квантовых систем

Данный параграф начнем с формулировок определений понятий сепарабельности и несепарабельности состояний квантовых систем, принятых в настоящее время в квантовой теории [56; 59].

Определение 2.4.1. Состояние $|\psi\rangle\in\mathbb{C}^{2^n}$ называется **сепарабельным** состоянием (говорят также **незапутанным** состоянием), если имеет место равенство

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle,$$

где $|\psi_1\rangle \in \mathbb{C}^{2^{n_1}}$, $|\psi_1\rangle \in \mathbb{C}^{2^{n_2}}$; n, n_1 и n_2 – натуральные числа, такие, что

$$n_1 + n_2 = n.$$

Определение 2.4.2. Состояние $|\psi\rangle \in \mathbb{C}^{2^n}$ называется **несепарабельным** состоянием (говорят также **запутанным** состоянием), если оно не является сепарабельным состоянием.

Пусть ABC – трехкубитная квантовая система, состоящая из трех однокубитных квантовых систем A, B и C. Будем полагать, что в квантовой системе ABC кубит A – первый кубит, кубит B – второй кубит и кубит C – третий кубит в соответствии с записью ABC. Данный порядок следования кубитов не обладает никаким преимуществом по отношению к другим порядкам следования и взят за основу, так же как и в параграфе 2.3, исключительно из необходимости достижения определенности в порядке следования кубитов в исходной квантовой системе ABC. Всюду далее в этом параграфе будем сохранять указанный порядок следования кубитов, если специально не будет оговорен другой порядок следования.

Любое состояние $|\psi\rangle \in \mathbb{C}^8$ квантовой системы ABC либо не представимо в виде тензорного произведения состояний меньших размерностей, либо представимо. В последнем случае математическую форму представления $|\psi\rangle$ в виде тензорного произведения можно задать, как указано в параграфе 2.3, в виде одного из следующих равенств:

1) $|\psi\rangle = |\psi_1\rangle \otimes |\psi_{23}\rangle$,

где $|\psi_1\rangle \in \mathbb{C}^2$, $|\psi_{23}\rangle \in \mathbb{C}^4$, $|\psi_{23}\rangle$ – состояние, не представимое в виде тензорного произведения состояний меньших размерностей;

2) $|\psi\rangle = |\psi_{12}\rangle \otimes |\psi_3\rangle$,

где $|\psi_{12}\rangle \in \mathbb{C}^4$, $|\psi_3\rangle \in \mathbb{C}^2$, $|\psi_{12}\rangle$ – состояние, не представимое в виде тензорного произведения состояний меньших размерностей;

3) $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \otimes |\psi_3\rangle$,

где $|\psi_1\rangle \in \mathbb{C}^2$, $|\psi_2\rangle \in \mathbb{C}^2$, $|\psi_3\rangle \in \mathbb{C}^2$.

Как и в параграфе 2.3, эти равенства можно трактовать следующим образом. Первое равенство соответствует ситуации, когда состояние $|\psi_1\rangle \in \mathbb{C}^2$ однокубитной подсистемы A является чистым состоянием, а двухкубитная подсистема BC находится в чистом несепарабельном состоянии $|\psi_{23}\rangle \in \mathbb{C}^4$.

Второе равенство соответствует ситуации, когда двухкубитная подсистема AB находится в чистом несепарабельном состоянии $|\psi_{12}\rangle \in \mathbb{C}^4$, а однокубитная подсистема C находится в чистом состоянии $|\psi_3\rangle \in \mathbb{C}^2$.

Третье равенство соответствует ситуации, когда однокубитные подсистемы A, B и C исходной трехкубитной квантовой системы ABC находятся соответственно в чистых состояниях $|\psi_1\rangle \in \mathbb{C}^2$, $|\psi_2\rangle \in \mathbb{C}^2$, $|\psi_3\rangle \in \mathbb{C}^2$.

Обратим теперь внимание на ситуацию, которая не может быть отнесена к перечисленным выше. Она характеризуется тем, что двухкубитная подсистема AC исходной квантовой системы ABC находится в чистом несепарабельном состоянии $|\psi_{13}\rangle \in \mathbb{C}^4$, а однокубитная квантовая система B находится в чистом состоянии $|\psi_2\rangle \in \mathbb{C}^2$. Приведем пример такого состояния.

Пример 2.4.3. Рассмотрим следующее состояние квантовой системы ABC:

$$|\psi\rangle = \frac{|000\rangle + |101\rangle}{\sqrt{2}}.$$

Покажем, что в этом случае для состояния $|\psi_2\rangle$ кубита B справедливо равенство

$$|\psi_2\rangle = |0\rangle.$$

Для этого проведем проективное измерение в вычислительном базисе $\{|0\rangle, |1\rangle\}$ над подсистемой квантовой системы ABC, состоящей из кубита B. Полное множество ортогональных проекторов такого измерения состоит из проекторов M_0 и M_1, где

$$M_0 = |0\rangle\langle 0| = \begin{pmatrix} 1 \\ 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix},$$
$$M_1 = |1\rangle\langle 1| = \begin{pmatrix} 0 \\ 1 \end{pmatrix}\begin{pmatrix} 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

Так как в данном случае кубит B не рассматривается в качестве изолированной квантовой системы, то измерение над кубитом B проводится как измерение над подсистемой квантовой системы ABC, что, в соответствии с утверждением 1.2.24, означает осуществление измерения над квантовой системой ABC, определяемое множеством операторов

$$\{\mathbf{I}_2 \otimes M_0 \otimes \mathbf{I}_2,\ \mathbf{I}_2 \otimes M_1 \otimes \mathbf{I}_2\}.$$

Тогда, в соответствии с (1.2.1), при проведении этого измерения с вероятностью

$$\begin{aligned}
&p(0) = \langle\psi|(\mathbf{I}_2 \otimes M_0 \otimes \mathbf{I}_2)^*(\mathbf{I}_2 \otimes M_0 \otimes \mathbf{I}_2)|\psi\rangle = \\
&= \frac{1}{\sqrt{2}}\left(\langle 0|\mathbf{I}_2 \otimes \langle 0|M_0 \otimes \langle 0|\mathbf{I}_2 + \langle 1|\mathbf{I}_2 \otimes \langle 0|M_0 \otimes \langle 1|\mathbf{I}_2\right) \\
&\frac{1}{\sqrt{2}}\left(\mathbf{I}_2|0\rangle \otimes M_0|0\rangle \otimes \mathbf{I}_2|0\rangle + \mathbf{I}_2|1\rangle \otimes M_0|0\rangle \otimes \mathbf{I}_2|1\rangle\right) = \\
&= \frac{1}{2}\left(\langle 000| + \langle 101|\right)\left(|000\rangle + |101\rangle\right) = 1
\end{aligned}$$

получаем результат, связанный с проектором M_0. Это означает, что кубит B находится в состоянии

$$|\psi_2\rangle = |0\rangle$$

в ситуации, когда квантовая система ABC находится в состоянии $|\psi\rangle$.

Аналогично можно показать, что, когда квантовая система ABC находится в состоянии $|\psi\rangle$, двухкубитная подсистема AC квантовой системы ABC находится в состоянии

$$|\psi_{13}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}.$$

В силу справедливости равенств

$$|\psi_2\rangle \otimes |\psi_{13}\rangle = \frac{|000\rangle + |011\rangle}{\sqrt{2}}$$

и

$$|\psi_{13}\rangle \otimes |\psi_2\rangle = \frac{|000\rangle + |110\rangle}{\sqrt{2}}$$

ясно, что состояние $|\psi\rangle$ не представимо в виде тензорного произведения состояний $|\psi_2\rangle$ и $|\psi_{13}\rangle$ ни при каком порядке следования сомножителей. Однако если рассматривать квантовую систему BAC, отличающуюся от исходной квантовой системы ABC только порядком следования кубитов, то ее состояние представимо в виде тензорного произведения $|\psi_2\rangle \otimes |\psi_{13}\rangle$. Получается, что состояние одной и той же квантовой системы может быть сепарабельным и несепарабельным в смысле определений 2.4.1 и 2.4.2 в зависимости от того, в каком порядке следования рассматриваются подсистемы данной системы.

Пример 2.4.3 показывает, что в случаях трех- и более кубитных квантовых систем появляются противоречивые ситуации в смысле одновременной сепарабельности и несепарабельности состояния в зависимости от принимаемого порядка следования подсистем квантовой системы. И причиной этому являются, наряду с другими обстоятельствами, и определения 2.4.1 и 2.4.2, сформулированные и возможно адекватно отражающие ситуацию только для двухкубитных квантовых систем. Эти определения не вполне пригодны для изучения связей между подсистемами квантовых систем, имеющими в своем составе более чем две подсистемы. Картина связей между подсистемами в этих случаях более сложная, чем у двухкубитных систем, и она пока еще мало изучена. В связи с этим уместно процитировать следующее положение [50, стр. 704]:

«…следует отметить, что пока изучение запутанности только начинается, и не совсем ясно, насколько улучшится наше понимание квантовых вычислений и квантовой информации в результате изучения количественных мер запутанности. Мы сносно понимаем свойства чистых состояний квантовых систем из двух компонент, но очень плохо разбираемся в системах, состоящих из трех и более компонент…».

Определенную ясность в направлении исключения указанного рода противоречивых интерпретаций может внести попытка переосмысления понятия сепарабельности относительно состояний квантовых систем, его новое определение, учитывающее многокомпонентность квантовой системы. Но, в целях сохранения возможности эффективного использования уже полученных результатов для двухкомпонентных систем, желательно это сделать таким образом, чтобы новое определение совпадало с имеющимся определением 2.4.1 в случаях, когда квантовая система состоит из двух подсистем или она рассматривается как двухкомпонентная система. Далее в данном параграфе и в параграфе 2.5 будут изложены некоторые результаты исследований в этом направлении.

Пусть $A_1A_2 \ldots A_n$ – квантовая система, состоящая из n кубитов $A_1, A_2, \ldots, A_n$; $\mathbb{S}_n$ – симметрическая группа подстановок [27] на множестве $\{1, 2, \ldots, n\}$; $M_n^{(t)}$ – множество разбиений натурального числа n на t слагаемых, где $t \in \{2, 3, \ldots, n\}$, то есть $M_n^{(t)}$ – множество упорядоченных наборов натуральных чисел $(k_1, k_2, \ldots, k_t)$, таких, что справедливо равенство

$$k_1 + k_2 + \ldots + k_t = n.$$

Замечание. Разбиения натуральных чисел, рассматриваемые в данной работе, отличаются от одноименных математических объектов [64] следующим: учитывается порядок частей в конечной последовательности $(k_1,\ k_2,\ \ldots,\ k_t)$; отсутствует требование невозрастания к конечной последовательности $(k_1,\ k_2,\ \ldots,\ k_t)$; разбиения, состоящие из одной части, не рассматриваются.

Пусть $\left|\psi\right\rangle \in \mathbb{C}^{2^n}$ – произвольное состояние n-кубитной квантовой системы $A_1A_2\ldots A_n$. Из (1.1.1) следует, что состояние $\left|\psi\right\rangle$ можно представить в виде

$$\left|\psi\right\rangle = \alpha_0 \underbrace{\left|000\ldots00\right\rangle}_{n} + \alpha_1 \left|000\ldots01\right\rangle + \alpha_2 \left|000\ldots10\right\rangle + \ldots + \alpha_{2^n-1} \left|111\ldots11\right\rangle =$$

$$= \sum_{\phi=0}^{2^n-1} \alpha_\phi \left|\phi\right\rangle = \sum_{\phi=0}^{2^n-1} \alpha_\phi \left|\phi_1\phi_2\ldots\phi_n\right\rangle,$$

где

$$\alpha_0, \alpha_1, \alpha_2, \ldots, \alpha_{2^n-1} \in \mathbb{C},\ \left|\alpha_0\right|^2 + \left|\alpha_1\right|^2 + \ldots + \left|\alpha_{2^n-1}\right|^2 = 1;$$

$$\phi \in \left\{0, 1, \ldots, 2^n - 1\right\},\ \phi = \phi_1 \cdot 2^{n-1} + \phi_2 \cdot 2^{n-2} + \ldots + \phi_n \cdot 2^0,\ \phi_m \in \{0;1\},\ m = \overline{1,n};$$

$$\left|\phi\right\rangle = \left|\phi_1\phi_2\ldots\phi_n\right\rangle = \left|\phi_1\right\rangle\left|\phi_2\right\rangle\ldots\left|\phi_n\right\rangle = \left|\phi_1\right\rangle \otimes \left|\phi_2\right\rangle \otimes \ldots \otimes \left|\phi_n\right\rangle.$$

Тогда для любой подстановки $s = \begin{pmatrix} 1 & 2 & \ldots & n \\ s(1) & s(2) & \ldots & s(n) \end{pmatrix} \in \mathbb{S}_n$ состояние $\left|\psi^{(s)}\right\rangle$ квантовой системы $A_{s(1)}A_{s(2)}\ldots A_{s(n)}$, в которой кубиты рассматриваются в порядке, определяемом перестановкой $(s(1),\ s(2),\ \ldots,\ s(n))$ чисел 1, 2, …, n, задается равенством

$$\left|\psi^{(s)}\right\rangle = \sum_{\phi=0}^{2^n-1} \alpha_\phi \left|\phi_{s(1)}\phi_{s(2)}\cdots\phi_{s(n)}\right\rangle.$$

Определение 2.4.4.

Пусть $m_{n,t}^{(j)} \in M_n^{(t)}$, $m_{n,t}^{(j)} = (k_1,\ k_2,\ \ldots,\ k_t)$, $j \in \left\{1,\ 2,\ \ldots,\ \left|M_n^{(t)}\right|\right\}$, $\left|M_n^{(t)}\right|$ – мощность множества $M_n^{(t)}$, $t \in \{2,\ 3,\ \ldots,\ n\}$; $s \in \mathbb{S}_n$.

Состояние $|\psi\rangle \in \mathbb{C}^{2^n}$ n-кубитной квантовой системы $A_1A_2\ldots A_n$ называется $\left(s;\ m_{n,t}^{(j)}\right)$**-сепарабельным состоянием**, если для состояния $\left|\psi^{(s)}\right\rangle$ квантовой системы

$$A_{s(1)}A_{s(2)}\ldots A_{s(k_1)}A_{s(k_1+1)}\ldots A_{s(k_1+k_2)}A_{s(k_1+k_2+1)}\ldots A_{s(k_1+k_2+\ldots+k_{t-1})}$$
$$A_{s(k_1+k_2+\ldots+k_{t-1}+1)}\ldots A_{s(n)} \tag{2.4.5}$$

верно равенство

$$\left|\psi^{(s)}\right\rangle = \left|\psi_{1,k_1}^{(s)}\right\rangle \otimes \left|\psi_{2,k_2}^{(s)}\right\rangle \otimes \ldots \otimes \left|\psi_{t,k_t}^{(s)}\right\rangle, \tag{2.4.6}$$

где $\left|\psi_{i,k_i}^{(s)}\right\rangle$ – состояние подсистемы

$$A_{s(k_1+k_2+\ldots+k_{i-1}+1)}A_{s(k_1+k_2+\ldots+k_{i-1}+2)}\ldots A_{s(k_1+k_2+\ldots+k_{i-1}+k_i)} \tag{2.4.7}$$

квантовой системы (2.4.5), $i=\overline{1,t}$.

Состояние $|\psi\rangle$ n-кубитной квантовой системы $A_1A_2\ldots A_n$ называется $\left(s;\ m_{n,t}^{(j)}\right)$**-несепарабельным состоянием**, если оно не является $\left(s;\ m_{n,t}^{(j)}\right)$-сепарабельным состоянием.

Определение 2.4.8. Пусть $s \in \mathbb{S}_n$. Состояние $|\psi\rangle$ n-кубитной квантовой системы $A_1A_2\ldots A_n$ называется $(s;\ *)$**-сепарабельным состоянием**, если найдутся число $t \in \{2,\ 3,\ \ldots,\ n\}$ и разбиение $m_{n,t}^{(j)} \in M_n^{(t)}$, такие, что состояние $|\psi\rangle$ является $\left(s;\ m_{n,t}^{(j)}\right)$-сепарабельным состоянием квантовой системы $A_1A_2\ldots A_n$.

Состояние $|\psi\rangle$ n-кубитной квантовой системы $A_1A_2\ldots A_n$ называется $(s;\ *)$**-несепарабельным состоянием**, если оно не является $(s;\ *)$-сепарабельным состоянием.

Определение 2.4.9. Состояние $|\psi\rangle$ n-кубитной квантовой системы $A_1A_2\ldots A_n$ называется $\left(*;\ m_{n,t}^{(j)}\right)$**-сепарабельным состоянием**, если найдется подстановка $s \in \mathbb{S}_n$, такая, что состояние $|\psi\rangle$ является $\left(s;\ m_{n,t}^{(j)}\right)$-сепарабельным состоянием квантовой системы $A_1A_2\ldots A_n$.

Состояние $|\psi\rangle$ n-кубитной квантовой системы $A_1A_2\ldots A_n$ называется $\left(*;\ m_{n,t}^{(j)}\right)$**-несепарабельным состоянием**, если оно не является $\left(*;\ m_{n,t}^{(j)}\right)$-сепарабельным состоянием.

Определение 2.4.10. Состояние $|\psi\rangle$ n-кубитной квантовой системы $A_1A_2\ldots A_n$ называется t**-сепарабельным состоянием**, если найдутся подстановка $s \in \mathbb{S}_n$ и разбиение $m_{n,t}^{(j)} \in M_n^{(t)}$, такие, что состояние $|\psi\rangle$ является $\left(s;\ m_{n,t}^{(j)}\right)$-сепарабельным состоянием квантовой системы $A_1A_2\ldots A_n$, где $t \in \{2,\ 3,\ \ldots,\ n\}$.

Состояние $|\psi\rangle$ n-кубитной квантовой системы $A_1A_2\ldots A_n$ называется t**-несепарабельным состоянием**, если оно не является t-сепарабельным состоянием.

Определение 2.4.11. Состояние $|\psi\rangle$ n-кубитной квантовой системы $A_1A_2\ldots A_n$ называется **сепарабельным состоянием**, если найдется число $t \in \{2,\ 3,\ \ldots,\ n\}$, такое, что состояние $|\psi\rangle$ является t-сепарабельным состоянием квантовой системы $A_1A_2\ldots A_n$.

Состояние $|\psi\rangle$ n-кубитной квантовой системы $A_1A_2\ldots A_n$ называется **несепарабельным состоянием**, если оно не является сепарабельным состоянием.

Имеет смысл привести определение 2.4.11 к форме, позволяющей его автономное, без ссылок на другие определения использование. Это можно сделать следующим образом.

Определение 2.4.12. Состояние $|\psi\rangle$ n-кубитной квантовой системы $A_1A_2\ldots A_n$ называется **сепарабельным состоянием**, если найдется подстановка $s \in \mathbb{S}_n$, такая, что состояние $|\psi^{(s)}\rangle$ квантовой системы $A_{s(1)}A_{s(2)}\ldots A_{s(n)}$ разлагается в тензорное произведение состояний размерности меньшей, чем 2^n.

Вторая часть определения 2.4.12 совпадает со второй частью определения 2.4.11.

Замечание 2.4.13. Очевидно, что при $n = 2$ первая часть определения 2.4.12 совпадает по смыслу с определением 2.4.1, а вторая часть определения 2.4.12 совпадает по смыслу с определением 2.4.2. Таким образом, выполнено требование, чтобы новое определение сепарабельности совпадало с имеющимся определением 2.4.1 в случаях, когда квантовая система состоит из двух подсистем или она рассматривается как двухкомпонентная система.

Представляет интерес рассмотрение определений 2.4.4, 2.4.8 – 2.4.12 в случаях, когда число кубитов n превышает 2. Очевидно, самым простым для понимания и наглядным является случай, когда $n = 3$. Этот случай будет рассмотрен в следующем параграфе.

Всюду далее в данной работе начиная с параграфа 2.5 понятия, где используются слова сепарабельность и несепарабельность, во всех их разновидностях относительно состояний квантовых систем по смыслу совпадают с понятиями, введенными в параграфе 2.4 через определения 2.4.4, 2.4.8 – 2.4.12.

§ 2.5. Несепарабельные состояния трехкубитных квантовых систем

В продолжение изложения подходов к определению понятия несепарабельности многокубитных систем, начатого в параграфе 2.4, положим $n = 3$. Тогда мы имеем дело с трехкубитной квантовой системой $A_1A_2A_3$, и симметрическая группа подстановок $\mathbb{S}_3$ состоит из следующих подстановок:

$$s_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix},\ s_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},\ s_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$
$$s_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},\ s_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},\ s_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

Множество возможных разбиений числа $n = 3$ на $t \in \{2, 3\}$ слагаемых состоит из следующих разбиений:

$$m_{3,2}^{(1)} = (1, 2),\ m_{3,2}^{(2)} = (2, 1),\ m_{3,3}^{(1)} = (1, 1, 1).$$

Напомним, что в вычислительном базисе из векторов

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

произвольное трехкубитное состояние $|\psi\rangle \in \mathbb{C}^8$ можно представить в следующем общем виде:

$$\begin{aligned} |\psi\rangle = a_0|000\rangle + a_1|001\rangle + a_2|010\rangle + a_3|011\rangle + \\ + a_4|100\rangle + a_5|101\rangle + a_6|110\rangle + a_7|111\rangle, \end{aligned} \tag{2.5.1}$$

где $a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7 \in \mathbb{C}$,

$$|a_0|^2 + |a_1|^2 + |a_2|^2 + |a_3|^2 + |a_4|^2 + |a_5|^2 + |a_6|^2 + |a_7|^2 = 1. \tag{2.5.2}$$

Таким образом, для состояния $|\psi\rangle$ справедливо равенство

$$|\psi\rangle = \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_7 \end{pmatrix}.$$

Поставим задачу определения того, каким условиям должны удовлетворять координаты a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7 состояния $|\psi\rangle$ квантовой системы $A_1A_2A_3$, при выполнении которых состояние $|\psi\rangle$ является $\left(s_i; m_{3,t}^{(j)}\right)$-**несепарабельным состоянием**, где

$$i \in \{0, 1, 2, 3, 4, 5\}\,;\ t \in \{2, 3\}\,;$$

$$j \in \{1, 2\} \text{ при } t = 2;\ j = 1 \text{ при } t = 3.$$

Через координаты состояния $|\psi\rangle$ определим наборы величин $V_{tj}^{(i)}$, где $i \in \{0, 1, 2, 3, 4, 5\}$; $t \in \{2, 3\}$; $j \in \{1, 2\}$ при $t = 2$; $j = 1$ при $t = 3$, положив:

$$\begin{gathered} V_{21}^{(0)} = \Big\{ V_{211}^{(0)} = a_0a_5 - a_1a_4,\ V_{212}^{(0)} = a_0a_6 - a_2a_4,\ V_{213}^{(0)} = a_0a_7 - a_3a_4, \\ V_{214}^{(0)} = a_1a_6 - a_2a_5,\ V_{215}^{(0)} = a_1a_7 - a_3a_5,\ V_{216}^{(0)} = a_2a_7 - a_3a_6 \Big\}, \end{gathered} \tag{2.5.3}$$

$$\begin{gathered} V_{22}^{(0)} = \Big\{ V_{221}^{(0)} = a_0a_3 - a_1a_2,\ V_{222}^{(0)} = a_0a_5 - a_1a_4 = V_{221}^{(0)},\ V_{223}^{(0)} = a_0a_7 - a_1a_6, \\ V_{224}^{(0)} = a_2a_5 - a_3a_4,\ V_{225}^{(0)} = a_2a_7 - a_3a_6 = V_{216}^{(0)},\ V_{226}^{(0)} = a_4a_7 - a_5a_6 \Big\}, \end{gathered} \tag{2.5.4}$$

$$\begin{gathered} V_{31}^{(0)} = \Big\{ V_{311}^{(0)} = V_{211}^{(0)} = V_{222}^{(0)},\ V_{312}^{(0)} = V_{212}^{(0)},\ V_{313}^{(0)} = V_{213}^{(0)},\ V_{314}^{(0)} = V_{214}^{(0)}, \\ V_{315}^{(0)} = V_{215}^{(0)},\ V_{316}^{(0)} = V_{216}^{(0)} = V_{225}^{(0)},\ V_{317}^{(0)} = V_{221}^{(0)},\ V_{318}^{(0)} = V_{223}^{(0)}, \\ V_{319}^{(0)} = V_{224}^{(0)},\ V_{3110}^{(0)} = V_{226}^{(0)} \Big\}, \end{gathered} \tag{2.5.5}$$

$$\begin{gathered} V_{21}^{(1)} = \Big\{ V_{211}^{(1)} = a_0a_3 - a_1a_2,\ V_{212}^{(1)} = a_0a_6 - a_2a_4,\ V_{213}^{(1)} = a_0a_7 - a_2a_5, \\ V_{214}^{(1)} = a_1a_6 - a_3a_4,\ V_{215}^{(1)} = a_1a_7 - a_3a_5,\ V_{216}^{(1)} = a_4a_7 - a_5a_6 \Big\}, \end{gathered} \tag{2.5.6}$$

$$\begin{gathered} V_{22}^{(1)} = \Big\{ V_{221}^{(1)} = a_0a_5 - a_1a_4,\ V_{222}^{(1)} = a_0a_3 - a_1a_2 = V_{211}^{(1)},\ V_{223}^{(1)} = a_0a_7 - a_1a_6, \\ V_{224}^{(1)} = a_3a_4 - a_2a_5,\ V_{225}^{(1)} = a_4a_7 - a_5a_6 = V_{216}^{(1)},\ V_{226}^{(1)} = a_2a_7 - a_3a_6 \Big\}, \end{gathered} \tag{2.5.7}$$

$$V_{31}^{(1)} = \{V_{311}^{(1)} = V_{211}^{(1)} = V_{222}^{(1)},\ V_{312}^{(1)} = V_{212}^{(1)},\ V_{313}^{(1)} = V_{213}^{(1)},\ V_{314}^{(1)} = V_{214}^{(1)},$$
$$V_{315}^{(1)} = V_{215}^{(1)},\ V_{316}^{(1)} = V_{216}^{(1)} = V_{225}^{(1)},\ V_{317}^{(1)} = V_{221}^{(1)},\ V_{318}^{(1)} = V_{223}^{(1)}, \quad (2.5.8)$$
$$V_{319}^{(1)} = V_{224}^{(1)},\ V_{3110}^{(1)} = V_{226}^{(1)}\},$$

$$V_{21}^{(2)} = \{V_{211}^{(2)} = a_0a_5 - a_1a_4,\ V_{212}^{(2)} = a_0a_3 - a_1a_2,\ V_{213}^{(2)} = a_0a_7 - a_1a_6,$$
$$V_{214}^{(2)} = a_3a_4 - a_2a_5,\ V_{215}^{(2)} = a_4a_7 - a_5a_6,\ V_{216}^{(2)} = a_2a_7 - a_3a_6\}, \quad (2.5.9)$$

$$V_{22}^{(2)} = \{V_{221}^{(2)} = a_0a_6 - a_2a_4,\ V_{222}^{(2)} = a_0a_5 - a_1a_4 = V_{211}^{(2)},\ V_{223}^{(2)} = a_0a_7 - a_3a_4,$$
$$V_{224}^{(2)} = a_2a_5 - a_1a_6,\ V_{225}^{(2)} = a_2a_7 - a_3a_6 = V_{216}^{(2)},\ V_{226}^{(2)} = a_1a_7 - a_3a_5\}, \quad (2.5.10)$$

$$V_{31}^{(2)} = \{V_{311}^{(2)} = V_{211}^{(2)} = V_{222}^{(2)},\ V_{312}^{(2)} = V_{212}^{(2)},\ V_{313}^{(2)} = V_{213}^{(2)},\ V_{314}^{(2)} = V_{214}^{(2)},$$
$$V_{315}^{(2)} = V_{215}^{(2)},\ V_{316}^{(2)} = V_{216}^{(2)} = V_{225}^{(2)},\ V_{317}^{(2)} = V_{221}^{(2)},\ V_{318}^{(2)} = V_{223}^{(2)}, \quad (2.5.11)$$
$$V_{319}^{(2)} = V_{224}^{(2)},\ V_{3110}^{(2)} = V_{226}^{(2)}\},$$

$$V_{21}^{(3)} = \{V_{211}^{(3)} = a_0a_6 - a_2a_4,\ V_{212}^{(3)} = a_0a_5 - a_1a_4,\ V_{213}^{(3)} = a_0a_7 - a_3a_4,$$
$$V_{214}^{(3)} = a_2a_5 - a_1a_6,\ V_{215}^{(3)} = a_2a_7 - a_3a_6,\ V_{216}^{(3)} = a_1a_7 - a_3a_5\}, \quad (2.5.12)$$

$$V_{22}^{(3)} = \{V_{221}^{(3)} = a_0a_3 - a_1a_2,\ V_{222}^{(3)} = a_0a_6 - a_2a_4 = V_{211}^{(3)},\ V_{223}^{(3)} = a_0a_7 - a_2a_5,$$
$$V_{224}^{(3)} = a_1a_6 - a_3a_4,\ V_{225}^{(3)} = a_1a_7 - a_3a_5 = V_{216}^{(3)},\ V_{226}^{(3)} = a_4a_7 - a_5a_6\}, \quad (2.5.13)$$

$$V_{31}^{(3)} = \{V_{311}^{(3)} = V_{211}^{(3)} = V_{222}^{(3)},\ V_{312}^{(3)} = V_{212}^{(3)},\ V_{313}^{(3)} = V_{213}^{(3)},\ V_{314}^{(3)} = V_{214}^{(3)},$$
$$V_{315}^{(3)} = V_{215}^{(3)},\ V_{316}^{(3)} = V_{216}^{(3)} = V_{225}^{(3)},\ V_{317}^{(3)} = V_{221}^{(3)},\ V_{318}^{(3)} = V_{223}^{(3)}, \quad (2.5.14)$$
$$V_{319}^{(3)} = V_{224}^{(3)},\ V_{3110}^{(3)} = V_{226}^{(3)}\},$$

$$V_{21}^{(4)} = \{V_{211}^{(4)} = a_0a_6 - a_2a_4,\ V_{212}^{(4)} = a_0a_3 - a_1a_2,\ V_{213}^{(4)} = a_0a_7 - a_5a_6,$$
$$V_{214}^{(4)} = a_3a_4 - a_1a_6,\ V_{215}^{(4)} = a_4a_7 - a_5a_6,\ V_{216}^{(4)} = a_1a_7 - a_3a_5\}, \quad (2.5.15)$$

$$V_{22}^{(4)} = \left\{V_{221}^{(4)} = a_0a_5 - a_1a_4,\ V_{222}^{(4)} = a_0a_6 - a_2a_4 = V_{211}^{(4)},\ V_{223}^{(4)} = a_0a_7 - a_3a_4,\right.$$
$$\left.V_{224}^{(4)} = a_1a_6 - a_2a_5,\ V_{225}^{(4)} = a_1a_7 - a_3a_5 = V_{216}^{(4)},\ V_{226}^{(4)} = a_2a_7 - a_3a_6\right\}, \quad (2.5.16)$$

$$V_{31}^{(4)} = \left\{V_{311}^{(4)} = V_{211}^{(4)} = V_{222}^{(4)},\ V_{312}^{(4)} = V_{212}^{(4)},\ V_{313}^{(4)} = V_{213}^{(4)},\ V_{314}^{(4)} = V_{214}^{(4)},\right.$$
$$V_{315}^{(4)} = V_{215}^{(4)},\ V_{316}^{(4)} = V_{216}^{(4)} = V_{225}^{(4)},\ V_{317}^{(4)} = V_{221}^{(4)},\ V_{318}^{(4)} = V_{223}^{(4)}, \quad (2.5.17)$$
$$\left.V_{319}^{(4)} = V_{224}^{(4)},\ V_{3110}^{(4)} = V_{226}^{(4)}\right\},$$

$$V_{21}^{(5)} = \left\{V_{211}^{(5)} = a_0a_3 - a_1a_2,\ V_{212}^{(5)} = a_0a_5 - a_1a_4,\ V_{213}^{(5)} = a_0a_7 - a_1a_6,\right.$$
$$\left.V_{214}^{(5)} = a_2a_5 - a_3a_4,\ V_{215}^{(5)} = a_2a_7 - a_3a_6,\ V_{216}^{(5)} = a_4a_7 - a_5a_6\right\}, \quad (2.5.18)$$

$$V_{22}^{(5)} = \left\{V_{221}^{(5)} = a_0a_6 - a_2a_4,\ V_{222}^{(5)} = a_0a_3 - a_1a_2 = V_{211}^{(5)},\ V_{223}^{(5)} = a_0a_7 - a_2a_5,\right.$$
$$\left.V_{224}^{(5)} = a_3a_4 - a_1a_6,\ V_{225}^{(5)} = a_4a_7 - a_5a_6 = V_{216}^{(5)},\ V_{226}^{(5)} = a_1a_7 - a_3a_5\right\}, \quad (2.5.19)$$

$$V_{31}^{(5)} = \left\{V_{311}^{(5)} = V_{211}^{(5)} = V_{222}^{(5)},\ V_{312}^{(5)} = V_{212}^{(5)},\ V_{313}^{(5)} = V_{213}^{(5)},\ V_{314}^{(5)} = V_{214}^{(5)},\right.$$
$$V_{315}^{(5)} = V_{215}^{(5)},\ V_{316}^{(5)} = V_{216}^{(5)} = V_{225}^{(5)},\ V_{317}^{(5)} = V_{221}^{(5)},\ V_{318}^{(5)} = V_{223}^{(5)}, \quad (2.5.20)$$
$$\left.V_{319}^{(5)} = V_{224}^{(5)},\ V_{3110}^{(5)} = V_{226}^{(5)}\right\}.$$

Используя определенные равенствами (2.5.3) – (2.5.20) наборы величин $V_{tj}^{(i)}$, где $i \in \{0, 1, 2, 3, 4, 5\}$; $t \in \{2, 3\}$; $j \in \{1, 2\}$ при $t = 2$; $j = 1$ при $t = 3$, сформулируем следующее утверждение.

Утверждение 2.5.21. Состояние $|\psi\rangle$ трехкубитной квантовой системы $A_1A_2A_3$ является $\left(s_i;\ m_{3,t}^{(j)}\right)$-сепарабельным состоянием тогда и только тогда, когда равны нулю все величины из набора $V_{tj}^{(i)}$, где $i \in \{0, 1, 2, 3, 4, 5\}$; $t \in \{2, 3\}$; $j \in \{1, 2\}$ при $t = 2$; $j = 1$ при $t = 3$.

Доказательство данного утверждения приведем ниже в данном параграфе. Вначале обратим внимание на следствия, вытекающие из данного утверждения.

Первым приведем следствие, непосредственно вытекающее из утверждения 2.5.21. В нем изложено решение задачи, сформулированной выше, и в нем используется понятие $\left(s_i;\ m_{3,t}^{(j)}\right)$-несепарабельности, введенное в определении 2.4.4, в отношении состояния трехкубитной квантовой системы.

Следствие 2.5.22. Состояние $|\psi\rangle$ трехкубитной квантовой системы $A_1A_2A_3$ является $\left(s_i;\ m_{3,t}^{(j)}\right)$-несепарабельным состоянием тогда и только тогда, когда не равна нулю хотя бы одна величина из набора $V_{tj}^{(i)}$, где $i \in \{0,\ 1,\ 2,\ 3,\ 4,\ 5\}$; $t \in \{2,\ 3\}$; $j \in \{1,\ 2\}$ при $t = 2$; $j = 1$ при $t = 3$.

Из равенств (2.5.3) – (2.5.20) следует, что справедливо равенство

$$V_{31}^{(i)} = V_{21}^{(i)} \cup V_{22}^{(i)} \tag{2.5.23}$$

для каждого $i \in \{0,\ 1,\ 2,\ 3,\ 4,\ 5\}$.

Учитывая (2.5.23), из утверждения 2.5.21 получаем следствие, в котором используется понятие $(s_i;\ *)$-несепарабельности, введенное в определении 2.4.8, в отношении состояния трехкубитной квантовой системы.

Следствие 2.5.24. Пусть $i \in \{0,\ 1,\ 2,\ 3,\ 4,\ 5\}$. Состояние $|\psi\rangle$ трехкубитной квантовой системы $A_1A_2A_3$ является $(s_i;\ *)$-несепарабельным состоянием тогда и только тогда, когда в каждом из наборов $V_{21}^{(i)}$ и $V_{22}^{(i)}$ имеется хотя бы одна величина, не равная нулю.

Используя понятие $\left(*;\ m_{n,t}^{(j)}\right)$-несепарабельности, введенное в определении 2.4.9, в отношении состояния трехкубитной квантовой системы, из утверждения 2.5.21 получаем:

Следствие 2.5.25.

а) Пусть $j \in \{1,\ 2\}$. Состояние $|\psi\rangle$ трехкубитной квантовой системы $A_1A_2A_3$ является $\left(*;\ m_{3,2}^{(j)}\right)$-несепарабельным состоянием тогда и только тогда, когда для любого $i \in \{0,\ 1,\ 2,\ 3,\ 4,\ 5\}$ в наборе $V_{2j}^{(i)}$ имеется хотя бы одна величина, не равная нулю.

б) Состояние $|\psi\rangle$ трехкубитной квантовой системы $A_1A_2A_3$ является $\left(*;\ m_{3,3}^{(1)}\right)$-несепарабельным состоянием тогда и только тогда, когда для любого $i \in \{0,\ 1,\ 2,\ 3,\ 4,\ 5\}$ в наборе $V_{31}^{(i)}$ имеется хотя бы одна величина, не равная нулю.

Используя понятие t-несепарабельности, введенное в определении 2.4.10, в отношении состояния трехкубитной квантовой системы, из утверждения 2.5.21 получаем:

Следствие 2.5.26.

а) Состояние $|\psi\rangle$ трехкубитной квантовой системы $A_1A_2A_3$ является 2-несепарабельным состоянием тогда и только тогда, когда для любого $i \in \{0,\ 1,\ 2,\ 3,\ 4,\ 5\}$ и для любого $j \in \{1,\ 2\}$ в наборе $V_{2j}^{(i)}$ имеется хотя бы одна величина, не равная нулю.

б) Состояние $|\psi\rangle$ трехкубитной квантовой системы $A_1A_2A_3$ является 3-несепарабельным состоянием тогда и только тогда, когда для любого $i \in \{0,\ 1,\ 2,\ 3,\ 4,\ 5\}$ в наборе $V_{31}^{(i)}$ имеется хотя бы одна величина, не равная нулю.

Используя понятие несепарабельности, введенное в определении 2.4.11, в отношении состояния трехкубитной квантовой системы, и учитывая равенство (2.5.23), из утверждения 2.5.21 получаем

Следствие 2.5.27.

а) Состояние $|\psi\rangle$ трехкубитной квантовой системы $A_1A_2A_3$ является несепарабельным состоянием тогда и только тогда, когда для любого

$i \in \{0,\ 1,\ 2,\ 3,\ 4,\ 5\}$ и для любого $j \in \{1,\ 2\}$ в наборе $V_{2j}^{(i)}$ имеется хотя бы одна величина, не равная нулю.

б) **Критерий Константин₃ (Критерий К₃)**. Состояние $|\psi\rangle$ трехкубитной квантовой системы $A_1A_2A_3$ является несепарабельным состоянием тогда и только тогда, когда для любого $i \in \{0,\ 1,\ 2\}$ в наборе $V_{21}^{(i)}$ имеется хотя бы одна величина, не равная нулю.

Приведем пример 2.5.28, в котором вышеизложенные результаты применяются к трехкубитному состоянию из примера 2.4.3.

Пример 2.5.28. Рассмотрим следующее состояние квантовой системы $A_1A_2A_3$:

$$|\psi\rangle = \frac{|000\rangle + |101\rangle}{\sqrt{2}}.$$

Из равенства (2.5.1) для состояния $|\psi\rangle$ имеем

$$|\psi\rangle = \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_7 \end{pmatrix} = \begin{pmatrix} 1/\sqrt{2} \\ 0 \\ 0 \\ 0 \\ 0 \\ 1/\sqrt{2} \\ 0 \\ 0 \end{pmatrix}.$$

Подставляя эти значения координат состояния $|\psi\rangle$ в равенства (2.5.3) – (2.5.20), получаем:

$$V_{21}^{(0)} = \{½,0,0,0,0,0\},\ V_{22}^{(0)} = \{0,½,0,0,0,0\},\ V_{31}^{(0)} = \{½,0,0,0,0,0,0,0,0,0\},$$

$$V_{21}^{(1)} = \{0,0,0,0,0,0\},\ V_{22}^{(1)} = \{½,0,0,0,0,0\},\ V_{31}^{(1)} = \{0,0,0,0,0,0,½,0,0,0\},$$

$$V_{21}^{(2)} = \{½,0,0,0,0,0\},\ V_{22}^{(2)} = \{0,½,0,0,0,0\},\ V_{31}^{(2)} = \{½,0,0,0,0,0,0,0,0,0\},$$

$V_{21}^{(3)} = \{0, ½, 0, 0, 0, 0\}$, $V_{22}^{(3)} = \{0, 0, 0, 0, 0, 0\}$, $V_{31}^{(3)} = \{0, ½, 0, 0, 0, 0, 0, 0, 0, 0\}$,

$V_{21}^{(4)} = \{0, 0, 0, 0, 0, 0\}$, $V_{22}^{(4)} = \{½, 0, 0, 0, 0, 0\}$, $V_{31}^{(4)} = \{0, 0, 0, 0, 0, 0, ½, 0, 0, 0\}$,

$V_{21}^{(5)} = \{0, ½, 0, 0, 0, 0\}$, $V_{22}^{(5)} = \{0, 0, 0, 0, 0, 0\}$, $V_{31}^{(5)} = \{0, ½, 0, 0, 0, 0, 0, 0, 0, 0\}$.

Из следствий 2.5.22, 2.5.24 – 2.5.27, с учетом вычисленных значений величин в каждом наборе $V_{tj}^{(i)}$, (где $i \in \{0,\ 1,\ 2,\ 3,\ 4,\ 5\}$; $t \in \{2,\ 3\}$; $j \in \{1,\ 2\}$ при $t = 2$; $j = 1$ при $t = 3$), для состояния $|\psi\rangle$ имеем, что оно является:

- $\left(s_0;\ m_{3,t}^{(j)}\right)$-несепарабельным состоянием для любых $t \in \{2,\ 3\}$ и j, таких, что $j \in \{1,\ 2\}$ при $t = 2$ и $j = 1$ при $t = 3$, из-за того, что при таких значениях индексов t и j каждый из наборов $V_{tj}^{(0)}$ содержит элемент, не равный нулю;
- $\left(s_1;\ m_{3,t}^{(j)}\right)$-несепарабельным состоянием для любых $t \in \{2,\ 3\}$ и j, таких, что $j = 2$ при $t = 2$ и $j = 1$ при $t = 3$, из-за того, что при таких значениях индексов t и j каждый из наборов $V_{tj}^{(1)}$ содержит элемент, не равный нулю;
- $\left(s_1;\ m_{3,2}^{(1)}\right)$-сепарабельным состоянием, так как в наборе $V_{21}^{(1)}$ все элементы равны нулю;
- $\left(s_2;\ m_{3,t}^{(j)}\right)$-несепарабельным состоянием для любых $t \in \{2,\ 3\}$ и j, таких, что $j \in \{1,\ 2\}$ при $t = 2$ и $j = 1$ при $t = 3$, из-за того, что при таких значениях индексов t и j каждый из наборов $V_{tj}^{(2)}$ содержит элемент, не равный нулю;
- $\left(s_3;\ m_{3,t}^{(j)}\right)$-несепарабельным состоянием для любых $t \in \{2,\ 3\}$ и $j = 1$ из-за того, что при таких значениях индексов t и j каждый из наборов $V_{tj}^{(3)}$ содержит элемент, не равный нулю;

- $\left(s_3;\ m_{3,2}^{(2)}\right)$-сепарабельным состоянием, так как в наборе $V_{22}^{(3)}$ все элементы равны нулю;
- $\left(s_4;\ m_{3,t}^{(j)}\right)$-несепарабельным состоянием для любых $t \in \{2,\ 3\}$ и j, таких, что $j = 2$ при $t = 2$ и $j = 1$ при $t = 3$, из-за того, что при таких значениях индексов t и j каждый из наборов $V_{tj}^{(4)}$ содержит элемент, не равный нулю;
- $\left(s_4;\ m_{3,2}^{(1)}\right)$-сепарабельным состоянием, так как в наборе $V_{21}^{(4)}$ все элементы равны нулю;
- $\left(s_5;\ m_{3,t}^{(j)}\right)$-несепарабельным состоянием для любых $t \in \{2,\ 3\}$ и $j = 1$ из-за того, что при таких значениях индексов t и j каждый из наборов $V_{tj}^{(5)}$ содержит элемент, не равный нулю;
- $\left(s_5;\ m_{3,2}^{(2)}\right)$-сепарабельным состоянием, так как в наборе $V_{22}^{(5)}$ все элементы равны нулю;
- $(s_i;\ *)$-несепарабельным состоянием для любого $i \in \{0,\ 2\}$;
- $(s_i;\ *)$-сепарабельным состоянием для любого $i \in \{1,\ 3,\ 4,\ 5\}$;
- $\left(*;\ m_{3,t}^{(j)}\right)$-сепарабельным состоянием для любых $j \in \{1,\ 2\}$ и $t = 2$;
- $\left(*;\ m_{3,3}^{(1)}\right)$-несепарабельным состоянием;
- 2-сепарабельным состоянием;
- 3-несепарабельным состоянием;
- сепарабельным состоянием.

Теперь приступим к обещанному выше доказательству утверждения 2.5.21.

Доказательство утверждения 2.5.21. Пусть $i = 0$. Утверждение 2.5.21 при данном значении индекса $i = 0$ сводится к утверждению 2.3.4, сформулированному и доказанному в параграфе 2.3. Действительно, отвечающая этому значению индекса $i = 0$ подстановка s_0 из симметрической группы подстановок $\mathbb{S}_3$ является тождественным преобразованием. Следовательно, для любого состояния $|\psi\rangle$ трехкубитной квантовой системы $A_1A_2A_3$ справедливо равенство

$$\left|\psi^{(s_0)}\right\rangle = |\psi\rangle,$$

где, напомним, при $s \in \mathbb{S}_3$ состояние $\left|\psi^{(s)}\right\rangle$ – это состояние квантовой системы $A_{s(1)}A_{s(2)}A_{s(3)}$.

Теперь, чтобы воспользоваться утверждением 2.3.4 из параграфа 2.3, положим $A_1A_2A_3$ = ABC и последовательно переберем все возможные значения остальных индексов t и j.

Первой рассмотрим пару значений $t = 2$, $j = 1$. Тогда учитывая, что соответствующий этой паре набор величин $V_{21}^{(0)}$ совпадает с набором величин V_1, V_2, V_3, V_4, V_5, V_6, определенных в параграфе 2.3 (см. (2.3.3)), и соответствующее разбиение $m_{3,2}^{(1)}$ числа 3 совпадает с (1, 2), убеждаемся, что в данном случае утверждение 2.5.21 совпадает с пунктом (а) утверждения 2.3.4.

Следующая пара значений – это $t = 2$, $j = 2$. Соответствующий этой паре набор величин $V_{22}^{(0)}$ совпадает с набором величин Y_1, Y_2, Y_3, Y_4, Y_5, Y_6, определенных в параграфе 2.3 (см. (2.3.3)), и соответствующее разбиение $m_{3,2}^{(2)}$ числа 3 совпадает с $(2, 1)$. Отсюда следует, что в данном случае утверждение 2.5.21 совпадает уже с другим пунктом утверждения 2.3.4, а именно – с пунктом (б).

Наконец, рассмотрим последнюю пару значений $t = 3$ и $j = 1$. В этом случае соответствующий набор величин $V_{31}^{(0)}$ совпадает с объединением наборов $V_{21}^{(0)}$ и $V_{22}^{(0)}$. И поэтому равенство нулю всех величин из набора $V_{31}^{(0)}$ эквивалентно равенству нулю всех величин каждого из наборов

$V_{21}^{(0)}$ и $V_{22}^{(0)}$, что, в свою очередь, равносильно одновременной $\left(s_0;\ m_{3,2}^{(1)}\right)$-сепарабельности и $\left(s_0;\ m_{3,2}^{(2)}\right)$-сепарабельности состояния $|\psi\rangle$ трехкубитной квантовой системы $A_1A_2A_3$. Таким образом, равенство нулю всех величин из набора $V_{31}^{(0)}$ равносильно выполнению для состояния $|\psi\rangle$ следующих двух равенств:

$$|\psi\rangle = |\varphi_1\rangle \otimes |\varphi_{23}\rangle \tag{2.5.29}$$

и

$$|\psi\rangle = |\varphi_{12}\rangle \otimes |\varphi_3\rangle, \tag{2.5.30}$$

где

$$|\varphi_1\rangle = \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix}$$

– состояние однокубитной квантовой системы A_1,

$$|\varphi_{23}\rangle = \begin{pmatrix} \beta_0 \\ \beta_1 \\ \beta_2 \\ \beta_3 \end{pmatrix}$$

– состояние двухкубитной квантовой системы A_2A_3,

$$|\varphi_{12}\rangle = \begin{pmatrix} \gamma_0 \\ \gamma_1 \\ \gamma_2 \\ \gamma_3 \end{pmatrix}$$

– состояние двухкубитной квантовой системы A_1A_2,

$$|\varphi_3\rangle = \begin{pmatrix} \sigma_0 \\ \sigma_1 \end{pmatrix}$$

– состояние однокубитной квантовой системы A_3;

$$\alpha_0,\ \alpha_1,\ \beta_0,\ \beta_1,\ \beta_2,\ \beta_3,\ \gamma_0,\ \gamma_1,\ \gamma_2,\ \gamma_3,\ \sigma_0,\ \sigma_1 \in \mathbb{C}.$$

Совокупность равенств (2.5.29) и (2.5.30) равносильна цепочке равенств

$$|\psi\rangle = \begin{pmatrix} \alpha_0\beta_0 \\ \alpha_0\beta_1 \\ \alpha_0\beta_2 \\ \alpha_0\beta_3 \\ \alpha_1\beta_0 \\ \alpha_1\beta_1 \\ \alpha_1\beta_2 \\ \alpha_1\beta_3 \end{pmatrix} = \begin{pmatrix} \gamma_0\sigma_0 \\ \gamma_0\sigma_1 \\ \gamma_1\sigma_0 \\ \gamma_1\sigma_1 \\ \gamma_2\sigma_0 \\ \gamma_2\sigma_1 \\ \gamma_3\sigma_0 \\ \gamma_3\sigma_1 \end{pmatrix}. \tag{2.5.31}$$

Из условия, что вектор $\begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix}$ является состоянием однокубитной квантовой системы, следует, что комплексные числа α_0 и α_1 не могут быть одновременно равны нулю, то есть хотя бы одно из этих чисел отлично от нуля. Для определенности положим, что $\alpha_0 \neq 0$. В этом случае из равенств (2.5.31) следует справедливость следующей цепочки равенств:

$$\beta_0\beta_3 - \beta_1\beta_2 = \frac{1}{\alpha_0^2}\left(\alpha_0^2\beta_0\beta_3 - \alpha_0^2\beta_1\beta_2\right) =$$

$$= \frac{1}{\alpha_0^2}\left(\alpha_0\beta_0\alpha_0\beta_3 - \alpha_0\beta_1\alpha_0\beta_2\right) = \frac{1}{\alpha_0^2}\left(\gamma_0\sigma_0\gamma_1\sigma_1 - \gamma_0\sigma_1\gamma_1\sigma_0\right) = 0.$$

Отсюда и из утверждения 2.2.8 следует, что состояние $|\varphi_{23}\rangle$ двухкубитной квантовой системы A_2A_3 является сепарабельным состоянием, то есть справедливо равенство

$$|\varphi_{23}\rangle = |\phi_2\rangle \otimes |\phi_3\rangle,$$

где $|\phi_2\rangle$ – состояние однокубитной квантовой системы A_2, а $|\phi_3\rangle$ – состояние однокубитной квантовой системы A_3. Отсюда и из (2.5.29) следует, что

$$\left|\psi\right\rangle = \left|\varphi_1\right\rangle \otimes \left|\phi_2\right\rangle \otimes \left|\phi_3\right\rangle,$$

и тем самым доказано, что условие равенства нулю всех величин из набора $V_{31}^{(0)}$ влечет $\left(s_0;\ m_{3,3}^{(1)}\right)$-сепарабельность состояния $\left|\psi\right\rangle$ квантовой системы $A_1A_2A_3$.

Теперь докажем в обратную сторону, а именно, то, что если состояние $\left|\psi\right\rangle$ квантовой системы $A_1A_2A_3$ является $\left(s_0;\ m_{3,3}^{(1)}\right)$-сепарабельным состоянием, то равны нулю все величины из набора $V_{31}^{(0)}$. Действительно, условие, что состояние $\left|\psi\right\rangle$ является $\left(s_0;\ m_{3,3}^{(1)}\right)$-сепарабельным состоянием, влечет за собой справедливость равенства

$$\left|\psi\right\rangle = \left|\phi_1\right\rangle \otimes \left|\phi_2\right\rangle \otimes \left|\phi_3\right\rangle,$$

где $\left|\phi_k\right\rangle$ – состояние квантовой системы A_k, $k = \overline{1,3}$. Тогда, полагая

$$\left|\varphi_1\right\rangle = \left|\phi_1\right\rangle,\ \left|\varphi_{23}\right\rangle = \left|\phi_2\right\rangle \otimes \left|\phi_3\right\rangle,\ \left|\varphi_{12}\right\rangle = \left|\phi_1\right\rangle \otimes \left|\phi_2\right\rangle,\ \left|\varphi_3\right\rangle = \left|\phi_3\right\rangle,$$

имеем

$$\left|\psi\right\rangle = \left|\varphi_1\right\rangle \otimes \left|\varphi_{23}\right\rangle$$

и

$$\left|\psi\right\rangle = \left|\varphi_{12}\right\rangle \otimes \left|\varphi_3\right\rangle,$$

где $\left|\varphi_1\right\rangle$ – состояние однокубитной квантовой системы A_1, $\left|\varphi_{23}\right\rangle$ – состояние двухкубитной квантовой системы A_2A_3, $\left|\varphi_{12}\right\rangle$ – состояние двухкубитной квантовой системы A_1A_2, $\left|\varphi_3\right\rangle$ – состояние однокубитной квантовой системы A_3. Последние два равенства означают соответственно, что состояние $\left|\psi\right\rangle$ является $\left(s_0;\ m_{3,2}^{(1)}\right)$-сепарабельным состоянием и $\left(s_0;\ m_{3,2}^{(2)}\right)$-сепарабельным состоянием, что, в свою очередь, влечет равенство нулю всех величин из наборов $V_{21}^{(0)}$ и $V_{22}^{(0)}$, а следовательно, и из набора $V_{31}^{(0)}$ как объединения наборов $V_{21}^{(0)}$ и $V_{22}^{(0)}$.

Таким образом, утверждение 2.5.21 для случая $i = 0$ полностью доказано. Эту часть доказательства будем считать первой частью доказательства утверждения 2.5.21.

Теперь приступим ко второй части доказательства утверждения 2.5.21.

Пусть $i > 0$. Из равенства (2.5.1) следует, что

$$|\psi\rangle = \sum_{k=0}^{7} a_k \,|\delta_{k1}\delta_{k2}\delta_{k3}\rangle,$$

где $\delta_{kr} \in \{0,\ 1\}$, $k = 4\delta_{k1} + 2\delta_{k2} + \delta_{k3}$, $r = \overline{1,3}$, $k = \overline{0,7}$. Тогда для состояния $\left|\psi^{(s_i)}\right\rangle$ трехкубитной квантовой системы $\mathrm{A}_{s_i(1)}\mathrm{A}_{s_i(2)}\mathrm{A}_{s_i(3)} = \mathrm{B}_1\mathrm{B}_2\mathrm{B}_3$ (здесь B_r – новое обозначение кубита $\mathrm{A}_{s_i(r)}$, $r = \overline{1,3}$), верна цепочка равенств

$$\left|\psi^{(s_i)}\right\rangle = \sum_{k=0}^{7} a_k \left|\delta_{ks_i(1)}\delta_{ks_i(2)}\delta_{ks_i(3)}\right\rangle = \sum_{k=0}^{7} b_k \,|\delta_{k1}\delta_{k2}\delta_{k3}\rangle,$$

где

$$b_k = a_{\breve{s}_i^{-1}(k)}, \tag{2.5.32}$$

$\breve{s}_i^{-1}$ – подстановка на множестве чисел $\{0,\ 1,\ \ldots,\ 7\}$, обратная к подстановке $\breve{s}_i$, задаваемой равенством

$$\breve{s}_i(k) = 4\delta_{ks_i(1)} + 2\delta_{ks_i(2)} + \delta_{ks_i(3)}, \tag{2.5.33}$$

для любого $k \in \{0,\ 1,\ \ldots,\ 7\}$.

Обратим теперь внимание на то, что условие, заключающееся в $\left(s_i;\ m_{3,t}^{(j)}\right)$-сепарабельности состояния $|\psi\rangle$ квантовой системы $\mathrm{A}_1\mathrm{A}_2\mathrm{A}_3$, равносильно условию $\left(s_0;\ m_{3,t}^{(j)}\right)$-сепарабельности состояния $\left|\psi^{(s_i)}\right\rangle$ квантовой системы $\mathrm{B}_1\mathrm{B}_2\mathrm{B}_3$, где $t \in \{2,\ 3\}$; $j \in \{1,\ 2\}$ при $t = 2$; $j = 1$ при

$t = 3$. Положим $W_{tj}^{(0)}$ – набор величин, получающийся из набора величин $V_{tj}^{(0)}$ заменой каждого коэффициента a_k на коэффициент b_k для любого $k \in \{0,\ 1,\ \ldots,\ 7\}$. Тогда из первой части доказательства утверждения 2.5.21 следует, что состояние $\left|\psi^{(s_i)}\right\rangle$ квантовой системы $B_1B_2B_3$ – $\left(s_0;\ m_{3,t}^{(j)}\right)$-сепарабельное состояние тогда и только тогда, когда равны нулю все величины из набора $W_{tj}^{(0)}$, где $t \in \{2,\ 3\}$; $j \in \{1,\ 2\}$ при $t = 2$; $j = 1$ при $t = 3$. И, таким образом, имеем, что состояние $|\psi\rangle$ квантовой системы $A_1A_2A_3$ – $\left(s_i;\ m_{3,t}^{(j)}\right)$-сепарабельное состояние тогда и только тогда, когда равны нулю все величины из набора $W_{tj}^{(0)}$, где $t \in \{2,\ 3\}$; $j \in \{1,\ 2\}$ при $t = 2$; $j = 1$ при $t = 3$. Наконец, обратим внимание на то, что соотношения, определяемые равенством (2.5.32), влекут справедливость равенства

$$W_{tj}^{(0)} = V_{tj}^{(i)}$$

(что можно непосредственно проверить, используя (2.5.3) – (2.5.20)). Следовательно, состояние $|\psi\rangle$ квантовой системы $A_1A_2A_3$ – $\left(s_i;\ m_{3,t}^{(j)}\right)$-сепарабельное состояние тогда и только тогда, когда равны нулю все величины из набора $V_{tj}^{(i)}$. Утверждение 2.5.21 доказано полностью.

§ 2.6. Состояния четырехкубитных квантовых систем

В вычислительном базисе из векторов

$$|0000\rangle,\ |0001\rangle,\ |0010\rangle,\ |0011\rangle, |0100\rangle,\ |0101\rangle,\ |0110\rangle,\ |0111\rangle,$$

$$|1000\rangle,\ |1001\rangle,\ |1010\rangle,\ |1011\rangle,\ |1100\rangle,\ |1101\rangle,\ |1110\rangle,\ |1111\rangle$$

произвольное четырехкубитное состояние можно представить в следующем общем виде:

$$\begin{aligned}|\psi\rangle = a_0|0000\rangle + a_1|0001\rangle + a_2|0010\rangle + a_3|0011\rangle + \\ + a_4|0100\rangle + a_5|0101\rangle + a_6|0110\rangle + a_7|0111\rangle + \\ + a_8|1000\rangle + a_9|1001\rangle + a_{10}|1010\rangle + a_{11}|1011\rangle + \\ + a_{12}|1100\rangle + a_{13}|1101\rangle + a_{14}|1110\rangle + a_{15}|1111\rangle,\end{aligned} \qquad (2.6.1)$$

где $a_0,\ a_1,\ \ldots,\ a_{15} \in \mathbb{C}$,

$$|a_0|^2 + |a_1|^2 + \ldots + |a_{15}|^2 = 1. \qquad (2.6.2)$$

Из (2.6.1) и (2.6.2) следует, что любой нормированный вектор шестнадцатимерного гильбертова пространства $\mathbb{C}^{16}$ над полем комплексных чисел $\mathbb{C}$ может служить состоянием четырехкубитной квантовой системы. Поэтому нормированные векторы гильбертова пространства $\mathbb{C}^{16}$ будем также называть состояниями четырехкубитных квантовых систем или четырехкубитными состояниями.

Как и в случае трехкубитных квантовых систем, для произвольного состояния четырехкубитной квантовой системы условие неразложимости в тензорное произведение состояний меньшей размерности и условие несепарабельности не являются равносильными. Из несепарабельности состояния четырехкубитной квантовой системы следует его неразложимость в тензорное произведение состояний меньшей размерности. Но обратное в общем случае неверно, то есть из неразложимости состояния четырехкубитной квантовой системы в тензорное произведение состояний меньшей размерности не следует его несепарабельность. Частными случаями подтверждения последнего утверждения могут служить четырехкубитные состояния $\left|\psi_{72}^{(4)}\right\rangle$ и $\left|\psi_{82}^{(4)}\right\rangle$, представленные в параграфе 5.3.

Следующее утверждение представляет собой критерий неразложимости состояния четырехкубитной квантовой системы в тензорное произведение состояний меньшей размерности. В формулировке этого утверждения используются наборы величин V_0, V_1 и V_2, определенные ниже в данном параграфе равенствами (2.6.5), (2.6.6) и (2.6.7) соответственно.

Утверждение 2.6.3. Состояние $|\psi\rangle \in \mathbb{C}^{16}$ четырехкубитной квантовой системы неразложимо в тензорное произведение состояний меньшей размерности тогда и только тогда, когда каждый из трех наборов величин V_0, V_1 и V_2 содержит хотя бы одну величину, неравную нулю.

Критерий несепарабельности состояния четырехкубитной квантовой системы (то есть **критерий Константин$_4$**) представим в виде следующего утверждения, в формулировке которого используются наборы величин V_0, V_1, …, V_6, определенные ниже в данном параграфе равенствами (2.6.5), (2.6.6), …, (2.6.11) соответственно.

Утверждение 2.6.4. Критерий Константин$_4$ (Критерий К$_4$). Состояние $|\psi\rangle \in \mathbb{C}^{16}$ четырехкубитной квантовой системы является несепарабельным состоянием тогда и только тогда, когда каждый из семи наборов величин V_0, V_1, …, V_6 содержит хотя бы одну величину, неравную нулю.

Утверждения 2.6.3 и 2.6.4 доказываются аналогично соответствующим утверждениям для состояний трехкубитных квантовых систем, сформулированным и доказанным ранее в данной главе.

Для состояния $|\psi\rangle \in \mathbb{C}^{16}$, заданного равенством (2.6.1), указанные выше наборы величин V_0, V_1, …, V_6 определяются следующими равенствами:

$$\begin{aligned}
V_0 = \{&a_0a_9 - a_1a_8,\ a_0a_{10} - a_2a_8,\ a_0a_{11} - a_3a_8,\ a_0a_{12} - a_4a_8,\\
&a_0a_{13} - a_5a_8,\ a_0a_{14} - a_6a_8,\ a_0a_{15} - a_7a_8,\\
&a_1a_{10} - a_2a_9,\ a_1a_{11} - a_3a_9,\ a_1a_{12} - a_4a_9,\ a_1a_{13} - a_5a_9,\\
&a_1a_{14} - a_6a_9,\ a_1a_{15} - a_7a_9,\ a_2a_{11} - a_3a_{10},\\
&a_2a_{12} - a_4a_{10},\ a_2a_{13} - a_5a_{10},\ a_2a_{14} - a_6a_{10},\ a_2a_{15} - a_7a_{10},\\
&a_3a_{12} - a_4a_{11},\ a_3a_{13} - a_5a_{11},\ a_3a_{14} - a_6a_{11},\ a_3a_{15} - a_7a_{11},\\
&a_4a_{13} - a_5a_{12},\ a_4a_{14} - a_6a_{12},\ a_4a_{15} - a_7a_{12},\\
&a_5a_{14} - a_6a_{13},\ a_5a_{15} - a_7a_{13},\ a_6a_{15} - a_7a_{14}\},
\end{aligned} \tag{2.6.5}$$

$$
\begin{gathered}
V_1=\{a_0a_5-a_1a_4,\ a_0a_6-a_2a_4,\ a_0a_7-a_3a_4,\ a_0a_9-a_1a_8,\ a_0a_{10}-a_2a_8,\\
a_0a_{11}-a_3a_8,\ a_0a_{13}-a_1a_{12},\ a_0a_{14}-a_2a_{12},\ a_0a_{15}-a_3a_{12},\ a_1a_6-a_2a_5,\\
a_1a_7-a_3a_5,\ a_1a_{10}-a_2a_9,\ a_1a_{11}-a_3a_9,\ a_1a_{14}-a_2a_{13},\ a_1a_{15}-a_3a_{13},\\
a_2a_7-a_3a_6,\ a_2a_{11}-a_3a_{10},\ a_2a_{15}-a_3a_{14},\ a_4a_9-a_5a_8,\ a_4a_{10}-a_6a_8,\\
a_4a_{11}-a_7a_8,\ a_4a_{13}-a_5a_{12},\ a_4a_{14}-a_6a_{12},\ a_4a_{15}-a_7a_{12}, a_5a_{10}-a_6a_9,\\
a_5a_{11}-a_7a_9,\ a_5a_{14}-a_6a_{13},\ a_5a_{15}-a_7a_{13}, a_6a_{11}-a_7a_{10},\ a_6a_{15}-a_7a_{14},\\
a_8a_{13}-a_9a_{12},\ a_8a_{14}-a_{10}a_{12},\ a_8a_{15}-a_{11}a_{12},\\
a_9a_{14}-a_{10}a_{13},\ a_9a_{15}-a_{11}a_{13},\ a_{10}a_{15}-a_{11}a_{14}\},
\end{gathered}
\tag{2.6.6}
$$

$$
\begin{aligned}
V_2=\{&a_0a_3-a_1a_2,\ a_0a_5-a_1a_4,\ a_0a_7-a_1a_6,\ a_0a_9-a_1a_8,\\
&a_0a_{11}-a_1a_{10},\ a_0a_{13}-a_1a_{12},\ a_0a_{15}-a_1a_{14},\\
&a_2a_5-a_3a_4,\ a_2a_7-a_3a_6,\ a_2a_9-a_3a_8,\\
&a_2a_{11}-a_3a_{10},\ a_2a_{13}-a_3a_{12},\ a_2a_{15}-a_3a_{14},\\
&a_4a_7-a_5a_6,\ a_4a_9-a_5a_8,\ a_4a_{11}-a_5a_{10},\\
&a_4a_{13}-a_5a_{12},\ a_4a_{15}-a_5a_{14},\\
&a_6a_9-a_7a_8,\ a_6a_{11}-a_7a_{10},\ a_6a_{13}-a_7a_{12},\ a_6a_{15}-a_7a_{14},\\
&a_8a_{11}-a_9a_{10},\ a_8a_{13}-a_9a_{12},\ a_8a_{15}-a_9a_{14},\\
&a_{10}a_{13}-a_{11}a_{12},\ a_{10}a_{15}-a_{11}a_{14},\ a_{12}a_{15}-a_{13}a_{14}\},
\end{aligned}
\tag{2.6.7}
$$

$$
\begin{aligned}
V_3=\{&a_0a_5-a_1a_4,\ a_0a_6-a_2a_4,\ a_0a_7-a_3a_4,\ a_0a_{12}-a_8a_4,\\
&a_0a_{13}-a_9a_4,\ a_0a_{14}-a_{10}a_4,\ a_0a_{15}-a_{11}a_4,\\
&a_1a_6-a_2a_5,\ a_1a_7-a_3a_5,\ a_1a_{12}-a_8a_5,\ a_1a_{13}-a_9a_5,\\
&a_1a_{14}-a_{10}a_5,\ a_1a_{15}-a_{11}a_5,\ a_2a_7-a_3a_6,\ a_2a_{12}-a_8a_6,\\
&a_2a_{13}-a_9a_6,\ a_2a_{14}-a_{10}a_6,\ a_2a_{15}-a_{11}a_6,\\
&a_3a_{12}-a_8a_7,\ a_3a_{13}-a_9a_7,\ a_3a_{14}-a_{10}a_7,\ a_3a_{15}-a_{11}a_7,\\
&a_8a_{13}-a_9a_{12},\ a_8a_{14}-a_{10}a_{12},\ a_8a_{15}-a_{11}a_{12},\\
&a_9a_{14}-a_{10}a_{13},\ a_9a_{15}-a_{11}a_{13},\ a_{10}a_{15}-a_{11}a_{14}\},
\end{aligned}
\tag{2.6.8}
$$

$$
\begin{aligned}
&V_4 = \{a_0a_3 - a_1a_2,\ a_0a_6 - a_4a_2,\ a_0a_7 - a_5a_2,\ a_0a_{10} - a_8a_2, \\
&a_0a_{11} - a_9a_2,\ a_0a_{14} - a_{12}a_2,\ a_0a_{15} - a_{13}a_2,\ a_1a_6 - a_4a_3, \\
&a_1a_7 - a_5a_3,\ a_1a_{10} - a_8a_3,\ a_1a_{11} - a_9a_3,\ a_1a_{14} - a_{12}a_3, \\
&a_1a_{15} - a_{13}a_3,\ a_4a_7 - a_5a_6,\ a_4a_{10} - a_8a_6,\ a_4a_{11} - a_9a_6, \\
&a_4a_{14} - a_{12}a_6,\ a_4a_{15} - a_{13}a_6, \\
&a_5a_{10} - a_8a_7,\ a_5a_{11} - a_9a_7,\ a_5a_{14} - a_{12}a_7,\ a_5a_{15} - a_{13}a_7, \\
&a_8a_{11} - a_9a_{10},\ a_8a_{14} - a_{12}a_{10},\ a_8a_{15} - a_{13}a_{10}, \\
&a_9a_{14} - a_{12}a_{11},\ a_9a_{15} - a_{13}a_{11},\ a_{12}a_{15} - a_{13}a_{14}\},
\end{aligned}
\tag{2.6.9}
$$

$$
\begin{aligned}
&V_5 = \{a_0a_9 - a_1a_8,\ a_0a_{12} - a_4a_8,\ a_0a_{13} - a_5a_8,\ a_0a_3 - a_1a_2, \\
&a_0a_6 - a_4a_2, a_0a_7 - a_5a_2,\ a_0a_{11} - a_1a_{10},\ a_0a_{14} - a_4a_{10}, \\
&a_0a_{15} - a_5a_{10}, a_1a_{12} - a_4a_9,\ a_1a_{13} - a_5a_9,\ a_1a_6 - a_4a_3, \\
&a_1a_7 - a_5a_3,\ a_1a_{14} - a_4a_{11},\ a_1a_{15} - a_5a_{11}, a_4a_{13} - a_5a_{12}, \\
&a_4a_7 - a_5a_6,\ a_4a_{15} - a_5a_{14}, a_8a_3 - a_9a_2,\ a_8a_6 - a_{12}a_2, \\
&a_8a_7 - a_{13}a_2, a_8a_{11} - a_9a_{10},\ a_8a_{14} - a_{12}a_{10},\ a_8a_{15} - a_{13}a_{10}, \\
&a_9a_6 - a_{12}a_3,\ a_9a_7 - a_{13}a_3,\ a_9a_{14} - a_{12}a_{11},\ a_9a_{15} - a_{13}a_{11}, \\
&a_{12}a_7 - a_{13}a_6,\ a_{12}a_{15} - a_{13}a_{14}, \\
&a_2a_{11} - a_3a_{10},\ a_2a_{14} - a_6a_{10},\ a_2a_{15} - a_7a_{10}, \\
&a_3a_{14} - a_6a_{11},\ a_3a_{15} - a_7a_{11},\ a_6a_{15} - a_7a_{14}\},
\end{aligned}
\tag{2.6.10}
$$

$$
\begin{aligned}
&V_6 = \{a_0a_{10} - a_2a_8,\ a_0a_{12} - a_4a_8,\ a_0a_{14} - a_6a_8,\ a_0a_3 - a_2a_1, \\
&a_0a_5 - a_4a_1, a_0a_7 - a_6a_1,\ a_0a_{11} - a_2a_9,\ a_0a_{13} - a_4a_9, \\
&a_0a_{15} - a_6a_9, a_2a_{12} - a_4a_{10},\ a_2a_{14} - a_6a_{10},\ a_2a_5 - a_4a_3, \\
&a_2a_7 - a_6a_3,\ a_2a_{13} - a_4a_{11},\ a_2a_{15} - a_6a_{11}, a_4a_{14} - a_6a_{12}, \\
&a_4a_7 - a_6a_5,\ a_4a_{15} - a_6a_{13}, a_8a_3 - a_{10}a_1,\ a_8a_5 - a_{12}a_1, \\
&a_8a_7 - a_{14}a_1, a_8a_{11} - a_{10}a_9,\ a_8a_{13} - a_{12}a_9,\ a_8a_{15} - a_{14}a_9, \\
&a_{10}a_5 - a_{12}a_3,\ a_{10}a_7 - a_{14}a_3,\ a_{10}a_{13} - a_{12}a_{11},\ a_{10}a_{15} - a_{14}a_{11}, \\
&a_{12}a_7 - a_{14}a_5,\ a_{12}a_{15} - a_{14}a_{13}, \\
&a_1a_{11} - a_3a_9,\ a_1a_{13} - a_5a_9,\ a_1a_{15} - a_7a_9, \\
&a_3a_{13} - a_5a_{11},\ a_3a_{15} - a_7a_{11},\ a_5a_{15} - a_7a_{13}\}.
\end{aligned}
\tag{2.6.11}
$$

Выводы по главе 2

1. В настоящее время уже экспериментально подтверждена техническая возможность искусственного создания и сохранения несепарабельных квантовых состояний в формах, пригодных для решения прикладных задач криптографии и связи.

2. Существует вычислительно несложный и удобный для практических и теоретических применений критерий несепарабельности состояния двухкубитной квантовой системы, основанный на отличии от нуля разности произведений крайних и средних коэффициентов разложения, представляющего состояние в вычислительном базисе.

3. Сформулированы новые определения понятий сепарабельности и несепарабельности относительно состояний квантовых систем, учитывающие сложную специфику связей составных компонент многокубитных квантовых систем. Определения, по существу, используют элементы симметрической группы подстановок на номерах кубитов, составляющих квантовую систему, и различного рода разбиений квантовой системы на подсистемы. В случае двухкубитных состояний новые определения понятий сепарабельности и несепарабельности совпадают с известными [56; 59].

4. В силу того, что определение 2.4.12 (эквивалентное определение – 2.4.11) занимает одно из центральных мест в данной работе, имеет смысл повторить его и в части выводов к главе 2.

Состояние $|\psi\rangle$ n-кубитной квантовой системы $A_1A_2\ldots A_n$ называется **сепарабельным состоянием**, если найдется подстановка $s \in \mathbb{S}_n$, такая, что состояние $\left|\psi^{(s)}\right\rangle$ квантовой системы $A_{s(1)}A_{s(2)}\ldots A_{s(n)}$ разлагается в тензорное произведение состояний размерности меньшей, чем 2^n.

Состояние $|\psi\rangle$ n-кубитной квантовой системы $A_1A_2\ldots A_n$ называется **несепарабельным состоянием**, если оно не является сепарабельным состоянием.

5. Сформулирован и доказан эффективный для практических применений и вычислительно несложный критерий – **критерий К$_3$** (**критерий Константин$_3$**) несепарабельности состояний трехкубитных квантовых систем. В силу большой значимости этого критерия для выявления несепарабельных состояний трехкубитных квантовых систем имеет смысл привести его автономное изложение и в части выводов к главе 2, что и будет осуществлено далее.

В вычислительном базисе из векторов

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

произвольное состояние $|\psi\rangle \in \mathbb{C}^8$ трехкубитной квантовой системы можно представить в следующем общем виде:

$$|\psi\rangle = a_0|000\rangle + a_1|001\rangle + a_2|010\rangle + a_3|011\rangle +$$
$$+ a_4|100\rangle + a_5|101\rangle + a_6|110\rangle + a_7|111\rangle,$$

где $\mathbb{C}$ – поле комплексных чисел, $a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7 \in \mathbb{C}$, $|a_0|^2 + |a_1|^2 + |a_2|^2 + |a_3|^2 + |a_4|^2 + |a_5|^2 + |a_6|^2 + |a_7|^2 = 1$.

Определим наборы величин V_0, V_1 и V_2 через следующие равенства:

$$V_0 = \{a_0a_5 - a_1a_4,\ a_0a_6 - a_2a_4,\ a_0a_7 - a_3a_4,$$
$$a_1a_6 - a_2a_5,\ a_1a_7 - a_3a_5,\ a_2a_7 - a_3a_6\},$$
$$V_1 = \{a_0a_3 - a_1a_2,\ a_0a_6 - a_2a_4,\ a_0a_7 - a_2a_5,$$
$$a_1a_6 - a_3a_4,\ a_1a_7 - a_3a_5,\ a_4a_7 - a_5a_6\},$$
$$V_2 = \{a_0a_5 - a_1a_4,\ a_0a_3 - a_1a_2,\ a_0a_7 - a_1a_6,$$
$$a_3a_4 - a_2a_5,\ a_4a_7 - a_5a_6,\ a_2a_7 - a_3a_6\}.$$

Тогда имеет место следующее утверждение.

Утверждение (критерий К$_3$). Состояние $|\psi\rangle$ трехкубитной квантовой системы $A_1A_2A_3$ является несепарабельным состоянием тогда и только тогда, когда для любого $i \in \{0, 1, 2\}$ в наборе V_i имеется хотя бы одна величина, неравная нулю.

6. Сформулирован **критерий $К_4$** (**критерий $Константин_4$**) несепарабельности состояний четырехкубитных квантовых систем.

7. Критерий $К_3$ и **критерий $К_4$** иллюстрируют эффективную возможность решения задачи бинарной классификации (сепарабельные и несепарабельные состояния) для состояний многокубитной квантовой системы. Однако надо отметить, что для решения задачи бинарной классификации состояний квантовой системы из n кубитов (где n – натуральное число, $n > 1$) число наборов величин, которые необходимо проверить на условие содержания ненулевого элемента, равно $2^{n-1} - 1$. В то же время при решении задачи выяснения неразложимости (или разложимости) состояния квантовой системы в тензорное произведение состояний меньшей размерности число наборов величин, которые необходимо проверить на условие содержания ненулевого элемента, равно $n - 1$.

ГЛАВА 3

Достаточные признаки несепарабельности состояний многокубитных квантовых систем

Введение к главе 3

В связи с решением задачи о бинарной классификации состояний многокубитных квантовых систем (то есть задачи определения, к какому из двух классов – классу сепарабельных состояний или классу несепарабельных состояний – принадлежит заданное многокубитное состояние) представляют интерес в вычислительном плане несложно проверяемые (на наличие или отсутствие) признаки многокубитного состояния, по которым можно определить, несепарабельно это состояние или нет.

Выявление набора вышеуказанных признаков может быть предметом отдельных будущих исследований. Однако в общем случае (т. е. при условии, что число кубитов n – произвольное натуральное число) некоторые достаточные признаки несепарабельности состояний квантовой системы из n кубитов могут быть установлены через использование соответствующих этим состояниям булевых масок или нумераторов [1; 5; 6; 48]. Глава 3, посвященная данному кругу вопросов, состоит из трех параграфов.

В параграфе 3.1 вводится понятие булевой маски состояния многокубитной квантовой системы. На булеву маску распространяются определения разного типа понятий сепарабельности и несепарабельности, аналогичные для квантовых состояний. Формулируется и доказывается утверждение о том, что из несепарабельности любого типа для булевой маски состояния многокубитной квантовой системы следует несепарабельность того же типа для самого состояния.

Обратное в общем случае неверно, то есть из несепарабельности состояния многокубитной квантовой системы не следует несепарабельность его булевой маски. В подтверждение этого приводится пример несепарабельного состояния двухкубитной квантовой системы, булева маска которого является сепарабельной.

Учитывая, что вопрос сепарабельности или несепарабельности для булевой маски состояния многокубитной квантовой системы решается проще, чем для самого состояния, можно говорить о выявлении эффективного подхода для определения несепарабельности состояния в том случае, когда несепарабельной является его булева маска.

Другой подход для выявления несепарабельных квантовых состояний многокубитных квантовых систем основан на использовании их нумераторов весов. Проработке данного подхода посвящен параграф 3.2. Как и в случае булевых масок, так и в случае нумераторов весов удается получить только достаточные условия для несепарабельности состояний.

В параграфе 3.3 приведено полное решение задачи бинарной классификации для булевых масок трехкубитных квантовых систем. Разработан и изложен **алгоритм К$_3$** для выявления, сепарабельно или нет произвольное состояние трехкубитной квантовой системы. В названии **алгоритма К$_3$** буква **К** – это первая буква имени **Константин**, а индекс **3** связан с числом кубитов в трехкубитной квантовой системе.

§ 3.1. Булевы маски состояний квантовых систем

Определение 3.1.1. Вектор $B_\psi = \left(b_0,\, b_1,\, \ldots,\, b_{2^n-1}\right)^{\mathrm{T}} \in \mathbb{C}^{2^n}$ называется **булевой маской** состояния $\left|\psi\right\rangle = \left(a_0,\, a_1,\, \ldots,\, a_{2^n-1}\right)^{\mathrm{T}} \in \mathbb{C}^{2^n}$ (здесь T – знак транспонирования) n-кубитной квантовой системы $A_1A_2\ldots A_n$, если для любого $k \in \left\{0,\, 1,\, \ldots,\, 2^n-1\right\}$ справедливо равенство

$$b_k = \begin{cases} 0, \text{ если } a_k = 0; \\ 1 \text{ в противном случае.} \end{cases}$$

Для булевых масок определения разного типа сепарабельности и несепарабельности во многом аналогичны соответствующим определениям 2.4.4, 2.4.8 – 2.4.11 из параграфа 2.4 для состояний квантовых систем. Для осуществления соответствующих формулировок данных определений напомним некоторые обозначения, введенные в параграфе 2.4: $\mathbb{S}_n$ – симметрическая группа подстановок [27] на множестве $\{1, 2, \ldots, n\}$; $M_n^{(t)}$ – множество разбиений натурального числа n на t слагаемых, где $t \in \{2, 3, \ldots, n\}$, то есть $M_n^{(t)}$ – множество упорядоченных наборов натуральных чисел $(k_1, k_2, \ldots, k_t)$, таких, что справедливо равенство

$$k_1 + k_2 + \ldots + k_t = n.$$

Определение 3.1.2.

Пусть $s \in \mathbb{S}_n$, $m_{n,t}^{(j)} \in M_n^{(t)}$, $m_{n,t}^{(j)} = (k_1, k_2, \ldots, k_t)$, $j \in \left\{1, 2, \ldots, \left|M_n^{(t)}\right|\right\}$, $\left|M_n^{(t)}\right|$ – мощность множества $M_n^{(t)}$, $t \in \{2, 3, \ldots, n\}$.

Булева маска B_ψ состояния $|\psi\rangle$ n-кубитной квантовой системы $A_1A_2\ldots A_n$ называется $\left(s;\, m_{n,t}^{(j)}\right)$**-сепарабельной булевой маской**, если для булевой маски $B_{\psi^{(s)}}$ состояния $\left|\psi^{(s)}\right\rangle$ квантовой системы

$$\begin{gathered} A_{s(1)}A_{s(2)}\ldots A_{s(k_1)}A_{s(k_1+1)}\ldots A_{s(k_1+k_2)}A_{s(k_1+k_2+1)}\ldots A_{s(k_1+k_2+\ldots+k_{t-1})} \\ A_{s(k_1+k_2+\ldots+k_{t-1}+1)}\ldots A_{s(n)} \end{gathered} \tag{3.1.3}$$

справедливо равенство

$$\begin{gathered} B_{\psi^{(s)}} = \left(c_{10}, c_{11}, \ldots, c_{1(2^{k_1}-1)}\right)^{\mathrm{T}} \otimes \left(c_{20}, c_{21}, \ldots, c_{2(2^{k_2}-1)}\right)^{\mathrm{T}} \otimes \ldots \\ \ldots \otimes \left(c_{t0}, c_{t1}, \ldots, c_{t(2^{k_t}-1)}\right)^{\mathrm{T}}, \end{gathered} \tag{3.1.4}$$

где $c_{qr^{(q)}} \in \{0, 1\}$, $q \in \{1, 2, \ldots, t\}$, $r^{(q)} \in \left\{0, 1, \ldots, 2^{k_q} - 1\right\}$.

Определение 3.1.5. Булева маска B_ψ состояния $|\psi\rangle$ n-кубитной квантовой системы $A_1A_2\ldots A_n$ называется $(s;\ *)$**-сепарабельной булевой маской**, если найдется разбиение $m_{n,t}^{(j)} \in M_n^{(t)}$, такое, что булева маска B_ψ является $\left(s;\ m_{n,t}^{(j)}\right)$-сепарабельной булевой маской.

Определение 3.1.6. Булева маска B_ψ состояния $|\psi\rangle$ n-кубитной квантовой системы $A_1A_2\ldots A_n$ называется $\left(*;\ m_{n,t}^{(j)}\right)$**-сепарабельной булевой маской**, если найдется подстановка $s \in \mathbb{S}_n$, такая, что булева маска B_ψ является $\left(s;\ m_{n,t}^{(j)}\right)$-сепарабельной булевой маской.

Определение 3.1.7. Булева маска B_ψ состояния $|\psi\rangle$ n-кубитной квантовой системы $A_1A_2\ldots A_n$ называется t**-сепарабельной булевой маской**, если найдутся подстановка $s \in \mathbb{S}_n$ и разбиение $m_{n,t}^{(j)} \in M_n^{(t)}$, такие, что булева маска B_ψ является $\left(s;\ m_{n,t}^{(j)}\right)$-сепарабельной булевой маской, где $t \in \{2, 3, \ldots, n\}$.

Определение 3.1.8. Булева маска B_ψ состояния $|\psi\rangle$ n-кубитной квантовой системы $A_1A_2\ldots A_n$ называется **сепарабельной булевой маской**, если найдется число $t \in \{2, 3, \ldots, n\}$, такое, что B_ψ является t-сепарабельной булевой маской.

Определение 3.1.9. Булева маска B_ψ состояния $|\psi\rangle$ n-кубитной квантовой системы $A_1A_2\ldots A_n$ называется $\left(s;\ m_{n,t}^{(j)}\right)$**-несепарабельной булевой маской** (соответственно $(s;\ *)$**-несепарабельной**, $\left(*;\ m_{n,t}^{(j)}\right)$-

несепарабельной, t-несепарабельной, **несепарабельной**), если она не является $\left(s;\ m_{n,t}^{(j)}\right)$-сепарабельной булевой маской (соответственно не является $(s;\ *)$-сепарабельной, $\left(*;\ m_{n,t}^{(j)}\right)$-сепарабельной**,** t-сепарабельной, сепарабельной).

Имеет место следующее утверждение.

Утверждение 3.1.10. Если булева маска B_ψ состояния $|\psi\rangle$ n-кубитной квантовой системы $A_1A_2\ldots A_n$ является $\left(s;\ m_{n,t}^{(j)}\right)$-несепарабельной булевой маской (или $(s;\ *)$-несепарабельной, или $\left(*;\ m_{n,t}^{(j)}\right)$-несепарабельной, или t-несепарабельной, или несепарабельной), то состояние $|\psi\rangle$ является $\left(s;\ m_{n,t}^{(j)}\right)$-несепарабельным состоянием (соответственно $(s;\ *)$-несепарабельным, $\left(*;\ m_{n,t}^{(j)}\right)$-несепарабельным, t-несепарабельным, несепарабельным).

Доказательство данного утверждения приведем в этом параграфе ниже. Пока же обратим внимание на то, что обращение утверждения 3.1.10 в общем случае неверно, то есть в общем случае несепарабельность булевой маски состояния не является необходимым условием для несепарабельности самого состояния. Это видно, в частности, из следующего примера.

Пример 3.1.11. Рассмотрим двухкубитное состояние

$$|\psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle = \frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle - \frac{1}{2}|11\rangle.$$

Так как

$$ad - bc = \frac{1}{2}\cdot\frac{1}{2} - \frac{1}{2}\cdot\left(-\frac{1}{2}\right) = \frac{1}{2} \neq 0,$$

то данное состояние является несепарабельным состоянием в соответствии с утверждением 2.28. Однако его булева маска

$$B_\psi = |00\rangle + |01\rangle + |10\rangle + |11\rangle$$

является сепарабельной булевой маской, так как справедливо равенство

$$B_\psi = (|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle),$$

где $|0\rangle + |1\rangle$ – булева маска однокубитного состояния $\dfrac{|0\rangle + |1\rangle}{\sqrt{2}}$.

Приведем теперь доказательство утверждения 3.1.10.

Доказательство. Утверждение 3.1.10 состоит из нескольких частей. Все они доказываются примерно одинаково. Поэтому ограничимся доказательством той части утверждения, в которой утверждается, что из несепарабельности булевой маски B_ψ состояния $|\psi\rangle$ следует несепарабельность самого состояния $|\psi\rangle$.

Докажем методом от противного. Допустим, что булева маска B_ψ состояния $|\psi\rangle$ несепарабельна, а само состояние $|\psi\rangle$ является сепарабельным состоянием.

Из сепарабельности состояния $|\psi\rangle$ следует, что найдется подстановка $s \in \mathbb{S}_n$, такая, что для состояния $|\psi^{(s)}\rangle$ квантовой системы (3.1.3) справедливо равенство

$$|\psi^{(s)}\rangle = |\psi_1\rangle \otimes |\psi_2\rangle, \tag{3.1.12}$$

где

$$|\psi_1\rangle = \left(a_{10},\ a_{11},\ \ldots,\ a_{1(2^{t_1}-1)}\right)^{\mathrm{T}} \tag{3.1.13}$$

– состояние квантовой системы из t_1 кубитов;

$$|\psi_2\rangle = \left(a_{20},\ a_{21},\ \ldots,\ a_{2(2^{t_2}-1)}\right)^{\mathrm{T}} \tag{3.1.14}$$

– состояние квантовой системы из t_2 кубитов;
t_1 и t_2 – некоторые натуральные числа, такие, что справедливо равенство

$$t_1 + t_2 = n;$$

координаты состояний $|\psi_1\rangle$ и $|\psi_2\rangle$ удовлетворяют условиям

$$a_{qr^{(q)}} \in \mathbb{C},\ r^{(q)} \in \left\{0,\ 1,\ \ldots,\ 2^{t_q}-1\right\},\ q \in \{1,2\},$$

$$\sum_{r^{(q)}=0}^{2^{t_q}-1} \left|a_{qr^{(q)}}\right|^2 = 1 .$$

Из равенств (3.1.12) – (3.1.14) следует, что каждая координата состояния $\left|\psi^{(s)}\right\rangle$ равна произведению соответствующей координаты состояния $|\psi_1\rangle$ и соответствующей координаты состояния $|\psi_2\rangle$. При этом координата состояния $\left|\psi^{(s)}\right\rangle$ не равна нулю тогда и только тогда, когда не равны нулю сомножители в произведении. Отсюда следует, что для булевой маски $B_{\psi^{(s)}}$ состояния $\left|\psi^{(s)}\right\rangle$ справедливо равенство

$$B_{\psi^{(s)}} = B_{\psi_1} \otimes B_{\psi_2} ,$$

где B_{ψ_1} и B_{ψ_2} – булевы маски состояний $|\psi_1\rangle$ и $|\psi_2\rangle$ соответственно.

Отсюда и из определения 3.1.8 следует, что булева маска B_ψ является сепарабельной булевой маской, что противоречит исходному предположению о несепарабельности B_ψ. Следовательно, предположение о сепарабельности состояния $|\psi\rangle$ неверно, то есть $|\psi\rangle$ является несепарабельным состоянием. Доказательство завершено.

Используя булевы маски, удается получить содержательные результаты о несепарабельности состояний многокубитных квантовых систем. В этом можно убедиться на примере трехкубитных состояний. Соответствующие результаты представлены в параграфе 3.3.

§ 3.2. Нумераторы весов состояний квантовых систем

Напомним (см. § 1.1), что состоянием квантовой системы из n ($n \geq 1$) кубитов является любой нормированный вектор $|\psi\rangle$, принадлежащий n-й тензорной степени $\mathbb{C}^{2^n}$ гильбертова пространства $\mathbb{C}^2$, то есть 2^n-мерного гильбертова пространства $\mathbb{C}^{2^n} = \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \ldots \otimes \mathbb{C}^2$ над полем комплексных чисел $\mathbb{C}$, где $\otimes$ – знак операции тензорного произведения [25; 26; 55].

Этот вектор $|\psi\rangle$, называемый **суперпозицией** (**линейной комбинацией**), можно представить в следующем виде:

$$|\psi\rangle = \alpha_0 \underbrace{|000\ldots00\rangle}_{n} + \alpha_1 |000\ldots01\rangle +$$
$$+\alpha_2 |000\ldots10\rangle + \ldots + \alpha_{2^n-1} |111\ldots11\rangle, \tag{3.2.1}$$

где

$$\alpha_0, \alpha_1, \alpha_2, \ldots \alpha_{2^n-1} \in \mathbb{C},\ |\alpha_0|^2 + |\alpha_1|^2 + \ldots + |\alpha_{2^n-1}|^2 = 1, \tag{3.2.2}$$

$$\begin{aligned} &|\varphi_1\varphi_2\varphi_3\ldots\varphi_{n-1}\varphi_n\rangle = |\varphi_1\rangle|\varphi_2\rangle|\varphi_3\rangle\ldots|\varphi_{n-1}\rangle|\varphi_n\rangle = \\ &= |\varphi_1\rangle \otimes |\varphi_2\rangle \otimes |\varphi_3\rangle \otimes \ldots \otimes |\varphi_{n-1}\rangle \otimes |\varphi_n\rangle, \end{aligned} \tag{3.2.3}$$

$$\varphi_m \in \{0;\ 1\},\ m = \overline{1, n},$$

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

Состояния $\underbrace{|000\ldots00\rangle}_{n}$, $|000\ldots01\rangle$, …, $|111\ldots11\rangle$ называются **состояниями вычислительного базиса** в случае квантовой системы из n кубитов. Они составляют ортонормированный базис гильбертова пространства $\mathbb{C}^{2^n}$.

Вычислительный базис квантовой системы из n кубитов обозначим через B_n, то есть

$$B_n = \{\underbrace{|000\ldots00\rangle}_{n}, |000\ldots01\rangle, \ldots, |111\ldots11\rangle\}. \qquad (3.2.4)$$

Определение 3.2.5. Пусть $|\phi\rangle = |\varphi_1\varphi_2\varphi_3\ldots\varphi_{n-1}\varphi_n\rangle$ – произвольное состояние из вычислительного базиса, где $\varphi_m \in \{0;\ 1\}$, $m = \overline{1, n}$. Число отличных от нуля элементов в конечной последовательности $\{\varphi_1, \varphi_2, \ldots, \varphi_n\}$ длины n называется **весом** состояния $|\phi\rangle$ и обозначается $\mathrm{wt}(|\phi\rangle)$.

Определение 3.2.6. Нумератором весов состояния $|\psi\rangle$ квантовой системы из n кубитов, заданного равенством (3.2.1), называется многочлен

$$N_{|\psi\rangle}(x, y) = \sum_{k=0}^{n} \eta_k(|\psi\rangle) x^k y^{n-k}$$

от двух формальных переменных x и y, где $\eta_k(|\psi\rangle)$ – число состояний веса k из вычислительного базиса B_n, входящих с ненулевыми коэффициентами в правую часть равенства (3.2.1).

Определение 3.2.7. Характеристической функцией состояния $|\psi\rangle$ квантовой системы из n кубитов, заданного равенством (3.2.1), называется функция $\chi_{|\psi\rangle}(|\phi\rangle)$ с областью определения B_n и множеством значений $\{0;\ 1\}$, такая, что для любого состояния $|\phi\rangle \in B_n$ справедливо равенство $\chi_{|\psi\rangle}(|\phi\rangle) = 1$, если состояние $|\phi\rangle$ входит с ненулевым коэффициентом в равенство (3.2.1), и справедливо равенство $\chi_{|\psi\rangle}(|\phi\rangle) = 0$ – в противном случае.

Справедливы следующие утверждения.

Утверждение 3.2.8. Для нумератора весов $N_{|\psi\rangle}(x, y)$ состояния $|\psi\rangle$ справедливо равенство

$$N_{|\psi\rangle}(x, y) = \sum_{|\phi\rangle \in B_n} \chi_{|\psi\rangle}(|\phi\rangle)\, x^{\mathrm{wt}(|\phi\rangle)} y^{n-\mathrm{wt}(|\phi\rangle)}.$$

Утверждение 3.2.9. Пусть для состояния $|\psi\rangle$ квантовой системы из n кубитов выполняется равенство

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle,$$

где $|\psi_1\rangle$ – состояние квантовой системы из n_1 кубитов, $|\psi_2\rangle$ – состояние квантовой системы из $n_2 = n - n_1$ кубитов; n_1, n_2 – натуральные числа. Тогда для любого состояния $|\phi\rangle = |\varphi_1\, \varphi_2\, \varphi_3 \ldots \varphi_{n-1}\, \varphi_n\rangle \in B_n$ справедливо равенство

$$\chi_{|\psi\rangle}(|\phi\rangle) = \chi_{|\psi_1\rangle}(|\phi_1\rangle)\, \chi_{|\psi_2\rangle}(|\phi_2\rangle),$$

где $|\phi_1\rangle = |\varphi_1\, \varphi_2 \ldots \varphi_{n_1}\rangle \in B_{n_1}$, $|\phi_2\rangle = |\varphi_{n_1+1}\, \varphi_{n_1+2} \ldots \varphi_n\rangle \in B_{n_2}$; $\chi_{|\psi_1\rangle}$, $\chi_{|\psi_2\rangle}$ – характеристические функции состояний $|\psi_1\rangle$ и $|\psi_2\rangle$ соответственно.

Утверждение 3.2.10. Пусть для состояния $|\psi\rangle$ квантовой системы из n кубитов выполняется равенство

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle,$$

где $|\psi_1\rangle$ – состояние квантовой системы из n_1 кубитов, $|\psi_2\rangle$ – состояние квантовой системы из $n_2 = n - n_1$ кубитов; n_1, n_2 – натуральные числа. Тогда для нумератора весов $N_{|\psi\rangle}(x,\, y)$ состояния $|\psi\rangle$ справедливо равенство

$$N_{|\psi\rangle}(x,\, y) = N_{|\psi_1\rangle}(x,\, y) \cdot N_{|\psi_2\rangle}(x,\, y),$$

где $N_{|\psi_1\rangle}(x,\, y)$ и $N_{|\psi_2\rangle}(x,\, y)$ – нумераторы весов состояний $|\psi_1\rangle$ и $|\psi_2\rangle$ соответственно.

Из утверждения 3.2.10 вытекает

Следствие 3.2.11. Если нумератор весов $N_{|\psi\rangle}(x, y)$ состояния $|\psi\rangle$ квантовой системы из n кубитов не раскладывается в произведение нумераторов двух состояний меньшей размерности, чем размерность исходного состояния, то состояние $|\psi\rangle$ является несепарабельным состоянием.

Доказательства утверждений 3.2.8, 3.2.9 и 3.2.10 приведем в этом параграфе ниже. Теперь же заметим, что в виде следствия 3.2.11 мы получили достаточное условие для эффективного выявления несепарабельных состояний квантовых систем. Однако надо не забывать, что это условие включает в себя и ситуацию, когда нумератор весов $N_{|\psi\rangle}(x, y)$ может быть разложен только в произведение двух многочленов от переменных (x, y), хотя бы один из которых не является нумератором весов некоторого квантового состояния. В этом случае исходное состояние также является несепарабельным. Приведем иллюстрирующий пример.

Пример 3.2.12. Пусть

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

Известно, что состояние $|\psi\rangle$ – несепарабельное состояние (это, в частности, следует из утверждения 2.2.8).

Непосредственно из определения 3.2.6 нумератора весов $N_{|\psi\rangle}(x, y)$ состояния $|\psi\rangle$ получаем

$$N_{|\psi\rangle}(x, y) = 2xy.$$

Хотя нумератор весов $N_{|\psi\rangle}(x, y)$ разложи́м на множители, его возможные делители $2x$ и $2y$ не могут являться нумераторами какого-либо состояния квантовой системы из одного кубита.

Можно указать на более жесткое достаточное условие для несепарабельности квантового состояния. Оно представлено в формулируемом ниже следствии 3.2.13.

Следствие 3.2.13. Если нумератор весов $N_{|\psi\rangle}(x, y)$ состояния $|\psi\rangle$ квантовой системы из n кубитов является неприводимым многочленом над кольцом целых чисел от двух переменных (x, y), то состояние $|\psi\rangle$ является несепарабельным состоянием.

Далее последовательно проведем доказательства сформулированных выше утверждений 3.2.8, 3.2.9 и 3.2.10.

Доказательство утверждения 3.2.8. По определению 3.2.6 имеем

$$N_{|\psi\rangle}(x, y) = \sum_{k=0}^{n} \eta_k(|\psi\rangle) x^k y^{n-k} . \tag{3.2.14}$$

Для величины $\eta_k(|\psi\rangle)$ справедливо равенство

$$\eta_k(|\psi\rangle) = \sum_{|\phi\rangle \in B_n, \mathrm{wt}(|\phi\rangle)=k} \chi_{|\psi\rangle}(|\phi\rangle) \tag{3.2.15}$$

для любого $k \in \{0, 1, \ldots, n\}$.

Подставив правую часть равенства (3.2.15) вместо $\eta_k(|\psi\rangle)$ в правую часть равенства (3.2.14), получаем

$$N_{|\psi\rangle}(x, y) = \sum_{k=0}^{n} \left(\sum_{|\phi\rangle \in B_n, \mathrm{wt}(|\phi\rangle)=k} \chi_{|\psi\rangle}(|\phi\rangle) \right) x^k y^{n-k} =$$

$$= \sum_{k=0}^{n} \left(\sum_{|\phi\rangle \in B_n, \mathrm{wt}(|\phi\rangle)=k} \chi_{|\psi\rangle}(|\phi\rangle) x^{\mathrm{wt}(|\phi\rangle)} y^{n-\mathrm{wt}(|\phi\rangle)} \right).$$

Отсюда, учитывая свойство коммутативности операции сложения многочленов и то, что значения весов всех состояний из вычислительного базиса B_n полностью исчерпываются значениями от 0 до n, получаем

$$N_{|\psi\rangle}(x, y) = \sum_{|\phi\rangle \in B_n} \chi_{|\psi\rangle}(|\phi\rangle) x^{\mathrm{wt}(|\phi\rangle)} y^{n-\mathrm{wt}(|\phi\rangle)} .$$

Утверждение 3.2.8 доказано.

Доказательство утверждения 3.2.9. Пусть выполняется равенство

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle .$$

Выпишем по аналогии с (3.2.1) выражения для представлений состояний $|\psi\rangle$, $|\psi_1\rangle$ и $|\psi_2\rangle$ в соответствующих им вычислительных базисах:

$$|\psi\rangle = \alpha_0 \underbrace{|000\ldots00\rangle}_{n} + \alpha_1 |000\ldots01\rangle +$$
$$+\alpha_2 |000\ldots10\rangle + \ldots + \alpha_{2^n-1} |111\ldots11\rangle , \tag{3.2.16}$$

$$|\psi_1\rangle == \alpha_{10} \underbrace{|000\ldots00\rangle}_{n_1} + \alpha_{11} |000\ldots01\rangle +$$
$$+\alpha_{12} |000\ldots10\rangle + \ldots + \alpha_{1\left(2^{n_1}-1\right)} |111\ldots11\rangle , \tag{3.2.17}$$

$$|\psi_2\rangle == \alpha_{20} \underbrace{|000\ldots00\rangle}_{n_2} + \alpha_{21} |000\ldots01\rangle +$$
$$+\alpha_{22} |000\ldots10\rangle + \ldots + \alpha_{2\left(2^{n_2}-1\right)} |111\ldots11\rangle , \tag{3.2.18}$$

Подставив правые части этих равенств в выражение

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$$

вместо состояний $|\psi\rangle$, $|\psi_1\rangle$ и $|\psi_2\rangle$ соответственно, после этого выполнив операцию тензорного произведения в левой части этого равенства и затем приравняв коэффициенты перед одинаковыми состояниями вычислительного базиса B_n в левой и правой частях результирующего выражения, получим равенство

$$\alpha_t = \alpha_{1t_1} \cdot \alpha_{2t_2} , \tag{3.2.19}$$

для коэффициентов перед каждым состоянием $|\phi\rangle = |\varphi_1\varphi_2\varphi_3\ldots\varphi_{n-1}\varphi_n\rangle \in B_n$, где

$$t = 2^{n-1}\varphi_1 + 2^{n-2}\varphi_2 + \ldots + 2^0\varphi_n ,$$

$$t_1 = 2^{n_1-1}\varphi_1 + 2^{n_1-2}\varphi_2 + \ldots + 2^0\varphi_{n_1},$$

$$t_2 = 2^{n_2-1}\varphi_{n_1+1} + 2^{n_2-2}\varphi_{n_1+2} + \ldots + 2^0\varphi_n,$$

α_t – коэффициент в (3.2.16) перед состоянием
$|\phi\rangle = |\varphi_1\varphi_2\varphi_3\ldots\varphi_{n-1}\varphi_n\rangle \in B_n$,
α_{1t_1} – коэффициент в (3.2.17) перед состоянием $|\phi_1\rangle = |\varphi_1\varphi_2\ldots\varphi_{n_1}\rangle \in B_{n_1}$,
α_{2t_2} – коэффициент в (3.2.18) перед состоянием
$|\phi_2\rangle = |\varphi_{n_1+1}\varphi_{n_1+2}\ldots\varphi_n\rangle \in B_{n_2}$.

Из (3.2.19) получаем, что коэффициент α_t не равен нулю тогда и только тогда, когда не равен нулю каждый из коэффициентов α_{1t_1} и α_{2t_2}.

Рассмотрим случай, когда $\alpha_t \neq 0$. В этом случае из определения 3.2.7 следует, что $\chi_{|\psi\rangle}(|\phi\rangle) = 1$. Одновременно с этим из неравенства $\alpha_t \neq 0$ в соответствии с (3.2.19) следует справедливость неравенств $\alpha_{1t_1} \neq 0$ и $\alpha_{2t_2} \neq 0$, которые, в свою очередь, по определению 3.2.7 влекут за собой соответственно справедливость равенств $\chi_{|\psi_1\rangle}(|\phi_1\rangle) = 1$ и $\chi_{|\psi_2\rangle}(|\phi_2\rangle) = 1$. Следовательно, в этом случае равенство $\chi_{|\psi\rangle}(|\phi\rangle) = \chi_{|\psi_1\rangle}(|\phi_1\rangle)\chi_{|\psi_2\rangle}(|\phi_2\rangle)$ выполнено.

Рассмотрим случай, когда $\alpha_t = 0$. В этом случае из определения 3.2.7 следует, что $\chi_{|\psi\rangle}(|\phi\rangle) = 0$. Одновременно с этим из равенства $\alpha_t = 0$ в соответствии с (3.2.19) следует справедливость хотя бы одного из равенств $\alpha_{1t_1} = 0$ или $\alpha_{2t_2} = 0$, что, в свою очередь, влечет за собой по определению 3.2.7 справедливость хотя бы одного из равенств $\chi_{|\psi_1\rangle}(|\phi_1\rangle) = 0$ и $\chi_{|\psi_2\rangle}(|\phi_2\rangle) = 0$. Следовательно, и в этом случае равенство $\chi_{|\psi\rangle}(|\phi\rangle) = \chi_{|\psi_1\rangle}(|\phi_1\rangle) \cdot \chi_{|\psi_2\rangle}(|\phi_2\rangle)$ выполнено.

Таким образом, равенство $\chi_{|\psi\rangle}(|\phi\rangle)=\chi_{|\psi_1\rangle}(|\phi_1\rangle)\cdot\chi_{|\psi_2\rangle}(|\phi_2\rangle)$ справедливо для всех возможных значений характеристических функций, входящих в него. Утверждение 3.2.9 доказано.

Доказательство утверждения 3.2.10. Пусть выполняется равенство

$$|\psi\rangle=|\psi_1\rangle\otimes|\psi_2\rangle.$$

Тогда из утверждения 3.2.9 следует, что для любого состояния $|\phi\rangle=|\varphi_1\varphi_2\varphi_3\ldots\varphi_{n-1}\varphi_n\rangle\in B_n$ справедливо равенство

$$\chi_{|\psi\rangle}(|\phi\rangle)=\chi_{|\psi_1\rangle}(|\phi_1\rangle)\cdot\chi_{|\psi_2\rangle}(|\phi_2\rangle), \tag{3.2.20}$$

где $|\phi_1\rangle=|\varphi_1\varphi_2\ldots\varphi_{n_1}\rangle\in B_{n_1}$, $|\phi_2\rangle=|\varphi_{n_1+1}\varphi_{n_1+2}\ldots\varphi_n\rangle\in B_{n_2}$.

Из утверждения 3.2.8 для нумератора весов состояния $|\psi\rangle$ имеем

$$N_{|\psi\rangle}(x,y)=\sum_{|\phi\rangle\in B_n}\chi_{|\psi\rangle}(|\phi\rangle)x^{\mathrm{wt}(|\phi\rangle)}y^{n-\mathrm{wt}(|\phi\rangle)}. \tag{3.2.21}$$

Заменив $\chi_{|\psi\rangle}(|\phi\rangle)$ под знаком суммы в правой части равенства (3.2.21) на правую часть $\chi_{|\psi_1\rangle}(|\phi_1\rangle)\cdot\chi_{|\psi_2\rangle}(|\phi_2\rangle)$ равенства (3.2.20), получим

$$N_{|\psi\rangle}(x,y)=\sum_{|\phi\rangle\in B_n}\left(\chi_{|\psi_1\rangle}(|\phi_1\rangle)\cdot\chi_{|\psi_2\rangle}(|\phi_2\rangle)\right)x^{\mathrm{wt}(|\phi\rangle)}y^{n-\mathrm{wt}(|\phi\rangle)}. \tag{3.2.22}$$

Учитывая равенства

$$|\phi\rangle=|\phi_1\rangle\otimes|\phi_2\rangle,\ n=n_1+n_2,\ \mathrm{wt}(|\phi\rangle)=\mathrm{wt}(|\phi_1\rangle)+\mathrm{wt}(|\phi_2\rangle),$$

из равенства (3.2.22) получаем

$$N_{|\psi\rangle}(x,y)=\sum_{(|\phi_1\rangle\otimes|\phi_2\rangle)\in B_n}\left(\chi_{|\psi_1\rangle}(|\phi_1\rangle)\chi_{|\psi_2\rangle}(|\phi_2\rangle)\right)\times$$
$$\times x^{\left(\mathrm{wt}(|\phi_1\rangle)+\mathrm{wt}(|\phi_2\rangle)\right)}y^{(n_1+n_2)-\left(\mathrm{wt}(|\phi_1\rangle)+\mathrm{wt}(|\phi_2\rangle)\right)}=$$

$$= \sum_{(|\phi_1\rangle \otimes |\phi_2\rangle) \in B_n} \left(\chi_{|\psi_1\rangle}(|\phi_1\rangle) x^{\mathrm{wt}(|\phi_1\rangle)} y^{n_1 - \mathrm{wt}(|\phi_1\rangle)} \right) \times \left(\chi_{|\psi_2\rangle}(|\phi_2\rangle) x^{\mathrm{wt}(|\phi_2\rangle)} y^{n_2 - \mathrm{wt}(|\phi_2\rangle)} \right) =$$

$$= \left(\sum_{|\phi_1\rangle \in B_{n_1}} \chi_{|\psi_1\rangle}(|\phi_1\rangle) x^{\mathrm{wt}(|\phi_1\rangle)} y^{n_1 - \mathrm{wt}(|\phi_1\rangle)} \right) \times \left(\sum_{|\phi_2\rangle \in B_{n_2}} \chi_{|\psi_2\rangle}(|\phi_2\rangle) x^{\mathrm{wt}(|\phi_2\rangle)} y^{n_2 - \mathrm{wt}(|\phi_2\rangle)} \right).$$

Отсюда и из утверждения 3.2.8 получаем искомое равенство

$$N_{|\psi\rangle}(x, y) = N_{|\psi_1\rangle}(x, y) N_{|\psi_2\rangle}(x, y).$$

Утверждение 3.2.10 доказано.

§ 3.3. Решение задачи бинарной классификации состояний трехкубитных квантовых систем на основе их булевых масок

Пусть $B_\psi = (b_0, b_1, \ldots, b_7)^{\mathrm{T}}$ – булева маска трехкубитного состояния $|\psi\rangle = (a_0, a_1, \ldots, a_7)^{\mathrm{T}}$, где $a_k \in \mathbb{C}$, $k \in \{0, 1, \ldots, 7\}$,

$$|a_0|^2 + |a_1|^2 + |a_2|^2 + |a_3|^2 + |a_4|^2 + |a_5|^2 + |a_6|^2 + |a_7|^2 = 1; \qquad (3.3.1)$$

$$b_k = \begin{cases} 0, \text{ если } a_k = 0; \\ 1 \text{ в противном случае.} \end{cases} \qquad (3.3.2)$$

Для булевой маски B_ψ справедливы утверждения, подобные утверждению 2.5.21 и следствиям 2.5.22, 2.5.24 – 2.5.27 из утверждения 2.5.21. Соответствующие формулировки можно получить из формулировок указанного утверждения и следствий из него путем замены состояния $|\psi\rangle$ на его булеву маску B_ψ и замены набора величин $V_{tj}^{(i)}$ на набор $W_{tj}^{(i)}$, где $i \in \{0, 1, 2, 3, 4, 5\}$; $t \in \{2, 3\}$; $j \in \{1, 2\}$ при t = 2; j = 1 при t = 3; набор величин $W_{tj}^{(i)}$ получается из набора $V_{tj}^{(i)}$ при замене a_k на b_k ($k \in \{0, 1, \ldots, 7\}$) в выражениях (см. (2.5.3) – (2.5.20)), определяющих величины в наборе $V_{tj}^{(i)}$. Доказательства полученных подобным образом утверждений аналогичны доказательствам утверждения 2.5.21 и следствий 2.5.22, 2.5.24 – 2.5.27, так как при доказательстве последних равенство (3.3.1), всегда справедливое для координат вектора $|\psi\rangle$, но не всегда справедливое для координат вектора B_ψ, не использовалось. Или, по-другому, свойство разложимости вектора над полем комплексных чисел в тензорное произведение векторов не зависит от значения нормы вектора.

Забегая вперед, скажем, что число сепарабельных булевых масок состояний квантовых систем из трех кубитов равно 81, а число несепарабельных – 174 (общее число булевых масок трехкубитных квантовых систем равно 255).

Из пункта (б) следствия 2.5.27 с учетом вышесказанного для булевых масок трехкубитных квантовых состояний непосредственно получаем критерий их несепарабельности, который, для удобства ссылок, сформулируем в виде следующего утверждения.

Утверждение 3.3.3. Булева маска $B_\psi = (b_0,\ b_1,\ \ldots,\ b_7)^{\mathrm{T}}$ состояния $|\psi\rangle = (a_0,\ a_1,\ \ldots,\ a_7)^{\mathrm{T}}$ трехкубитной квантовой системы $A_1A_2A_3$ является несепарабельной булевой маской тогда и только тогда, когда для любого $i \in \{0,\ 1,\ 2\}$ в наборе $W_{21}^{(i)}$ имеется хотя бы одна величина, не равная нулю, где

$$W_{21}^{(0)} = \{b_0b_5 - b_1b_4,\ b_0b_6 - b_2b_4,\ b_0b_7 - b_3b_4,\ b_1b_6 - b_2b_5,\ b_1b_7 - b_3b_5,\ b_2b_7 - b_3b_6\}, \tag{3.3.4}$$

$$W_{21}^{(1)} = \{b_0b_3 - b_1b_2,\ b_0b_6 - b_2b_4,\ b_0b_7 - b_2b_5,\ b_1b_6 - b_3b_4,\ b_1b_7 - b_3b_5,\ b_4b_7 - b_5b_6\}, \tag{3.3.5}$$

$$W_{21}^{(2)} = \{b_0b_5 - b_1b_4,\ b_0b_3 - b_1b_2,\ b_0b_7 - b_1b_6,\ b_3b_4 - b_2b_5,\ b_4b_7 - b_5b_6,\ b_2b_7 - b_3b_6\}. \tag{3.3.6}$$

Следовательно, булева маска B_ψ состояния $|\psi\rangle$ трехкубитной квантовой системы является сепарабельной булевой маской тогда и только тогда, когда хотя бы в одном из наборов $W_{21}^{(0)}$, $W_{21}^{(1)}$ и $W_{21}^{(2)}$ все величины равны нулю.

Обозначим через U_i множество всех трехкубитных булевых масок, для каждой из которых все величины в наборе $W_{21}^{(i)}$ равны нулю, где $i \in \{0, 1, 2\}$. Тогда множество U, задаваемое равенством

$$U = U_0 \cup U_1 \cup U_2,$$

совпадает с множеством всех сепарабельных булевых масок состояний квантовых систем из трех кубитов. Поставим и решим задачу описания элементов множества U.

Из пункта (a) утверждения 2.3.4 следует, что для любого вектора $(b_0, b_1, \ldots, b_7)^{\mathrm{T}} \in U_0$ справедливо равенство

$$(b_0, b_1, \ldots, b_7)^{\mathrm{T}} = (\alpha_0, \alpha_1)^{\mathrm{T}} \otimes (v_0, v_1, v_2, v_3)^{\mathrm{T}},$$

где $(\alpha_0, \alpha_1)^{\mathrm{T}}$ – булева маска состояния однокубитной квантовой системы, $(v_0, v_1, v_2, v_3)^{\mathrm{T}}$ – булева маска состояния двухкубитной квантовой системы. Отсюда, учитывая, что координаты векторов $(\alpha_0, \alpha_1)^{\mathrm{T}}$ и $(v_0, v_1, v_2, v_3)^{\mathrm{T}}$ принадлежат множеству $\{0, 1\}$, получаем следующую структуру вектора $(b_0, b_1, \ldots, b_7)^{\mathrm{T}}$:

$$(b_0, b_1, b_2, b_3)^{\mathrm{T}} = \tau \cdot (b_4, b_5, b_6, b_7)^{\mathrm{T}}$$

или

$$(b_4, b_5, b_6, b_7)^{\mathrm{T}} = \tau \cdot (b_0, b_1, b_2, b_3)^{\mathrm{T}}$$

для некоторого $\tau \in \{0, 1\}$. То есть вектор $(b_0, b_1, \ldots, b_7)^{\mathrm{T}}$ состоит из двух последовательных четырехмерных двоичных векторов $(b_0, b_1, b_2, b_3)^{\mathrm{T}}$ и

$(b_4,\ b_5,\ b_6,\ b_7)^{\mathrm{T}}$, которые либо совпадают, либо один из них нулевой вектор, а другой ненулевой.

Таким образом, множество U_0 состоит из двоичных ненулевых восьмимерных векторов $(b_0,\ b_1,\ \ldots,\ b_7)^{\mathrm{T}}$, структурно состоящих из двух последовательно расположенных двоичных четырехмерных векторов $(b_0,\ b_1,\ b_2,\ b_3)^{\mathrm{T}}$ и $(b_4,\ b_5,\ b_6,\ b_7)^{\mathrm{T}}$, из которых хотя бы один пропорционален другому с коэффициентом пропорциональности $\tau \in \{0,\ 1\}$. Такая структура элементов множества U_0 влечет за собой для мощности множества U_0 справедливость равенства

$$|U_0| = 45.$$

При этом само множество U_0 представляется следующей таблицей.

Таблица 3.3.7. Таблица элементов множества U_0

№ п/п	$(b_0,\ b_1,\ \ldots,\ b_7)^{\mathrm{T}}$	№ п/п	$(b_0,\ b_1,\ \ldots,\ b_7)^{\mathrm{T}}$	№ п/п	$(b_0,\ b_1,\ \ldots,\ b_7)^{\mathrm{T}}$
1	$(0000\ 0001)^{\mathrm{T}}$	16	$(0001\ 0000)^{\mathrm{T}}$	31	$(0001\ 0001)^{\mathrm{T}}$
2	$(0000\ 0010)^{\mathrm{T}}$	17	$(0010\ 0000)^{\mathrm{T}}$	32	$(0010\ 0010)^{\mathrm{T}}$
3	$(0000\ 0011)^{\mathrm{T}}$	18	$(0011\ 0000)^{\mathrm{T}}$	33	$(0011\ 0011)^{\mathrm{T}}$
4	$(0000\ 0100)^{\mathrm{T}}$	19	$(0100\ 0000)^{\mathrm{T}}$	34	$(0100\ 0100)^{\mathrm{T}}$
5	$(0000\ 0101)^{\mathrm{T}}$	20	$(0101\ 0000)^{\mathrm{T}}$	35	$(0101\ 0101)^{\mathrm{T}}$
6	$(0000\ 0110)^{\mathrm{T}}$	21	$(0110\ 0000)^{\mathrm{T}}$	36	$(0110\ 0110)^{\mathrm{T}}$
7	$(0000\ 0111)^{\mathrm{T}}$	22	$(0111\ 0000)^{\mathrm{T}}$	37	$(0111\ 0111)^{\mathrm{T}}$
8	$(0000\ 1000)^{\mathrm{T}}$	23	$(1000\ 0000)^{\mathrm{T}}$	38	$(1000\ 1000)^{\mathrm{T}}$
9	$(0000\ 1001)^{\mathrm{T}}$	24	$(1001\ 0000)^{\mathrm{T}}$	39	$(1001\ 1001)^{\mathrm{T}}$
10	$(0000\ 1010)^{\mathrm{T}}$	25	$(1010\ 0000)^{\mathrm{T}}$	40	$(1010\ 1010)^{\mathrm{T}}$
11	$(0000\ 1011)^{\mathrm{T}}$	26	$(1011\ 0000)^{\mathrm{T}}$	41	$(1011\ 1011)^{\mathrm{T}}$
12	$(0000\ 1100)^{\mathrm{T}}$	27	$(1100\ 0000)^{\mathrm{T}}$	42	$(1100\ 1100)^{\mathrm{T}}$
13	$(0000\ 1101)^{\mathrm{T}}$	28	$(1101\ 0000)^{\mathrm{T}}$	43	$(1101\ 1101)^{\mathrm{T}}$
14	$(0000\ 1110)^{\mathrm{T}}$	29	$(1110\ 0000)^{\mathrm{T}}$	44	$(1110\ 1110)^{\mathrm{T}}$
15	$(0000\ 1111)^{\mathrm{T}}$	30	$(1111\ 0000)^{\mathrm{T}}$	45	$(1111\ 1111)^{\mathrm{T}}$

Из утверждения 2.5.21 и равенств (2.5.32) и (2.5.33) следует, что все элементы множества U_1 получаются из элементов множества U_0 путем перестановки их координат, индуцированной подстановкой

$$s_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

То есть, если

$$\left(b_0,\ b_1,\ \ldots,\ b_7\right)^{\mathrm{T}} \in U_0,$$

то справедливо включение

$$\left(b_{\breve{s}_1^{-1}(0)},\ b_{\breve{s}_1^{-1}(1)},\ \ldots,\ b_{\breve{s}_1^{-1}(7)}\right)^{\mathrm{T}} \in U_1,$$

где $\breve{s}_1^{-1}$ – подстановка на множестве чисел $\{0,\ 1,\ \ldots,\ 7\}$, обратная к подстановке $\breve{s}_1$, задаваемой равенством

$$\breve{s}_1(k) = 4\delta_{ks_1(1)} + 2\delta_{ks_1(2)} + \delta_{ks_1(3)},$$

для любого $k \in \{0,\ 1,\ \ldots,\ 7\}$, $\delta_{kr} \in \{0,\ 1\}$, $r = \overline{1,3}$, $k = 4\delta_{k1} + 2\delta_{k2} + \delta_{k3}$.

И, наоборот, все элементы множества U_0 получаются из элементов множества U_1 путем соответствующей перестановки их координат. А именно, если

$$\left(b_0,\ b_1,\ \ldots,\ b_7\right)^{\mathrm{T}} \in U_1,$$

то справедливо включение

$$\left(b_{\breve{s}_1(0)},\ b_{\breve{s}_1(1)},\ \ldots,\ b_{\breve{s}_1(7)}\right)^{\mathrm{T}} \in U_0.$$

По подстановке s_1 вычислим подстановку $\breve{s}_1$:

$$\breve{s}_1(0) = 4 \cdot 0 + 2 \cdot 0 + 0 = 0,$$

$$\breve{s}_1(1) = 4 \cdot 0 + 2 \cdot 0 + 1 = 1,$$

$$\breve{s}_1(2) = 4 \cdot 1 + 2 \cdot 0 + 0 = 4,$$

$$\breve{s}_1(3) = 4 \cdot 1 + 2 \cdot 0 + 1 = 5,$$

$$\breve{s}_1(4) = 4 \cdot 0 + 2 \cdot 1 + 0 = 2,$$

$$\breve{s}_1(5) = 4 \cdot 0 + 2 \cdot 1 + 1 = 3,$$

$$\breve{s}_1(6) = 4 \cdot 1 + 2 \cdot 1 + 0 = 6,$$

$$\breve{s}_1(7) = 4 \cdot 1 + 2 \cdot 1 + 1 = 7;$$

что в двустрочной записи представляется равенством

$$\breve{s}_1 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 0 & 1 & 4 & 5 & 2 & 3 & 6 & 7 \end{pmatrix}.$$

Очевидно, верно равенство

$$\breve{s}_1^{-1} = \breve{s}_1 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 0 & 1 & 4 & 5 & 2 & 3 & 6 & 7 \end{pmatrix}.$$

Из последнего равенства следует, что если

$$(b_0,\, b_1,\, b_2,\, b_3,\, b_4,\, b_5,\, b_6,\, b_7)^{\mathrm{T}} \in U_0,$$

то справедливо включение

$$(b_0,\, b_1,\, b_4,\, b_5,\, b_2,\, b_3,\, b_6,\, b_7)^{\mathrm{T}} \in U_1,$$

то есть все элементы множества U_1 получаются путем перестановки местами второй по номеру координаты с четвертой и третьей по номеру координаты с пятой в каждом элементе множества U_0. В результате получаем следующую таблицу, представляющую множество U_1.

Из таблицы 3.3.8 следует, что для числа элементов множества U_1, не принадлежащих множеству U_0, то есть для мощности множества $U_1 \setminus U_0$, справедливо равенство

$$|U_1 \setminus U_0| = 18.$$

По аналогии с множеством U_1, через элементы множества U_0 также вычисляются все элементы множества U_2. Только в этом случае соответствующая перестановка координат элементов множества U_0 индуцируется подстановкой

$$s_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

Таблица 3.3.8. Таблица элементов множества U_1. В этой таблице к порядковым номерам элементов, содержащихся также и в таблице 3.3.7, приписана спереди буква п

№ п/п	$(b_0, b_1, \ldots, b_7)^{\mathrm{T}}$	№ п/п	$(b_0, b_1, \ldots, b_7)^{\mathrm{T}}$	№ п/п	$(b_0, b_1, \ldots, b_7)^{\mathrm{T}}$
п1	(**0000 0001**)$^{\mathrm{T}}$	п16	(**0000 0100**)$^{\mathrm{T}}$	п31	(**0000 0101**)$^{\mathrm{T}}$
п2	(**0000 0010**)$^{\mathrm{T}}$	п17	(**0000 1000**)$^{\mathrm{T}}$	п32	(**0000 1010**)$^{\mathrm{T}}$
п3	(**0000 0011**)$^{\mathrm{T}}$	п18	(**0000 1100**)$^{\mathrm{T}}$	п33	(**0000 1111**)$^{\mathrm{T}}$
п4	(**0001 0000**)$^{\mathrm{T}}$	п19	(**0100 0000**)$^{\mathrm{T}}$	п34	(**0101 0000**)$^{\mathrm{T}}$
п5	(**0001 0001**)$^{\mathrm{T}}$	п20	(**0100 0100**)$^{\mathrm{T}}$	п35	(**0101 0101**)$^{\mathrm{T}}$
6	(0001 0010)$^{\mathrm{T}}$	21	(0100 1000)$^{\mathrm{T}}$	36	(0101 1010)$^{\mathrm{T}}$
7	(0001 0011)$^{\mathrm{T}}$	22	(0100 1100)$^{\mathrm{T}}$	37	(0101 1111)$^{\mathrm{T}}$
п8	(**0010 0000**)$^{\mathrm{T}}$	п23	(**1000 0000**)$^{\mathrm{T}}$	п38	(**1010 0000**)$^{\mathrm{T}}$
9	(0010 0001)$^{\mathrm{T}}$	24	(1000 0100)$^{\mathrm{T}}$	39	(1010 0101)$^{\mathrm{T}}$
п10	(**0010 0010**)$^{\mathrm{T}}$	п25	(**1000 1000**)$^{\mathrm{T}}$	п40	(**1010 1010**)$^{\mathrm{T}}$
11	(0010 0011)$^{\mathrm{T}}$	26	(1000 1100)$^{\mathrm{T}}$	41	(1010 1111)$^{\mathrm{T}}$
п12	(**0011 0000**)$^{\mathrm{T}}$	п27	(**1100 0000**)$^{\mathrm{T}}$	п42	(**1111 0000**)$^{\mathrm{T}}$
13	(0011 0001)$^{\mathrm{T}}$	28	(1100 0100)$^{\mathrm{T}}$	43	(1111 0101)$^{\mathrm{T}}$
14	(0011 0010)$^{\mathrm{T}}$	29	(1100 1000)$^{\mathrm{T}}$	44	(1111 1010)$^{\mathrm{T}}$
п15	(**0011 0011**)$^{\mathrm{T}}$	п30	(**1100 1100**)$^{\mathrm{T}}$	п45	(**1111 1111**)$^{\mathrm{T}}$

В этом случае

$$\breve{s}_2 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 0 & 4 & 2 & 6 & 1 & 5 & 3 & 7 \end{pmatrix}$$

и очевидно, что верно равенство

$$\breve{s}_2^{-1} = \breve{s}_2 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 0 & 4 & 2 & 6 & 1 & 5 & 3 & 7 \end{pmatrix}.$$

Из последнего равенства следует, что, если

$$(b_0, b_1, b_2, b_3, b_4, b_5, b_6, b_7)^{\mathrm{T}} \in U_0,$$

то справедливо включение

$$(b_0, b_4, b_2, b_6, b_1, b_5, b_3, b_7)^{\mathrm{T}} \in U_2,$$

то есть все элементы множества U_2 получаются путем перестановки местами первой по номеру координаты с четвертой и третьей по номеру координаты с шестой в каждом элементе множества U_0. В результате получаем следующую таблицу, представляющую множество U_2.

Таблица 3.3.9. Таблица элементов множества U_2. В этой таблице к порядковым номерам элементов, содержащихся также и в таблице 3.3.7, приписана спереди буква п

№ п/п	$(b_0, b_1, \ldots, b_7)^{\mathrm{T}}$	№ п/п	$(b_0, b_1, \ldots, b_7)^{\mathrm{T}}$	№ п/п	$(b_0, b_1, \ldots, b_7)^{\mathrm{T}}$
п1	$(\mathbf{0000\ 0001})^{\mathrm{T}}$	п16	$(\mathbf{0000\ 0010})^{\mathrm{T}}$	п31	$(\mathbf{0000\ 0011})^{\mathrm{T}}$
п2	$(\mathbf{0001\ 0000})^{\mathrm{T}}$	п17	$(\mathbf{0010\ 0000})^{\mathrm{T}}$	п32	$(\mathbf{0011\ 0000})^{\mathrm{T}}$
п3	$(\mathbf{0001\ 0001})^{\mathrm{T}}$	п18	$(\mathbf{0010\ 0010})^{\mathrm{T}}$	п33	$(\mathbf{0011\ 0011})^{\mathrm{T}}$
п4	$(\mathbf{0000\ 0100})^{\mathrm{T}}$	п19	$(\mathbf{0000\ 1000})^{\mathrm{T}}$	п34	$(\mathbf{0000\ 1100})^{\mathrm{T}}$
п5	$(\mathbf{0000\ 0101})^{\mathrm{T}}$	п20	$(\mathbf{0000\ 1010})^{\mathrm{T}}$	п35	$(\mathbf{0000\ 1111})^{\mathrm{T}}$
6	$(0001\ 0100)^{\mathrm{T}}$	21	$(0010\ 1000)^{\mathrm{T}}$	36	$(0011\ 1100)^{\mathrm{T}}$
7	$(0001\ 0101)^{\mathrm{T}}$	22	$(0010\ 1010)^{\mathrm{T}}$	37	$(0011\ 1111)^{\mathrm{T}}$
п8	$(\mathbf{0100\ 0000})^{\mathrm{T}}$	п23	$(\mathbf{1000\ 0000})^{\mathrm{T}}$	п38	$(\mathbf{1100\ 0000})^{\mathrm{T}}$
9	$(0100\ 0001)^{\mathrm{T}}$	24	$(1000\ 0010)^{\mathrm{T}}$	39	$(1100\ 0011)^{\mathrm{T}}$
п10	$(\mathbf{0101\ 0000})^{\mathrm{T}}$	п25	$(\mathbf{1010\ 0000})^{\mathrm{T}}$	п40	$(\mathbf{1111\ 0000})^{\mathrm{T}}$
11	$(0101\ 0001)^{\mathrm{T}}$	26	$(1010\ 0010)^{\mathrm{T}}$	41	$(1111\ 0011)^{\mathrm{T}}$
п12	$(\mathbf{0100\ 0100})^{\mathrm{T}}$	п27	$(\mathbf{1000\ 1000})^{\mathrm{T}}$	п42	$(\mathbf{1100\ 1100})^{\mathrm{T}}$
13	$(0100\ 0101)^{\mathrm{T}}$	28	$(1000\ 1010)^{\mathrm{T}}$	43	$(1100\ 1111)^{\mathrm{T}}$
14	$(0101\ 0100)^{\mathrm{T}}$	29	$(1010\ 1000)^{\mathrm{T}}$	44	$(1111\ 1100)^{\mathrm{T}}$
п15	$(\mathbf{0101\ 0101})^{\mathrm{T}}$	п30	$(\mathbf{1010\ 1010})^{\mathrm{T}}$	п45	$(\mathbf{1111\ 1111})^{\mathrm{T}}$

Из таблицы 3.3.9 следует, что для числа элементов множества U_2, не принадлежащих множеству U_0, то есть для мощности множества $U_2 \setminus U_0$, справедливо равенство

$$\left|U_2 \setminus U_0\right| = 18 .$$

Кроме того, пересечение множеств $U_1 \setminus U_0$ и $U_2 \setminus U_0$ равно пустому множеству. С учетом этого, для числа сепарабельных булевых масок состояний квантовой системы из трех кубитов, то есть для мощности множества

$$U = U_0 \cup U_1 \cup U_2,$$

справедлива следующая цепочка равенств

$$|U| = |U_0 \cup U_1 \cup U_2| = |U_0| + |U_1 \setminus U_0| + |U_2 \setminus U_0| = 45 + 18 + 18 = 81,$$

что и было выше в этом параграфе указано без соответствующего обоснования.

Используя таблицы 3.3.7, 3.3.8 и 3.3.9, представим множество U сепарабельных булевых масок состояний квантовой системы из трех кубитов в виде следующей таблицы.

Таблица 3.3.10. Таблица элементов множества U сепарабельных булевых масок состояний квантовой системы из трех кубитов

№ п/п	$(b_0, b_1, \ldots, b_7)^{\mathrm{T}}$	№ п/п	$(b_0, b_1, \ldots, b_7)^{\mathrm{T}}$	№ п/п	$(b_0, b_1, \ldots, b_7)^{\mathrm{T}}$
1	2	3	4	5	6
1	$(0000\ 0001)^{\mathrm{T}}$	28	$(1101\ 0000)^{\mathrm{T}}$	55	$(1000\ 1100)^{\mathrm{T}}$
2	$(0000\ 0010)^{\mathrm{T}}$	29	$(1110\ 0000)^{\mathrm{T}}$	56	$(1100\ 0100)^{\mathrm{T}}$
3	$(0000\ 0011)^{\mathrm{T}}$	30	$(1111\ 0000)^{\mathrm{T}}$	57	$(1100\ 1000)^{\mathrm{T}}$
4	$(0000\ 0100)^{\mathrm{T}}$	31	$(0001\ 0001)^{\mathrm{T}}$	58	$(0101\ 1010)^{\mathrm{T}}$
5	$(0000\ 0101)^{\mathrm{T}}$	32	$(0010\ 0010)^{\mathrm{T}}$	59	$(0101\ 1111)^{\mathrm{T}}$
6	$(0000\ 0110)^{\mathrm{T}}$	33	$(0011\ 0011)^{\mathrm{T}}$	60	$(1010\ 0101)^{\mathrm{T}}$
7	$(0000\ 0111)^{\mathrm{T}}$	34	$(0100\ 0100)^{\mathrm{T}}$	61	$(1010\ 1111)^{\mathrm{T}}$
8	$(0000\ 1000)^{\mathrm{T}}$	35	$(0101\ 0101)^{\mathrm{T}}$	62	$(1111\ 0101)^{\mathrm{T}}$
9	$(0000\ 1001)^{\mathrm{T}}$	36	$(0110\ 0110)^{\mathrm{T}}$	63	$(1111\ 1010)^{\mathrm{T}}$
10	$(0000\ 1010)^{\mathrm{T}}$	37	$(0111\ 0111)^{\mathrm{T}}$	64	$(0001\ 0100)^{\mathrm{T}}$
11	$(0000\ 1011)^{\mathrm{T}}$	38	$(1000\ 1000)^{\mathrm{T}}$	65	$(0001\ 0101)^{\mathrm{T}}$
12	$(0000\ 1100)^{\mathrm{T}}$	39	$(1001\ 1001)^{\mathrm{T}}$	66	$(0100\ 0001)^{\mathrm{T}}$
13	$(0000\ 1101)^{\mathrm{T}}$	40	$(1010\ 1010)^{\mathrm{T}}$	67	$(0101\ 0001)^{\mathrm{T}}$
14	$(0000\ 1110)^{\mathrm{T}}$	41	$(1011\ 1011)^{\mathrm{T}}$	68	$(0100\ 0101)^{\mathrm{T}}$
15	$(0000\ 1111)^{\mathrm{T}}$	42	$(1100\ 1100)^{\mathrm{T}}$	69	$(0101\ 0100)^{\mathrm{T}}$

Окончание табл. 3.3.10

1	2	3	4	5	6
16	$(0001\ 0000)^{\mathrm{T}}$	43	$(1101\ 1101)^{\mathrm{T}}$	70	$(0010\ 1000)^{\mathrm{T}}$
17	$(0010\ 0000)^{\mathrm{T}}$	44	$(1110\ 1110)^{\mathrm{T}}$	71	$(0010\ 1010)^{\mathrm{T}}$
18	$(0011\ 0000)^{\mathrm{T}}$	45	$(1111\ 1111)^{\mathrm{T}}$	72	$(1000\ 0010)^{\mathrm{T}}$
19	$(0100\ 0000)^{\mathrm{T}}$	46	$(0001\ 0010)^{\mathrm{T}}$	73	$(1010\ 0010)^{\mathrm{T}}$
20	$(0101\ 0000)^{\mathrm{T}}$	47	$(0001\ 0011)^{\mathrm{T}}$	74	$(1000\ 1010)^{\mathrm{T}}$
21	$(0110\ 0000)^{\mathrm{T}}$	48	$(0010\ 0001)^{\mathrm{T}}$	75	$(1010\ 1000)^{\mathrm{T}}$
22	$(0111\ 0000)^{\mathrm{T}}$	49	$(0010\ 0011)^{\mathrm{T}}$	76	$(0011\ 1100)^{\mathrm{T}}$
23	$(1000\ 0000)^{\mathrm{T}}$	50	$(0011\ 0001)^{\mathrm{T}}$	77	$(0011\ 1111)^{\mathrm{T}}$
24	$(1001\ 0000)^{\mathrm{T}}$	51	$(0011\ 0010)^{\mathrm{T}}$	78	$(1100\ 0011)^{\mathrm{T}}$
25	$(1010\ 0000)^{\mathrm{T}}$	52	$(0100\ 1000)^{\mathrm{T}}$	79	$(1111\ 0011)^{\mathrm{T}}$
26	$(1011\ 0000)^{\mathrm{T}}$	53	$(0100\ 1100)^{\mathrm{T}}$	80	$(1100\ 1111)^{\mathrm{T}}$
27	$(1100\ 0000)^{\mathrm{T}}$	54	$(1000\ 0100)^{\mathrm{T}}$	81	$(1111\ 1100)^{\mathrm{T}}$

Используя результаты, представленные в данном параграфе, и пункт (б) следствия 2.5.27 (**критерий К$_3$**), для решения задачи бинарной классификации состояний квантовой системы из трех кубитов (т. е. задачи определения, несепарабельно данное состояние или нет) предлагается **алгоритм К$_3$**, где **К** – первая буква имени **Константин**, а индекс **3** связан с числом кубитов в трехкубитной квантовой системе, состояния которой исследуются. Этот алгоритм состоит из трех этапов, называемых шагами. Второй этап может быть реализован в одной из двух форм в зависимости от наличия таблицы 3.3.10: в форме **шага 2**, если таблица 3.3.10 имеется в наличии; или в форме **шага 2′**, если таблица 3.3.10 отсутствует.

Алгоритм К$_3$

Шаг 1. По заданному состоянию $|\psi\rangle = (a_0,\ a_1,\ \ldots,\ a_7)^{\mathrm{T}}$ трехкубитной квантовой системы вычисляется его булева маска $(b_0,\ b_1,\ \ldots,\ b_7)^{\mathrm{T}}$ в соответствии с правилом

$$b_k = \begin{cases} 0, \text{ если } a_k = 0; \\ 1 \text{ в противном случае,} \end{cases}$$

где $k \in \{0,\ 1,\ \ldots,\ 7\}$.

Шаг 2. (Реализуется, если таблица 3.3.10 имеется в наличии.) Проверяется, принадлежит ли вектор $(b_0,\ b_1,\ \ldots,\ b_7)^{\mathrm{T}}$ таблице 3.3.10.

Если вектор $(b_0,\ b_1,\ \ldots,\ b_7)^{\mathrm{T}}$ не принадлежит таблице 3.3.10, то состояние $|\psi\rangle$ является несепарабельным состоянием и алгоритм завершен. В противном случае осуществляется переход к шагу 3.

Шаг 2′.(Реализуется, если таблица 3.3.10 отсутствует.) Проверяется, имеется ли среди трех векторов

$$(b_0,\ b_1,\ b_2,\ b_3,\ b_4,\ b_5,\ b_6,\ b_7)^{\mathrm{T}},$$

$$(b_0,\ b_1,\ b_4,\ b_5,\ b_2,\ b_3,\ b_6,\ b_7)^{\mathrm{T}}$$

и

$$(b_0,\ b_4,\ b_2,\ b_6,\ b_1,\ b_5,\ b_3,\ b_7)^{\mathrm{T}}$$

хотя бы один вектор, такой, что он структурно состоит из двух последовательно расположенных двоичных четырехмерных векторов, из которых хотя бы один пропорционален другому с коэффициентом пропорциональности $\tau \in \{0,\ 1\}$.

Если такого вектора не имеется, то состояние $|\psi\rangle$ является несепарабельным состоянием и алгоритм завершен. В противном случае – переход к шагу 3.

Шаг 3. Используя значения координат состояния $|\psi\rangle = (a_0,\ a_1,\ \ldots,\ a_7)^{\mathrm{T}}$, вычисляются следующие наборы величин:

$$V_{21}^{(0)} = \{a_0a_5 - a_1a_4,\ a_0a_6 - a_2a_4,\ a_0a_7 - a_3a_4,$$
$$a_1a_6 - a_2a_5,\ a_1a_7 - a_3a_5,\ a_2a_7 - a_3a_6\},$$

$$V_{21}^{(1)} = \{a_0a_3 - a_1a_2,\ a_0a_6 - a_2a_4,\ a_0a_7 - a_2a_5,$$
$$a_1a_6 - a_3a_4,\ a_1a_7 - a_3a_5,\ a_4a_7 - a_5a_6\},$$

$$V_{21}^{(2)} = \{a_0a_5 - a_1a_4,\ a_0a_3 - a_1a_2,\ a_0a_7 - a_1a_6,$$
$$a_3a_4 - a_2a_5,\ a_4a_7 - a_5a_6,\ a_2a_7 - a_3a_6\}.$$

Если среди наборов величин $V_{21}^{(0)}$, $V_{21}^{(1)}$ и $V_{21}^{(2)}$ имеется хотя бы один нулевой набор, то состояние $|\psi\rangle$ является сепарабельным состоянием и алгоритм завершен.

Если все три набора величин $V_{21}^{(0)}$, $V_{21}^{(1)}$ и $V_{21}^{(2)}$ являются ненулевыми, то состояние $|\psi\rangle$ является несепарабельным состоянием и алгоритм завершен.

Закончим данный параграф следующим замечанием.

Замечание 3.3.11. В случае решения задачи бинарной классификации состояний трехкубитных квантовых систем в **алгоритме К$_3$** можно было бы обойтись реализацией одного этапа, а именно – шага 3, который по существу является непосредственным применением **критерия К$_3$** (см пункт (б) следствия 2.5.27). Однако число наборов величин, которые необходимо вычислить для решения задачи бинарной классификации состояний квантовой системы из n кубитов, растет экспоненциально с ростом n. Поэтому в **алгоритме К$_n$** (**алгоритме Константин$_n$**) решения задачи бинарной классификации состояний в случае n кубитов, который во многом аналогичен **алгоритму К$_3$**, этапы, подобные первым двум шагам в **алгоритме К$_3$**, могут оказаться существенно полезными, что и может служить одним из возможных обоснований необходимости обращения внимания к булевым маскам состояний квантовых систем. В данной работе **алгоритм К$_n$** не приводится, так как основные математические идеи, заложенные в нем, представлены на примере **алгоритма К$_3$**.

Выводы по главе 3

1. Если булева маска состояния квантовой системы, состоящей из n кубитов (где $n \in \mathbb{N}$), является несепарабельной, то само состояние также является несепарабельным.

2. Выяснение вопроса несепарабельности для булевой маски состояния квантовой системы является менее трудоемкой в вычислительном плане задачей, чем для самого состояния. Поэтому подход, основанный на использовании булевых масок для определения несепарабельности состояний квантовых систем, оказывается эффективным подходом в решении задачи бинарной классификации состояний для случаев, когда булевы маски несепарабельны.

3. Если нумератор весов состояния квантовой системы, состоящей из n кубитов (где $n \in \mathbb{N}$), не равен произведению нумераторов весов состояний квантовых систем с числом кубитов, меньшим, чем n, то это состояние является несепарабельным.

4. Если нумератор весов состояния квантовой системы, состоящей из n кубитов (где $n \in \mathbb{N}$), является неприводимым многочленом над кольцом целых чисел, то это состояние является несепарабельным.

5. Нумераторы весов состояний квантовых систем позволяют получить эффективные достаточные условия несепарабельности этих состояний.

6. Число сепарабельных булевых масок состояний квантовых систем из трех кубитов равно 81, а число несепарабельных – 174 (общее число булевых масок трехкубитных квантовых систем равно 255).

7. Разработан и представлен эффективный **алгоритм К$_3$** (**алгоритм Константин$_3$**), позволяющий определить, сепарабельно или нет произвольное состояние квантовой системы из трех кубитов. И, тем самым, можно полагать, что задача бинарной классификации состояний

трехкубитных квантовых систем (то есть задача определения, к какому из двух классов – классу сепарабельных состояний или классу несепарабельных состояний – принадлежит заданное трехкубитное состояние) полностью решена в алгоритмическом плане.

8. **Алгоритм $К_3$** в настоящее время является существенным продвижением в решении актуальной для практических приложений задачи бинарной классификации состояний многокубитных квантовых систем.

9. Математические идеи, заложенные в **алгоритме $К_3$**, позволили также сделать обобщение до уровня **алгоритма $К_n$** (**алгоритма Константин$_n$**) решения задачи бинарной классификации состояний квантовых систем, состоящих из n кубитов, где $n > 3$.

ГЛАВА 4

Мера несепарабельности состояний квантовых систем

Введение к главе 4

Глава 4 состоит из шести параграфов.

В параграфе 4.1 рассматривается одна из мер несепарабельности состояний квантовых систем. Она представляет собой наиболее простой вариант меры квантовой запутанности и определяется через энтропию фон Неймана. Эта мера в квантовой теории используется для характеризации несепарабельности состояний двухкубитных квантовых систем. Исследуются свойства этой меры. Получено выражение значения меры несепарабельности состояния двухкубитной квантовой системы через коэффициенты разложения, представляющего данное состояние в вычислительном базисе (соотношение (4.1.8)). Установлена взаимосвязь между такими характеристиками состояний квантовых систем, как мера несепарабельности и согласованность (соотношение (4.1.9)).

В квантовой теории известно, что для любого состояния Белла двухкубитной квантовой системы характерно то, что ни один из двух кубитов, входящих в квантовую систему, не имеет определенного значения в смысле состояния. Но, как только один из них будет подвергнут измерению (результат которого будет совершенно случайным), то сразу же окажется, что другой имеет определенное значение. Это и есть одно из проявлений «необычных сверхвозможностей» передачи квантовой информации, так как во время измерения два кубита могут быть удаленными друг от друга на произвольно большое расстояние. В параграфе 4.1 в этом направлении получен результат более общего плана. А именно, доказано, что указанным свойством обладает каждое состояние двухкубитной квантовой системы с положительной мерой несепарабельности при специальном выборе операторов измерения этого состояния. Сам результат сформулирован в виде утверждения 4.1.16. Кроме того, в доказательстве данного утверждения приведены выражения для операторов измерений через базисы Шмидта подсистем исходной двухкубитной квантовой системы, реализация каждого из которых по отношению к одному из кубитов приводит другой кубит к вполне определенному состоянию, принадлежащему соответствующему базису Шмидта.

В параграфе 4.2 сформулировано и доказано утверждение 4.2.4. Полученный результат опишем качественно. По двум произвольным образом зафиксированным ортонормированным базисам двумерного гильбертова пространства над полем комплексных чисел строятся соответственно две пары проекторов. Каждая из пар определяет некоторое проективное измерение. Суть результата, представленного утверждением 4.2.4, заключается в полном описании состояний с максимальной мерой несепарабельности двухкубитной квантовой системы, обладающих тем свойством, что измерение одного из кубитов системы (результат которого будет совершенно случайным) приводит другой кубит к вполне определенному состоянию из соответствующего базиса. Полнота описания доведена до получения выражений для указанных состояний с максимальной мерой несепарабельности через векторы вышеуказанных ортонормированных базисов.

В параграфе 4.3 рассматривается более общая количественная мера несепарабельности (под названием **согласованность**) двухсоставной квантовой системы (не обязательно двухкубитной), отражающая запутанность друг с другом двух ее составляющих подсистем, как для чистого, так и для смешанного состояния. Приводятся результаты применения этой меры к трехкубитным и двухкубитным квантовым системам. Доказано, что данная количественная мера в случае двухкубитной квантовой системы совпадает с характеристикой C двухкубитной квантовой системы, введенной в параграфе 4.1 под названием **согласованность**.

Параграф 4.4 посвящен вопросам построения количественной характеристики ресурса несепарабельности состояний многокубитных квантовых систем. Представлена мера несепарабельности, названная **мера Виолетта**, или, кратко, **V-мера**. Для построения этой меры применен один из распространенных подходов к построению меры несепарабельности многокубитных квантовых систем, заключающийся в использовании в качестве меры функций от мер несепарабельности двухсоставных систем. **V-мера** (**мера Виолетта**) дает количественную характеристику ресурса несепарабельности состояний n-кубитной квантовой системы (где $n > 1$) с позиции наименее «надежного» звена (подсистемы исходной системы) по несепарабельности во всей системе.

В параграфе 4.5 общие результаты параграфа 4.4 применены к трехкубитным квантовым системам. Получено выражение для значения **V-меры** произвольного состояния трехкубитной квантовой системы через координаты состояния в вычислительном базисе. Приведены примеры вычисления значений **меры Виолетта** для некоторых состояний трехкубитной квантовой системы.

В параграфе 4.6 общие результаты параграфа 4.4 применены к четырехкубитным квантовым системам. Получено выражение для значения **V-меры** произвольного состояния четырехкубитной квантовой системы через координаты состояния в вычислительном базисе. Приведены примеры вычисления значений **меры Виолетта** для некоторых состояний четырехкубитной квантовой системы.

§ 4.1. Мера несепарабельности состояний двухкубитных квантовых систем

Несепарабельность квантовых состояний является физическим ресурсом принципиально нового типа, предоставляемым квантовой механикой [24; 29; 33; 47; 50; 52]. Несмотря на свою новизну, этот ресурс, как и любой другой физический ресурс (например, масса, энергия и т. д.), предполагает свое количественное описание путем использования меры квантовой несепарабельности. Существует несколько различных мер квантовой несепарабельности [72; 74; 80]. Среди них мы выделим меру несепарабельности, предложенную в работе [72], в силу того, что она и является наиболее простой в плане физического понимания ее смысла, и обладает относительной невысокой сложностью с точки зрения проведения необходимых вычислений для получения конкретных числовых значений.

Физическая простота этой меры обусловлена прежде всего тем, что она используется для характеризации несепарабельности квантовых систем в наипростейшем случае, а именно – квантовой системы в чистом состоянии, представленном в двухсоставном виде. То есть данная мера дает количественную характеристику несепарабельности между двумя квантовыми подсистемами, в совокупности составляющими всю квантовую систему, при условии, что вся квантовая система находится в чистом состоянии.

Невысокая вычислительная сложность этой меры связана с тем, что она определяется на основе энтропии фон Неймана [50], в которой используются вычислительно несложные элементарные матричные функции.

Определение 4.1.1. Энтропией фон Неймана квантовой системы называется величина $S(\rho)$, задаваемая равенством

$$S(\rho) = -\mathrm{tr}\left(\rho \log_2 \rho\right),$$

где ρ – матрица плотности квантовой системы.

Определение 4.1.2. Пусть $\rho_{\mathrm{A}}^{(\mathrm{AB})}$ – редуцированная матрица плотности подсистемы A двухсоставной квантовой системы AB в чистом состоянии $|\psi\rangle$. Мерой несепарабельности (запутанности) состояния $|\psi\rangle$ называется число $E(|\psi\rangle)$, задаваемое равенством

$$E(|\psi\rangle) = S\left(\rho_{\mathrm{A}}^{(\mathrm{AB})}\right).$$

Так как справедливо соотношение

$$S\left(\rho_{\mathrm{A}}^{(\mathrm{AB})}\right)=S\left(\rho_{\mathrm{B}}^{(\mathrm{AB})}\right),$$

то меру несепарабельности можно определить и через равенство

$$E\left(|\psi\rangle\right)=S\left(\rho_{\mathrm{B}}^{(\mathrm{AB})}\right),$$

где $\rho_{\mathrm{B}}^{(\mathrm{AB})}$ – редуцированная матрица плотности подсистемы B двухсоставной квантовой системы AB в чистом состоянии $|\psi\rangle$.

Обсудим введенную меру несепарабельности $E\left(|\psi\rangle\right)$.

Прежде всего заметим, что с физической точки зрения получение редуцированной матрицы плотности для подсистемы квантовой системы – это усреднение по всем внешним степеням свободы выделенной подсистемы (по ее внешнему окружению). В некотором отношении это проведение границы между подсистемой и ее окружением, когда подсистема может рассматриваться независимо от него. То есть подсистема как бы «вырезается» из более сложной структуры, каковой является двухсоставная квантовая система, и рассматривается в качестве самостоятельного объекта.

Каждая из подсистем A и B двухсоставной квантовой системы AB, в общем, находится в смешанном состоянии, хотя вся система AB находится в чистом состоянии. (Выражение «в общем» здесь используется для того, чтобы был включен и случай сепарабельности состояния $|\psi\rangle$, когда оно является тензорным произведением чистых состояний, трактуемых как частные случаи смешанных состояний; см. замечание в § 1.1). Редуцированные матрицы плотности $\rho_{\mathrm{A}}^{(\mathrm{AB})}$ и $\rho_{\mathrm{B}}^{(\mathrm{AB})}$ имеют смысл матриц плотности смешанных состояний соответственно подсистем A и B. Поэтому энтропия фон Неймана $S\left(\rho_{\mathrm{A}}^{(\mathrm{AB})}\right)$ ($S\left(\rho_{\mathrm{B}}^{(\mathrm{AB})}\right)$) смешанного состояния подсистемы A (подсистемы B) рассматривается как мера запутанности состояния подсистемы A с состояниями окружения B (как мера запутанности состояния B с состояниями окружения A). Таким образом, мера несепарабельности состояния $|\psi\rangle$ квантовой системы AB по сути есть мера запутанности состояний подсистем A и B между собой. Меру запутанности состояний подсистем A и B между собой можно понимать следующим образом.

Неопределенность (энтропия) в подсистеме B до измерения в A равна $S\left(\rho_{\mathrm{B}}^{(\mathrm{AB})}\right)$. После измерения в A неопределенность исчезает, и состояние подсистемы A становится нам известным и определенным, что влечет известность и определенность и состояния подсистемы B.

Аналогично, неопределенность (энтропия) в подсистеме A до измерения в B равна $S\left(\rho_{\mathrm{A}}^{(\mathrm{AB})}\right)$. После измерения в B неопределенность исчезает, и состояние подсистемы B становится известным и определенным, что влечет известность и определенность и состояния подсистемы A.

Поэтому количество приобретенной информации в обоих случаях равно

$$S\left(\rho_{\mathrm{B}}^{(\mathrm{AB})}\right)=S\left(\rho_{\mathrm{A}}^{(\mathrm{AB})}\right).$$

Для величины $E\left(|\psi\rangle\right)$ справедливо [24] следующее двойное неравенство:

$$0 \le E\left(|\psi\rangle\right) \le 1 .$$

При этом если $|\psi\rangle$ – сепарабельное состояние, то $E\left(|\psi\rangle\right)=0$.

Если же $|\psi\rangle$ – несепарабельное состояние, то $E\left(|\psi\rangle\right)>0$ и точное значение $E\left(|\psi\rangle\right)$ определяется неопределенностью состояний подсистем A и B, «взятых» по отдельности.

Напомним, что в вычислительном базисе из векторов $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$ произвольное двухкубитное состояние $|\psi\rangle$ квантовой системы AB можно представить в следующем общем виде:

$$|\psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle, \tag{4.1.3}$$

где a, b, c, $d \in \mathbb{C}$,

$$|a|^2 + |b|^2 + |c|^2 + |d|^2 = 1. \tag{4.1.4}$$

Представим меру несепарабельности двухкубитного состояния $|\psi\rangle$ как функцию от коэффициентов a, b, c, d разложения (4.1.3) по вычислительному базису из векторов $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$. Для этого сперва выпишем редуцированную матрицу плотности $\rho_{\mathrm{A}}^{(\mathrm{AB})}$ подсистемы A квантовой системы AB. Как следует из (2.2.22), для редуцированной матрицы плотности $\rho_{\mathrm{A}}^{(\mathrm{AB})}$ подсистемы A квантовой системы AB справедливо равенство

$$\rho_{\mathrm{A}}^{(\mathrm{AB})} = \begin{pmatrix} |a|^2 + |b|^2 & a\tilde{c} + b\tilde{d} \\ c\tilde{a} + d\tilde{b} & |c|^2 + |d|^2 \end{pmatrix}. \tag{4.1.5}$$

По определению 4.1.2 для меры несепарабельности состояния $|\psi\rangle$ имеем

$$E\left(|\psi\rangle\right) = S\left(\rho_{\mathrm{A}}^{(\mathrm{AB})}\right) = -\mathrm{tr}\left(\rho_{\mathrm{A}}^{(\mathrm{AB})} \log_2 \rho_{\mathrm{A}}^{(\mathrm{AB})}\right). \tag{4.1.6}$$

В правой части цепочки равенств (4.1.6) надо найти след (сумму диагональных элементов) матрицы, равной произведению двух матриц $\rho_{\mathrm{A}}^{(\mathrm{AB})}$ и $\log_2 \rho_{\mathrm{A}}^{(\mathrm{AB})}$. Напомним [25; 26; 45; 55], что сумма диагональных элементов матрицы равна сумме ее собственных значений.

Собственные значения матрицы $\rho_{\mathrm{A}}^{(\mathrm{AB})}$ найдем путем вычисления корней характеристического многочлена $\chi(\lambda)$ матрицы $\rho_{\mathrm{A}}^{(\mathrm{AB})}$. Для характеристического многочлена $\chi(\lambda)$ матрицы $\rho_{\mathrm{A}}^{(\mathrm{AB})}$ имеют место равенства [26]:

$$\chi(\lambda) = \det\left(\lambda \mathbf{I}_2 - \rho_{\mathrm{A}}^{(\mathrm{AB})}\right) =$$
$$= \left(\lambda - \left(|a|^2 + |b|^2\right)\right)\left(\lambda - \left(|c|^2 + |d|^2\right)\right) - \left(a\tilde{c} + b\tilde{d}\right)\left(c\tilde{a} + d\tilde{b}\right) =$$
$$= \lambda^2 - \lambda\left(|a|^2 + |b|^2 + |c|^2 + |d|^2\right) + \left(|a|^2 + |b|^2\right)\left(|c|^2 + |d|^2\right) -$$
$$-\left(|a|^2 |c|^2 + |b|^2 |d|^2 + a\tilde{b}\tilde{c}d + \tilde{a}bc\tilde{d}\right) =$$
$$= \lambda^2 - \lambda + |a|^2 |d|^2 + |b|^2 |c|^2 - a\tilde{b}\tilde{c}d - \tilde{a}bc\tilde{d} =$$
$$= \lambda^2 - \lambda + \left(ad - bc\right)\left(\tilde{a}\tilde{d} - \tilde{b}\tilde{c}\right) =$$
$$= \lambda^2 - \lambda + |ad - bc|^2 .$$

Для нахождения собственных значений решаем квадратное уравнение

$$\lambda^2 - \lambda + |ad - bc|^2 = 0 .$$

Корни его равны

$$\lambda_{1,2} = \frac{1 \pm \sqrt{1 - 4|ad - bc|^2}}{2}, \tag{4.1.7}$$

или

$$\lambda_1 = \frac{1 + \sqrt{1 - 4|ad - bc|^2}}{2}, \; \lambda_2 = \frac{1 - \sqrt{1 - 4|ad - bc|^2}}{2} .$$

Отсюда следует (с учетом того, что полагается $0 \log_2 0 = 0$) [50], что для меры несепарабельности двухкубитного состояния $|\psi\rangle$ имеет место следующая цепочка равенств

$$E\left(|\psi\rangle\right) = -\mathrm{tr}\left(\rho_{\mathrm{A}}^{(\mathrm{AB})} \log_2 \rho_{\mathrm{A}}^{(\mathrm{AB})}\right) = -\lambda_1 \log_2 \lambda_1 - \lambda_2 \log_2 \lambda_2 =$$
$$= -\left(\frac{1 + \sqrt{1 - 4|ad - bc|^2}}{2}\right)\log_2\left(\frac{1 + \sqrt{1 - 4|ad - bc|^2}}{2}\right) -$$
$$-\left(\frac{1 - \sqrt{1 - 4|ad - bc|^2}}{2}\right)\log_2\left(\frac{1 - \sqrt{1 - 4|ad - bc|^2}}{2}\right). \tag{4.1.8}$$

Рассматривая выражение (4.1.8) для меры запутанности $E(|\psi\rangle)$ двухкубитного состояния $|\psi\rangle$, мы обнаруживаем, что $E(|\psi\rangle)$ зависит от коэффициентов a, b, c, d разложения (4.1.3) по вычислительному базису из векторов $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$ не напрямую, а через выражение $|ad-bc|$, которое может, вообще говоря, принимать одно и то же значение необязательно для одинаковых наборов значений коэффициентов a, b, c, d. Обозначим

$$C = 2|ad-bc|.$$

В этом случае выражение для меры запутанности $E(|\psi\rangle)$ приобретает следующий вид

$$E(|\psi\rangle) =$$
$$= -\left(\frac{1+\sqrt{1-C^2}}{2}\right)\log_2\left(\frac{1+\sqrt{1-C^2}}{2}\right) - \left(\frac{1-\sqrt{1-C^2}}{2}\right)\log_2\left(\frac{1-\sqrt{1-C^2}}{2}\right) =$$
$$= H\left(\frac{1+\sqrt{1-C^2}}{2}\right), \tag{4.1.9}$$

где

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

– функция энтропии Шеннона [39].

Как мы видим, величина C является характеристикой двухкубитного состояния $|\psi\rangle$, непосредственно связанной с мерой запутанности $E(|\psi\rangle)$.

Характеристика C называется **согласованностью** (concurrence) двухкубитного состояния $|\psi\rangle$ [72; 73]. Для C справедливо двойное неравенство

$$0 \le C \le 1.$$

Максимальное значение меры запутанности $E(|\psi\rangle)$ для двухкубитного состояния $|\psi\rangle$ достигается при согласованности $C = 1$.

Заметим, что согласованность также используется в качестве меры несепарабельности квантовых состояний [80]. Более того, уже найдено удобное и общее выражение для вычисления согласованности в двухсоставных системах [86]. Частным случаем данного выражения является выражение для вычисления согласованности в двухкубитных квантовых системах, приведенное выше. Тем не менее, мера несепарабельности $E\left(|\psi\rangle\right)$, представленная определением 4.1.2, более привлекательна для использования по сравнению с другими мерами несепарабельности прежде всего наличием прямой связи этой меры с энтропией фон Неймана (см. определение 4.1.1) и энтропией Шеннона (см. (4.1.9)), и поэтому она имеет непосредственную теоретико-информационную трактовку.

Напомним, что для любого состояния Белла двухкубитной квантовой системы характерно то, что ни один из двух кубитов, входящих в квантовую систему, не имеет определенного значения состояния. Но, как только один из них будет подвергнут измерению (результат которого будет совершенно случайным), сразу же окажется, что другой имеет определенное значение состояния. В этом и проявляются «необычные сверхвозможности» передачи квантовой информации, так как во время измерения два кубита могут быть удаленными друг от друга на произвольно большое расстояние. Для математического описания данного явления в качестве запутанного состояния рассмотрим, например, состояние Белла

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

квантовой системы из двух кубитов. Используя равенство (4.1.8), получаем, что мера несепарабельности $E\left(|\psi_{00}\rangle\right)$ состояния $|\psi_{00}\rangle$ равна

$$E\left(|\psi_{00}\rangle\right) =$$

$$= -\left(\frac{1+\sqrt{1-4\left|\frac{1}{\sqrt{2}}\cdot\frac{1}{\sqrt{2}}-0\cdot 0\right|^2}}{2}\right)\log_2\left(\frac{1+\sqrt{1-4\left|\frac{1}{\sqrt{2}}\cdot\frac{1}{\sqrt{2}}-0\cdot 0\right|^2}}{2}\right) -$$

$$-\left(\frac{1-\sqrt{1-4\left|\frac{1}{\sqrt{2}}\cdot\frac{1}{\sqrt{2}}-0\cdot 0\right|^2}}{2}\right)\log_2\left(\frac{1-\sqrt{1-4\left|\frac{1}{\sqrt{2}}\cdot\frac{1}{\sqrt{2}}-0\cdot 0\right|^2}}{2}\right)=$$

$$=-\frac{1}{2}\log_2\frac{1}{2}-\frac{1}{2}\log_2\frac{1}{2}=1,$$

то есть принимает максимально возможное значение для двухкубитных состояний.

Проведем измерение над первым кубитом. Это измерение в случае одиночного кубита осуществляется двумя операторами измерения: $M_0=|0\rangle\langle 0|$ и $M_1=|1\rangle\langle 1|$. В случае же измерения первого кубита в двухкубитной квантовой системе, осуществление соответствующей процедуры удобно представить двумя операторами измерения: $M_0\otimes\mathbf{I}_2$ и $M_1\otimes\mathbf{I}_2$, где $\mathbf{I}_2$ – тождественный оператор, действующий в пространстве $\mathbb{C}^2$. Вероятность того, что в результате измерения будет получено состояние $|00\rangle$ (для первого кубита состояние $|0\rangle$), равна

$$p(|00\rangle)=p(0)=\langle\psi_{00}|(M_0\otimes\mathbf{I}_2)^*(M_0\otimes\mathbf{I}_2)|\psi_{00}\rangle=\langle\psi_{00}|(M_0\otimes\mathbf{I}_2)|\psi_{00}\rangle=$$

$$=\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 0 & 0 & 1\end{pmatrix}\cdot\frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\\0\end{pmatrix}=\frac{1}{2};$$

а после измерения система будет находиться в состоянии

$$\frac{(M_0\otimes\mathbf{I}_2)|\psi_{00}\rangle}{\sqrt{\langle\psi_{00}|(M_0\otimes\mathbf{I}_2)^*(M_0\otimes\mathbf{I}_2)|\psi_{00}\rangle}}=\begin{pmatrix}1\\0\\0\\0\end{pmatrix}=|00\rangle.$$

Вероятность того, что в результате измерения будет получено состояние $|11\rangle$ (для первого кубита состояние $|1\rangle$), равна

$$p(|11\rangle) = p(1) = \langle \psi_{00} | (M_1 \otimes \mathbf{I}_2)^* (M_1 \otimes \mathbf{I}_2) | \psi_{00} \rangle = \langle \psi_{00} | (M_1 \otimes \mathbf{I}_2) | \psi_{00} \rangle =$$

$$= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 0 & 1 \end{pmatrix} \cdot \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \frac{1}{2};$$

а после измерения система будет находиться в состоянии

$$\frac{(M_1 \otimes \mathbf{I}_2) | \psi_{00} \rangle}{\sqrt{\langle \psi_{00} | (M_1 \otimes \mathbf{I}_2)^* (M_1 \otimes \mathbf{I}_2) | \psi_{00} \rangle}} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = |11\rangle .$$

Очевидно, что последующее измерение второго кубита квантовой системы дает тот же результат, что и измерение первого кубита, то есть результаты измерений оказываются **коррелированными**.

Подобного рода корреляции результатов измерений присущи и остальным состояниям Белла $|\psi_{01}\rangle$, $|\psi_{10}\rangle$ и $|\psi_{11}\rangle$, мера несепарабельности каждой из которых также максимальна, то есть равна 1. Например, измеряя в вычислительном базисе первый кубит двухкубитной квантовой системы, находящейся в состоянии $|\psi_{11}\rangle$, получаем $|0\rangle$ с вероятностью 1,2 и $|1\rangle$ с вероятностью 1/2, а последующее измерение второго кубита дает результат, противоположный состоянию первого кубита, то есть получаем в первом случае обязательно $|1\rangle$, а во втором случае обязательно $|0\rangle$.

Аналогичные эффекты проявляются и при другом порядке измерения кубитов запутанной квантовой системы, находящейся в одном из состояний Белла, то есть при измерении сперва состояния второго кубита, а затем – первого кубита.

Однако вышеописанные эффекты не являются следствием только свойства несепарабельности квантовых состояний. Свою важную роль играют и операторы измерения. Проиллюстрируем это на конкретном примере. То есть приведем пример состояния двухкубитной квантовой системы, мера несепарабельности которой равна максимальному значению 1, но, в то же самое время, если любой один из двух кубитов будет подвергнут измерению в составе двухкубитной квантовой системы (первый – с использованием операторов $M_0 \otimes \mathbf{I}_2$ и $M_1 \otimes \mathbf{I}_2$, а второй – с использованием операторов $\mathbf{I}_2 \otimes M_0$ и $\mathbf{I}_2 \otimes M_1$), то другой оставшийся кубит не имеет определенного значения $|0\rangle$ или $|1\rangle$, то есть находится в состоянии суперпозиции. Таковым примером может служить любое из следующих квантовых состояний **Клюева** (**Клюев Александр Владимирович** – талантливый инженер-криптограф, один из первых в России начал внедрение квантовых технологий в практику обеспечения информационной безопасности):

$$|\varphi_1\rangle = -\frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle, \tag{4.1.10}$$

$$|\varphi_2\rangle = \frac{1}{2}|00\rangle - \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle, \tag{4.1.11}$$

$$|\varphi_3\rangle = \frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle - \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle, \tag{4.1.12}$$

$$|\varphi_4\rangle = \frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle - \frac{1}{2}|11\rangle. \tag{4.1.13}$$

Действительно, рассмотрим состояние $|\varphi_1\rangle$, определенное равенством (4.1.10). Из равенств (4.1.8) следует, что мера несепарабельности $E(|\varphi_1\rangle)$ состояния $|\varphi_1\rangle$ равна

$$E(|\varphi_1\rangle) =$$

$$= -\left(\frac{1+\sqrt{1-4\left|-\frac{1}{2}\cdot\frac{1}{2}-\frac{1}{2}\cdot\frac{1}{2}\right|^2}}{2}\right)\log_2\left(\frac{1+\sqrt{1-4\left|-\frac{1}{2}\cdot\frac{1}{2}-\frac{1}{2}\cdot\frac{1}{2}\right|^2}}{2}\right) -$$

$$-\left(\frac{1-\sqrt{1-4\left|-\frac{1}{2}\cdot\frac{1}{2}-\frac{1}{2}\cdot\frac{1}{2}\right|^2}}{2}\right)\log_2\left(\frac{1-\sqrt{1-4\left|-\frac{1}{2}\cdot\frac{1}{2}-\frac{1}{2}\cdot\frac{1}{2}\right|^2}}{2}\right) =$$

$$= -\frac{1}{2}\log_2\frac{1}{2} - \frac{1}{2}\log_2\frac{1}{2} = 1,$$

то есть $E\left(\left|\varphi_1\right\rangle\right)$ равна максимальному значению 1.

Аналогично можно показать, что мера несепарабельности каждого из остальных состояний Клюева $\left|\varphi_2\right\rangle$, $\left|\varphi_3\right\rangle$, $\left|\varphi_4\right\rangle$ равна 1.

Теперь измерим сперва состояние первого кубита двухкубитной квантовой системы, находящейся в состоянии $\left|\varphi_1\right\rangle$. Напомним, что это измерение в случае одиночного кубита осуществляется двумя операторами измерения: $M_0 = \left|0\right\rangle\left\langle 0\right|$ и $M_1 = \left|1\right\rangle\left\langle 1\right|$. В случае же измерения первого кубита в двухкубитной квантовой системе осуществление соответствующей процедуры удобно представить двумя операторами измерения: $M_0 \otimes \mathbf{I}_2$ и $M_1 \otimes \mathbf{I}_2$, где $\mathbf{I}_2$ – тождественный оператор, действующий в пространстве $\mathbb{C}^2$. Вероятность того, что в результате измерения для первого кубита будет получено состояние $\left|0\right\rangle$, равна

$$p\left(\left|0\right\rangle\right) = \left\langle\varphi_1\right|\left(M_0 \otimes \mathbf{I}_2\right)^*\left(M_0 \otimes \mathbf{I}_2\right)\left|\varphi_1\right\rangle = \left\langle\varphi_1\right|\left(M_0 \otimes \mathbf{I}_2\right)\left|\varphi_1\right\rangle =$$

$$= \frac{1}{2}\begin{pmatrix}-1 & 1 & 1 & 1\end{pmatrix}\cdot\frac{1}{2}\begin{pmatrix}-1\\ 1\\ 0\\ 0\end{pmatrix} = \frac{1}{4}\cdot 2 = \frac{1}{2};$$

а после измерения система будет находиться в состоянии

$$\frac{\left(M_0 \otimes \mathbf{I}_2\right)\left|\varphi_1\right\rangle}{\sqrt{\left\langle\varphi_1\right|\left(M_0 \otimes \mathbf{I}_2\right)^*\left(M_0 \otimes \mathbf{I}_2\right)\left|\varphi_1\right\rangle}} = \frac{1}{\sqrt{2}}\begin{pmatrix}-1\\ 1\\ 0\\ 0\end{pmatrix} = -\frac{1}{\sqrt{2}}\left|00\right\rangle + \frac{1}{\sqrt{2}}\left|01\right\rangle =$$

$$= \left|0\right\rangle \otimes \left(-\frac{1}{\sqrt{2}}\left|0\right\rangle + \frac{1}{\sqrt{2}}\left|1\right\rangle\right). \qquad (4.1.14)$$

Вероятность того, что в результате измерения для первого кубита будет получено состояние $|1\rangle$, равна

$$p(|1\rangle) = \langle\varphi_1|(M_1 \otimes \mathbf{I}_2)^*(M_1 \otimes \mathbf{I}_2)|\varphi_1\rangle = \langle\varphi_1|(M_1 \otimes \mathbf{I}_2)|\varphi_1\rangle =$$

$$= \frac{1}{2}\begin{pmatrix}-1 & 1 & 1 & 1\end{pmatrix} \cdot \frac{1}{2}\begin{pmatrix}0\\0\\1\\1\end{pmatrix} = \frac{1}{4}\cdot 2 = \frac{1}{2};$$

а после измерения система будет находиться в состоянии

$$\frac{(M_1 \otimes \mathbf{I}_2)|\varphi_1\rangle}{\sqrt{\langle\varphi_1|(M_1 \otimes \mathbf{I}_2)^*(M_1 \otimes \mathbf{I}_2)|\varphi_1\rangle}} = \frac{1}{\sqrt{2}}\begin{pmatrix}0\\0\\1\\1\end{pmatrix} = \frac{1}{\sqrt{2}}|10\rangle + \frac{1}{\sqrt{2}}|11\rangle =$$

$$= |1\rangle \otimes \left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right). \tag{4.1.15}$$

Из равенств (4.1.14) и (4.1.15) следует, что второй кубит не имеет определенного значения $|0\rangle$ или $|1\rangle$, точнее, находится соответственно в состояниях

$$-\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \text{ и } \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle,$$

являющихся суперпозициями состояний $|0\rangle$ и $|1\rangle$.

Аналогично обстоит дело и с остальными состояниями $|\varphi_2\rangle$, $|\varphi_3\rangle$ и $|\varphi_4\rangle$, а также и при другом порядке измерения кубитов запутанной квантовой системы, находящейся в одном из состояний $|\varphi_1\rangle$, $|\varphi_2\rangle$, $|\varphi_3\rangle$ и $|\varphi_4\rangle$: при измерении сперва состояния второго кубита, состояние первого кубита не имеет определенного значения $|0\rangle$ или $|1\rangle$, то есть находится в состоянии, являющемся суперпозицией состояний $|0\rangle$ и $|1\rangle$.

Однако, если перейти в пространствах состояний подсистем A и B двухкубитной квантовой системы AB к базисам Шмидта [50; 52; 87] $\{|\alpha_0\rangle, |\alpha_1\rangle\}$ и $\{|\beta_0\rangle, |\beta_1\rangle\}$ соответственно подсистем A и B для состояния $|\varphi_1\rangle$ квантовой системы AB, то получаем следующее разложение Шмидта для состояния

$$|\varphi_1\rangle = c_0|\alpha_0\rangle|\beta_0\rangle + c_1|\alpha_1\rangle|\beta_1\rangle.$$

Учитывая, что коэффициенты Шмидта c_0 и c_1 равны квадратным корням из собственных значений редуцированной матрицы плотности подсистемы A квантовой системы AB в состоянии $|\varphi_1\rangle$, из равенства (4.1.7) получаем $c_0 = c_1 = \dfrac{1}{\sqrt{2}}$, то есть

$$|\varphi_1\rangle = \frac{1}{\sqrt{2}}|\alpha_0\rangle|\beta_0\rangle + \frac{1}{\sqrt{2}}|\alpha_1\rangle|\beta_1\rangle.$$

Представим измерение первого кубита в двухкубитной квантовой системе AB двумя операторами измерения $P_0 \otimes \mathbf{I}_2$ и $P_1 \otimes \mathbf{I}_2$, где $P_0 = |\alpha_0\rangle\langle\alpha_0|$ и $P_1 = |\alpha_1\rangle\langle\alpha_1|$ – проекторы, $\mathbf{I}_2$ – тождественный оператор, действующий в пространстве $\mathbb{C}^2$. Получаем, что вероятность того, что в результате измерения первого кубита будет получено состояние $|\alpha_0\rangle$, равна

$$p(|\alpha_0\rangle) = \langle\varphi_1|(P_0 \otimes \mathbf{I}_2)^* (P_0 \otimes \mathbf{I}_2)|\varphi_1\rangle = \langle\varphi_1|(P_0 \otimes \mathbf{I}_2)|\varphi_1\rangle =$$
$$= \left\langle \varphi_1 \middle| \left(\frac{1}{\sqrt{2}}|\alpha_0\rangle \otimes |\beta_0\rangle \right) \right\rangle =$$
$$= \frac{1}{2}\Big\langle \big(\langle\alpha_0| \otimes \langle\beta_0|\big) \Big| \big(|\alpha_0\rangle \otimes |\beta_0\rangle\big) \Big\rangle + \frac{1}{2}\Big\langle \big(\langle\alpha_1| \otimes \langle\beta_1|\big) \Big| \big(|\alpha_0\rangle \otimes |\beta_0\rangle\big) \Big\rangle =$$
$$= \frac{1}{2} \cdot \langle\alpha_0|\alpha_0\rangle \cdot \langle\beta_0|\beta_0\rangle + \frac{1}{2} \cdot \langle\alpha_1|\alpha_0\rangle \cdot \langle\beta_1|\beta_0\rangle = \frac{1}{2} \cdot 1 \cdot 1 + \frac{1}{2} \cdot 0 \cdot 0 = \frac{1}{2};$$

а после измерения квантовая система AB будет находиться в состоянии

$$\frac{(P_0 \otimes \mathbf{I}_2)|\varphi_1\rangle}{\sqrt{\langle\varphi_1|(P_0 \otimes \mathbf{I}_2)^*(P_0 \otimes \mathbf{I}_2)|\varphi_1\rangle}} = \frac{1}{\sqrt{2}}|\alpha_0\rangle|\beta_0\rangle\sqrt{2} = |\alpha_0\rangle|\beta_0\rangle .$$

Аналогично, вероятность того, что в результате измерения первого кубита будет получено состояние $|\alpha_1\rangle$, равна

$$p(|\alpha_1\rangle) = \langle\varphi_1|(P_1 \otimes \mathbf{I}_2)^*(P_1 \otimes \mathbf{I}_2)|\varphi_1\rangle = \langle\varphi_1|(P_1 \otimes \mathbf{I}_2)|\varphi_1\rangle = \frac{1}{2};$$

а после измерения квантовая система AB будет находиться в состоянии

$$\frac{(P_1 \otimes \mathbf{I}_2)|\varphi_1\rangle}{\sqrt{\langle\varphi_1|(P_1 \otimes \mathbf{I}_2)^*(P_1 \otimes \mathbf{I}_2)|\varphi_1\rangle}} = |\alpha_1\rangle|\beta_1\rangle .$$

Таким образом, при соответствующих операторах измерения процедура измерения над первым кубитом двухкубитной квантовой системы AB приводит второй кубит к вполне определенному значению состояния, принадлежащему базису Шмидта $\{|\beta_0\rangle, |\beta_1\rangle\}$.

Аналогичная ситуация и в том случае, когда сперва измеряется второй кубит в составе двухкубитной квантовой системы AB с помощью операторов измерения $\mathbf{I}_2 \otimes Q_0$ и $\mathbf{I}_2 \otimes Q_1$, где $Q_0 = |\beta_0\rangle\langle\beta_0|$ и $Q_1 = |\beta_1\rangle\langle\beta_1|$, первый кубит имеет определенное значение, принадлежащее базису Шмидта $\{|\alpha_0\rangle, |\alpha_1\rangle\}$.

Обобщая приведенные выше примеры, можно сформулировать следующее утверждение.

Утверждение 4.1.16. Пусть двухкубитная квантовая система AB находится в состоянии $|\psi\rangle$ с мерой несепарабельности $E(|\psi\rangle) > 0$. Тогда для каждого из кубитов системы AB существует свое измерение в составе системы AB, такое, что как только один кубит будет подвергнут соответствующему ему измерению (результат которого будет случайным), то сразу же окажется, что другой кубит имеет вполне определенное значение состояния, принадлежащее базису Шмидта соответствующей однокубитной подсистемы A или B системы AB.

Доказательство. Из неравенства $E(|\psi\rangle) > 0$ следует, что $|\psi\rangle$ – несепарабельное состояние. Тогда число Шмидта состояния $|\psi\rangle$ равно 2 [40]. Следовательно, каждый из коэффициентов Шмидта c_0 и c_1 состояния $|\psi\rangle$ больше нуля [50]. Пусть $\{|\alpha_0\rangle, |\alpha_1\rangle\}$ и $\{|\beta_0\rangle, |\beta_1\rangle\}$ – базисы Шмидта соответственно подсистем A и B квантовой системы AB в состоянии $|\psi\rangle$. Тогда разложение Шмидта для состояния $|\psi\rangle$ имеет следующий вид:

$$|\psi\rangle = c_0 |\alpha_0\rangle|\beta_0\rangle + c_1 |\alpha_1\rangle|\beta_1\rangle.$$

Рассмотрим проекторы

$$P_0 = |\alpha_0\rangle\langle\alpha_0| \quad \text{и} \quad P_1 = |\alpha_1\rangle\langle\alpha_1|,$$

действующие в пространстве состояний подсистемы A квантовой системы AB, и проекторы

$$Q_0 = |\beta_0\rangle\langle\beta_0| \quad \text{и} \quad Q_1 = |\beta_1\rangle\langle\beta_1|,$$

действующие в пространстве состояний подсистемы B квантовой системы AB. Непосредственной проверкой путем проведения соответствующих вычислений можно убедиться, что операторы $P_0 \otimes \mathbf{I}_2$ и $P_1 \otimes \mathbf{I}_2$ составляют полную систему операторов измерения [50] в пространстве состояний квантовой системы AB, где $\mathbf{I}_2$ – тождественный оператор, действующий в пространстве $\mathbb{C}^2$. Измерению в случае одиночного кубита, представляющего подсистему A квантовой системы AB, осуществляемому двумя операторами измерения P_0 и P_1, соответствует измерение того же кубита в составе квантовой системы AB, осуществляемое двумя операторами измерения $P_0 \otimes \mathbf{I}_2$ и $P_1 \otimes \mathbf{I}_2$.

Аналогично, как и выше, путем проведения соответствующих вычислений можно убедиться, что операторы $\mathbf{I}_2 \otimes Q_0$ и $\mathbf{I}_2 \otimes Q_1$ составляют полную систему операторов измерения [50] в пространстве состояний квантовой системы AB. Измерению в случае одиночного кубита, представляющего подсистему B квантовой системы AB, осуществляемому двумя операторами измерения Q_0 и Q_1, соответствует измерение того же кубита в составе квантовой системы AB, осуществляемое двумя операторами измерения $\mathbf{I}_2 \otimes Q_0$ и $\mathbf{I}_2 \otimes Q_1$.

В случае измерения первого кубита в составе квантовой системы AB, осуществляемого двумя операторами измерения $P_0 \otimes \mathbf{I}_2$ и $P_1 \otimes \mathbf{I}_2$, получаем, что вероятность того, что в результате измерения первого кубита будет получено состояние $|\alpha_0\rangle$, равна

$$p(|\alpha_0\rangle) = \langle\psi|(P_0 \otimes \mathbf{I}_2)^* (P_0 \otimes \mathbf{I}_2)|\psi\rangle = \langle\psi|(P_0 \otimes \mathbf{I}_2)|\psi\rangle =$$
$$= \Big\langle\psi\Big|\big(c_0|\alpha_0\rangle \otimes |\beta_0\rangle\big)\Big\rangle =$$
$$= c_0^2 \Big\langle\big(\langle\alpha_0| \otimes \langle\beta_0|\big)\Big|\big(|\alpha_0\rangle \otimes |\beta_0\rangle\big)\Big\rangle + c_0 c_1 \Big\langle\big(\langle\alpha_1| \otimes \langle\beta_1|\big)\Big|\big(|\alpha_0\rangle \otimes |\beta_0\rangle\big)\Big\rangle =$$
$$= c_0^2 \cdot \langle\alpha_0|\alpha_0\rangle \cdot \langle\beta_0|\beta_0\rangle + c_0 c_1 \cdot \langle\alpha_1|\alpha_0\rangle \cdot \langle\beta_1|\beta_0\rangle =$$
$$= c_0^2 \cdot 1 \cdot 1 + c_0 c_1 \cdot 0 \cdot 0 = c_0^2 > 0; \tag{4.1.17}$$

а после измерения квантовая система AB будет находиться в состоянии

$$\frac{(P_0 \otimes \mathbf{I}_2)|\psi\rangle}{\sqrt{\langle\psi|(P_0 \otimes \mathbf{I}_2)^* (P_0 \otimes \mathbf{I}_2)|\psi\rangle}} = c_0|\alpha_0\rangle|\beta_0\rangle \frac{1}{|c_0|} = |\alpha_0\rangle|\beta_0\rangle \tag{4.1.18}$$

(последнее равенство справедливо, так как $c_0 > 0$).

Аналогично, вероятность того, что в результате измерения первого кубита будет получено состояние $|\alpha_1\rangle$, равна

$$p(|\alpha_1\rangle) = \langle\psi|(P_1 \otimes \mathbf{I}_2)^* (P_1 \otimes \mathbf{I}_2)|\psi\rangle = \langle\psi|(P_1 \otimes \mathbf{I}_2)|\psi\rangle = c_1^2 > 0\,; \tag{4.1.19}$$

а после измерения квантовая система AB будет находиться в состоянии

$$\frac{(P_1 \otimes \mathbf{I}_2)|\psi\rangle}{\sqrt{\langle\psi|(P_1 \otimes \mathbf{I}_2)^* (P_1 \otimes \mathbf{I}_2)|\psi\rangle}} = c_1|\alpha_1\rangle|\beta_1\rangle \frac{1}{|c_1|} = |\alpha_1\rangle|\beta_1\rangle \tag{4.1.20}$$

(последнее равенство справедливо, так как $c_1 > 0$).

Таким образом, при соответствующих операторах измерения $P_0 \otimes \mathbf{I}_2$ и $P_1 \otimes \mathbf{I}_2$ процедура измерения над первым кубитом двухкубитной квантовой системы AB приводит второй кубит к вполне определенному значению состояния, принадлежащему базису Шмидта $\{|\beta_0\rangle, |\beta_1\rangle\}$ подсистемы B квантовой системы AB.

Поступая точно также и в том случае, когда сперва измеряется второй кубит в составе двухкубитной квантовой системы AB с помощью операторов измерения $\mathbf{I}_2 \otimes Q_0$ и $\mathbf{I}_2 \otimes Q_1$, убеждаемся, что первый кубит имеет определенное значение состояния, принадлежащее базису Шмидта $\{|\alpha_0\rangle, |\alpha_1\rangle\}$ подсистемы A квантовой системы AB.

Утверждение доказано.

Если дополнительно к условиям утверждения 4.1.16 потребовать выполнение условия, что мера несепарабельности состояния $|\psi\rangle$ равна 1, то в этом случае для состояния $|\psi\rangle$ существует представление, в определенном смысле аналогичное представлениям состояний Белла. Сформулируем и докажем соответствующее утверждение.

Утверждение 4.1.21. Пусть двухкубитная квантовая система AB находится в несепарабельном состоянии $|\psi\rangle \in \mathbb{C}^4$ и пусть $E(|\psi\rangle) = 1$. Тогда

$$|\psi\rangle = \frac{|\alpha_0\rangle|\beta_0\rangle + |\alpha_1\rangle|\beta_1\rangle}{\sqrt{2}}, \qquad (4.1.22)$$

где $\{|\alpha_0\rangle, |\alpha_1\rangle\}$ и $\{|\beta_0\rangle, |\beta_1\rangle\}$ – базисы Шмидта соответственно подсистем A и B квантовой системы AB в состоянии $|\psi\rangle$.

Доказательство. Разложение Шмидта [56] для состояния $|\psi\rangle$ имеет следующий вид

$$|\psi\rangle = c_0|\alpha_0\rangle|\beta_0\rangle + c_1|\alpha_1\rangle|\beta_1\rangle, \qquad (4.1.23)$$

где c_0, c_1 – неотрицательные действительные числа, $c_0^2+c_1^2=1$, и действительные числа $\lambda_1=c_0^2$, $\lambda_2=c_1^2$ являются собственными значениями редуцированной матрицы плотности $\rho_{\text{A}}^{(\text{AB})}$ подсистемы A квантовой системы AB [50]. Тогда из цепочки равенств (4.1.8) следует, что

$$E\left(\left|\psi\right\rangle\right)=-c_0^2\log_2 c_0^2-c_1^2\log_2 c_1^2.$$

Отсюда, учитывая, что $c_1^2=1-c_0^2$ и $E\left(\left|\psi\right\rangle\right)=1$, получаем

$$-c_0^2\log_2 c_0^2-\left(1-c_0^2\right)\log_2\left(1-c_0^2\right)=1,$$

что влечет справедливость равенств: $c_0^2=\dfrac{1}{2}$ и $c_1^2=1-c_0^2=\dfrac{1}{2}$ [50]. Так как коэффициенты Шмидта c_0 и c_1 являются неотрицательными числами [50], то из предыдущего получаем $c_0=\dfrac{1}{\sqrt{2}}$ и $c_1=\dfrac{1}{\sqrt{2}}$.

Из последних равенств и равенства (4.1.23) вытекает справедливость равенства (4.1.22).

Утверждение доказано.

Замечание 4.1.24. Из последнего утверждения и цепочки равенств (4.1.8) следует, что любое состояние

$$\left|\psi\right\rangle=a\left|00\right\rangle+b\left|01\right\rangle+c\left|10\right\rangle+d\left|11\right\rangle,$$

где $a,\ b,\ c,\ d\in\mathbb{C}$, $|a|^2+|b|^2+|c|^2+|d|^2=1$, $\left|ad-bc\right|=\dfrac{1}{2}$,

подобно состояниям Белла в том смысле, что для каждого из кубитов двухкубитной квантовой системы AB в состоянии $\left|\psi\right\rangle$ существует свое измерение в составе системы AB, такое, что как только один кубит будет подвергнут соответствующему ему измерению (результат которого с вероятностью 1/2 будет равен одному из двух возможных состояний), то сразу же окажется, что другой кубит имеет вполне определенное значение состояния из соответствующего базиса, даже если во время измерения два кубита удалены друг от друга на произвольно большое расстояние.

Таким образом, «необычные сверхвозможности» передачи квантовой информации не являются свойством только состояний Белла. Это свойство присуще всем состояниям двухкубитной квантовой системы с мерой несепарабельности, отличной от нуля. А для квантовых состояний с мерой несепарабельности, равной 1, проявление данного свойства аналогично тому, что характерно состояниям Белла. Такими состояниями, например, являются двухкубитные квантовые состояния Клюева, заданные равенствами (4.1.10) – (4.1.13).

Учитывая важность состояний Клюева (имеющих, как было показано выше, максимальную меру несепарабельности) для различных приложений в криптографии и связи, параграф 4.1 завершим примером, в котором двухкубитные квантовые состояния Клюева представлены соответствующими разложениями Шмидта [50].

Пример 4.1.25. Если квантовая система AB, состоящая из двух кубитов A и B, находится в состоянии Клюева $|\varphi_1\rangle$, определенном равенством (4.1.10), то есть

$$|\varphi_1\rangle = -\frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle,$$

то справедливо равенство

$$|\varphi_1\rangle = \frac{1}{\sqrt{2}}|0\rangle\left(\frac{-|0\rangle + |1\rangle}{\sqrt{2}}\right) + \frac{1}{\sqrt{2}}|1\rangle\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right), \tag{4.1.26}$$

правая часть которого является разложением Шмидта для состояния $|\varphi_1\rangle$. При этом коэффициенты Шмидта равны

$$c_0 = \frac{1}{\sqrt{2}} \text{ и } c_1 = \frac{1}{\sqrt{2}}$$

и, следовательно, число Шмидта равно 2;

базис

$$\{|\alpha_0\rangle = |0\rangle,\ |\alpha_1\rangle = |1\rangle\}$$

является базисом Шмидта для однокубитной квантовой системы A;
базис

$$\left\{|\beta_0\rangle = \frac{-|0\rangle + |1\rangle}{\sqrt{2}},\ |\beta_1\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}\right\}$$

является базисом Шмидта для однокубитной квантовой системы B.

Если квантовая система AB, состоящая из двух кубитов A и B, находится в состоянии Клюева $|\varphi_2\rangle$, определенном равенством (4.1.11), то есть

$$|\varphi_2\rangle = \frac{1}{2}|00\rangle - \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle,$$

то справедливо равенство

$$|\varphi_2\rangle = \frac{1}{\sqrt{2}}|0\rangle\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) + \frac{1}{\sqrt{2}}|1\rangle\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right), \tag{4.1.27}$$

правая часть которого является разложением Шмидта для состояния $|\varphi_2\rangle$. При этом коэффициенты Шмидта равны

$$c_0 = \frac{1}{\sqrt{2}} \text{ и } c_1 = \frac{1}{\sqrt{2}}$$

и, следовательно, число Шмидта равно 2;
базис

$$\{|\alpha_0\rangle = |0\rangle,\ |\alpha_1\rangle = |1\rangle\}$$

является базисом Шмидта для однокубитной квантовой системы A;
базис

$$\left\{|\beta_0\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}},\ |\beta_1\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}\right\}$$

является базисом Шмидта для однокубитной квантовой системы B.

Если квантовая система AB, состоящая из двух кубитов A и B, находится в состоянии Клюева $|\varphi_3\rangle$, определенном равенством (4.1.12), то есть

$$|\varphi_3\rangle = \frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle - \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle,$$

то справедливо равенство

$$|\varphi_3\rangle = \frac{1}{\sqrt{2}}|0\rangle\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right) + \frac{1}{\sqrt{2}}|1\rangle\left(\frac{-|0\rangle+|1\rangle}{\sqrt{2}}\right), \tag{4.1.28}$$

правая часть которого является разложением Шмидта для состояния $|\varphi_3\rangle$. При этом коэффициенты Шмидта равны

$$c_0 = \frac{1}{\sqrt{2}} \text{ и } c_1 = \frac{1}{\sqrt{2}}$$

и, следовательно, число Шмидта равно 2;
базис

$$\{|\alpha_0\rangle = |0\rangle,\ |\alpha_1\rangle = |1\rangle\}$$

является базисом Шмидта для однокубитной квантовой системы A;
базис

$$\left\{|\beta_0\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}},\ |\beta_1\rangle = \frac{-|0\rangle+|1\rangle}{\sqrt{2}}\right\}$$

является базисом Шмидта для однокубитной квантовой системы B.

Если квантовая система AB, состоящая из двух кубитов A и B, находится в состоянии Клюева $|\varphi_4\rangle$, определенном равенством (4.1.13), то есть

$$|\varphi_4\rangle = \frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle - \frac{1}{2}|11\rangle,$$

то справедливо равенство

$$|\varphi_4\rangle = \frac{1}{\sqrt{2}}|0\rangle\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right) + \frac{1}{\sqrt{2}}|1\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right), \tag{4.1.29}$$

правая часть которого является разложением Шмидта для состояния $|\varphi_4\rangle$. При этом коэффициенты Шмидта равны

$$c_0 = \frac{1}{\sqrt{2}} \text{ и } c_1 = \frac{1}{\sqrt{2}}$$

и, следовательно, число Шмидта равно 2;
базис

$$\{|\alpha_0\rangle = |0\rangle,\ |\alpha_1\rangle = |1\rangle\}$$

является базисом Шмидта для однокубитной квантовой системы A;
базис

$$\left\{|\beta_0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}},\ |\beta_1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}\right\}$$

является базисом Шмидта для однокубитной квантовой системы B.

§ 4.2. Состояния с максимальной мерой несепарабельности двухкубитных квантовых систем

Пусть $\{|\alpha_0\rangle, |\alpha_1\rangle\}$ и $\{|\beta_0\rangle, |\beta_1\rangle\}$ – два произвольных ортонормированных базиса пространства $\mathbb{C}^2$. Положим

$$P_0 = |\alpha_0\rangle\langle\alpha_0|,\ P_1 = |\alpha_1\rangle\langle\alpha_1|;\ Q_0 = |\beta_0\rangle\langle\beta_0|,\ Q_1 = |\beta_1\rangle\langle\beta_1|; \quad (4.2.1)$$

$$|\omega_1\rangle = \frac{1}{\sqrt{2}}\varepsilon|\alpha_0\rangle|\beta_0\rangle + \frac{1}{\sqrt{2}}\delta|\alpha_1\rangle|\beta_1\rangle,$$

$$|\omega_2\rangle = \frac{1}{\sqrt{2}}\varepsilon|\alpha_0\rangle|\beta_1\rangle + \frac{1}{\sqrt{2}}\delta|\alpha_1\rangle|\beta_0\rangle, \quad (4.2.2)$$

где ε и δ – произвольные комплексные числа, по модулю равные единице; через Ω обозначим множество векторов вида $|\omega_1\rangle$ и $|\omega_2\rangle$, когда числа ε и δ пробегают множество всех комплексных чисел, по модулю равных единице, то есть

$$\Omega = \left\{ \left| \omega_1 \right\rangle, \left| \omega_2 \right\rangle \;\middle|\; \varepsilon,\ \delta \in \mathbb{C},\ \left| \varepsilon \right| = 1,\ \left| \delta \right| = 1 \right\}. \qquad (4.2.3)$$

Имеет место следующее утверждение [2].

Утверждение 4.2.4. Множество векторов Ω совпадает с множеством всех состояний двухкубитной квантовой системы AB с максимальной мерой несепарабельности, обладающих тем свойством, что:

- в случае измерения первого кубита в составе квантовой системы AB, осуществляемого двумя операторами измерения $P_0 \otimes \mathbf{I}_2$ и $P_1 \otimes \mathbf{I}_2$, второй кубит имеет вполне определенное значение состояния, принадлежащее базису $\left\{ \left| \beta_0 \right\rangle, \left| \beta_1 \right\rangle \right\}$ пространства $\mathbb{C}^2$;

- в случае измерения второго кубита в составе квантовой системы AB, осуществляемого двумя операторами измерения $\mathbf{I}_2 \otimes Q_0$ и $\mathbf{I}_2 \otimes Q_1$, первый кубит имеет вполне определенное значение состояния, принадлежащее базису $\left\{ \left| \alpha_0 \right\rangle, \left| \alpha_1 \right\rangle \right\}$ пространства $\mathbb{C}^2$.

Доказательство. Пусть $\left| \omega \right\rangle$ – состояние двухкубитной квантовой системы AB с максимальной мерой несепарабельности, обладающее тем свойством, что:

- в случае измерения первого кубита в составе квантовой системы AB, осуществляемого двумя операторами измерения $P_0 \otimes \mathbf{I}_2$ и $P_1 \otimes \mathbf{I}_2$, второй кубит имеет вполне определенное значение состояния, принадлежащее базису $\left\{ \left| \beta_0 \right\rangle, \left| \beta_1 \right\rangle \right\}$ пространства $\mathbb{C}^2$;

- в случае измерения второго кубита в составе квантовой системы AB, осуществляемого двумя операторами измерения $\mathbf{I}_2 \otimes Q_0$ и $\mathbf{I}_2 \otimes Q_1$, первый кубит имеет определенное значение состояния, принадлежащее базису $\left\{ \left| \alpha_0 \right\rangle, \left| \alpha_1 \right\rangle \right\}$ пространства $\mathbb{C}^2$.

Покажем, что состояние $\left| \omega \right\rangle$ принадлежит множеству Ω.

В базисе

$$\{|\alpha_0\rangle|\beta_0\rangle,\ |\alpha_0\rangle|\beta_1\rangle,\ |\alpha_1\rangle|\beta_0\rangle,\ |\alpha_1\rangle|\beta_1\rangle\}$$

пространства $\mathbb{C}^4$ состояние $|\omega\rangle$ представляется следующим разложением:

$$|\omega\rangle = a|\alpha_0\rangle|\beta_0\rangle + b|\alpha_0\rangle|\beta_1\rangle + c|\alpha_1\rangle|\beta_0\rangle + d|\alpha_1\rangle|\beta_1\rangle,$$

где

$$a,\ b,\ c,\ d \in \mathbb{C},$$

$$|a|^2 + |b|^2 + |c|^2 + |d|^2 = 1,$$

$$|a|^2 + |b|^2 \neq 0,\ |a|^2 + |c|^2 \neq 0,\ |b|^2 + |d|^2 \neq 0,\ |c|^2 + |d|^2 \neq 0.$$

Справедливость последних четырех неравенств вытекает из несепарабельности состояния $|\omega\rangle$.

В случае измерения первого кубита в составе квантовой системы AB, осуществляемого двумя операторами измерения $P_0 \otimes \mathbf{I}_2$ и $P_1 \otimes \mathbf{I}_2$, получаем, что после измерения квантовая система AB будет находиться либо в состоянии

$$\frac{(P_0 \otimes \mathbf{I}_2)|\omega\rangle}{\sqrt{\langle\omega|(P_0 \otimes \mathbf{I}_2)^*(P_0 \otimes \mathbf{I}_2)|\omega\rangle}} =$$

$$= \frac{1}{\sqrt{|a|^2 + |b|^2}} a|\alpha_0\rangle|\beta_0\rangle + \frac{1}{\sqrt{|a|^2 + |b|^2}} b|\alpha_0\rangle|\beta_1\rangle =$$

$$= |\alpha_0\rangle \otimes \left(\frac{a}{\sqrt{|a|^2 + |b|^2}} |\beta_0\rangle + \frac{b}{\sqrt{|a|^2 + |b|^2}} |\beta_1\rangle \right), \qquad (4.2.5)$$

либо в состоянии

$$\frac{(P_1 \otimes \mathbf{I}_2)|\omega\rangle}{\sqrt{\langle\omega|(P_1 \otimes \mathbf{I}_2)^*(P_1 \otimes \mathbf{I}_2)|\omega\rangle}} =$$

$$= \frac{1}{\sqrt{|c|^2 + |d|^2}} c|\alpha_1\rangle|\beta_0\rangle + \frac{1}{\sqrt{|c|^2 + |d|^2}} d|\alpha_1\rangle|\beta_1\rangle =$$

$$= |\alpha_1\rangle \otimes \left(\frac{c}{\sqrt{|c|^2 + |d|^2}} |\beta_0\rangle + \frac{d}{\sqrt{|c|^2 + |d|^2}} |\beta_1\rangle \right). \qquad (4.2.6)$$

В случае измерения второго кубита в составе квантовой системы AB, осуществляемого двумя операторами измерения $\mathbf{I}_2 \otimes Q_0$ и $\mathbf{I}_2 \otimes Q_1$, получаем, что после измерения квантовая система AB будет находиться либо в состоянии

$$\frac{(\mathbf{I}_2 \otimes Q_0)|\omega\rangle}{\sqrt{\langle\omega|(\mathbf{I}_2 \otimes Q_0)^*(\mathbf{I}_2 \otimes Q_0)|\omega\rangle}} =$$
$$= \frac{1}{\sqrt{|a|^2+|c|^2}} a|\alpha_0\rangle|\beta_0\rangle + \frac{1}{\sqrt{|a|^2+|c|^2}} c|\alpha_1\rangle|\beta_0\rangle =$$
$$= \left(\frac{a}{\sqrt{|a|^2+|c|^2}}|\alpha_0\rangle + \frac{c}{\sqrt{|a|^2+|c|^2}}|\alpha_1\rangle\right) \otimes |\beta_0\rangle, \tag{4.2.7}$$

либо в состоянии

$$\frac{(\mathbf{I}_2 \otimes Q_1)|\omega\rangle}{\sqrt{\langle\omega|(\mathbf{I}_2 \otimes Q_1)^*(\mathbf{I}_2 \otimes Q_1)|\omega\rangle}} =$$
$$= \frac{1}{\sqrt{|b|^2+|d|^2}} b|\alpha_0\rangle|\beta_1\rangle + \frac{1}{\sqrt{|b|^2+|d|^2}} d|\alpha_1\rangle|\beta_1\rangle =$$
$$= \left(\frac{b}{\sqrt{|b|^2+|d|^2}}|\alpha_0\rangle + \frac{d}{\sqrt{|b|^2+|d|^2}}|\alpha_1\rangle\right) \otimes |\beta_1\rangle. \tag{4.2.8}$$

Из (4.2.5) – (4.2.8), несепарабельности состояния $|\omega\rangle$ и выполнения условия, что если один из кубитов в составе квантовой системы AB будет подвергнут измерению, осуществляемому вышеописанными операторами измерения, то другой кубит в составе той же квантовой системы AB имеет вполне определенное значение состояния из соответствующего базиса пространства $\mathbb{C}^2$, следует, что: либо

$$b = c = 0,\ |a|^2 + |d|^2 = 1,\ a \neq 0, d \neq 0, \tag{4.2.9}$$

либо

$$a = d = 0,\ |b|^2 + |c|^2 = 1,\ b \neq 0, c \neq 0. \tag{4.2.10}$$

Далее рассмотрим по отдельности каждый из случаев (4.2.9) и (4.2.10).

Сперва рассмотрим случай (4.2.9). В этом случае из равенства (4.1.5) для редуцированной матрицы плотности $\rho_{\mathrm{A}}^{(\mathrm{AB})}$ подсистемы A квантовой системы AB справедливо равенство

$$\rho_{\mathrm{A}}^{(\mathrm{AB})} = \begin{pmatrix} |a|^2 & 0 \\ 0 & |d|^2 \end{pmatrix}. \tag{4.2.11}$$

С другой стороны, в силу того, что состояние $|\omega\rangle$ двухкубитной квантовой системы AB является состоянием с максимальной мерой несепарабельности, в соответствии с результатами, представленными в [41], справедливо равенство

$$\rho_{\mathrm{A}}^{(\mathrm{AB})} = \frac{1}{2}\mathbf{I}_2, \tag{4.2.12}$$

где $\mathbf{I}_2$ – единичная матрица размера 2×2.

Из равенств (4.2.11) и (4.2.12) вытекает справедливость равенств

$$|a|^2 = \frac{1}{2},\ |d|^2 = \frac{1}{2}. \tag{4.2.13}$$

В свою очередь, равенства (4.2.13) равносильны равенствам:

$$a = \frac{1}{\sqrt{2}}\varepsilon,\ d = \frac{1}{\sqrt{2}}\delta, \tag{4.2.14}$$

где ε и δ – произвольные комплексные числа, по модулю равные единице.

Собирая вместе равенства (4.2.9) и (4.2.14), для состояния $|\omega\rangle$ получаем следующее представление:

$$|\omega\rangle = \frac{1}{\sqrt{2}}\varepsilon|\alpha_0\rangle|\beta_0\rangle + \frac{1}{\sqrt{2}}\delta|\alpha_1\rangle|\beta_1\rangle,$$

что соответствует первому из равенств (4.2.3). Следовательно, $|\omega\rangle \in \Omega$.

Теперь рассмотрим случай (4.2.10). В этом случае из равенства (4.1.5) для редуцированной матрицы плотности $\rho_{\mathrm{A}}^{(\mathrm{AB})}$ подсистемы A квантовой системы AB справедливо равенство

$$\rho_{\mathrm{A}}^{(\mathrm{AB})} = \begin{pmatrix} |b|^2 & 0 \\ 0 & |c|^2 \end{pmatrix}. \tag{4.2.15}$$

Как и выше, в силу того, что состояние $|\omega\rangle$ двухкубитной квантовой системы AB является состоянием с максимальной мерой несепарабельности, в соответствии с результатами, представленными в [41], справедливо равенство (4.2.12).

Из равенств (4.2.12) и (4.2.15) вытекает справедливость равенств

$$|b|^2 = \frac{1}{2}, \;\; |c|^2 = \frac{1}{2}. \tag{4.2.16}$$

В свою очередь, равенства (4.2.16) равносильны равенствам:

$$b = \frac{1}{\sqrt{2}}\varepsilon, \;\; c = \frac{1}{\sqrt{2}}\delta, \tag{4.2.17}$$

где ε и δ – произвольные комплексные числа, по модулю равные единице.

Собирая вместе равенства (4.2.10) и (4.2.17), для состояния $|\omega\rangle$ получаем следующее представление:

$$|\omega\rangle = \frac{1}{\sqrt{2}}\varepsilon|\alpha_0\rangle|\beta_1\rangle + \frac{1}{\sqrt{2}}\delta|\alpha_1\rangle|\beta_0\rangle,$$

что соответствует второму из равенств (4.2.2). Следовательно, и в этом случае также $|\omega\rangle \in \Omega$. И, таким образом, утверждение 4.2.4 в одну сторону доказано.

Теперь покажем, что любое состояние $|\omega\rangle$, принадлежащее Ω, может быть состоянием двухкубитной квантовой системы AB с максимальной мерой несепарабельности, обладающим тем свойством, что:

- в случае измерения первого кубита в составе квантовой системы AB, осуществляемого двумя операторами измерения $P_0 \otimes \mathbf{I}_2$ и $P_1 \otimes \mathbf{I}_2$, второй кубит имеет вполне определенное значение состояния, принадлежащее базису $\{|\beta_0\rangle, |\beta_1\rangle\}$ пространства $\mathbb{C}^2$;

- в случае измерения второго кубита в составе квантовой системы AB, осуществляемого двумя операторами измерения $\mathbf{I}_2 \otimes Q_0$ и $\mathbf{I}_2 \otimes Q_1$, первый кубит имеет вполне определенное значение состояния, принадлежащее базису $\{|\alpha_0\rangle, |\alpha_1\rangle\}$ пространства $\mathbb{C}^2$.

Вычислим сперва меру несепарабельности $E(|\omega\rangle)$ состояния $|\omega\rangle$. Возможны случаи: $|\omega\rangle$ имеет представление вида $|\omega_1\rangle$ или вида $|\omega_2\rangle$ из (4.2.2).

Рассмотрим сначала случай, когда $|\omega\rangle$ имеет представление вида $|\omega_1\rangle$. В этом случае

$$|\omega\rangle = \frac{1}{\sqrt{2}}\varepsilon|\alpha_0\rangle|\beta_0\rangle + \frac{1}{\sqrt{2}}\delta|\alpha_1\rangle|\beta_1\rangle.$$

Тогда из равенства (4.1.5) следует, что для редуцированной матрицы плотности $\rho_{\mathrm{A}}^{(\mathrm{AB})}$ подсистемы A квантовой системы AB справедлива цепочка равенств

$$\rho_{\mathrm{A}}^{(\mathrm{AB})} = \begin{pmatrix} \left|\frac{1}{\sqrt{2}}\varepsilon\right|^2 & 0 \\ 0 & \left|\frac{1}{\sqrt{2}}\delta\right|^2 \end{pmatrix} = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix}. \tag{4.2.18}$$

Отсюда и из (4.1.16) следует, что для меры несепарабельности $E(|\omega\rangle)$ состояния $|\omega\rangle$ справедлива следующая цепочка равенств:

$$E(|\omega\rangle) = S\left(\rho_{\mathrm{A}}^{(\mathrm{AB})}\right) = -\mathrm{tr}\left(\rho_{\mathrm{A}}^{(\mathrm{AB})} \log_2 \rho_{\mathrm{A}}^{(\mathrm{AB})}\right) =$$

$$= -\mathrm{tr}\left(\begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix}\begin{pmatrix} \log_2 \frac{1}{2} & 0 \\ 0 & \log_2 \frac{1}{2} \end{pmatrix}\right) = -\mathrm{tr}\begin{pmatrix} \frac{1}{2}\log_2 \frac{1}{2} & 0 \\ 0 & \frac{1}{2}\log_2 \frac{1}{2} \end{pmatrix} =$$

$$-\frac{1}{2}\log_2 \frac{1}{2} - \frac{1}{2}\log_2 \frac{1}{2} = 1, \tag{4.2.19}$$

то есть состояние $|\omega\rangle$ является состоянием с максимальной мерой несепарабельности.

Далее, в случае измерения первого кубита в составе квантовой системы AB, осуществляемого двумя операторами измерения $P_0 \otimes \mathbf{I}_2$ и $P_1 \otimes \mathbf{I}_2$, получаем, что после измерения квантовая система AB будет находиться либо в состоянии

$$\frac{(P_0 \otimes \mathbf{I}_2)|\omega\rangle}{\sqrt{\langle\omega|(P_0 \otimes \mathbf{I}_2)^* (P_0 \otimes \mathbf{I}_2)|\omega\rangle}} =$$

$$= \frac{1}{\sqrt{\left|\frac{1}{\sqrt{2}}\varepsilon\right|^2 + |0|^2}} \cdot \frac{1}{\sqrt{2}}\varepsilon|\alpha_0\rangle|\beta_0\rangle = \varepsilon|\alpha_0\rangle|\beta_0\rangle, \tag{4.2.20}$$

либо в состоянии

$$\frac{(P_1 \otimes \mathbf{I}_2)|\omega\rangle}{\sqrt{\langle\omega|(P_1 \otimes \mathbf{I}_2)^* (P_1 \otimes \mathbf{I}_2)|\omega\rangle}} =$$

$$= \frac{1}{\sqrt{|0|^2 + \left|\frac{1}{\sqrt{2}}\delta\right|^2}} \cdot \frac{1}{\sqrt{2}}\delta|\alpha_1\rangle|\beta_1\rangle = \delta|\alpha_1\rangle|\beta_1\rangle. \tag{4.2.21}$$

В случае же измерения второго кубита в составе квантовой системы AB, осуществляемого двумя операторами измерения $\mathbf{I}_2 \otimes Q_0$ и $\mathbf{I}_2 \otimes Q_1$, получаем, что после измерения квантовая система AB будет находиться либо в состоянии

$$\frac{\left(\mathbf{I}_2 \otimes Q_0\right)|\omega\rangle}{\sqrt{\langle\omega|\left(\mathbf{I}_2 \otimes Q_0\right)^*\left(\mathbf{I}_2 \otimes Q_0\right)|\omega\rangle}} =$$

$$= \frac{1}{\sqrt{\left|\frac{1}{\sqrt{2}}\varepsilon\right|^2 + |0|^2}} \cdot \frac{1}{\sqrt{2}}\varepsilon|\alpha_0\rangle|\beta_0\rangle = \varepsilon|\alpha_0\rangle|\beta_0\rangle, \qquad (4.2.22)$$

либо в состоянии

$$\frac{\left(\mathbf{I}_2 \otimes Q_1\right)|\omega\rangle}{\sqrt{\langle\omega|\left(\mathbf{I}_2 \otimes Q_1\right)^*\left(\mathbf{I}_2 \otimes Q_1\right)|\omega\rangle}} =$$

$$= \frac{1}{\sqrt{|0|^2 + \left|\frac{1}{\sqrt{2}}\delta\right|^2}} \cdot \frac{1}{\sqrt{2}}\delta|\alpha_1\rangle|\beta_1\rangle = \delta|\alpha_1\rangle|\beta_1\rangle. \qquad (4.2.23)$$

Из равенств (4.2.20) – (4.2.23) следует, что состояние $|\omega\rangle$ обладает требуемым свойством, а именно:

- в случае измерения первого кубита в составе квантовой системы AB, осуществляемого двумя операторами измерения $P_0 \otimes \mathbf{I}_2$ и $P_1 \otimes \mathbf{I}_2$, второй кубит имеет вполне определенное значение состояния, принадлежащее базису $\{|\beta_0\rangle, |\beta_1\rangle\}$ пространства $\mathbb{C}^2$;
- в случае измерения второго кубита в составе квантовой системы AB, осуществляемого двумя операторами измерения $\mathbf{I}_2 \otimes Q_0$ и $\mathbf{I}_2 \otimes Q_1$, первый кубит имеет вполне определенное значение состояния, принадлежащее базису $\{|\alpha_0\rangle, |\alpha_1\rangle\}$ пространства $\mathbb{C}^2$.

Рассмотрим теперь случай, когда $|\omega\rangle$ имеет представление вида $|\omega_2\rangle$ из (4.2.2). В этом случае

$$|\omega\rangle = \frac{1}{\sqrt{2}}\varepsilon|\alpha_0\rangle|\beta_1\rangle + \frac{1}{\sqrt{2}}\delta|\alpha_1\rangle|\beta_0\rangle.$$

Тогда из равенства (4.1.5) следует, что для редуцированной матрицы плотности $\rho_{\mathrm{A}}^{(\mathrm{AB})}$ подсистемы A квантовой системы AB справедлива цепочка равенств (4.2.18).

Из (4.2.18) и (4.1.6) следует, что для меры несепарабельности $E\left(|\omega\rangle\right)$ состояния $|\omega\rangle$ справедлива цепочка равенств (4.2.19), то есть и в этом случае состояние $|\omega\rangle$ является состоянием с максимальной мерой несепарабельности.

Далее, в случае измерения первого кубита в составе квантовой системы AB, осуществляемого двумя операторами измерения $P_0 \otimes \mathbf{I}_2$ и $P_1 \otimes \mathbf{I}_2$, получаем, что после измерения квантовая система AB будет находиться либо в состоянии

$$\frac{\left(P_0 \otimes \mathbf{I}_2\right)|\omega\rangle}{\sqrt{\langle\omega|\left(P_0 \otimes \mathbf{I}_2\right)^*\left(P_0 \otimes \mathbf{I}_2\right)|\omega\rangle}} =$$

$$= \frac{1}{\sqrt{|0|^2 + \left|\frac{1}{\sqrt{2}}\varepsilon\right|^2}} \cdot \frac{1}{\sqrt{2}}\varepsilon|\alpha_0\rangle|\beta_1\rangle = \varepsilon|\alpha_0\rangle|\beta_1\rangle, \tag{4.2.24}$$

либо в состоянии

$$\frac{\left(P_1 \otimes \mathbf{I}_2\right)|\omega\rangle}{\sqrt{\langle\omega|\left(P_1 \otimes \mathbf{I}_2\right)^*\left(P_1 \otimes \mathbf{I}_2\right)|\omega\rangle}} =$$

$$= \frac{1}{\sqrt{\left|\frac{1}{\sqrt{2}}\delta\right|^2 + |0|^2}} \cdot \frac{1}{\sqrt{2}}\delta|\alpha_1\rangle|\beta_0\rangle = \delta|\alpha_1\rangle|\beta_0\rangle. \tag{4.2.25}$$

В случае же измерения второго кубита в составе квантовой системы AB, осуществляемого двумя операторами измерения $\mathbf{I}_2 \otimes Q_0$ и $\mathbf{I}_2 \otimes Q_1$, получаем, что после измерения квантовая система AB будет находиться либо в состоянии

$$\frac{(\mathbf{I}_2 \otimes Q_0)|\omega\rangle}{\sqrt{\langle\omega|(\mathbf{I}_2 \otimes Q_0)^*(\mathbf{I}_2 \otimes Q_0)|\omega\rangle}} =$$

$$= \frac{1}{\sqrt{|0|^2 + \left|\frac{1}{\sqrt{2}}\delta\right|^2}} \cdot \frac{1}{\sqrt{2}}\delta|\alpha_1\rangle|\beta_0\rangle = \delta|\alpha_1\rangle|\beta_0\rangle, \qquad (4.2.26)$$

либо в состоянии

$$\frac{(\mathbf{I}_2 \otimes Q_1)|\omega\rangle}{\sqrt{\langle\omega|(\mathbf{I}_2 \otimes Q_1)^*(\mathbf{I}_2 \otimes Q_1)|\omega\rangle}} =$$

$$= \frac{1}{\sqrt{\left|\frac{1}{\sqrt{2}}\varepsilon\right|^2 + |0|^2}} \cdot \frac{1}{\sqrt{2}}\varepsilon|\alpha_0\rangle|\beta_1\rangle = \varepsilon|\alpha_0\rangle|\beta_1\rangle. \qquad (4.2.27)$$

Наконец, из равенств (4.2.24) – (4.2.27) также следует, что состояние $|\omega\rangle$ обладает требуемым свойством, а именно:

- в случае измерения первого кубита в составе квантовой системы AB, осуществляемого двумя операторами измерения $P_0 \otimes \mathbf{I}_2$ и $P_1 \otimes \mathbf{I}_2$, второй кубит имеет вполне определенное значение состояния, принадлежащее базису $\{|\beta_0\rangle, |\beta_1\rangle\}$ пространства $\mathbb{C}^2$;

- в случае измерения второго кубита в составе квантовой системы AB, осуществляемого двумя операторами измерения $\mathbf{I}_2 \otimes Q_0$ и $\mathbf{I}_2 \otimes Q_1$, первый кубит имеет вполне определенное значение состояния, принадлежащее базису $\{|\alpha_0\rangle, |\alpha_1\rangle\}$ пространства $\mathbb{C}^2$.

Утверждение 4.2.4 доказано полностью.

Замечание 4.2.28. Результат, представленный в утверждении 4.2.4, до возможного предела расширяет класс несепарабельных состояний, пригодных для приложений в области криптографии и защищенной связи в той же степени, что и состояния Белла. Для уяснения данного факта напомним (см. § 1.3), что выбор вычислительного базиса равносилен, в известном смысле, выбору устройства измерения. Так как после проведения измерения на выходе устройства в качестве результата может быть (с соответствующей вероятностью) любое из состояний вычислительного базиса, соответствующего этому устройству. Имея в виду данное обстоятельство, можно сказать, что утверждение 4.2.4 для двух произвольным образом выбранных устройств измерения указывает явные выражения всех возможных состояний двухкубитной квантовой системы, аналогичных по своему поведению в процессе измерения состояниям Белла, когда однокубитные подсистемы квантовой системы измеряются в базисе из векторов $|0\rangle$ и $|1\rangle$. Поэтому парные комплексы указанных измерительных устройств и соответствующих им состояний в смысле утверждения 4.2.4 наследуют те же положительные потенциальные возможности в плане криптографических приложений, что и состояния Белла и устройства измерения их составляющих в базисе из векторов $|0\rangle$ и $|1\rangle$. Это не только наращивает элементную базу для криптографических приложений, что само по себе является существенно положительным фактором, но и позволяет расширить круг задач, решаемых с использованием ресурса несепарабельных квантовых состояний.

Наконец, имеет смысл обратить внимание и на тот факт, что равенства $E(|\omega\rangle)=1$ и $C(|\omega\rangle)=1$ эквивалентны, где $C(|\omega\rangle)$ – **согласованность** (concurrence) состояния $|\omega\rangle$. Как было указано в параграфе 4.1, наряду с функцией *E*, непосредственно связанной с такой информационной характеристикой квантовой системы, как энтропия фон Неймана, функция *C* также используется в качестве меры несепарабельности квантовых состояний. Функции *E* и *C* в случае двухкубитных систем в смысле кандидатов для количественного описания ресурса несепарабельности можно считать равноправными. Однако для количественной характеристики ресурса несепарабельности двухсоставных квантовых систем, не обязательно двухкубитных, состоящих из более чем двух кубитов, используется функция *C*, для которой уже найдено удобное и общее выражение, позволяющее эффективно вычислять согласованность в двухсоставных системах [86].

Согласованности как количественной характеристике ресурса несепарабельности двухсоставных квантовых систем посвящен следующий параграф 4.3.

§ 4.3. Мера несепарабельности состояний двухсоставных квантовых систем

Более общая, чем рассмотренная в параграфе 4.1, количественная мера несепарабельности (под названием **согласованность**) двухкубитной квантовой системы AB, отражающая запутанность друг с другом двух ее составляющих однокубитных подсистем A и B, как для чистого, так и для смешанного состояния была введена в работах [80; 91] с использованием «спин-флип» преобразования:

$$C_{\mathrm{A}}(\rho) = C_{\mathrm{B}}(\rho) = \max\{\lambda_1 - \lambda_2 - \lambda_3 - \lambda_4,\ 0\},$$

где ρ – матрица плотности квантовой системы AB; λ_1, λ_2, λ_3, λ_4 – расположенные в порядке убывания квадратные корни из собственных значений матрицы

$$\rho T \rho^* T\ ;$$

ρ^* – матрица, получаемая из матрицы ρ заменой каждого элемента в ρ на комплексно сопряженный элемент;

$$T = \sigma_{\mathbf{Y}} \otimes \sigma_{\mathbf{Y}}$$

– «спин-флип» матрица, то есть матрица (оператор) переворота спинов; $\sigma_{\mathbf{Y}}$ – вентиль Паули **Y** (см. § 1.3).

Впоследствии было найдено [86] более удобное и общее выражение для вычисления согласованности уже в произвольной составной квантовой системе AB:

$$C_{\mathrm{A}}(\rho)=\sqrt{2\left(1-\operatorname{tr}\left(\left[\rho_{\mathrm{A}}(\rho)\right]^{2}\right)\right)}, \qquad (4.3.1)$$

отражающее меру несепарабельности подсистемы A (любой размерности) со всем ее окружением B (также любой размерности), когда исходная система AB находится в состоянии, которое может быть как чистым, так и смешанным. В (4.3.1) ρ – матрица плотности многосоставной квантовой системы, $\rho_{\mathrm{A}}(\rho)$ – редуцированная матрица плотности [50] подсистемы A, когда исходная система имеет матрицу плотности ρ. При этом справедливо двойное неравенство

$$0 \le C_{\mathrm{A}}(\rho) \le \sqrt{2 \cdot \frac{M-1}{M}}, \qquad (4.3.2)$$

где

$$M=\min\left(D_{\mathrm{A}},\, D_{\mathrm{B}}\right), \qquad (4.3.3)$$

D_{A} и D_{B} – размерности пространств состояний подсистем A и B соответственно.

Развитию этих достижений на случай цепочек из кубитов посвящены работы [84; 92].

Для дальнейшего представляет интерес применение формулы (4.3.1) к двухкубитным квантовым системам в произвольных состояниях и трехкубитным квантовым системам в определенных несепарабельных состояниях. Так как для любой подсистемы A двух- или трехкубитной квантовой системы AB либо A состоит из одного кубита, либо ее окружение B состоит из одного кубита, то справедливо равенство

$$\min\left(D_{\mathrm{A}},\, D_{\mathrm{B}}\right)=2,$$

что влечет справедливость неравенства

$$0 \le C_{\mathrm{A}}(\rho) \le 1.$$

В случае квантовой системы AB из двух кубитов A и B, находящейся в состоянии $|\psi\rangle$, является оправданным также понятие меры несепарабельности состояния $|\psi\rangle$, под которым в данном параграфе понимается величина

$$C_{\mathrm{A}}\left(|\psi\rangle\right)=\sqrt{2\left(1-\operatorname{tr}\left(\left[\rho_{\mathrm{A}}\left(|\psi\rangle\right)\right]^2\right)\right)}, \tag{4.3.4}$$

где $\rho_{\mathrm{A}}\left(|\psi\rangle\right)$ – редуцированная матрица плотности кубита A, когда двухкубитная квантовая система AB находится в состоянии $|\psi\rangle$. При этом редуцированную матрицу плотности $\rho_{\mathrm{A}}\left(|\psi\rangle\right)$ подсистемы из кубита A обозначают также $\rho_{\mathrm{A}}^{(\mathrm{AB})}\left(|\psi\rangle\right)$.

Напомним, что в вычислительном базисе из векторов $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$ произвольное двухкубитное состояние $|\psi\rangle$ квантовой системы AB можно представить в следующем общем виде:

$$|\psi\rangle=a|00\rangle+b|01\rangle+c|10\rangle+d|11\rangle, \tag{4.3.5}$$

где $a,\ b,\ c,\ d\in\mathbb{C}$,

$$|a|^2+|b|^2+|c|^2+|d|^2=1. \tag{4.3.6}$$

Представим меру несепарабельности $C_{\mathrm{A}}\left(|\psi\rangle\right)$, заданную равенством (4.3.4), подсистемы из кубита A с подсистемой из кубита B, как функцию от коэффициентов a, b, c, d разложения (4.3.5) по вычислительному базису $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$. Для этого выпишем сперва редуцированную матрицу плотности $\rho_{\mathrm{A}}^{(\mathrm{AB})}\left(|\psi\rangle\right)$ подсистемы A квантовой системы AB, когда последняя находится в состоянии $|\psi\rangle$. Как следует из (2.2.22), для редуцированной матрицы плотности $\rho_{\mathrm{A}}^{(\mathrm{AB})}\left(|\psi\rangle\right)$ подсистемы A квантовой системы AB справедливо равенство

$$\rho_{\mathrm{A}}^{(\mathrm{AB})}\left(|\psi\rangle\right)=\begin{pmatrix}|a|^2+|b|^2 & a\tilde{c}+b\tilde{d}\\ c\tilde{a}+d\tilde{b} & |c|^2+|d|^2\end{pmatrix}. \tag{4.3.7}$$

Из равенств (4.3.4), (4.3.5) и (4.3.7) следует, что для меры несепарабельности $C_{\mathrm{A}}\left(|\psi\rangle\right)$ справедлива следующая цепочка равенств:

$$C_{\mathrm{A}}\left(|\psi\rangle\right)=$$

$$=\sqrt{2\left(1-\left[\left(|a|^2+|b|^2\right)^2+\left(a\tilde{c}+b\tilde{d}\right)\left(c\tilde{a}+d\tilde{b}\right)+\left(c\tilde{a}+d\tilde{b}\right)\left(a\tilde{c}+b\tilde{d}\right)+\left(|c|^2+|d|^2\right)^2\right]\right)}=$$

$$=\sqrt{2\left(1-\left[\left(|a|^2+|b|^2+|c|^2+|d|^2\right)^2-2\left(|a|^2|d|^2+|b|^2|c|^2-a\tilde{b}\tilde{c}d-\tilde{a}bc\tilde{d}\right)\right]\right)}=$$

$$=\sqrt{4\left(|a|^2|d|^2+|b|^2|c|^2-a\tilde{b}\tilde{c}d-\tilde{a}bc\tilde{d}\right)}=2\sqrt{(ad-bc)\left(\tilde{a}\tilde{d}-\tilde{b}\tilde{c}\right)}=$$

$$=2\sqrt{|ad-bc|^2}=2|ad-bc|.$$

То есть мера несепарабельности $C_{\mathrm{A}}\left(|\psi\rangle\right)$ подсистемы из кубита A двухкубитной квантовой системы AB в состоянии $|\psi\rangle$ с подсистемой из кубита B задается равенством

$$C_{\mathrm{A}}\left(|\psi\rangle\right)=2|ad-bc|, \tag{4.3.8}$$

что совпадает с характеристикой C двухкубитной квантовой системы, введенной в параграфе 4.1 под названием **согласованность**.

Однако именно возможность применения для вычисления меры несепарабельности любой подсистемы многосоставной квантовой системы произвольной размерности с остальной частью этой квантовой системы является принципиальным отличием выражения (4.3.1) меры несепарабельности под названием **согласованность**, рассматриваемой в данном параграфе, от одноименной характеристики двухкубитной квантовой системы из параграфа 4.1.

Теперь перейдем к трехкубитным квантовым системам. Начнем с состояния

$$\left|\psi^{(3)}\right\rangle=\alpha|001\rangle+\beta|110\rangle;\ \ \alpha,\ \beta\in\mathbb{C},\ |\alpha|>|\beta|>0,\ |\alpha|^2+|\beta|^2=1$$

квантовой системы ABC, состоящей из трех кубитов A, B и C, и по нему вычислим в соответствии с [50] редуцированную матрицу плотности $\rho_{\mathrm{A}}\left(\left|\psi^{(3)}\right\rangle\right)$ подсистемы, состоящей из кубита A:

$$\rho_{\text{A}}\left(\left|\psi^{(3)}\right\rangle\right)=\text{tr}_{\text{BC}}\left(\left|\psi^{(3)}\right\rangle\left\langle\psi^{(3)}\right|\right)=$$
$$=\text{tr}_{\text{BC}}\left(\left(\alpha|001\rangle+\beta|110\rangle\right)\left(\tilde{\alpha}\langle 001|+\tilde{\beta}\langle 110|\right)\right)=$$
$$=\text{tr}_{\text{BC}}\left(|\alpha|^2|001\rangle\langle 001|+\alpha\tilde{\beta}|001\rangle\langle 110|+\beta\tilde{\alpha}|110\rangle\langle 001|+|\beta|^2|110\rangle\langle 110|\right)=$$
$$=|\alpha|^2|0\rangle\langle 0|\,\text{tr}\left(|01\rangle\langle 01|\right)+\alpha\tilde{\beta}|0\rangle\langle 1|\,\text{tr}\left(|01\rangle\langle 10|\right)+$$
$$+\beta\tilde{\alpha}|1\rangle\langle 0|\,\text{tr}\left(|10\rangle\langle 01|\right)+|\beta|^2|1\rangle\langle 1|\,\text{tr}\left(|10\rangle\langle 10|\right)=$$
$$=\begin{pmatrix}|\alpha|^2 & 0\\ 0 & |\beta|^2\end{pmatrix}.$$

Подставив полученное выражение для редуцированной матрицы плотности в выражение для меры $C_{\text{A}}\left(\left|\psi^{(3)}\right\rangle\right)$ несепарабельности кубита A с двухкубитной подсистемой BC трехкубитной квантовой системы ABC в состоянии $\left|\psi^{(3)}\right\rangle$, получим

$$C_{\text{A}}\left(\left|\psi^{(3)}\right\rangle\right)=\sqrt{2\left(1-\text{tr}\left(\left[\rho_{\text{A}}\left(\left|\psi^{(3)}\right\rangle\right)\right]^2\right)\right)}=$$
$$=\sqrt{2\left(1-\left(|\alpha|^4+|\beta|^4\right)\right)}=\sqrt{4|\alpha|^2|\beta|^2}=2|\alpha||\beta|. \tag{4.3.9}$$

Аналогично получаем меры несепарабельности

$$C_{\text{B}}\left(\left|\psi^{(3)}\right\rangle\right)=2|\alpha||\beta| \tag{4.3.10}$$

и

$$C_{\text{C}}\left(\left|\psi^{(3)}\right\rangle\right)=2|\alpha||\beta| \tag{4.3.11}$$

каждого из кубитов B и C с соответствующей остальной частью квантовой системы ABC в состоянии $\left|\psi^{(3)}\right\rangle$.

Наконец, в качестве примеров вычислим, применив равенство (4.3.8), меру несепарабельности кубита B с кубитом C в двухкубитной квантовой системе BC, когда она находится в одном из состояний

$$\left|\psi_1^{(2)}\right\rangle = \frac{\alpha^2}{\sqrt{|\alpha|^4+|\beta|^4}}|01\rangle + \frac{\beta^2}{\sqrt{|\alpha|^4+|\beta|^4}}|10\rangle,\ \left|\psi_2^{(2)}\right\rangle = \frac{|01\rangle+|10\rangle}{\sqrt{2}},$$

$$\left|\psi_3^{(2)}\right\rangle = \frac{\alpha^2}{\sqrt{|\alpha|^4+|\beta|^4}}|01\rangle - \frac{\beta^2}{\sqrt{|\alpha|^4+|\beta|^4}}|10\rangle,\ \left|\psi_4^{(2)}\right\rangle = \frac{|01\rangle-|10\rangle}{\sqrt{2}},$$

где $\alpha,\ \beta \in \mathbb{C}$, $|\alpha| > |\beta| > 0$, $|\alpha|^2 + |\beta|^2 = 1$:

$$C_{\mathrm{B}}\left(\left|\psi_1^{(2)}\right\rangle\right) = \frac{2|\alpha|^2|\beta|^2}{|\alpha|^4+|\beta|^4}, \tag{4.3.12}$$

$$C_{\mathrm{C}}\left(\left|\psi_1^{(2)}\right\rangle\right) = \frac{2|\alpha|^2|\beta|^2}{|\alpha|^4+|\beta|^4}, \tag{4.3.13}$$

$$C_{\mathrm{B}}\left(\left|\psi_2^{(2)}\right\rangle\right) = 1, \tag{4.3.14}$$

$$C_{\mathrm{C}}\left(\left|\psi_2^{(2)}\right\rangle\right) = 1, \tag{4.3.15}$$

$$C_{\mathrm{B}}\left(\left|\psi_3^{(2)}\right\rangle\right) = \frac{2|\alpha|^2|\beta|^2}{|\alpha|^4+|\beta|^4}, \tag{4.3.16}$$

$$C_{\mathrm{C}}\left(\left|\psi_3^{(2)}\right\rangle\right) = \frac{2|\alpha|^2|\beta|^2}{|\alpha|^4+|\beta|^4}, \tag{4.3.17}$$

$$C_{\mathrm{B}}\left(\left|\psi_4^{(2)}\right\rangle\right) = 1, \tag{4.3.18}$$

$$C_{\mathrm{C}}\left(\left|\psi_4^{(2)}\right\rangle\right) = 1. \tag{4.3.19}$$

§ 4.4. Мера несепарабельности состояний многокубитных квантовых систем

Одним из распространенных подходов к построению меры несепарабельности многокубитных квантовых систем является рассмотрение функций [43; 44] от мер несепарабельности двухсоставных систем, то есть от мер запутанности каждой подсистемы данной системы со всем ее окружением, представляющим собой ту часть всей системы, которая остается после исключения рассматриваемой подсистемы. На основе такого подхода построена, например, мера, представленная в работе [81]. По сути, в итоге получается, что эта мера является суммой мер несепарабельности (то есть согласованности) между каждым кубитом и остальными.

Но вместе с тем имеются работы, в которых представлены меры, построенные на иных, отличных от вышеуказанного, подходах. Обзор некоторых публикаций приведен в работе [62], посвященной решению задачи построения меры несепарабельности состояний многочастичных квантовых систем.

В целом, можно отметить, что универсальная мера несепарабельности состояний многокубитных квантовых систем, приемлемая как с теоретико-информационных, так и с физических позиций, ко времени написания данной книги не построена. Актуальность решения этой задачи не понижается, а, наоборот, повышается с течением времени, так как накапливаются как теоретические знания, так и экспериментальные результаты относительно ресурса несепарабельности состояний квантовых систем, требующие при своем анализе количественных характеристик.

В этом параграфе предлагается новое решение задачи построения меры несепарабельности многокубитных квантовых систем. В этом решении также используется указанный выше подход.

Пусть $\mathrm{A}_1\mathrm{A}_2\ldots\mathrm{A}_n$ – квантовая система, состоящая из $n > 1$ кубитов $\mathrm{A}_1, \mathrm{A}_2, \ldots, \mathrm{A}_n$; $\mathbb{S}_n$ – симметрическая группа подстановок [27] на множестве $\{1, 2, \ldots, n\}$; $|\psi\rangle$ – состояние n-кубитной квантовой системы $\mathrm{A}_1\mathrm{A}_2\ldots\mathrm{A}_n$, $|\psi\rangle \in \mathbb{C}^{2^n}$.

Рассмотрим подсистемы $\mathrm{A}(s,k)$ и $\mathrm{B}(s,n-k)$ квантовой системы $\mathrm{A}_{s(1)}\mathrm{A}_{s(2)}\ldots\mathrm{A}_{s(n)}$, состоящие соответственно из кубитов $\mathrm{A}_{s(1)}$, $\mathrm{A}_{s(2)}$, …, $\mathrm{A}_{s(k)}$ и $\mathrm{A}_{s(k+1)}$, $\mathrm{A}_{s(k+2)}$, …, $\mathrm{A}_{s(n)}$, то есть

$$\mathrm{A}(s,k) = \mathrm{A}_{s(1)}\mathrm{A}_{s(2)}\ldots\mathrm{A}_{s(k)} \qquad (4.4.1)$$

и

$$\mathrm{B}(s, n-k) = \mathrm{A}_{s(k+1)}\mathrm{A}_{s(k+2)}\ldots\mathrm{A}_{s(n)}, \tag{4.4.2}$$

где s – произвольная подстановка из симметрической группы $\mathbb{S}_n$,

$$s = \begin{pmatrix} 1 & 2 & \ldots & n \\ s(1) & s(2) & \ldots & s(n) \end{pmatrix},$$

k – натуральное число, $k \in \{1,\ 2,\ \ldots,\ n-1\}$.

Пусть $\rho(s)$ – матрица плотности квантовой системы $\mathrm{A}_{s(1)}\mathrm{A}_{s(2)}\ldots\mathrm{A}_{s(n)}$, находящейся в состоянии $\left|\psi^{(s)}\right\rangle$ (см. параграф 2.4), то есть

$$\rho(s) = \left|\psi^{(s)}\right\rangle\left\langle\psi^{(s)}\right|. \tag{4.4.3}$$

Тогда, подставив в равенстве (4.3.1) $\rho(s)$ вместо ρ и $\mathrm{A}(s,k)$ вместо A, получаем меру несепарабельности $C_{\mathrm{A}(s,k)}(\rho(s))$ подсистемы $\mathrm{A}(s,k)$ с подсистемой $\mathrm{B}(s,\ n-k)$, то есть

$$C_{\mathrm{A}(s,k)}(\rho(s)) = \sqrt{2\left(1 - \mathrm{tr}\left(\left[\rho_{\mathrm{A}(s,k)}(\rho(s))\right]^2\right)\right)}, \tag{4.4.4}$$

где $\rho_{\mathrm{A}(s,k)}(\rho(s))$ – редуцированная матрица плотности [50] подсистемы $\mathrm{A}(s,k)$, когда система $\mathrm{A}_{s(1)}\mathrm{A}_{s(2)}\ldots\mathrm{A}_{s(n)}$ имеет матрицу плотности $\rho(s)$.

Размерность пространства состояний подсистемы $\mathrm{A}(s,k)$ равна 2^k, а размерность пространства состояний подсистемы $\mathrm{B}(s,n-k)$ равна 2^{n-k}. Тогда, как следует из (4.3.2) и (4.3.3), для величины $C_{\mathrm{A}(s,k)}(\rho(s))$ справедливо двойное неравенство

$$0 \le C_{\mathrm{A}(s,k)}(\rho(s)) \le \sqrt{2 - \frac{1}{2^{m(k)-1}}}, \tag{4.4.5}$$

где $m(k) = \min(k,\ n-k)$.

Из (4.4.5) очевидным образом следует справедливость следующего двойного неравенства

$$0 \le \left(2 - \frac{1}{2^{m(k)-1}}\right)^{-0,5} \cdot C_{\mathrm{A}(s,k)}\left(\rho(s)\right) \le 1. \tag{4.4.6}$$

Величину $\left(2 - \frac{1}{2^{m(k)-1}}\right)^{-0,5} C_{\mathrm{A}(s,k)}\left(\rho(s)\right)$ назовем **нормированной мерой несепарабельности** подсистемы $\mathrm{A}(s,k)$ с подсистемой $\mathrm{B}(s, n-k)$.

С учетом (4.4.6) корректна формулировка следующего определения.

Определение 4.4.7. Пусть n – произвольное натуральное число, превосходящее число 1. Каждому состоянию $|\psi\rangle \in \mathbb{C}^{2^n}$ n-кубитной квантовой системы $\mathrm{A}_1\mathrm{A}_2\ldots\mathrm{A}_n$ поставим в соответствие число $V(|\psi\rangle)$, задаваемое равенством:

$$V(|\psi\rangle) = \min_{s \in \mathbb{S}_n} \min_{k \in \{1,2,\ldots,n-1\}} \left(\left(2 - \frac{1}{2^{m(k)-1}}\right)^{-0,5} \cdot C_{\mathrm{A}(s,k)}\left(\rho(s)\right)\right). \tag{4.4.8}$$

Величина $V(|\psi\rangle)$, определенная равенством (4.4.8), называется **мерой несепарабельности** состояния $|\psi\rangle$ n-кубитной квантовой системы $\mathrm{A}_1\mathrm{A}_2\ldots\mathrm{A}_n$ или **мерой несепарабельности** квантовой системы $\mathrm{A}_1\mathrm{A}_2\ldots\mathrm{A}_n$, *находящейся в состоянии* $|\psi\rangle$.

Замечание 4.4.9. В обозначении $V(|\psi\rangle)$ меры несепарабельности состояния $|\psi\rangle$ n-кубитной квантовой системы $\mathrm{A}_1\mathrm{A}_2\ldots\mathrm{A}_n$ буква V взята как первая буква имени **Виолетта** в латинском написании. При этом саму функцию V, определенную на множестве всех состояний n-кубитной квантовой системы для любого натурального числа $n > 1$ и сопоставляющую каждому состоянию $|\psi\rangle$ данной квантовой системы число $V(|\psi\rangle)$, равное мере несепарабельности этого состояния, назовем **мера Виолетта** или, кратко, **V-мера**.

Дальнейшая часть данного параграфа будет посвящена исследованию и обсуждению свойств **V-меры**. При этом будем полагать, что $|\psi\rangle$ – произвольное состояние n-кубитной квантовой системы, где $n > 1$.

Из свойств тензорного произведения матриц и меры несепарабельности, определенной равенством (4.3.1), следует справедливость следующих утверждений 4.4.10, 4.4.11 и 4.4.13.

Утверждение 4.4.10. Для любого состояния $|\psi\rangle$ n-кубитной квантовой системы (где $n > 1$) имеет место двойное неравенство

$$0 \le V(|\psi\rangle) \le 1.$$

Равенство

$$V(|\psi\rangle) = 0$$

справедливо тогда и только тогда, когда состояние $|\psi\rangle$ является сепарабельным состоянием.

Утверждение 4.4.11. Для любых $n > 1$, $s \in \mathbb{S}_n$, $k \in \{1, 2, \ldots, n-1\}$ справедливо равенство

$$C_{\mathrm{A}(s,k)}(\rho(s)) = C_{\mathrm{B}(s,n-k)}(\rho(s)).$$

Из этого утверждения непосредственно вытекает

Следствие 4.4.12. Для состояний двухкубитных квантовых систем **V-мера** совпадает с согласованностью (concurrence).

Утверждение 4.4.13. Для любых $n > 1$, $k \in \{1, 2, \ldots, n-1\}$ и $s \in \mathbb{S}_n$, $t \in \mathbb{S}_n$, таких, что два множества чисел $\{s(1), s(2), \ldots, s(k)\}$ и $\{t(1), t(2), \ldots, t(k)\}$ совпадают, имеет место равенство

$$C_{\mathrm{A}(s,k)}\left(\rho(s)\right)=C_{\mathrm{A}(t,k)}\left(\rho(t)\right).$$

Из утверждений 4.4.11 и 4.4.13 вытекает справедливость следующего утверждения.

Утверждение 4.4.14.

а) Пусть $n>1$ и n – нечетное натуральное число. Для $k\in\left\{1,\ 2,\ \ldots,\ \dfrac{n-1}{2}\right\}$ положим

$$\mathbb{S}_n(k)=$$
$$=\left\{s\in\mathbb{S}_n\ \middle|\ s(1)<s(2)<\ldots<s(k),\ s(k+1)<s(k+2)<\ldots<s(n)\right\}. \quad (4.4.15)$$

Тогда справедливо равенство

$$V\left(|\psi\rangle\right)=\min_{k\in\left\{1,2,\ldots,\frac{n-1}{2}\right\}}\ \min_{s\in\mathbb{S}_n(k)}\left(\left(2-\frac{1}{2^{k-1}}\right)^{-0,5}\cdot C_{\mathrm{A}(s,k)}\left(\rho(s)\right)\right). \quad (4.4.16)$$

б) Пусть $n>1$ и n – четное натуральное число. Для $k\in\left\{1,\ 2,\ \ldots,\ \dfrac{n}{2}-1\right\}$ положим, что $\mathbb{S}_n(k)$ определяется равенством (4.4.15), а множество $\mathbb{S}_n\left(\dfrac{n}{2}\right)$ определим следующим образом:

$$\mathbb{S}_n\left(\frac{n}{2}\right)=$$
$$=\left\{s\in\mathbb{S}_n\ \middle|\ s(1)=1,\ s(2)<\ldots<s\left(\frac{n}{2}\right),\ s\left(\frac{n}{2}+1\right)<s\left(\frac{n}{2}+2\right)<\ldots<s(n)\right\}. \quad (4.4.17)$$

Тогда справедливо равенство

$$V\left(|\psi\rangle\right)=\min_{k\in\left\{1,2,\ldots,\frac{n}{2}\right\}}\ \min_{s\in\mathbb{S}_n(k)}\left(\left(2-\frac{1}{2^{k-1}}\right)^{-0,5}\cdot C_{\mathrm{A}(s,k)}\left(\rho(s)\right)\right). \quad (4.4.18)$$

Замечание 4.4.19. Утверждение 4.4.14 может быть использовано для уменьшения трудоемкости вычисления меры несепарабельности

$V(|\psi\rangle)$ состояний многокубитной квантовой системы. Действительно, если для вычисления меры несепарабельности $V(|\psi\rangle)$ использовать равенство (4.4.8), то необходимо вычислить $n!(n-1)$ величин нормированной меры несепарабельности двухсоставных квантовых систем и выбрать среди них наименьшую. В случае же применения утверждения 4.4.14 необходимо вычислить, следуя формулам (4.4.16) или (4.4.18) (в зависимости от четности числа кубитов n в квантовой системе), $2^{n-1}-1$ величин нормированной меры несепарабельности двухсоставных квантовых систем и выбрать среди них наименьшую.

Завершая данный параграф, отметим, что построенная **V-мера** (**мера Виолетта**) дает количественную характеристику ресурса несепарабельности состояний n-кубитной квантовой системы (где $n > 1$) с позиции наименее «надежного» звена (подсистемы исходной системы) по несепарабельности во всей системе.

В следующих параграфах 4.5 и 4.6 общие результаты данного параграфа будут применены к трехкубитным и четырехкубитным квантовым системам.

§ 4.5. Мера несепарабельности состояний трехкубитных квантовых систем

Если $|\psi\rangle \in \mathbb{C}^8$ является состоянием квантовой системы $A_1A_2A_3$, состоящей из трех кубитов A_1, A_2 и A_3, то, напомним, в вычислительном базисе из векторов $|000\rangle$, $|001\rangle$, $|010\rangle$, $|011\rangle$,$|100\rangle$, $|101\rangle$, $|110\rangle$, $|111\rangle$ имеет место равенство

$$\begin{aligned}|\psi\rangle = a_0|000\rangle + a_1|001\rangle + a_2|010\rangle + a_3|011\rangle + \\ +a_4|100\rangle + a_5|101\rangle + a_6|110\rangle + a_7|111\rangle,\end{aligned} \tag{4.5.1}$$

где a_0, a_1, a_2, a_3, a_4, a_5, a_6, $a_7 \in \mathbb{C}$,

$$|a_0|^2 + |a_1|^2 + |a_2|^2 + |a_3|^2 + |a_4|^2 + |a_5|^2 + |a_6|^2 + |a_7|^2 = 1. \tag{4.5.2}$$

Поставим **задачу** выразить **V-меру** $V(|\psi\rangle)$ состояния $|\psi\rangle$ квантовой системы $A_1A_2A_3$ через амплитуды a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7 состояния $|\psi\rangle$.

Решение поставленной задачи представим в виде следующего утверждения.

Утверждение 4.5.3. Имеет место равенство

$$V(|\psi\rangle) = 2\cdot\min\left\{\left(|a_0a_5 - a_1a_4|^2 + |a_0a_6 - a_2a_4|^2 + |a_0a_7 - a_3a_4|^2 + \right.\right.$$
$$\left. + |a_1a_6 - a_2a_5|^2 + |a_1a_7 - a_3a_5|^2 + |a_2a_7 - a_3a_6|^2\right)^{\frac{1}{2}},$$
$$\left(|a_0a_3 - a_1a_2|^2 + |a_0a_6 - a_2a_4|^2 + |a_0a_7 - a_2a_5|^2 + \right.$$
$$\left. + |a_1a_6 - a_3a_4|^2 + |a_1a_7 - a_3a_5|^2 + |a_4a_7 - a_5a_6|^2\right)^{\frac{1}{2}},$$
$$\left(|a_0a_5 - a_1a_4|^2 + |a_0a_3 - a_1a_2|^2 + |a_0a_7 - a_1a_6|^2 + \right.$$
$$\left.\left. + |a_3a_4 - a_2a_5|^2 + |a_4a_7 - a_5a_6|^2 + |a_2a_7 - a_3a_6|^2\right)^{\frac{1}{2}}\right\}.$$

Доказательство данного утверждения приведем далее ниже. Перед этим разберем несколько примеров вычисления **V-меры** состояний трехкубитной квантовой системы.

Пример 4.5.4. Для состояния

$$|\psi\rangle = \frac{|000\rangle + |111\rangle}{\sqrt{2}}$$

имеем

$$a_0 = \frac{1}{\sqrt{2}},\ \ a_1 = a_2 = a_3 = a_4 = a_5 = a_6 = 0,\ a_7 = \frac{1}{\sqrt{2}}.$$

Из утверждения 4.5.3 следует, что **V-мера** состояния $|\psi\rangle$ равна

$$V(|\psi\rangle) = 2\cdot\min\left\{\frac{1}{2},\ \frac{1}{2},\ \frac{1}{2}\right\} = 1$$

и, следовательно, в соответствии с утверждением 4.4.10, состояние $|\psi\rangle$ является несепарабельным состоянием.

Пример 4.5.5.

$$|\psi\rangle = \frac{|000\rangle + |101\rangle}{\sqrt{2}},$$

имеем

$$a_0 = \frac{1}{\sqrt{2}},\ a_1 = a_2 = a_3 = a_4 = 0,\ a_5 = \frac{1}{\sqrt{2}},\ a_6 = a_7 = 0.$$

Из утверждения 4.5.3 следует, что **V-мера** состояния $|\psi\rangle$ равна

$$V(|\psi\rangle) = 2 \cdot \min\left\{\frac{1}{2},\ 0,\ \frac{1}{2}\right\} = 0$$

и, следовательно, в соответствии с утверждением 4.4.10, состояние $|\psi\rangle$ является сепарабельным состоянием.

Пример 4.5.6.

$$|\psi\rangle = \frac{|001\rangle + |010\rangle + |100\rangle}{\sqrt{3}},$$

имеем

$$a_0 = 0,\ a_1 = \frac{1}{\sqrt{3}},\ a_2 = \frac{1}{\sqrt{3}},\ a_3 = 0,\ a_4 = \frac{1}{\sqrt{3}},\ a_5 = a_6 = a_7 = 0.$$

Из утверждения 4.5.3 следует, что **V-мера** состояния $|\psi\rangle$ равна

$$V(|\psi\rangle) = 2 \cdot \min\left\{\frac{\sqrt{2}}{3},\ \frac{\sqrt{2}}{3},\ \frac{\sqrt{2}}{3}\right\} = \frac{2\sqrt{2}}{3}$$

и, следовательно, в соответствии с утверждением 4.4.10, состояние $|\psi\rangle$ является несепарабельным состоянием.

Далее приведем **доказательство** утверждения 4.5.3.

Из пункта (а) утверждения 4.4.14 для V-меры состояния $|\psi\rangle$ следует справедливость равенства

$$V\left(|\psi\rangle\right)=\min_{s\in\mathbb{S}_3(1)}\left(\left(2-\frac{1}{2^{1-1}}\right)^{-0,5}\cdot C_{\mathrm{A}(s,1)}\left(\rho(s)\right)\right)=\min_{s\in\mathbb{S}_3(1)}C_{\mathrm{A}(s,1)}\left(\rho(s)\right),\ (4.5.7)$$

где в соответствии с (4.4.15)

$$\mathbb{S}_3(1)=\left\{s\in\mathbb{S}_3\ \middle|\ s(2)<s(3)\right\}=$$
$$=\left\{s_0=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\ s_1=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},\ s_5=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\right\}. \qquad (4.5.8)$$

(В (4.5.8) сохранена нумерация элементов симметрической группы $\mathbb{S}_3$, принятая в параграфе 2.5.)

Из равенств (4.5.7) и (4.5.8) следует, что

$$V\left(|\psi\rangle\right)=\min\left\{C_{\mathrm{A}(s_0,1)}\left(\rho(s_0)\right),\ C_{\mathrm{A}(s_1,1)}\left(\rho(s_1)\right),\ C_{\mathrm{A}(s_5,1)}\left(\rho(s_5)\right)\right\}.\ (4.5.9)$$

Из равенства (4.4.1) следует, что

$$\mathrm{A}(s_0,\,1)=\mathrm{A}_{s_0(1)}=\mathrm{A}_1. \qquad (4.5.10)$$

Из равенства (4.4.3) и определения $\left|\psi^{(s)}\right\rangle$ в параграфе 2.4 следует, что

$$\rho(s_0)=\left|\psi^{(s_0)}\right\rangle\left\langle\psi^{(s_0)}\right|=|\psi\rangle\langle\psi|. \qquad (4.5.11)$$

Далее, положив A = A_1, B = A_2 и C = A_3, из равенств (2.3.13) и (2.3.14), с учетом равенств (4.5.10) и (4.5.11), получаем

$$\mathrm{tr}\left(\left[\rho_{\mathrm{A}(s_0,1)}\left(\rho(s_0)\right)\right]^2\right)=$$
$$=1+2(\tilde a_0a_1a_4\tilde a_5+\tilde a_0a_2a_4\tilde a_6+\tilde a_0a_3a_4\tilde a_7+a_0\tilde a_1\tilde a_4a_5+\tilde a_1a_2a_5\tilde a_6+\tilde a_1a_3a_5\tilde a_7+$$
$$+a_0\tilde a_2\tilde a_4a_6+a_1\tilde a_2\tilde a_5a_6+\tilde a_2a_3a_6\tilde a_7+a_0\tilde a_3\tilde a_4a_7+a_1\tilde a_3\tilde a_5a_7+a_2\tilde a_3\tilde a_6a_7-$$
$$-|a_0|^2|a_5|^2-|a_0|^2|a_6|^2-|a_0|^2|a_7|^2-|a_1|^2|a_4|^2-|a_1|^2|a_6|^2-|a_1|^2|a_7|^2-$$
$$-|a_2|^2|a_4|^2-|a_2|^2|a_5|^2-|a_2|^2|a_7|^2-|a_3|^2|a_4|^2-|a_3|^2|a_5|^2-|a_3|^2|a_6|^2).\ (4.5.12)$$

Из (4.4.4) и (4.5.12) получаем

$$C_{\mathrm{A}(s_0,1)}\left(\rho\left(s_0\right)\right)=$$

$$=(4(|a_0|^2|a_5|^2+|a_0|^2|a_6|^2+|a_0|^2|a_7|^2+|a_1|^2|a_4|^2+|a_1|^2|a_6|^2+|a_1|^2|a_7|^2+$$

$$+|a_2|^2|a_4|^2+|a_2|^2|a_5|^2+|a_2|^2|a_7|^2+|a_3|^2|a_4|^2+|a_3|^2|a_5|^2+|a_3|^2|a_6|^2-$$

$$-\tilde{a}_0a_1a_4\tilde{a}_5-\tilde{a}_0a_2a_4\tilde{a}_6-\tilde{a}_0a_3a_4\tilde{a}_7-a_0\tilde{a}_1\tilde{a}_4a_5-\tilde{a}_1a_2a_5\tilde{a}_6-\tilde{a}_1a_3a_5\tilde{a}_7-$$

$$-a_0\tilde{a}_2\tilde{a}_4a_6-a_1\tilde{a}_2\tilde{a}_5a_6-\tilde{a}_2a_3a_6\tilde{a}_7-a_0\tilde{a}_3\tilde{a}_4a_7-a_1\tilde{a}_3\tilde{a}_5a_7-a_2\tilde{a}_3\tilde{a}_6a_7))^{1/2}=$$

$$=2\Big(\left(a_0a_5-a_1a_4\right)\left(\tilde{a}_0\tilde{a}_5-\tilde{a}_1\tilde{a}_4\right)+\left(a_0a_6-a_2a_4\right)\left(\tilde{a}_0\tilde{a}_6-\tilde{a}_2\tilde{a}_4\right)+$$

$$+\left(a_0a_7-a_3a_4\right)\left(\tilde{a}_0\tilde{a}_7-\tilde{a}_3\tilde{a}_4\right)+\left(a_1a_6-a_2a_5\right)\left(\tilde{a}_1\tilde{a}_6-\tilde{a}_2\tilde{a}_5\right)+$$

$$+\left(a_1a_7-a_3a_5\right)\left(\tilde{a}_1\tilde{a}_7-\tilde{a}_3\tilde{a}_5\right)+\left(a_2a_7-a_3a_6\right)\left(\tilde{a}_2\tilde{a}_7-\tilde{a}_3\tilde{a}_6\right)\Big)^{1/2}=$$

$$=2\Big(|a_0a_5-a_1a_4|^2+|a_0a_6-a_2a_4|^2+|a_0a_7-a_3a_4|^2+$$

$$+|a_1a_6-a_2a_5|^2+|a_1a_7-a_3a_5|^2+|a_2a_7-a_3a_6|^2\Big)^{1/2}.$$

То есть справедливо равенство

$$C_{\mathrm{A}(s_0,1)}\left(\rho\left(s_0\right)\right)=$$

$$=2\Big(|a_0a_5-a_1a_4|^2+|a_0a_6-a_2a_4|^2+|a_0a_7-a_3a_4|^2+$$

$$+|a_1a_6-a_2a_5|^2+|a_1a_7-a_3a_5|^2+|a_2a_7-a_3a_6|^2\Big)^{1/2}. \tag{4.5.13}$$

Далее, из определения $\left|\psi^{(s)}\right\rangle$ в параграфе 2.4 следует, что величины $C_{\mathrm{A}(s_1,1)}\left(\rho\left(s_1\right)\right)$ и $C_{\mathrm{A}(s_5,1)}\left(\rho\left(s_5\right)\right)$ можно получить из правой части равенства (4.5.13) применением к индексам координат состояния $|\psi\rangle$ соответственно подстановок

$$\breve{s}_1^{-1}=\begin{pmatrix}0&1&2&3&4&5&6&7\\0&1&4&5&2&3&6&7\end{pmatrix}$$

и

$$\breve{s}_5^{-1}=\begin{pmatrix}0&1&2&3&4&5&6&7\\0&2&4&6&1&3&5&7\end{pmatrix}$$

на множестве чисел $\{0,1,\ldots,7\}$, обратных к подстановкам

$$\breve{s}_1 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 0 & 1 & 4 & 5 & 2 & 3 & 6 & 7 \end{pmatrix}$$

и

$$\breve{s}_5 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 0 & 4 & 1 & 5 & 2 & 6 & 3 & 7 \end{pmatrix},$$

определяемых по s_1 и s_5 с помощью равенства (2.5.33). В результате имеем

$$C_{\mathrm{A}(s_1,1)}\left(\rho(s_1)\right) = 2\Big(\left|a_0a_3 - a_1a_2\right|^2 + \left|a_0a_6 - a_2a_4\right|^2 + \left|a_0a_7 - a_2a_5\right|^2 + \\ + \left|a_1a_6 - a_3a_4\right|^2 + \left|a_1a_7 - a_3a_5\right|^2 + \left|a_4a_7 - a_5a_6\right|^2\Big)^{1/2}, \qquad (4.5.14)$$

$$C_{\mathrm{A}(s_5,1)}\left(\rho(s_5)\right) = 2\Big(\left|a_0a_5 - a_1a_4\right|^2 + \left|a_0a_3 - a_1a_2\right|^2 + \left|a_0a_7 - a_1a_6\right|^2 + \\ + \left|a_3a_4 - a_2a_5\right|^2 + \left|a_4a_7 - a_5a_6\right|^2 + \left|a_2a_7 - a_3a_6\right|^2\Big)^{1/2}. \qquad (4.5.15)$$

Из равенств (4.5.9), (4.5.13), (4.5.14) и (4.5.15) следует справедливость утверждения 4.5.3.

§ 4.6. Мера несепарабельности состояний четырехкубитных квантовых систем

Если $|\psi\rangle \in \mathbb{C}^{16}$ является состоянием квантовой системы $\mathrm{A}_1\mathrm{A}_2\mathrm{A}_3\mathrm{A}_4$, состоящей из четырех кубитов A_1, A_2, A_3 и A_4, то в вычислительном базисе из векторов

$$|0000\rangle,\ |0001\rangle,\ |0010\rangle,\ |0011\rangle, |0100\rangle,\ |0101\rangle,\ |0110\rangle,\ |0111\rangle, \\ |1000\rangle,\ |1001\rangle,\ |1010\rangle,\ |1011\rangle,\ |1100\rangle,\ |1101\rangle,\ |1110\rangle,\ |1111\rangle$$

имеет место равенство

$$|\psi\rangle = a_0|0000\rangle + a_1|0001\rangle + a_2|0010\rangle + a_3|0011\rangle + \\ + a_4|0100\rangle + a_5|0101\rangle + a_6|0110\rangle + a_7|0111\rangle +$$

$$+a_8|1000\rangle + a_9|1001\rangle + a_{10}|1010\rangle + a_{11}|1011\rangle +$$
$$+a_{12}|1100\rangle + a_{13}|1101\rangle + a_{14}|1110\rangle + a_{15}|1111\rangle, \quad (4.6.1)$$

где $a_0,\ a_1,\ \ldots,\ a_{15} \in \mathbb{C}$,

$$|a_0|^2 + |a_1|^2 + \ldots + |a_{15}|^2 = 1. \quad (4.6.2)$$

Поставим **задачу** выразить **V-меру** $V(|\psi\rangle)$ состояния $|\psi\rangle$ квантовой системы $A_1A_2A_3A_4$ через амплитуды a_0, a_1, …, a_{15} состояния $|\psi\rangle$.

Решение поставленной задачи представим в виде следующего утверждения, в формулировке которого используются величины Z_0, Z_1, …, Z_6, определенные ниже в данном параграфе равенствами (4.6.4), (4.6.5), …, (4.6.10) соответственно.

Утверждение 4.6.3. Имеет место равенство

$$V(|\psi\rangle) = 2 \cdot \min\{Z_0,\ Z_1,\ \ldots,\ Z_6\}.$$

Доказательство данного утверждения аналогично доказательству утверждения 4.5.3 из параграфа 4.5.

Для состояния $|\psi\rangle \in \mathbb{C}^{16}$, заданного равенством (4.6.1), указанные выше величины Z_0, Z_1, …, Z_6 определяются следующими равенствами:

$$Z_0 = \Big(|a_0a_9 - a_1a_8|^2 + |a_0a_{10} - a_2a_8|^2 + |a_0a_{11} - a_3a_8|^2 + |a_0a_{12} - a_4a_8|^2 +$$
$$+|a_0a_{13} - a_5a_8|^2 + |a_0a_{14} - a_6a_8|^2 + |a_0a_{15} - a_7a_8|^2 +$$
$$+|a_1a_{10} - a_2a_9|^2 + |a_1a_{11} - a_3a_9|^2 + |a_1a_{12} - a_4a_9|^2 + |a_1a_{13} - a_5a_9|^2 +$$
$$+|a_1a_{14} - a_6a_9|^2 + |a_1a_{15} - a_7a_9|^2 + |a_2a_{11} - a_3a_{10}|^2 +$$
$$+|a_2a_{12} - a_4a_{10}|^2 + |a_2a_{13} - a_5a_{10}|^2 + |a_2a_{14} - a_6a_{10}|^2 + |a_2a_{15} - a_7a_{10}|^2 +$$
$$+|a_3a_{12} - a_4a_{11}|^2 + |a_3a_{13} - a_5a_{11}|^2 + |a_3a_{14} - a_6a_{11}|^2 + |a_3a_{15} - a_7a_{11}|^2 +$$
$$+|a_4a_{13} - a_5a_{12}|^2 + |a_4a_{14} - a_6a_{12}|^2 + |a_4a_{15} - a_7a_{12}|^2 +$$
$$+|a_5a_{14} - a_6a_{13}|^2 + |a_5a_{15} - a_7a_{13}|^2 + |a_6a_{15} - a_7a_{14}|^2\Big)^{1/2}, \quad (4.6.4)$$

$$Z_1 = \sqrt{\frac{2}{3}} \cdot$$

$$\Big(|a_0a_5 - a_1a_4|^2 + |a_0a_6 - a_2a_4|^2 + |a_0a_7 - a_3a_4|^2 + |a_0a_9 - a_1a_8|^2 + |a_0a_{10} - a_2a_8|^2 +$$
$$+ |a_0a_{11} - a_3a_8|^2 + |a_0a_{13} - a_1a_{12}|^2 + |a_0a_{14} - a_2a_{12}|^2 + |a_0a_{15} - a_3a_{12}|^2 +$$
$$+ |a_1a_6 - a_2a_5|^2 + |a_1a_7 - a_3a_5|^2 + |a_1a_{10} - a_2a_9|^2 +$$
$$+ |a_1a_{11} - a_3a_9|^2 + |a_1a_{14} - a_2a_{13}|^2 + |a_1a_{15} - a_3a_{13}|^2 +$$
$$+ |a_2a_7 - a_3a_6|^2 + |a_2a_{11} - a_3a_{10}|^2 + |a_2a_{15} - a_3a_{14}|^2 +$$
$$+ |a_4a_9 - a_5a_8|^2 + |a_4a_{10} - a_6a_8|^2 + |a_4a_{11} - a_7a_8|^2 +$$
$$+ |a_4a_{13} - a_5a_{12}|^2 + |a_4a_{14} - a_6a_{12}|^2 + |a_4a_{15} - a_7a_{12}|^2 +$$
$$+ |a_5a_{10} - a_6a_9|^2 + |a_5a_{11} - a_7a_9|^2 + |a_5a_{14} - a_6a_{13}|^2 + |a_5a_{15} - a_7a_{13}|^2 +$$
$$+ |a_6a_{11} - a_7a_{10}|^2 + |a_6a_{15} - a_7a_{14}|^2 +$$
$$+ |a_8a_{13} - a_9a_{12}|^2 + |a_8a_{14} - a_{10}a_{12}|^2 + |a_8a_{15} - a_{11}a_{12}|^2 +$$
$$+ |a_9a_{14} - a_{10}a_{13}|^2 + |a_9a_{15} - a_{11}a_{13}|^2 + |a_{10}a_{15} - a_{11}a_{14}|^2 \Big)^{1/2}, \qquad (4.6.5)$$

$$Z_2 = \Big(|a_0a_3 - a_1a_2|^2 + |a_0a_5 - a_1a_4|^2 + |a_0a_7 - a_1a_6|^2 + |a_0a_9 - a_1a_8|^2 +$$
$$+ |a_0a_{11} - a_1a_{10}|^2 + |a_0a_{13} - a_1a_{12}|^2 + |a_0a_{15} - a_1a_{14}|^2 +$$
$$+ |a_2a_5 - a_3a_4|^2 + |a_2a_7 - a_3a_6|^2 + |a_2a_9 - a_3a_8|^2 +$$
$$+ |a_2a_{11} - a_3a_{10}|^2 + |a_2a_{13} - a_3a_{12}|^2 + |a_2a_{15} - a_3a_{14}|^2 +$$
$$+ |a_4a_7 - a_5a_6|^2 + |a_4a_9 - a_5a_8|^2 + |a_4a_{11} - a_5a_{10}|^2 +$$
$$+ |a_4a_{13} - a_5a_{12}|^2 + |a_4a_{15} - a_5a_{14}|^2 +$$
$$+ |a_6a_9 - a_7a_8|^2 + |a_6a_{11} - a_7a_{10}|^2 + |a_6a_{13} - a_7a_{12}|^2 + |a_6a_{15} - a_7a_{14}|^2 +$$
$$+ |a_8a_{11} - a_9a_{10}|^2 + |a_8a_{13} - a_9a_{12}|^2 + |a_8a_{15} - a_9a_{14}|^2 +$$
$$+ |a_{10}a_{13} - a_{11}a_{12}|^2 + |a_{10}a_{15} - a_{11}a_{14}|^2 + |a_{12}a_{15} - a_{13}a_{14}|^2 \Big)^{1/2}, \qquad (4.6.6)$$

$$Z_3 = \left(|a_0a_5 - a_1a_4|^2 + |a_0a_6 - a_2a_4|^2 + |a_0a_7 - a_3a_4|^2 + |a_0a_{12} - a_8a_4|^2 + \right.$$
$$+ |a_0a_{13} - a_9a_4|^2 + |a_0a_{14} - a_{10}a_4|^2 + |a_0a_{15} - a_{11}a_4|^2 +$$
$$+ |a_1a_6 - a_2a_5|^2 + |a_1a_7 - a_3a_5|^2 + |a_1a_{12} - a_8a_5|^2 +$$
$$+ |a_1a_{13} - a_9a_5|^2 + |a_1a_{14} - a_{10}a_5|^2 + |a_1a_{15} - a_{11}a_5|^2 +$$
$$+ |a_2a_7 - a_3a_6|^2 + |a_2a_{12} - a_8a_6|^2 + |a_2a_{13} - a_9a_6|^2 +$$
$$+ |a_2a_{14} - a_{10}a_6|^2 + |a_2a_{15} - a_{11}a_6|^2 +$$
$$+ |a_3a_{12} - a_8a_7|^2 + |a_3a_{13} - a_9a_7|^2 + |a_3a_{14} - a_{10}a_7|^2 + |a_3a_{15} - a_{11}a_7|^2 +$$
$$+ |a_8a_{13} - a_9a_{12}|^2 + |a_8a_{14} - a_{10}a_{12}|^2 + |a_8a_{15} - a_{11}a_{12}|^2 +$$
$$\left. + |a_9a_{14} - a_{10}a_{13}|^2 + |a_9a_{15} - a_{11}a_{13}|^2 + |a_{10}a_{15} - a_{11}a_{14}|^2 \right)^{1/2}, \qquad (4.6.7)$$

$$Z_4 = \left(|a_0a_3 - a_1a_2|^2 + |a_0a_6 - a_4a_2|^2 + |a_0a_7 - a_5a_2|^2 + |a_0a_{10} - a_8a_2|^2 + \right.$$
$$+ |a_0a_{11} - a_9a_2|^2 + |a_0a_{14} - a_{12}a_2|^2 + |a_0a_{15} - a_{13}a_2|^2 +$$
$$+ |a_1a_6 - a_4a_3|^2 + |a_1a_7 - a_5a_3|^2 + |a_1a_{10} - a_8a_3|^2 +$$
$$+ |a_1a_{11} - a_9a_3|^2 + |a_1a_{14} - a_{12}a_3|^2 + |a_1a_{15} - a_{13}a_3|^2 +$$
$$+ |a_4a_7 - a_5a_6|^2 + |a_4a_{10} - a_8a_6|^2 + |a_4a_{11} - a_9a_6|^2 +$$
$$+ |a_4a_{14} - a_{12}a_6|^2 + |a_4a_{15} - a_{13}a_6|^2 +$$
$$+ |a_5a_{10} - a_8a_7|^2 + |a_5a_{11} - a_9a_7|^2 + |a_5a_{14} - a_{12}a_7|^2 + |a_5a_{15} - a_{13}a_7|^2 +$$
$$+ |a_8a_{11} - a_9a_{10}|^2 + |a_8a_{14} - a_{12}a_{10}|^2 + |a_8a_{15} - a_{13}a_{10}|^2 +$$
$$\left. + |a_9a_{14} - a_{12}a_{11}|^2 + |a_9a_{15} - a_{13}a_{11}|^2 + |a_{12}a_{15} - a_{13}a_{14}|^2 \right)^{1/2}, \qquad (4.6.8)$$

$$Z_5 = \sqrt{\frac{2}{3}} \cdot$$

$$\left(|a_0a_9 - a_1a_8|^2 + |a_0a_{12} - a_4a_8|^2 + |a_0a_{13} - a_5a_8|^2 + |a_0a_3 - a_1a_2|^2 + |a_0a_6 - a_4a_2|^2 + \right.$$
$$+ |a_0a_7 - a_5a_2|^2 + |a_0a_{11} - a_1a_{10}|^2 + |a_0a_{14} - a_4a_{10}|^2 + |a_0a_{15} - a_5a_{10}|^2 +$$

$$+\left|a_1a_{12}-a_4a_9\right|^2+\left|a_1a_{13}-a_5a_9\right|^2+\left|a_1a_6-a_4a_3\right|^2+\left|a_1a_7-a_5a_3\right|^2+$$
$$+\left|a_1a_{14}-a_4a_{11}\right|^2+\left|a_1a_{15}-a_5a_{11}\right|^2+\left|a_4a_{13}-a_5a_{12}\right|^2+\left|a_4a_7-a_5a_6\right|^2+$$
$$+\left|a_4a_{15}-a_5a_{14}\right|^2+\left|a_8a_3-a_9a_2\right|^2+\left|a_8a_6-a_{12}a_2\right|^2+\left|a_8a_7-a_{13}a_2\right|^2+$$
$$+\left|a_8a_{11}-a_9a_{10}\right|^2+\left|a_8a_{14}-a_{12}a_{10}\right|^2+\left|a_8a_{15}-a_{13}a_{10}\right|^2+$$
$$+\left|a_9a_6-a_{12}a_3\right|^2+\left|a_9a_7-a_{13}a_3\right|^2+\left|a_9a_{14}-a_{12}a_{11}\right|^2+\left|a_9a_{15}-a_{13}a_{11}\right|^2+$$
$$+\left|a_{12}a_7-a_{13}a_6\right|^2+\left|a_{12}a_{15}-a_{13}a_{14}\right|^2+$$
$$+\left|a_2a_{11}-a_3a_{10}\right|^2+\left|a_2a_{14}-a_6a_{10}\right|^2+\left|a_2a_{15}-a_7a_{10}\right|^2+$$
$$+\left|a_3a_{14}-a_6a_{11}\right|^2+\left|a_3a_{15}-a_7a_{11}\right|^2+\left|a_6a_{15}-a_7a_{14}\right|^2\Big)^{1/2}, \qquad (4.6.9)$$

$$Z_6=\sqrt{\frac{2}{3}}\cdot$$
$$\Big(\left|a_0a_{10}-a_2a_8\right|^2+\left|a_0a_{12}-a_4a_8\right|^2+\left|a_0a_{14}-a_6a_8\right|^2+\left|a_0a_3-a_2a_1\right|^2+\left|a_0a_5-a_4a_1\right|^2+$$
$$+\left|a_0a_7-a_6a_1\right|^2+\left|a_0a_{11}-a_2a_9\right|^2+\left|a_0a_{13}-a_4a_9\right|^2+\left|a_0a_{15}-a_6a_9\right|^2+$$
$$+\left|a_2a_{12}-a_4a_{10}\right|^2+\left|a_2a_{14}-a_6a_{10}\right|^2+\left|a_2a_5-a_4a_3\right|^2+$$
$$+\left|a_2a_7-a_6a_3\right|^2+\left|a_2a_{13}-a_4a_{11}\right|^2+\left|a_2a_{15}-a_6a_{11}\right|^2+$$
$$+\left|a_4a_{14}-a_6a_{12}\right|^2+\left|a_4a_7-a_6a_5\right|^2+\left|a_4a_{15}-a_6a_{13}\right|^2+$$
$$+\left|a_8a_3-a_{10}a_1\right|^2+\left|a_8a_5-a_{12}a_1\right|^2+\left|a_8a_7-a_{14}a_1\right|^2+$$
$$+\left|a_8a_{11}-a_{10}a_9\right|^2+\left|a_8a_{13}-a_{12}a_9\right|^2+\left|a_8a_{15}-a_{14}a_9\right|^2+$$
$$+\left|a_{10}a_5-a_{12}a_3\right|^2+\left|a_{10}a_7-a_{14}a_3\right|^2+\left|a_{10}a_{13}-a_{12}a_{11}\right|^2+\left|a_{10}a_{15}-a_{14}a_{11}\right|^2+$$
$$+\left|a_{12}a_7-a_{14}a_5\right|^2+\left|a_{12}a_{15}-a_{14}a_{13}\right|^2+$$
$$+\left|a_1a_{11}-a_3a_9\right|^2+\left|a_1a_{13}-a_5a_9\right|^2+\left|a_1a_{15}-a_7a_9\right|^2+$$
$$+\left|a_3a_{13}-a_5a_{11}\right|^2+\left|a_3a_{15}-a_7a_{11}\right|^2+\left|a_5a_{15}-a_7a_{13}\right|^2\Big)^{1/2}. \qquad (4.6.10)$$

Разберем несколько примеров вычисления **V-меры** состояний четырехкубитной квантовой системы.

Пример 4.6.11. Для состояния

$$|\psi\rangle = \frac{|0000\rangle + |1111\rangle}{\sqrt{2}}$$

имеем в вычислительном базисе следующие значения амплитуд:

$$a_0 = \frac{1}{\sqrt{2}}, \ a_1 = a_2 = \ldots = a_{14} = 0, \ a_{15} = \frac{1}{\sqrt{2}}.$$

Тогда, воспользовавшись равенствами (4.6.4), (4.6.5), …, (4.6.10), находим значения величин Z_0, Z_1, …, Z_6:

$$Z_0 = \frac{1}{2}, \ Z_1 = \frac{1}{\sqrt{6}}, \ Z_2 = Z_3 = Z_4 = \frac{1}{2}, \ Z_5 = \frac{1}{\sqrt{6}}, \ Z_6 = \frac{1}{\sqrt{6}}.$$

Из утверждения 4.6.3 следует, что **V-мера** состояния $|\psi\rangle$ равна

$$V(|\psi\rangle) = 2 \cdot \min\{Z_0, \ Z_1, \ \ldots, \ Z_6\} =$$
$$= 2 \cdot \min\left\{\frac{1}{2}, \frac{1}{\sqrt{6}}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{\sqrt{6}}, \frac{1}{\sqrt{6}}\right\} = 2 \cdot \frac{1}{\sqrt{6}} = \sqrt{\frac{2}{3}}$$

и, следовательно, в соответствии с утверждением 4.4.10, состояние $|\psi\rangle$ является несепарабельным состоянием.

Пример 4.6.12. Для состояния

$$|\psi\rangle = \frac{|0101\rangle + |0111\rangle + |1010\rangle + |1011\rangle + |1101\rangle + |1110\rangle}{\sqrt{6}}$$

имеем в вычислительном базисе следующие значения амплитуд:

$$a_0 = a_1 = a_2 = a_3 = a_4 = 0, \ a_5 = \frac{1}{\sqrt{6}}, \ a_6 = 0, \ a_7 = \frac{1}{\sqrt{6}},$$

$$a_8 = a_9 = 0, \ a_{10} = a_{11} = \frac{1}{\sqrt{6}}, \ a_{12} = 0, \ a_{13} = a_{14} = \frac{1}{\sqrt{6}}, \ a_{15} = 0.$$

Тогда, воспользовавшись равенствами (4.6.4), (4.6.5), …, (4.6.10), находим значения величин Z_0, Z_1, …, Z_6:

$$Z_0 = \frac{\sqrt{7}}{6},\ Z_1 = \frac{1}{\sqrt{6}},\ Z_2 = Z_3 = Z_4 = \frac{\sqrt{7}}{6},\ Z_5 = \frac{1}{\sqrt{6}},\ Z_6 = \frac{1}{\sqrt{6}}.$$

Из утверждения 4.6.3 следует, что **V-мера** состояния $|\psi\rangle$ равна

$$V(|\psi\rangle) = 2\cdot\min\{Z_0,\ Z_1,\ \ldots,\ Z_6\} =$$
$$= 2\cdot\min\left\{\frac{\sqrt{7}}{6},\ \frac{1}{\sqrt{6}},\ \frac{\sqrt{7}}{6},\ \frac{\sqrt{7}}{6},\ \frac{\sqrt{7}}{6},\ \frac{1}{\sqrt{6}},\ \frac{1}{\sqrt{6}}\right\} = 2\cdot\frac{1}{\sqrt{6}} = \sqrt{\frac{2}{3}}$$

и, следовательно, в соответствии с утверждением 4.4.10, состояние $|\psi\rangle$ является несепарабельным состоянием.

Пример 4.6.13. Для состояния

$$|\psi\rangle = \frac{|0001\rangle - |1000\rangle}{\sqrt{2}}$$

имеем в вычислительном базисе следующие значения амплитуд:

$$a_0 = 0,\ a_1 = \frac{1}{\sqrt{2}},\ a_2 = a_3 = \ldots = a_7 = 0,\ a_8 = -\frac{1}{\sqrt{2}},\ a_9 = a_{10} = \ldots = a_{15} = 0.$$

Тогда, воспользовавшись равенствами (4.6.4), (4.6.5), …, (4.6.10), находим значения величин $Z_0, Z_1, \ldots, Z_6$:

$$Z_0 = \frac{1}{2},\ Z_1 = \frac{1}{\sqrt{6}},\ Z_2 = \frac{1}{2},\ Z_3 = 0,\ Z_4 = 0,\ Z_5 = \frac{1}{\sqrt{6}},\ Z_6 = 0.$$

Из утверждения 4.6.3 следует, что **V-мера** состояния $|\psi\rangle$ равна

$$V(|\psi\rangle) = 2\cdot\min\{Z_0,\ Z_1,\ \ldots,\ Z_6\} = 2\cdot\min\left\{\frac{1}{2},\ \frac{1}{\sqrt{6}},\ \frac{1}{2},\ 0,\ 0,\ \frac{1}{\sqrt{6}},\ 0\right\} = 0$$

и, следовательно, в соответствии с утверждением 4.4.10, состояние $|\psi\rangle$ является сепарабельным состоянием.

Пример 4.6.14. Для состояния

$$|\psi\rangle = \frac{|0111\rangle - |1110\rangle}{\sqrt{2}}$$

имеем в вычислительном базисе следующие значения амплитуд:

$$a_0 = a_1 = \ldots = a_6 = 0\,,\ a_7 = \frac{1}{\sqrt{2}}\,,\ a_9 = a_{10} = \ldots = a_{13} = 0\,,\ a_{14} = -\frac{1}{\sqrt{2}}\,,\ a_{15} = 0\,.$$

Тогда, воспользовавшись равенствами (4.6.4), (4.6.5), …, (4.6.10), находим значения величин Z_0, Z_1, …, Z_6:

$$Z_0 = \frac{1}{2}\,,\ Z_1 = \frac{1}{\sqrt{6}}\,,\ Z_2 = \frac{1}{2}\,,\ Z_3 = 0\,,\ Z_4 = 0\,,\ Z_5 = \frac{1}{\sqrt{6}}\,,\ Z_6 = 0\,.$$

Из утверждения 4.6.4 следует, что **V-мера** состояния $|\psi\rangle$ равна

$$V\left(|\psi\rangle\right) = 2\cdot\min\left\{Z_0,\ Z_1,\ \ldots,\ Z_6\right\} = 2\cdot\min\left\{\frac{1}{2},\ \frac{1}{\sqrt{6}},\ \frac{1}{2},\ 0,\ 0,\ \frac{1}{\sqrt{6}},\ 0\right\} = 0$$

и, следовательно, в соответствии с утверждением 4.4.10, состояние $|\psi\rangle$ является сепарабельным состоянием.

Пример 4.6.15. Для состояния

$$|\psi\rangle = \frac{1}{\sqrt{12}}|0011\rangle - \frac{2}{\sqrt{12}}|0101\rangle + \frac{1}{\sqrt{12}}|0110\rangle +$$
$$+\frac{1}{\sqrt{12}}|1001\rangle - \frac{2}{\sqrt{12}}|1010\rangle + \frac{1}{\sqrt{12}}|1100\rangle$$

имеем в вычислительном базисе следующие значения амплитуд:

$$a_0 = a_1 = a_2 = 0\,,\ a_3 = \frac{1}{\sqrt{12}}\,,\ a_4 = 0\,,\ a_5 = -\frac{2}{\sqrt{12}}\,,\ a_6 = \frac{1}{\sqrt{12}}\,,\ a_7 = a_8 = 0\,,$$
$$a_9 = \frac{1}{\sqrt{12}}\,,\ a_{10} = -\frac{2}{\sqrt{12}}\,,\ a_{11} = 0\,,\ a_{12} = \frac{1}{\sqrt{12}}\,,\ a_{13} = a_{14} = a_{15} = 0\,.$$

Тогда, воспользовавшись равенствами (4.6.4), (4.6.5), …, (4.6.10), находим значения величин Z_0, Z_1, …, Z_6:

$$Z_0 = \frac{1}{2}\,,\ Z_1 = \frac{\sqrt{5}}{6}\,,\ Z_2 = Z_3 = Z_4 = \frac{1}{2}\,,\ Z_5 = \frac{\sqrt{2}}{3}\,,\ Z_6 = \frac{\sqrt{5}}{6}\,.$$

Из утверждения 4.6.3 следует, что **V-мера** состояния $|\psi\rangle$ равна

$$V\left(\left|\psi\right\rangle\right) = 2 \cdot \min\left\{Z_0,\ Z_1,\ \ldots,\ Z_6\right\} =$$
$$= 2 \cdot \min\left\{\frac{1}{2},\ \frac{\sqrt{5}}{6},\ \frac{1}{2},\ \frac{1}{2},\ \frac{1}{2},\ \frac{\sqrt{2}}{3},\ \frac{\sqrt{5}}{6}\right\} = 2 \cdot \frac{\sqrt{5}}{6} = \frac{\sqrt{5}}{3}$$

и, следовательно, в соответствии с утверждением 4.4.10, состояние $\left|\psi\right\rangle$ является несепарабельным состоянием.

Выводы по главе 4

1. Установлено, что для любого состояния с положительной мерой несепарабельности двухкубитной квантовой системы характерно то, что ни один из двух кубитов, входящих в квантовую систему, не имеет определенного состояния. Но, как только один из них будет подвергнут специально выбранному измерению (результат которого будет случайным), сразу же другой кубит окажется в определенном состоянии.

2. Получено полное описание состояний с максимальной мерой несепарабельности двухкубитной квантовой системы для проективных измерений, операторы которых построены на векторах произвольных ортонормированных базисов двумерного гильбертова пространства над полем комплексных чисел, обладающих тем свойством, что ни один из двух кубитов, входящих в квантовую систему, не имеет определенного состояния. Но, как только один из них будет подвергнут измерению (результат которого будет с вероятностью 1/2 совпадать с одним из базисных векторов), сразу же другой кубит окажется в вполне определенном состоянии.

3. Рассмотрена мера несепарабельности двухсоставных квантовых систем под названием **согласованность**. Показано, что в случае двухкубитных квантовых систем она совпадает с соответствующей одноименной характеристикой двухкубитной квантовой системы. Для примера вычислены меры несепарабельности подсистем квантовых систем с остальными частями систем в некоторых частных случаях.

4. Построена количественная характеристика ресурса несепарабельности состояний многокубитных квантовых систем. Эта характеристика названа **мера Виолетта (V-мера)**.

Для произвольного состояния трехкубитной квантовой системы получено выражение значения этой меры через амплитуды состояния в вычислительном базисе. Учитывая новизну и значимость этого результата, представляется уместным его автономное изложение и в части выводов к главе 4, что и осуществлено ниже.

Для **V-меры** состояния

$$\begin{gathered}|\psi\rangle = a_0|000\rangle + a_1|001\rangle + a_2|010\rangle + a_3|011\rangle + \\ + a_4|100\rangle + a_5|101\rangle + a_6|110\rangle + a_7|111\rangle,\end{gathered}$$

где $a_0,\ a_1,\ a_2,\ a_3,\ a_4,\ a_5,\ a_6,\ a_7 \in \mathbb{C}$,

$$|a_0|^2 + |a_1|^2 + |a_2|^2 + |a_3|^2 + |a_4|^2 + |a_5|^2 + |a_6|^2 + |a_7|^2 = 1,$$

справедливо равенство:

$$\begin{aligned}V\left(|\psi\rangle\right) = 2\cdot\min\Big\{&\Big(|a_0a_5 - a_1a_4|^2 + |a_0a_6 - a_2a_4|^2 + |a_0a_7 - a_3a_4|^2 + \\ &+ |a_1a_6 - a_2a_5|^2 + |a_1a_7 - a_3a_5|^2 + |a_2a_7 - a_3a_6|^2\Big)^{\frac{1}{2}}, \\ &\Big(|a_0a_3 - a_1a_2|^2 + |a_0a_6 - a_2a_4|^2 + |a_0a_7 - a_2a_5|^2 + \\ &+ |a_1a_6 - a_3a_4|^2 + |a_1a_7 - a_3a_5|^2 + |a_4a_7 - a_5a_6|^2\Big)^{\frac{1}{2}}, \\ &\Big(|a_0a_5 - a_1a_4|^2 + |a_0a_3 - a_1a_2|^2 + |a_0a_7 - a_1a_6|^2 + \\ &+ |a_3a_4 - a_2a_5|^2 + |a_4a_7 - a_5a_6|^2 + |a_2a_7 - a_3a_6|^2\Big)^{\frac{1}{2}}\Big\}.\end{aligned}$$

5. Для произвольного состояния четырехкубитной квантовой системы получено выражение значения **V-меры** через амплитуды состояния в вычислительном базисе.

ГЛАВА 5

Стационарные состояния спиновых квантовых систем в постоянном магнитном поле и мера их несепарабельности

Введение к главе 5

Глава 5 состоит из трёх параграфов и посвящена исследованию двухкубитных, трёхкубитных и четырёхкубитных квантовых систем, состоящих из кубитов-спинов-½ с одним и тем же гиромагнитным отношением и находящихся в постоянном магнитном поле.

Вычислены стационарные состояния указанных квантовых систем и соответствующие им уровни энергии.

Для стационарных состояний исследованы следующие вопросы:

- разложимости и неразложимости в тензорное произведение состояний меньшей размерности, чем размерность исходного состояния;
- сепарабельности и несепарабельности;
- вычисления меры несепарабельности стационарных состояний.

Главная задача, решаемая в данной главе, состоит в исследовании ресурса несепарабельности относительно стационарных состояний квантовых систем, достаточно широко и глубоко изучаемых в физической науке. Это позволит проиллюстрировать реалистичность, в определённом смысле, ресурса несепарабельности как нового ресурса для приложений в области информационных и телекоммуникационных технологий.

Более конкретно материал по решению указанной выше задачи распределён по параграфам следующим образом.

В параграфе 5.1 исследуется квантовая система AB, которая состоит из двух кубитов-спинов-½ A и B с одним и тем же гиромагнитным отношением ν и находится в постоянном внешнем магнитном поле.

В параграфе 5.2 исследуется квантовая система ABC, которая состоит из трёх кубитов-спинов-½ A, B и C с одним и тем же гиромагнитным отношением ν и находится в постоянном внешнем магнитном поле.

В параграфе 5.3 исследуется квантовая система ABCD, которая состоит из четырёх кубитов-спинов-½ A, B, C и D с одним и тем же гиромагнитным отношением ν и находится в постоянном внешнем магнитном поле.

Материал, представленный в разных параграфах, отличается не только числом кубитов в квантовой системе. Картина распределения меры несепарабельности изменяется при переходе от одного параграфа к другому как количественно, так и в принципиально качественном плане. Так, например, в параграфе 5.1 для двухкубитных систем свойство несепарабельности стационарного состояния равносильно неразложимости состояния в тензорное произведение состояний меньшей размерности, чем размерность исходного состояния. Однако при переходе к параграфам 5.2 и 5.3 можно указать стационарные состояния, которые неразложимы в тензорное произведение состояний меньшей размерности, чем размерность исходного состояния, но тем не менее являются сепарабельными состояниями.

§ 5.1. Стационарные состояния квантовой системы, состоящей из двух кубитов-спинов-½, и значения их V-меры

Рассмотрим квантовую систему AB из двух кубитов-спинов-½ A и B с одним и тем же гиромагнитным отношением ν, находящуюся в постоянном внешнем магнитном поле с вектором магнитной индукции $\mathbf{M}$, направленным по оси Z, то есть $\mathbf{M} = (0, 0, M)$, где M – модуль вектора магнитной индукции, $M \geq 0$. J – константа взаимодействия в квантовой системе AB [16; 42; 50].

Утверждение 5.1.1. Квантовая система AB имеет следующие стационарные состояния:

$$\left|\psi_1^{(2)}\right\rangle = |11\rangle e^{-\left(\frac{i}{\hbar}\right)E_1 t}, \ \left|\psi_2^{(2)}\right\rangle = |00\rangle e^{-\left(\frac{i}{\hbar}\right)E_2 t},$$

$$\left|\psi_3^{(2)}\right\rangle = \left(\frac{|01\rangle + |10\rangle}{\sqrt{2}}\right) e^{-\left(\frac{i}{\hbar}\right)E_3 t}, \ \left|\psi_4^{(2)}\right\rangle = \left(\frac{|01\rangle - |10\rangle}{\sqrt{2}}\right) e^{-\left(\frac{i}{\hbar}\right)E_4 t}, \quad (5.1.2)$$

где

$$E_1 = \left(\frac{J}{4} + \omega\right)\hbar, \ E_2 = \left(\frac{J}{4} - \omega\right)\hbar, \ E_3 = \frac{J}{4}\hbar, \ E_4 = -\frac{3J}{4}\hbar, \quad (5.1.3)$$

ω – резонансная частота каждого из спинов A и B, $\omega = \nu M$; E_k – энергия стационарного состояния $\left|\psi_k^{(2)}\right\rangle$, $k \in \{1, 2, 3, 4\}$, t – время, $\hbar$ – приведённая постоянная Планка, $i = \sqrt{-1}$ – мнимая единица.

Доказательство утверждения 5.1.1 приведём ниже в этом параграфе. Перед этим отметим:

а) состояния $\left|\psi_1^{(2)}\right\rangle$ и $\left|\psi_2^{(2)}\right\rangle$ являются сепарабельными состояниями квантовой системы AB и, как следует из утверждения 4.4.10, имеют нулевое значение **V-меры**, то есть

$$V\left(\left|\psi_1^{(2)}\right\rangle\right) = V\left(\left|\psi_2^{(2)}\right\rangle\right) = 0;$$

б) состояния $\left|\psi_3^{(2)}\right\rangle$ и $\left|\psi_4^{(2)}\right\rangle$ являются несепарабельными состояниями квантовой системы AB и в соответствии со следствием 4.4.12 и равенством (4.3.8) для значений **V-меры** этих состояний справедливы равенства:

$$V\left(\left|\psi_3^{(2)}\right\rangle\right) = 2 \cdot \left| 0 \cdot 0 - \frac{1}{\sqrt{2}} e^{-\left(\frac{i}{\hbar}\right)E_3 t} \cdot \frac{1}{\sqrt{2}} e^{-\left(\frac{i}{\hbar}\right)E_3 t} \right| = 1,$$

$$V\left(\left|\psi_4^{(2)}\right\rangle\right) = 2 \cdot \left| 0 \cdot 0 - \frac{1}{\sqrt{2}} e^{-\left(\frac{i}{\hbar}\right)E_4 t} \cdot \left(-\frac{1}{\sqrt{2}}\right) e^{-\left(\frac{i}{\hbar}\right)E_4 t} \right| = 1.$$

Таким образом, среди стационарных состояний рассматриваемой квантовой системы AB имеются сепарабельные состояния и несепарабельные состояния, причём несепарабельные состояния имеют максимальное значение **V-меры** и неразложимы в тензорное произведение состояний кубитов A и B. А сепарабельные состояния разложимы в тензорное произведение состояний кубитов A и B. Полученные результаты находятся в полном согласии с тем фактом, что в случае двухкубитной квантовой системы условие неразложимости состояния в тензорное произведение состояний её однокубитных подсистем равносильно условию несепарабельности состояния.

Докажем теперь, что равенства (5.1.2) и (5.1.3) задают для квантовой системы AB стационарные состояния и соответствующие им уровни энергии, то есть докажем утверждение 5.1.1.

Для гамильтониана $\mathbf{H}_2$ обсуждаемой квантовой системы справедливо равенство [42; 50; 54; 57]:

$$\mathbf{H}_2 = \hbar \cdot J\left(\frac{1}{2}\sigma_{\mathbf{X}} \otimes \frac{1}{2}\sigma_{\mathbf{X}} + \frac{1}{2}\sigma_{\mathbf{Y}} \otimes \frac{1}{2}\sigma_{\mathbf{Y}} + \frac{1}{2}\sigma_{\mathbf{Z}} \otimes \frac{1}{2}\sigma_{\mathbf{Z}}\right) -$$
$$-\omega\hbar\left(\frac{1}{2}\sigma_{\mathbf{Z}} \otimes \mathbf{I}_2\right) - \omega\hbar\left(\mathbf{I}_2 \otimes \frac{1}{2}\sigma_{\mathbf{Z}}\right),$$

где $\mathbf{I}_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $\sigma_{\mathbf{X}} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $\sigma_{\mathbf{Y}} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$, $\sigma_{\mathbf{Z}} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

Выполнив соответствующие вычисления, имеем

$$\mathbf{H}_2 = \begin{pmatrix} R+r & 0 & 0 & 0 \\ 0 & -R & 2R & 0 \\ 0 & 2R & -R & 0 \\ 0 & 0 & 0 & R-r \end{pmatrix}, \qquad (5.1.4)$$

где $R = \frac{1}{4}J\hbar$, $r = (-\omega\hbar)$.

Для характеристического многочлена $\chi_{\mathbf{H}_2}(\lambda)$ матрицы $\mathbf{H}_2$, заданной равенством (5.1.4), справедлива цепочка равенств

$$\chi_{\mathbf{H}_2}(\lambda) = \left|\lambda \mathbf{I}_4 - \mathbf{H}_2\right| =$$
$$= (\lambda - (R + r))(\lambda - (R - r))(\lambda - R)(\lambda - (-3R)), \qquad (5.1.5)$$

где $\mathbf{I}_4$ – единичная матрица размера 4×4 [37], $\left|\lambda \mathbf{I}_4 - \mathbf{H}_2\right|$ – определитель матрицы $\lambda \mathbf{I}_4 - \mathbf{H}_2$.

Решив уравнение

$$\chi_{\mathbf{H}_2}(\lambda) = 0,$$

находим следующие собственные значения матрицы $\mathbf{H}_2$:

$$\lambda_1 = R + r = \left(\frac{J}{4} - \omega\right)\hbar, \; \lambda_2 = R - r = \left(\frac{J}{4} + \omega\right)\hbar,$$
$$\lambda_3 = R = \frac{J}{4}\hbar, \; \lambda_4 = -3R = -\frac{3J}{4}\hbar. \qquad (5.1.6)$$

Так как $E_k = \lambda_k$ ($k \in \{1, 2, 3, 4\}$) [47], то из (5.1.6) следует справедливость равенств (5.1.3) для уровней энергии стационарных состояний квантовой системы AB.

Далее, проверив для каждого $k \in \{1, 2, 3, 4\}$ справедливость равенства

$$\mathbf{H}_2 \left|\psi_k^{(2)}\right\rangle = E_k \left|\psi_k^{(2)}\right\rangle$$

с учётом свойств и аналитической формы стационарного состояния квантовой системы [57], убеждаемся в том, что равенства (5.1.2) задают стационарные состояния квантовой системы AB. Утверждение 5.1.1 полностью доказано.

§ 5.2. Стационарные состояния квантовой системы, состоящей из трёх кубитов-спинов-½, и значения их V-меры

Рассмотрим квантовую систему ABC из трёх кубитов-спинов-½ A, B и C с одним и тем же гиромагнитным отношением ν, находящуюся в постоянном внешнем магнитном поле с вектором магнитной индукции

M, направленным по оси Z, то есть $\mathbf{M} = (0,\ 0,\ M)$, где M – модуль вектора магнитной индукции, $M \geq 0$. J – константа взаимодействия в квантовой системе АВС [16; 50].

Утверждение 5.2.1. Квантовая система АВС имеет следующие 6 уровней энергии, соответствующие стационарным состояниям:

$$E_1 = \left(\frac{3J}{4} - \frac{3\omega}{2}\right)\hbar,\ E_2 = \left(\frac{3J}{4} + \frac{3\omega}{2}\right)\hbar,\ E_3 = \left(\frac{3J}{4} + \frac{\omega}{2}\right)\hbar,$$

$$E_4 = \left(-\frac{3J}{4} + \frac{\omega}{2}\right)\hbar,\ E_5 = \left(\frac{3J}{4} - \frac{\omega}{2}\right)\hbar,\ E_6 = \left(-\frac{3J}{4} - \frac{\omega}{2}\right)\hbar,$$

где ω – резонансная частота каждого из спинов А, В и С, $\omega = \nu M$; $\hbar$ – приведённая постоянная Планка, $i = \sqrt{-1}$ – мнимая единица. При этом уровни энергии E_1, E_2, E_3 и E_5 являются невырожденными уровнями энергии, а E_4 и E_6 являются двукратно вырожденными уровнями энергии.

Утверждение 5.2.2. В качестве стационарных состояний квантовой системы АВС можно указать следующие состояния:

- стационарные состояния

$$\left|\psi_1^{(3)}\right\rangle = |000\rangle e^{-\left(\frac{i}{\hbar}\right)E_1 t},\ \left|\psi_2^{(3)}\right\rangle = |111\rangle e^{-\left(\frac{i}{\hbar}\right)E_2 t},$$

$$\left|\psi_3^{(3)}\right\rangle = \left(\frac{1}{\sqrt{3}}|011\rangle + \frac{1}{\sqrt{3}}|101\rangle + \frac{1}{\sqrt{3}}|110\rangle\right)e^{-\left(\frac{i}{\hbar}\right)E_3 t} \quad \text{и}$$

$$\left|\psi_5^{(3)}\right\rangle = \left(\frac{1}{\sqrt{3}}|001\rangle + \frac{1}{\sqrt{3}}|010\rangle + \frac{1}{\sqrt{3}}|100\rangle\right)e^{-\left(\frac{i}{\hbar}\right)E_5 t}$$

соответствуют невырожденным уровням энергии E_1, E_2, E_3 и E_5;

- стационарные состояния

$$\left|\psi_{41}^{(3)}\right\rangle = \left(-\frac{1}{\sqrt{2}}|011\rangle + \frac{1}{\sqrt{2}}|110\rangle\right)e^{-\left(\frac{i}{\hbar}\right)E_4 t},$$

$$\left|\psi_{42}^{(3)}\right\rangle = \left(-\frac{1}{\sqrt{6}}|011\rangle + \frac{2}{\sqrt{6}}|101\rangle - \frac{1}{\sqrt{6}}|110\rangle\right)e^{-\left(\frac{i}{\hbar}\right)E_4 t}$$

соответствуют двукратно вырожденному уровню энергии E_4;

- стационарные состояния

$$\left|\psi_{61}^{(3)}\right\rangle = \left(\frac{1}{\sqrt{2}}|001\rangle - \frac{1}{\sqrt{2}}|100\rangle\right)e^{-\left(\frac{i}{\hbar}\right)E_6 t},$$

$$\left|\psi_{62}^{(3)}\right\rangle = \left(\frac{1}{\sqrt{6}}|001\rangle - \frac{2}{\sqrt{6}}|010\rangle + \frac{1}{\sqrt{6}}|100\rangle\right)e^{-\left(\frac{i}{\hbar}\right)E_6 t}$$

соответствуют двукратно вырожденному уровню энергии E_6.

Доказательство справедливости утверждений 5.2.1 и 5.2.2 приведём ниже в этом параграфе. Перед этим отметим:

а) применив **критерий К₃** (см. пункт 5 выводов по главе 2) к стационарным состояниям $\left|\psi_1^{(3)}\right\rangle$, $\left|\psi_2^{(3)}\right\rangle$, $\left|\psi_{41}^{(3)}\right\rangle$ и $\left|\psi_{61}^{(3)}\right\rangle$ квантовой системы ABC, можно установить, что эти состояния являются **сепарабельными** состояниями; сепарабельные состояния $\left|\psi_1^{(3)}\right\rangle$ и $\left|\psi_2^{(3)}\right\rangle$ **разложимы** в тензорное произведение состояний однокубитных подсистем A, B и C квантовой системы ABC, а сепарабельные состояния $\left|\psi_{41}^{(3)}\right\rangle$ и $\left|\psi_{61}^{(3)}\right\rangle$ **неразложимы** в тензорное произведение состояний размерностей меньших, чем 8 (это вытекает из следствия 2.3.5 утверждения 2.3.4);

б) применив **критерий К₃** (см. пункт 5 выводов по главе 2) к стационарным состояниям$\left|\psi_3^{(3)}\right\rangle$, $\left|\psi_{42}^{(3)}\right\rangle$, $\left|\psi_5^{(3)}\right\rangle$ и $\left|\psi_{62}^{(3)}\right\rangle$ квантовой системы ABC, можно установить, что эти состояния являются **несепарабельными** состояниями;

в) использовав формулу, приведённую в утверждении 4.5.3 для значений **V-меры** трёхкубитных квантовых систем, для вычисления **V-меры** стационарных состояний квантовой системы ABC, получим:

$$V\left(\left|\psi_1^{(3)}\right\rangle\right) = V\left(\left|\psi_2^{(3)}\right\rangle\right) = V\left(\left|\psi_{41}^{(3)}\right\rangle\right) = V\left(\left|\psi_{61}^{(3)}\right\rangle\right) = 0;$$

$$V\left(\left|\psi_3^{(3)}\right\rangle\right)=\frac{2\sqrt{2}}{3};$$

$$V\left(\left|\psi_{42}^{(3)}\right\rangle\right)=\frac{\sqrt{5}}{3};$$

$$V\left(\left|\psi_5^{(3)}\right\rangle\right)=\frac{2\sqrt{2}}{3};$$

$$V\left(\left|\psi_{62}^{(3)}\right\rangle\right)=\frac{\sqrt{5}}{3}.$$

Докажем теперь справедливость утверждения 5.2.1.

Для гамильтониана $\mathbf{H}_3$ квантовой системы ABC справедливо равенство [50; 57]:

$$\mathbf{H}_3=\hbar\cdot J\left(\frac{1}{2}\sigma_{\mathbf{X}}\otimes\frac{1}{2}\sigma_{\mathbf{X}}\otimes\mathbf{I}_2+\frac{1}{2}\sigma_{\mathbf{Y}}\otimes\frac{1}{2}\sigma_{\mathbf{Y}}\otimes\mathbf{I}_2+\frac{1}{2}\sigma_{\mathbf{Z}}\otimes\frac{1}{2}\sigma_{\mathbf{Z}}\otimes\mathbf{I}_2+\right.$$

$$+\frac{1}{2}\sigma_{\mathbf{X}}\otimes\mathbf{I}_2\otimes\frac{1}{2}\sigma_{\mathbf{X}}+\frac{1}{2}\sigma_{\mathbf{Y}}\otimes\mathbf{I}_2\otimes\frac{1}{2}\sigma_{\mathbf{Y}}+\frac{1}{2}\sigma_{\mathbf{Z}}\otimes\mathbf{I}_2\otimes\frac{1}{2}\sigma_{\mathbf{Z}}+$$

$$\left.+\mathbf{I}_2\otimes\frac{1}{2}\sigma_{\mathbf{X}}\otimes\frac{1}{2}\sigma_{\mathbf{X}}+\mathbf{I}_2\otimes\frac{1}{2}\sigma_{\mathbf{Y}}\otimes\frac{1}{2}\sigma_{\mathbf{Y}}+\mathbf{I}_2\otimes\frac{1}{2}\sigma_{\mathbf{Z}}\otimes\frac{1}{2}\sigma_{\mathbf{Z}}\right)-$$

$$-\omega\hbar\left(\frac{1}{2}\sigma_{\mathbf{Z}}\otimes\mathbf{I}_2\otimes\mathbf{I}_2\right)-\omega\hbar\left(\mathbf{I}_2\otimes\frac{1}{2}\sigma_{\mathbf{Z}}\otimes\mathbf{I}_2\right)-\omega\hbar\left(\mathbf{I}_2\otimes\mathbf{I}_2\otimes\frac{1}{2}\sigma_{\mathbf{Z}}\right),\quad(5.2.3)$$

где $\mathbf{I}_2=\begin{pmatrix}1&0\\0&1\end{pmatrix}$, $\sigma_{\mathbf{X}}=\begin{pmatrix}0&1\\1&0\end{pmatrix}$, $\sigma_{\mathbf{Y}}=\begin{pmatrix}0&-i\\i&0\end{pmatrix}$, $\sigma_{\mathbf{Z}}=\begin{pmatrix}1&0\\0&-1\end{pmatrix}$.

Выполнив соответствующие вычисления, из (5.2.3) имеем

$$\mathbf{H}_3=$$

$$\begin{pmatrix}
3R+3r&0&0&0&0&0&0&0\\
0&-R+r&2R&0&2R&0&0&0\\
0&2R&-R+r&0&2R&0&0&0\\
0&0&0&-R-r&0&2R&2R&0\\
0&2R&2R&0&-R+r&0&0&0\\
0&0&0&2R&0&-R-r&2R&0\\
0&0&0&2R&0&2R&-R-r&0\\
0&0&0&0&0&0&0&3R-3r
\end{pmatrix},\quad(5.2.4)$$

где $R=\frac{1}{4}J\hbar$, $r=\left(-\frac{1}{2}\omega\hbar\right)$.

Для характеристического многочлена $\chi_{\mathbf{H}_3}(\lambda)$ матрицы $\mathbf{H}_3$, заданной равенством (5.2.4), справедливо равенство

$$\chi_{\mathbf{H}_3}(\lambda)=\left|\lambda\mathbf{I}_8-\mathbf{H}_3\right|=$$
$$=(\lambda-(3R+3r))(\lambda-(3R-3r))(\lambda-(3R-r))\cdot$$
$$\cdot(\lambda-(-3R-r))^2(\lambda-(3R+r))(\lambda-(-3R+r))^2,$$

где $\mathbf{I}_8$ – единичная матрица размера 8×8 [37], $\left|\lambda\mathbf{I}_8-\mathbf{H}_3\right|$ – определитель матрицы $\lambda\mathbf{I}_8-\mathbf{H}_3$.

Решив уравнение

$$\chi_{\mathbf{H}_3}(\lambda)=0,$$

находим следующие собственные значения матрицы $\mathbf{H}_3$:

$$\lambda_1=3R+3r=\left(\frac{3J}{4}-\frac{3\omega}{2}\right)\hbar,\quad \lambda_2=3R-3r=\left(\frac{3J}{4}+\frac{3\omega}{2}\right)\hbar,$$
$$\lambda_3=3R-r=\left(\frac{3J}{4}+\frac{\omega}{2}\right)\hbar,\quad \lambda_{4,5}=-3R-r=\left(-\frac{3J}{4}+\frac{\omega}{2}\right)\hbar,$$
$$\lambda_6=3R+r=\left(\frac{3J}{4}-\frac{\omega}{2}\right)\hbar,\quad \lambda_{7,8}=-3R+r=\left(-\frac{3J}{4}-\frac{\omega}{2}\right)\hbar. \qquad (5.2.5)$$

Так как собственные значения гамильтониана равны уровням энергии стационарных состояний [47], то из (5.2.5) следует справедливость утверждения 5.2.1.

Докажем справедливость утверждения 5.2.2. Проверив для каждого $k\in\{1,\ 2,\ 3,\ 5\}$ выполнимость равенства

$$\mathbf{H}_3\left|\psi_k^{(3)}\right\rangle=E_k\left|\psi_k^{(3)}\right\rangle,$$

а также проверив выполнимость равенств

$$\mathbf{H}_3\left|\psi_{41}^{(3)}\right\rangle = E_4\left|\psi_{41}^{(3)}\right\rangle,\ \mathbf{H}_3\left|\psi_{42}^{(3)}\right\rangle = E_4\left|\psi_{42}^{(3)}\right\rangle,$$

$$\mathbf{H}_3\left|\psi_{61}^{(3)}\right\rangle = E_6\left|\psi_{61}^{(3)}\right\rangle,\ \mathbf{H}_3\left|\psi_{62}^{(3)}\right\rangle = E_6\left|\psi_{62}^{(3)}\right\rangle,$$

с учётом свойств и аналитической формы стационарного состояния квантовой системы [57], убеждаемся в справедливости утверждения 5.2.2.

§ 5.3. Стационарные состояния квантовой системы, состоящей из четырёх кубитов-спинов-½, и значения их V-меры

Рассмотрим квантовую систему ABCD из четырёх кубитов-спинов-½ A, B, Cи D с одним и тем же гиромагнитным отношением ν, находящуюся в постоянном внешнем магнитном поле с вектором магнитной индукции **M**, направленным по оси Z, то есть $\mathbf{M} = (0,\ 0,\ M)$, где M – модуль вектора магнитной индукции, $M \geq 0$. J – константа взаимодействия в квантовой системе ABCD [50].

Утверждение 5.3.1. Квантовая система ABCD имеет следующие 9 уровней энергии, соответствующие стационарным состояниям:

$$E_1 = \left(\frac{3J}{2} - 2\omega\right)\hbar,\ E_2 = \left(\frac{3J}{2} - \omega\right)\hbar,\ E_3 = \left(\frac{3J}{2} + \omega\right)\hbar,$$

$$E_4 = \frac{3J}{2}\hbar,\ E_5 = \left(\frac{3J}{2} + 2\omega\right)\hbar,\ E_6 = -\frac{J}{2}\hbar,$$

$$E_7 = \left(-\frac{J}{2} - \omega\right)\hbar,\ E_8 = \left(-\frac{J}{2} + \omega\right)\hbar,\ E_9 = -\frac{3J}{2}\hbar,$$

где ω – резонансная частота каждого из спинов A, B, C и D, $\omega = \nu M$; $\hbar$ – приведённая постоянная Планка, $i = \sqrt{-1}$ – мнимая единица. При этом уровни E_1, E_2, E_3, E_4 и E_5 являются невырожденными уровнями энергии, уровни E_6, E_7 и E_8 являются трёхкратно вырожденными уровнями энергии, а E_9 – двукратно вырожденным уровнем энергии.

Утверждение 5.3.2. В качестве стационарных состояний квантовой системы ABCD можно указать следующие состояния:

- стационарные состояния

$$\left|\psi_1^{(4)}\right\rangle = |0000\rangle e^{-\left(\frac{i}{\hbar}\right)E_1 t},$$

$$\left|\psi_2^{(4)}\right\rangle = \left(\frac{1}{2}|0001\rangle + \frac{1}{2}|0010\rangle + \frac{1}{2}|0100\rangle + \frac{1}{2}|1000\rangle\right) e^{-\left(\frac{i}{\hbar}\right)E_2 t},$$

$$\left|\psi_3^{(4)}\right\rangle = \left(\frac{1}{2}|0111\rangle + \frac{1}{2}|1011\rangle + \frac{1}{2}|1101\rangle + \frac{1}{2}|1110\rangle\right) e^{-\left(\frac{i}{\hbar}\right)E_3 t},$$

$$\left|\psi_4^{(4)}\right\rangle = \left(\frac{1}{\sqrt{6}}|0011\rangle + \frac{1}{\sqrt{6}}|0101\rangle + \frac{1}{\sqrt{6}}|0110\rangle +\right.$$

$$\left. + \frac{1}{\sqrt{6}}|1001\rangle + \frac{1}{\sqrt{6}}|1010\rangle + \frac{1}{\sqrt{6}}|1100\rangle\right) e^{-\left(\frac{i}{\hbar}\right)E_4 t},$$

$$\left|\psi_5^{(4)}\right\rangle = |1111\rangle e^{-\left(\frac{i}{\hbar}\right)E_5 t}$$

соответствуют невырожденным уровням энергии E_1, E_2, E_3, E_4 и E_5;

- стационарные состояния

$$\left|\psi_{61}^{(4)}\right\rangle = \left(\frac{1}{\sqrt{2}}|0011\rangle - \frac{1}{\sqrt{2}}|1100\rangle\right) e^{-\left(\frac{i}{\hbar}\right)E_6 t},$$

$$\left|\psi_{62}^{(4)}\right\rangle = \left(\frac{1}{\sqrt{2}}|0101\rangle - \frac{1}{\sqrt{2}}|1010\rangle\right) e^{-\left(\frac{i}{\hbar}\right)E_6 t},$$

$$\left|\psi_{63}^{(4)}\right\rangle = \left(\frac{1}{\sqrt{2}}|0110\rangle - \frac{1}{\sqrt{2}}|1001\rangle\right) e^{-\left(\frac{i}{\hbar}\right)E_6 t}$$

соответствуют трёхкратно вырожденному уровню энергии E_6;

- стационарные состояния

$$\left|\psi_{71}^{(4)}\right\rangle = \left(\frac{1}{\sqrt{2}}|0001\rangle - \frac{1}{\sqrt{2}}|1000\rangle\right) e^{-\left(\frac{i}{\hbar}\right)E_7 t},$$

$$\left|\psi_{72}^{(4)}\right\rangle = \left(\frac{1}{\sqrt{2}}|0010\rangle - \frac{1}{\sqrt{2}}|0100\rangle\right)e^{-\left(\frac{i}{\hbar}\right)E_7 t},$$

$$\left|\psi_{73}^{(4)}\right\rangle = \left(\frac{1}{2}|0001\rangle - \frac{1}{2}|0010\rangle - \frac{1}{2}|0100\rangle + \frac{1}{2}|1000\rangle\right)e^{-\left(\frac{i}{\hbar}\right)E_7 t}$$

соответствуют трёхкратно вырожденному уровню энергии E_7;

- стационарные состояния

$$\left|\psi_{81}^{(4)}\right\rangle = \left(\frac{1}{\sqrt{2}}|0111\rangle - \frac{1}{\sqrt{2}}|1110\rangle\right)e^{-\left(\frac{i}{\hbar}\right)E_8 t},$$

$$\left|\psi_{82}^{(4)}\right\rangle = \left(\frac{1}{\sqrt{2}}|1011\rangle - \frac{1}{\sqrt{2}}|1101\rangle\right)e^{-\left(\frac{i}{\hbar}\right)E_8 t},$$

$$\left|\psi_{83}^{(4)}\right\rangle = \left(\frac{1}{2}|0111\rangle - \frac{1}{2}|1011\rangle - \frac{1}{2}|1101\rangle + \frac{1}{2}|1110\rangle\right)e^{-\left(\frac{i}{\hbar}\right)E_8 t}$$

соответствуют трёхкратно вырожденному уровню энергии E_8;

- стационарные состояния

$$\left|\psi_{91}^{(4)}\right\rangle = \left(\frac{1}{\sqrt{12}}|0011\rangle - \frac{2}{\sqrt{12}}|0101\rangle + \frac{1}{\sqrt{12}}|0110\rangle + \right.$$

$$\left. + \frac{1}{\sqrt{12}}|1001\rangle - \frac{2}{\sqrt{12}}|1010\rangle + \frac{1}{\sqrt{12}}|1100\rangle\right)e^{-\left(\frac{i}{\hbar}\right)E_9 t},$$

$$\left|\psi_{92}^{(4)}\right\rangle = \left(\frac{1}{2}|0011\rangle - \frac{1}{2}|0110\rangle - \frac{1}{2}|1001\rangle + \frac{1}{2}|1100\rangle\right)e^{-\left(\frac{i}{\hbar}\right)E_9 t}$$

соответствуют двукратно вырожденному уровню энергии E_9.

К вопросу доказательства справедливости утверждений 5.3.1 и 5.3.2 обратимся ниже в этом параграфе. Перед этим отметим:

а) применив **критерий К$_4$** (см. утверждение 2.6.4) к стационарным состояниям $\left|\psi_1^{(4)}\right\rangle$, $\left|\psi_5^{(4)}\right\rangle$, $\left|\psi_{71}^{(4)}\right\rangle$, $\left|\psi_{72}^{(4)}\right\rangle$, $\left|\psi_{81}^{(4)}\right\rangle$, $\left|\psi_{82}^{(4)}\right\rangle$ и $\left|\psi_{92}^{(4)}\right\rangle$ квантовой системы ABCD, можно установить, что эти состояния являются

сепарабельными состояниями; сепарабельные состояния $\left|\psi_1^{(4)}\right\rangle$, $\left|\psi_5^{(4)}\right\rangle$, $\left|\psi_{72}^{(4)}\right\rangle$ и $\left|\psi_{82}^{(4)}\right\rangle$ **разложимы** в тензорное произведение состояний размерностей меньших, чем 16, а сепарабельные состояния $\left|\psi_{71}^{(4)}\right\rangle$, $\left|\psi_{81}^{(4)}\right\rangle$ и $\left|\psi_{92}^{(4)}\right\rangle$ **неразложимы** в тензорное произведение состояний размерностей меньших, чем 16 (это вытекает из утверждения 2.6.3);

б) применив **критерий К₄** (см. утверждение 2.6.4) к стационарным состояниям $\left|\psi_2^{(4)}\right\rangle$, $\left|\psi_3^{(4)}\right\rangle$, $\left|\psi_4^{(4)}\right\rangle$, $\left|\psi_{61}^{(4)}\right\rangle$, $\left|\psi_{62}^{(4)}\right\rangle$, $\left|\psi_{63}^{(4)}\right\rangle$, $\left|\psi_{73}^{(4)}\right\rangle$, $\left|\psi_{83}^{(4)}\right\rangle$ и $\left|\psi_{91}^{(4)}\right\rangle$ квантовой системы ABCD, можно установить, что эти состояния являются **несепарабельными** состояниями;

в) использовав формулу, приведённую в утверждении 4.6.3 для значений **V-меры** четырёхкубитных квантовых систем, для вычисления **V-меры** стационарных состояний квантовой системы ABCD, получим:

$$V\left(\left|\psi_1^{(4)}\right\rangle\right) = V\left(\left|\psi_5^{(4)}\right\rangle\right) = V\left(\left|\psi_{71}^{(4)}\right\rangle\right) = V\left(\left|\psi_{72}^{(4)}\right\rangle\right) =$$

$$= V\left(\left|\psi_{81}^{(4)}\right\rangle\right) = V\left(\left|\psi_{82}^{(4)}\right\rangle\right) = V\left(\left|\psi_{92}^{(4)}\right\rangle\right) = 0,$$

$$V\left(\left|\psi_2^{(4)}\right\rangle\right) = V\left(\left|\psi_3^{(4)}\right\rangle\right) = V\left(\left|\psi_4^{(4)}\right\rangle\right) = V\left(\left|\psi_{61}^{(4)}\right\rangle\right) =$$

$$= V\left(\left|\psi_{62}^{(4)}\right\rangle\right) = V\left(\left|\psi_{63}^{(4)}\right\rangle\right) = V\left(\left|\psi_{73}^{(4)}\right\rangle\right) = V\left(\left|\psi_{83}^{(4)}\right\rangle\right) = \sqrt{\frac{2}{3}},$$

$$V\left(\left|\psi_{91}^{(4)}\right\rangle\right) = \frac{\sqrt{5}}{3}.$$

Докажем теперь справедливость утверждения 5.3.1.

Для гамильтониана $\mathbf{H}_4$ квантовой системы ABCD справедливо равенство [50; 57]:

$$\mathbf{H}_4 = \hbar \cdot J \cdot$$

$$\cdot\left(\frac{1}{2}\sigma_\mathbf{X} \otimes \frac{1}{2}\sigma_\mathbf{X} \otimes \mathbf{I}_2 \otimes \mathbf{I}_2 + \frac{1}{2}\sigma_\mathbf{Y} \otimes \frac{1}{2}\sigma_\mathbf{Y} \otimes \mathbf{I}_2 \otimes \mathbf{I}_2 + \frac{1}{2}\sigma_\mathbf{Z} \otimes \frac{1}{2}\sigma_\mathbf{Z} \otimes \mathbf{I}_2 \otimes \mathbf{I}_2 +\right.$$

$$+\frac{1}{2}\sigma_{\mathbf{X}}\otimes\mathbf{I}_2\otimes\frac{1}{2}\sigma_{\mathbf{X}}\otimes\mathbf{I}_2+\frac{1}{2}\sigma_{\mathbf{Y}}\otimes\mathbf{I}_2\otimes\frac{1}{2}\sigma_{\mathbf{Y}}\otimes\mathbf{I}_2+\frac{1}{2}\sigma_{\mathbf{Z}}\otimes\mathbf{I}_2\otimes\frac{1}{2}\sigma_{\mathbf{Z}}\otimes\mathbf{I}_2+$$

$$+\frac{1}{2}\sigma_{\mathbf{X}}\otimes\mathbf{I}_2\otimes\mathbf{I}_2\otimes\frac{1}{2}\sigma_{\mathbf{X}}+\frac{1}{2}\sigma_{\mathbf{Y}}\otimes\mathbf{I}_2\otimes\mathbf{I}_2\otimes\frac{1}{2}\sigma_{\mathbf{Y}}+\frac{1}{2}\sigma_{\mathbf{Z}}\otimes\mathbf{I}_2\otimes\mathbf{I}_2\otimes\frac{1}{2}\sigma_{\mathbf{Z}}+$$

$$+\mathbf{I}_2\otimes\frac{1}{2}\sigma_{\mathbf{X}}\otimes\frac{1}{2}\sigma_{\mathbf{X}}\otimes\mathbf{I}_2+\mathbf{I}_2\otimes\frac{1}{2}\sigma_{\mathbf{Y}}\otimes\frac{1}{2}\sigma_{\mathbf{Y}}\otimes\mathbf{I}_2+\mathbf{I}_2\otimes\frac{1}{2}\sigma_{\mathbf{Z}}\otimes\frac{1}{2}\sigma_{\mathbf{Z}}\otimes\mathbf{I}_2+$$

$$+\mathbf{I}_2\otimes\frac{1}{2}\sigma_{\mathbf{X}}\otimes\mathbf{I}_2\otimes\frac{1}{2}\sigma_{\mathbf{X}}+\mathbf{I}_2\otimes\frac{1}{2}\sigma_{\mathbf{Y}}\otimes\mathbf{I}_2\otimes\frac{1}{2}\sigma_{\mathbf{Y}}+\mathbf{I}_2\otimes\frac{1}{2}\sigma_{\mathbf{Z}}\otimes\mathbf{I}_2\otimes\frac{1}{2}\sigma_{\mathbf{Z}}+$$

$$\left.+\mathbf{I}_2\otimes\mathbf{I}_2\otimes\frac{1}{2}\sigma_{\mathbf{X}}\otimes\frac{1}{2}\sigma_{\mathbf{X}}+\mathbf{I}_2\otimes\mathbf{I}_2\otimes\frac{1}{2}\sigma_{\mathbf{Y}}\otimes\frac{1}{2}\sigma_{\mathbf{Y}}+\mathbf{I}_2\otimes\mathbf{I}_2\otimes\frac{1}{2}\sigma_{\mathbf{Z}}\otimes\frac{1}{2}\sigma_{\mathbf{Z}}\right)-$$

$$-\omega\hbar\left(\frac{1}{2}\sigma_{\mathbf{Z}}\otimes\mathbf{I}_2\otimes\mathbf{I}_2\otimes\mathbf{I}_2\right)-\omega\hbar\left(\mathbf{I}_2\otimes\frac{1}{2}\sigma_{\mathbf{Z}}\otimes\mathbf{I}_2\otimes\mathbf{I}_2\right)-$$

$$-\omega\hbar\left(\mathbf{I}_2\otimes\mathbf{I}_2\otimes\frac{1}{2}\sigma_{\mathbf{Z}}\otimes\mathbf{I}_2\right)-\omega\hbar\left(\mathbf{I}_2\otimes\mathbf{I}_2\otimes\mathbf{I}_2\otimes\frac{1}{2}\sigma_{\mathbf{Z}}\right), \qquad (5.3.3)$$

где $\mathbf{I}_2=\begin{pmatrix}1&0\\0&1\end{pmatrix}$, $\sigma_{\mathbf{X}}=\begin{pmatrix}0&1\\1&0\end{pmatrix}$, $\sigma_{\mathbf{Y}}=\begin{pmatrix}0&-i\\i&0\end{pmatrix}$, $\sigma_{\mathbf{Z}}=\begin{pmatrix}1&0\\0&-1\end{pmatrix}$.

Выполнив соответствующие вычисления, из (5.3.3) имеем

$$\mathbf{H}_4=$$

$$\begin{pmatrix}
3R+2r&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&r&R&0&R&0&0&0&R&0&0&0&0&0&0&0\\
0&R&r&0&R&0&0&0&R&0&0&0&0&0&0&0\\
0&0&0&-R&0&R&R&0&0&R&R&0&0&0&0&0\\
0&R&R&0&r&0&0&0&R&0&0&0&0&0&0&0\\
0&0&0&R&0&-R&R&0&0&R&0&0&R&0&0&0\\
0&0&0&R&0&R&-R&0&0&0&R&0&R&0&0&0\\
0&0&0&0&0&0&0&-r&0&0&0&R&0&R&R&0\\
0&R&R&0&R&0&0&0&r&0&0&0&0&0&0&0\\
0&0&0&R&0&R&0&0&0&-R&R&0&R&0&0&0\\
0&0&0&R&0&0&R&0&0&R&-R&0&R&0&0&0\\
0&0&0&0&0&0&0&R&0&0&0&-r&0&R&R&0\\
0&0&0&0&0&R&R&0&0&R&R&0&-R&0&0&0\\
0&0&0&0&0&0&0&R&0&0&0&R&0&-r&R&0\\
0&0&0&0&0&0&0&R&0&0&0&R&0&R&-r&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&3R-2r
\end{pmatrix}, \quad (5.3.4)$$

где $R = \frac{1}{2}J\hbar$, $r = \left(-\omega\hbar\right)$.

Для характеристического многочлена $\chi_{\mathbf{H}_4}\left(\lambda\right)$ матрицы $\mathbf{H}_4$, заданной равенством (5.3.4), справедливо равенство

$$\chi_{\mathbf{H}_4}\left(\lambda\right) = \left|\lambda\mathbf{I}_{16} - \mathbf{H}_4\right| =$$
$$= \left(\lambda - (3R+2r)\right)\left(\lambda - (3R+r)\right)\left(\lambda - 3R\right)\times$$
$$\times\left(\lambda - (3R-r)\right)\left(\lambda - (3R-2r)\right)\left(\lambda - (-R)\right)^3\times$$
$$\times\left(\lambda - (-R+r)\right)^3\left(\lambda - (-R-r)\right)^3\left(\lambda - (-3R)\right)^2,$$

где $\mathbf{I}_{16}$ – единичная матрица размера 16×16, $\left|\lambda\mathbf{I}_{16} - \mathbf{H}_4\right|$ – определитель матрицы $\lambda\mathbf{I}_{16} - \mathbf{H}_4$.

Решив уравнение

$$\chi_{\mathbf{H}_4}\left(\lambda\right) = 0,$$

находим следующие собственные значения матрицы $\mathbf{H}_4$:

$$\lambda_1 = 3R + 2r = \left(\frac{3J}{2} - 2\omega\right)\hbar,\ \lambda_2 = 3R + r = \left(\frac{3J}{2} - \omega\right)\hbar,$$

$$\lambda_3 = 3R - r = \left(\frac{3J}{2} + \omega\right)\hbar,\ \lambda_4 = 3R = \frac{3J}{2}\hbar,$$

$$\lambda_{5,6,7} = -R = -\frac{J}{2}\hbar,\ \lambda_{8,9,10} = -R + r = \left(-\frac{J}{2} - \omega\right)\hbar,$$

$$\lambda_{11,12,13} = -R - r = \left(-\frac{J}{2} + \omega\right)\hbar,\ \lambda_{14,15} = -3R = -\frac{3J}{2}\hbar,$$

$$\lambda_{16} = 3R - 2r = \left(\frac{3J}{2} + 2\omega\right)\hbar. \tag{5.3.5}$$

Так как собственные значения гамильтониана равны уровням энергии стационарных состояний [47], то из (5.3.5) следует справедливость утверждения 5.3.1.

Докажем справедливость утверждения 5.3.2. Проверив для каждого $k \in \{1,\ 2,\ 3,\ 4,\ 5\}$ выполнимость равенства

$$\mathbf{H}_4 \left|\psi_k^{(4)}\right\rangle = E_k \left|\psi_k^{(4)}\right\rangle$$

и проверив для каждого $k \in \{6,7,8\}$ выполнимость равенств

$$\mathbf{H}_4 \left|\psi_{k1}^{(4)}\right\rangle = E_k \left|\psi_{k1}^{(4)}\right\rangle,\ \mathbf{H}_4 \left|\psi_{k2}^{(4)}\right\rangle = E_k \left|\psi_{k2}^{(4)}\right\rangle,\ \mathbf{H}_4 \left|\psi_{k3}^{(4)}\right\rangle = E_k \left|\psi_{k3}^{(4)}\right\rangle,$$

а также проверив выполнимость равенств

$$\mathbf{H}_4 \left|\psi_{91}^{(4)}\right\rangle = E_9 \left|\psi_{91}^{(4)}\right\rangle,\ \mathbf{H}_4 \left|\psi_{92}^{(4)}\right\rangle = E_9 \left|\psi_{92}^{(4)}\right\rangle$$

с учётом свойств и аналитической формы стационарного состояния квантовой системы [57], убеждаемся в справедливости утверждения 5.3.2.

Выводы по главе 5

1. Установлено, что из четырёх стационарных состояний двухкубитной квантовой системы, состоящей из кубитов-спинов-½ с одним и тем же гиромагнитным отношением и находящейся в постоянном магнитном поле, два состояния являются сепарабельными и два – несепарабельными. Причём значение **V-меры** каждого из несепарабельных состояний равно максимально возможному значению – 1.

2. Установлено, что из восьми стационарных состояний трёхкубитной квантовой системы, состоящей из кубитов-спинов-½ с одним и тем же гиромагнитным отношением и находящейся в постоянном магнитном поле, четыре состояния являются сепарабельными и четыре – несепарабельными. Причём наибольшее значение **V-меры** несепарабельных состояний равно $\frac{2\sqrt{2}}{3}$, что меньше максимально возможного значения 1. Из четырёх сепарабельных стационарных состояний два со-

стояния разложимы в тензорное произведение состояний меньшей размерности, два состояния неразложимы.

3. Установлено, что из шестнадцати стационарных состояний четырёхкубитной квантовой системы, состоящей из кубитов-спинов-½ с одним и тем же гиромагнитным отношением и находящейся в постоянном магнитном поле, семь состояний являются сепарабельными, а девять – несепарабельными. Причём наибольшее значение **V-меры** несепарабельных состояний равно $\sqrt{\frac{2}{3}}$, что меньше максимально возможного значения 1 и наибольшего значения $\frac{2\sqrt{2}}{3}$ **V-меры** несепарабельных стационарных трёхкубитных состояний, рассмотренных в параграфе 5.2. Из семи сепарабельных стационарных состояний четыре состояния разложимы в тензорное произведение состояний меньшей размерности, три состояния неразложимы.

ГЛАВА 6

Протокол детерминированной квантовой связи (ATF-технология связи)

Введение к главе 6

В главе 6 разработан и представлен протокол детерминированной квантовой связи без классического канала на основе использования ресурса несепарабельных состояний многокубитных квантовых систем – **ATF-**технология связи. Здесь аббревиатура **ATF** – это первые буквы соответственно имен Александр, Татьяна и Физули в латинском написании.

Глава 6 состоит из шести параграфов.

Параграф 6.1 начинается с формулировки **гипотезы Татьяна** (или, кратко, **гипотезы T**) о свойствах двухкубитных квантовых систем, связанных с таким явлением, как квантовый фазовый переход. Обосновывается тезис о том, что квантовый фазовый переход обусловлен понижением меры несепарабельности (**V-меры**) кубитов до определенной границы, названной в данной работе **граница Ксения** или, кратко, **граница K**. Он реализуется при переходе **границы Ксения**. Указаны состояния, в которые переходит квантовая система в результате квантового фазового перехода. Показано, что **гипотезе T** не противоречат известные результаты о квантовом фазовом переходе.

В параграфе 6.2 разработан и предложен способ дистанционного изменения меры несепарабельности (**V-меры**) двухкубитных квантовых систем. Способ представлен в виде пошагово описанного **алгоритма Александр** (или, кратко, **алгоритма A**). Используются свойства трехкубитной квантовой системы в специально приготовленном состоянии, позволяющем двум из кубитов находиться после выполнения **алгоритма A** с определенными (вычисленными) вероятностями в одном из четырех состояний, где **V-мера** кубитов может быть как больше, так и меньше исходных значений меры несепарабельности каждого кубита с остальной частью трехкубитной квантовой системы.

Параграф 6.3 имеет вспомогательный характер и является дополнением к параграфу 6.2. В этом параграфе приводятся доказательства неравенств, использованных в параграфе 6.2.

В параграфе 6.4 изложен протокол детерминированной квантовой связи (под названием **ATF-**технология связи), составными компонентами которого являются способ дистанционного изменения меры несепарабельности (**V-меры**) двухкубитных квантовых систем и предположение справедливости **гипотезы Татьяна** относительно свойств двухкубитных квантовых систем, обусловленных таким физическим явлением, как квантовый фазовый переход. Связь – симплексная, с привязкой ко времени. Протокол детерминированной связи предполагает побитную передачу сообщения, представленного в двоичном виде, от одного абонента к другому, удаленному от первого в пространстве. Для передачи каждого бита используется свой отдельный массив трехкубитных квантовых систем в специальном несепарабельном состоянии, один кубит каждого из которых находится у абонента, передающего сообщение, а два других кубита – у абонента, принимающего сообщение. Действия абонента, передающего сообщение, совпадают с теми, которые представлены в известной технологии квантовой телепортации [50]. А действия абонента, принимающего сообщение, заключаются в проведении измерений над парами кубитов, которые составляют его части массивов исходных трехкубитных квантовых систем, и решении статистической задачи проверки простой гипотезы с альтернативой – также простой гипотезой. Действия абонентов разнесены во времени, то есть абонент, принимающий сообщение, начинает свои действия только после окончания действий передающей стороны, что требует предварительных временны́х договоренностей.

Параграф 6.5 посвящен задаче определения области изменения значений модулей амплитуд состояний трехкубитных квантовых систем, используемых в протоколе детерминированной квантовой связи. Данная задача возникает в связи с необходимостью обеспечения квантового фазового перехода в подходящих двухкубитных квантовых системах абонента, принимающего сообщение, после окончания действий передающей стороны.

В параграфе 6.6 рассмотрен вопрос определения значения объема выборки L по заданным значениям ошибок первого и второго рода и решение статистической задачи проверки по выборке заданного объема L простой гипотезы

$$H_0 : P(|01\rangle) = |\alpha|^2$$

с альтернативой – тоже простой гипотезой

$$H_1 : P(|01\rangle) = |\alpha|^2 + |\beta|^4 .$$

В **ATF**-технологии связи выполнение практических действий в соответствии с этим решением осуществляет абонент, принимающий сообщение, при определении каждого очередного бита сообщения.

§ 6.1. Гипотеза Т

Данный параграф начнем с формулировки гипотезы **Татьяна**, которую для краткости будем называть также гипотезой **Т**.

Гипотеза Т (**гипотеза Татьяна**). Существуют квантовая система из двух кубитов и действительное число $\alpha_{\mathrm{K}} \geq \frac{1}{\sqrt{2}}$, такие, что состояния этой квантовой системы $a|01\rangle + b|10\rangle$ и $|01\rangle$ статистически неотличимы при измерениях в вычислительном базисе из векторов $|00\rangle$, $|01\rangle$, $|10\rangle$ и $|11\rangle$ при условии, что верно неравенство $|a| > \alpha_{\mathrm{K}}$, где $a, b \in \mathbb{C}$, $|a| > |b| > 0$, $|a|^2 + |b|^2 = 1$.

Вычислительный базис из векторов $|00\rangle$, $|01\rangle$, $|10\rangle$ и $|11\rangle$ будем далее называть просто вычислительным базисом.

Если **гипотеза T** верна и BC – соответствующая квантовая система из двух кубитов B и C, то число α_{K} назовем **амплитудная граница Ксения**, или, короче, **амплитудная граница K**, и при необходимости указать связь этого числа с квантовой системой BC будем применять для него также обозначение α_{KBC}.

Состояние $\left|\psi^{(2)}\right\rangle = a|01\rangle + b|10\rangle$, где $a,\ b \in \mathbb{C}$, $|a| > |b| > 0$, $|a|^2 + |b|^2 = 1$, является несепарабельным состоянием квантовой системы BC, и при этом справедливо (см. следствие 4.4.12) равенство

$$V\left(\left|\psi^{(2)}\right\rangle\right) = C_{\text{B}}\left(\left|\psi^{(2)}\right\rangle\right).$$

Как следует из (4.3.10), мера несепарабельности $C_{\text{B}}\left(\left|\psi^{(2)}\right\rangle\right)$ кубита B с остальной частью квантовой системы BC (т.е. с кубитом C), когда BC находится в состоянии $\left|\psi^{(2)}\right\rangle$, равна $2|a||b|$.

Теперь заметим, что при выполнении условия $\alpha_{\text{KBC}} \geq \dfrac{1}{\sqrt{2}}$ неравенство

$$|a| > \alpha_{\text{KBC}} \tag{6.1.1}$$

равносильно неравенству

$$2|a||b| < 2\alpha_{\text{KBC}} \cdot \sqrt{1-\alpha_{\text{KBC}}^2}\ . \tag{6.1.2}$$

Действительно, рассмотрим функцию $f(x) = x\sqrt{1-x^2}$, где $x \in \left(\dfrac{1}{\sqrt{2}};\ 1\right)$. Производная $f'(x)$ этой функции равна

$$f'(x) = \sqrt{1-x^2} + x \cdot \frac{1}{2} \cdot \frac{-2x}{\sqrt{1-x^2}} = \frac{1-2x^2}{\sqrt{1-x^2}},$$

и при $x \in \left(\frac{1}{\sqrt{2}};\ 1 \right)$ она отрицательна. Следовательно, функция $f(x) = x\sqrt{1-x^2}$ убывает на промежутке $\left(\frac{1}{\sqrt{2}};\ 1 \right)$ [44]. Отсюда и из того, что $|a| \in \left(\frac{1}{\sqrt{2}};\ 1 \right)$, следует, что неравенства $|a| > \alpha_{\text{KBC}}$ и $2f\left(|a|\right) < 2f\left(\alpha_{\text{KBC}}\right)$ эквивалентны при $\alpha_{\text{KBC}} \in \left(\frac{1}{\sqrt{2}};\ 1 \right)$.

Остается рассмотреть случай $\alpha_{\text{KBC}} = \frac{1}{\sqrt{2}}$. В этом случае $f\left(\alpha_{\text{KBC}}\right) = \frac{1}{2}$, и, допустив, что $f\left(|a|\right) \geq \frac{1}{2}$, получаем $|a| = \frac{1}{\sqrt{2}}$, что противоречит условию $|a| > \alpha_{\text{KBC}}$.

Таким образом, неравенства (6.1.1) и (6.1.2) эквивалентны при $\alpha_{\text{KBC}} \geq \frac{1}{\sqrt{2}}$.

Теперь, с учетом неравенства (6.1.2), **гипотеза Т** может быть переформулирована следующим образом:

Существуют квантовая система ВС из двух кубитов В и С и действительное число $\alpha_{\text{KBC}} > \frac{1}{\sqrt{2}}$, такие, что состояния этой квантовой системы $a|01\rangle + b|10\rangle$ и $|01\rangle$ статистически неотличимы при измерениях в вычислительном базисе при условии, что квантовая система ВС в состоянии $\left|\psi^{(2)}\right\rangle = a|01\rangle + b|10\rangle$ (где $a,\ b \in \mathbb{C}$, $|a| > |b| > 0$, $|a|^2 + |b|^2 = 1$) обладает мерой несепарабельности $V\left(\left|\psi^{(2)}\right\rangle\right)$ меньшей, чем

$$V_{\text{KBC}} = 2\alpha_{\text{KBC}} \cdot \sqrt{1-\alpha_{\text{KBC}}^2}\ . \qquad (6.1.3)$$

Именно этой формулировки **гипотезы Т** и будем далее придерживаться.

Число V_{KBC} назовем **ресурсной границей Ксения**, или просто **границей Ксения** квантовой системы ВС.

Покажем, что **гипотеза Т** не противоречит современным представлениям об известном физическом явлении под названием «**квантовый фазовый переход**» [42]. В этих целях заметим, что к естественным двухуровневым квантовым ячейкам – кубитам – относятся электронные, протонные, нейтронные, ядерные и другие спины со спиновым числом 1/2 [24], [29], [38], [54], [79], [82]. Проекция каждого спина на выбранное направление (например, как часто полагают, по оси *Z*) может быть направлена либо вверх (по направлению) (обозначается $|\uparrow\rangle = |0\rangle = \begin{pmatrix}1\\0\end{pmatrix}$), либо вниз (против направления) (обозначается $|\downarrow\rangle = |1\rangle = \begin{pmatrix}0\\1\end{pmatrix}$).

Рассмотрим квантовую систему из двух таких кубитов, находящуюся в постоянном внешнем магнитном поле с вектором магнитной индукции **M**, направленным по оси *Z*, то есть $\mathbf{M} = (0,\ 0,\ M)$, где M – модуль вектора магнитной индукции, $M \geq 0$. J – константа взаимодействия в квантовой системе ВС [42; 50; 54].

В этом случае квантовая система ВС имеет следующие стационарные состояния [7]:

$$\left|\psi_1^{(2)}\right\rangle = |11\rangle e^{-\left(\frac{i}{\hbar}\right)E_1 t},\ \left|\psi_2^{(2)}\right\rangle = |00\rangle e^{-\left(\frac{i}{\hbar}\right)E_2 t},$$

$$\left|\psi_3^{(2)}\right\rangle = \left(\sqrt{\varepsilon}\,|01\rangle + \sqrt{1-\varepsilon}\,|10\rangle\right) e^{-\left(\frac{i}{\hbar}\right)E_3 t},$$

$$\left|\psi_4^{(2)}\right\rangle = \left(\sqrt{1-\varepsilon}\,|01\rangle - \sqrt{\varepsilon}\,|10\rangle\right) e^{-\left(\frac{i}{\hbar}\right)E_4 t}, \tag{6.1.4}$$

где

$$\varepsilon = \frac{1}{2}\left(1 - \frac{X}{\sqrt{1+X^2}}\right); \tag{6.1.5}$$

$$X = \frac{\omega_1 - \omega_2}{J} = \frac{M}{J}\left(v_1 - v_2\right), \tag{6.1.6}$$

ω_1, ω_2 – резонансные частоты соответственно спинов B и C, $\omega_1 = v_1 M$, $\omega_2 = v_2 M$; v_1, v_2 – гиромагнитные отношения спинов B и C; E_k – энергия стационарного состояния $\left|\psi_k^{(2)}\right\rangle$, $k \in \{1,\ 2,\ 3,\ 4\}$,

$$E_1 = \left(\frac{J}{4} + \frac{\omega_1 + \omega_2}{2}\right)\hbar,\quad E_2 = \left(\frac{J}{4} - \frac{\omega_1 + \omega_2}{2}\right)\hbar,$$

$$E_3 = \left(-\frac{J}{4} + \frac{J\sqrt{1+X^2}}{2}\right)\hbar,\quad E_4 = \left(-\frac{J}{4} - \frac{J\sqrt{1+X^2}}{2}\right)\hbar; \qquad (6.1.7)$$

t – время, $\hbar$ – приведенная постоянная Планка, $i = \sqrt{-1}$ – мнимая единица.

Докажем справедливость равенств (6.1.4) и (6.1.7).

Для гамильтониана **H** обсуждаемой квантовой системы справедливо равенство [7; 50; 54; 57]

$$\begin{gathered}\mathbf{H} = \hbar \cdot J\left(\frac{1}{2}\sigma_{\mathbf{X}} \otimes \frac{1}{2}\sigma_{\mathbf{X}} + \frac{1}{2}\sigma_{\mathbf{Y}} \otimes \frac{1}{2}\sigma_{\mathbf{Y}} + \frac{1}{2}\sigma_{\mathbf{Z}} \otimes \frac{1}{2}\sigma_{\mathbf{Z}}\right) - \\ - v_1\hbar M\left(\frac{1}{2}\sigma_{\mathbf{Z}} \otimes \mathbf{I}\right) - v_2\hbar M\left(\mathbf{I} \otimes \frac{1}{2}\sigma_{\mathbf{Z}}\right),\end{gathered} \qquad (6.1.8)$$

где $\mathbf{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $\sigma_{\mathbf{X}} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $\sigma_{\mathbf{Y}} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$, $\sigma_{\mathbf{Z}} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

Осуществив соответствующие вычисления, имеем

$$\mathbf{H} = \hbar \cdot \begin{pmatrix} \frac{J}{4} - \frac{\omega_1}{2} - \frac{\omega_2}{2} & 0 & 0 & 0 \\ 0 & -\frac{J}{4} - \frac{\omega_1}{2} + \frac{\omega_2}{2} & 0 & 0 \\ 0 & 0 & -\frac{J}{4} + \frac{\omega_1}{2} - \frac{\omega_2}{2} & 0 \\ 0 & 0 & 0 & \frac{J}{4} + \frac{\omega_1}{2} + \frac{\omega_2}{2} \end{pmatrix}, \qquad (6.1.9)$$

где $\omega_1 = v_1 M$, $\omega_2 = v_2 M$.

Для характеристического многочлена $\chi_{\mathbf{H}}(\lambda)$ матрицы **H** справедливо равенство

$$\chi_{\mathbf{H}}(\lambda) = \\ = \left(\lambda - \left(\frac{J}{4} - \frac{\omega_1 + \omega_2}{2}\right)\hbar\right) \cdot \left(\lambda - \left(\frac{J}{4} + \frac{\omega_1 + \omega_2}{2}\right)\hbar\right) \cdot \\ \cdot \left(\lambda^2 + \frac{1}{2}J\hbar\lambda + \left(\frac{3}{16}J^2\hbar^2 + \left(\frac{\omega_1 - \omega_2}{2}\right)^2 \hbar^2\right)\right). \tag{6.1.10}$$

Решив уравнение

$$\chi_{\mathbf{H}}(\lambda) = 0,$$

находим следующие собственные значения матрицы **H**:

$$\lambda_1 = \left(\frac{J}{4} + \frac{\omega_1 + \omega_2}{2}\right)\hbar, \quad \lambda_2 = \left(\frac{J}{4} - \frac{\omega_1 + \omega_2}{2}\right)\hbar,$$

$$\lambda_3 = \left(-\frac{J}{4} + \frac{J\sqrt{1 + X^2}}{2}\right)\hbar, \quad \lambda_4 = \left(-\frac{J}{4} - \frac{J\sqrt{1 + X^2}}{2}\right)\hbar. \tag{6.1.11}$$

Так как $E_k = \lambda_k$ ($k \in \{1, 2, 3, 4\}$) [57], то из (6.1.11) следует справедливость равенств (6.1.7).

Далее, для каждого $k \in \{1, 2, 3, 4\}$ решив уравнение

$$\mathbf{H}\left|\psi_k^{(2)}\right\rangle = \lambda_k \left|\psi_k^{(2)}\right\rangle$$

относительно неизвестного $\left|\psi_k^{(2)}\right\rangle$, находим стационарное состояние $\left|\psi_k^{(2)}\right\rangle$ и тем самым убеждаемся в справедливости равенств (6.1.4).

Среди стационарных состояний (6.1.4) квантовой системы ВС обратим внимание на состояния $\left|\psi_3^{(2)}\right\rangle$ и $\left|\psi_4^{(2)}\right\rangle$.

Если $v_1 = v_2$, то $\omega_1 = \omega_2$ и, следовательно, $X = 0$ и $\varepsilon = \dfrac{1}{2}$ (см. (6.1.6), (6.1.5)), что влечет за собой справедливость равенств:

$$\left|\psi_3^{(2)}\right\rangle = \left(\frac{|01\rangle + |10\rangle}{\sqrt{2}}\right) e^{-i\left(\frac{J}{4}\right)t}, \quad \left|\psi_4^{(2)}\right\rangle = \left(\frac{|01\rangle - |10\rangle}{\sqrt{2}}\right) e^{-i\left(\frac{-3J}{4}\right)t}. \quad (6.1.12)$$

Из равенств (6.1.12) следует, что при $\nu_1 = \nu_2$ амплитуды стационарных состояний $\left|\psi_3^{(2)}\right\rangle$, $\left|\psi_4^{(2)}\right\rangle$ и их энергии не зависят от величины модуля M вектора магнитной индукции. Также в этих состояниях от магнитного поля не зависит мера несепарабельности кубитов квантовой системы ВС, равная в этом случае максимальному значению 1.

Рассмотрим теперь случай, когда $\nu_1 \neq \nu_2$. Не ограничивая общности, положим для определенности, что $\nu_1 < \nu_2$. Тогда $\omega_1 < \omega_2$ и, следовательно, $X < 0$ при $M > 0$ и X убывает при возрастании M (см. (6.1.6)). Отсюда и из (6.1.5) следует, что величина $\sqrt{\varepsilon}$, равная модулю левой амплитуды состояния $\left|\psi_3^{(2)}\right\rangle$ и модулю правой амплитуды состояния $\left|\psi_4^{(2)}\right\rangle$ (см. (6.1.4)), возрастает при возрастании M и ее минимальное значение равно $\frac{1}{\sqrt{2}}$, оно достигается при $M = 0$, то есть при отсутствии внешнего магнитного поля. Предельное значение $\sqrt{\varepsilon}$ при $M \to \infty$ равно 1, и оно, если судить по (6.1.5), недостижимо ни при каком конечном значении M. Одновременно с этим величина $\sqrt{1-\varepsilon}$, равная модулю правой амплитуды состояния $\left|\psi_3^{(2)}\right\rangle$ и модулю левой амплитуды состояния $\left|\psi_4^{(2)}\right\rangle$ (см. (6.1.4)), убывает при возрастании M; ее максимальное значение равно $\frac{1}{\sqrt{2}}$ и достигается при $M = 0$, то есть при отсутствии внешнего магнитного поля. Предельное значение $\sqrt{1-\varepsilon}$ при $M \to \infty$ равно 0, и оно, если судить по (6.1.5), недостижимо ни при каком конечном значении M. При этом мера несепарабельности (**V-мера**) квантовой системы ВС в состояниях $\left|\psi_3^{(2)}\right\rangle$ и $\left|\psi_4^{(2)}\right\rangle$, равная

$$V\left(\left|\psi_3^{(2)}\right\rangle\right)=V\left(\left|\psi_4^{(2)}\right\rangle\right)=2\sqrt{\varepsilon}\sqrt{1-\varepsilon}=$$
$$=\frac{1}{\sqrt{1+X^2}}=\frac{J}{\sqrt{J^2+M^2\left(\nu_1-\nu_2\right)^2}}, \qquad (6.1.13)$$

убывает при возрастании M и принимает свое максимальное значение 1 при $M = 0$, то есть при отсутствии внешнего магнитного поля.

Таким образом, судя по (6.1.13), мера несепарабельности кубитов квантовой системы ВС в состояниях $\left|\psi_3^{(2)}\right\rangle$ и $\left|\psi_4^{(2)}\right\rangle$ стремится к 0 при $M\to\infty$, но не достигает своего предельного значения 0 ни при каком конечном значении M.

Однако, с другой стороны, из результатов, представленных в работах [18; 23; 42; 47; 57; 58; 89], следует, что начиная с определенного значения $M_{\text{КВС}}$ модуля вектора магнитной индукции постоянного внешнего магнитного поля мера несепарабельности кубитов квантовой системы ВС скачкообразно принимает нулевое значение. Это явление и называют **квантовым фазовым переходом** [42]. Поэтому в соответствии с (6.1.13) и определением параметра $V_{\text{КВС}}$ (см. (6.1.3)) естественно предположение, что

$$V_{\text{КВС}}\geq\frac{J}{\sqrt{J^2+M_{\text{КВС}}^2\left(\nu_1-\nu_2\right)^2}}. \qquad (6.1.14)$$

Таким образом, при выполнении соотношения $M\geq M_{\text{КВС}}$ стационарные состояния квантовой системы являются сепарабельными. В некоторых из указанных выше работ (например, в [18; 23; 42; 47; 58]) это явление объясняется с позиций классической физики (а затем декларируется, что такое объяснение не противоречит положениям квантовой механики) на основе «наглядных представлений о прецессии магнитных моментов», и отмечается, что оно аналогично явлению, обнаруженному Ф. Пашеном и Е. Баком в 1912 г. (и поэтому получившему название явление **Пашена–Бака**), заключающемуся в разрыве спин-орбитальной связи атома в сильном магнитном поле [47]. Отличие только в том, что в случае двух спинов в магнитном поле речь идет о разрыве спин-спиновой связи в сильном магнитном поле из-за того, что при достаточно большой индукции магнитного поля суммарная энергия взаимодействия магнитных моментов (соответствующих рассматриваемым спинам) с магнитным полем становится больше энергии спин-спинового взаимодействия.

Довольно подробно описываемое выше явление разбирается и в известной работе [57] на примере атома водорода. При этом вычислены как энергии стационарных состояний, так и сами стационарные состояния в виде векторов четырехмерного гильбертова пространства. Если полагать, что кубитом B является спин электрона, а кубитом C – спин протона в атоме водорода, то полученные в работе [57] результаты (с точностью до обозначений и отдельных уточнений) совпадают с (6.1.7) и (6.1.4). Более того, в работе [57] явно указывается, на какие состояния заменятся состояния $\left|\psi_3^{(2)}\right\rangle$ и $\left|\psi_4^{(2)}\right\rangle$, когда выполняется условие $M \geq M_{\text{КВС}}$ (так называемое «сильное магнитное поле» [18; 23; 47; 57; 58]), которое в данном случае влечет (см. (6.1.14)) тот факт, что мера несепарабельности квантовой системы BC не превышает значения $V_{\text{КВС}}$. Ими оказываются соответственно состояния $|01\rangle$ и $|10\rangle$, каждое из которых само от себя статистически не отличается при измерениях в вычислительном базисе.

Таким образом, **гипотеза T** не противоречит известным физическим представлениям, связанным с явлением квантового фазового перехода. Однако надо отметить следующее. В работах [18; 23; 42; 47; 57; 58; 89]), на которые мы ссылались выше, рассматриваются только стационарные состояния. Тогда как в **гипотезе T** этого ограничения нет. Речь в этой гипотезе идет о произвольных состояниях, не обязательно стационарных. Поэтому необходимость экспериментальной проверки выполнимости **гипотезы T** не исключается.

§ 6.2. Способ дистанционного изменения меры несепарабельности двухкубитных квантовых систем

Способ дистанционного изменения меры несепарабельности квантовых систем представим в виде **алгоритма Александр** (имя Александр алгоритму присвоил первый из авторов книги и далее по тексту алгоритм Александр будем для краткости называть **алгоритм А**), изложение которого осуществим ниже в стиле, близком тому, которого придерживаются авторы известной монографии [50] при описании технологии квантовой телепортации.

Алиса и Боб, будучи вместе, приготовили квантовую систему из трех кубитов A, B и C в состоянии

$$\left|\psi^{(3)}\right\rangle = \alpha\,|001\rangle + \beta\,|110\rangle\,, \tag{6.2.1}$$

где $\alpha,\ \beta \in \mathbb{C}$, $|\alpha| > |\beta| > 0$, $|\alpha|^2 + |\beta|^2 = 1$.

В связи с равенством (6.2.1) напомним обозначение $\left|\kappa_1\kappa_2\ldots\kappa_r\right\rangle$:

$$\left|\kappa_1\kappa_2\ldots\kappa_r\right\rangle = \left|\kappa_1\right\rangle\left|\kappa_2\right\rangle\ldots\left|\kappa_r\right\rangle = \left|\kappa_1\right\rangle \otimes \left|\kappa_2\right\rangle \otimes \ldots \otimes \left|\kappa_r\right\rangle,$$

где $\kappa_1,\ \kappa_2,\ \ldots,\ \kappa_r \in \{0,\ 1\}$, $|0\rangle = |\uparrow\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $|1\rangle = |\downarrow\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, r – произвольное натуральное число, $\otimes$ – знак тензорного произведения [50].

При расставании у Алисы остается кубит A, а Боб берет кубиты B и C. Они договариваются о том, что через определенное, заранее оговоренное ими время Алиса возьмет дополнительно еще один кубит D в состоянии $\left|\psi^{(1)}\right\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ и осуществит над кубитами D и A последовательность действий (названную в данной работе **алгоритмом А**), аналогичных тем, которые осуществляются Алисой в технологии квантовой телепортации [50]. В результате, как это покажут ниже соответствующие вычисления, пара кубитов Боба B и C будет представлять собою квантовую систему в несепарабельном состоянии. Предполагается, что между удаленными друг от друга Алисой и Бобом нет классического канала связи и поэтому исключена любая передача с использованием классического канала связи Бобу информации о результате последовательности действий Алисы. Что можно сказать о состоянии квантовой системы, состоящей из кубитов Боба, и мере его несепарабельности (то есть **V-мере**), предварительно не подвергая эту квантовую систему никаким воздействиям?

На этот вопрос предлагается следующий ответ: двухкубитная квантовая система BC из кубитов Боба будет находиться в одном из четырех несепарабельных состояний

$$\left|\psi_1^{(2)}\right\rangle = \frac{\alpha^2}{\sqrt{|\alpha|^4+|\beta|^4}}|01\rangle + \frac{\beta^2}{\sqrt{|\alpha|^4+|\beta|^4}}|10\rangle,\ \left|\psi_2^{(2)}\right\rangle = \frac{|01\rangle+|10\rangle}{\sqrt{2}},$$
$$\left|\psi_3^{(2)}\right\rangle = \frac{\alpha^2}{\sqrt{|\alpha|^4+|\beta|^4}}|01\rangle - \frac{\beta^2}{\sqrt{|\alpha|^4+|\beta|^4}}|10\rangle,\ \left|\psi_4^{(2)}\right\rangle = \frac{|01\rangle-|10\rangle}{\sqrt{2}} \tag{6.2.2}$$

с вероятностями

$$\frac{|\alpha|^4+|\beta|^4}{2},\ |\alpha|^2|\beta|^2,\ \frac{|\alpha|^4+|\beta|^4}{2},\ |\alpha|^2|\beta|^2, \tag{6.2.3}$$

соответственно. Вычисления для обоснования данного ответа приведем ниже. А здесь же обратим внимание на следующее. Модуль амплитуды $\frac{|\alpha|^2}{\sqrt{|\alpha|^4+|\beta|^4}}$ при компоненте $|01\rangle$ в состояниях $\left|\psi_1^{(2)}\right\rangle$ и $\left|\psi_3^{(2)}\right\rangle$ больше $|\alpha|$, то есть справедливо неравенство

$$\frac{|\alpha|^2}{\sqrt{|\alpha|^4+|\beta|^4}} > |\alpha|$$

(доказательство этого неравенства приводится в параграфе 6.3). И, кроме того, мера несепарабельности каждого из кубитов A, B и C с остальной частью квантовой системы ABC до выполнения действий Алисы, то есть тогда, когда квантовая система ABC находилась в состоянии $\left|\psi^{(3)}\right\rangle$ (см. (6.2.1), (4.3.9), (4.3.10), (4.3.11)), равна $2|\alpha||\beta|$, а после выполнения действий Алисы по **алгоритму A** мера несепарабельности кубита A равна нулю (и это естественно, так как ресурс несепарабельности израсходовался в результате действий Алисы); а мера несепарабельности каждого из кубитов Боба B и C в соответствии с (4.3.8) либо равна $\dfrac{2|\alpha|^2|\beta|^2}{|\alpha|^4+|\beta|^4}$ (с вероятностью $|\alpha|^4+|\beta|^4$), что меньше первоначального значения $2|\alpha||\beta|$, либо равна 1 (с вероятностью $2|\alpha|^2|\beta|^2$), что больше первоначального значения $2|\alpha||\beta|$ (то есть меры несепарабельности каждого из кубитов являются одинаково распределенными случайными величинами со значением математического ожидания $\left(|\alpha|^4+|\beta|^4\right)\cdot\dfrac{2|\alpha|^2|\beta|^2}{|\alpha|^4+|\beta|^4}+2|\alpha|^2|\beta|^2\cdot 1=4|\alpha|^2|\beta|^2$).

Таким образом, можно сделать следующий вывод: ресурс несепарабельности можно дистанционно как уменьшить, так и увеличить.

Однако при этом надо отметить следующие две особенности рассматриваемого явления: во-первых, «привязка ко времени», то есть изначально Алиса и Боб должны договориться о времени действий Алисы и Боб получает (или теряет) определенную часть соответствующего физического ресурса после завершения времени их выполнения; во-вторых, получение физического ресурса Бобом от Алисы является не детерминированным, а случайным явлением. И Боб не знает точно значения меры несепарабельности каждого из своих кубитов даже в предположении, что действия Алисы уже выполнены (то есть **алгоритм A** завершен) и ему об этом известно. Все, чем он располагает – это вероятностное распределение случайной величины, равной мере несепарабельности (**V-мере**) квантовой системы BC. Математическое ожидание этой случайной величины равно $4|\alpha|^2|\beta|^2$, что меньше первоначального значения $2|\alpha||\beta|$ меры несепарабельности каждого из кубитов Боба. Об этом свидетельствуют и графики на рис. 6.2.4, наглядно иллюстрирующие соотношение между величинами

$$y = 2|\alpha||\beta| = 2|\alpha|\sqrt{1-|\alpha|^2}$$

(сплошная линия) и

$$y = 4|\alpha|^2|\beta|^2 = 4|\alpha|^2\left(1-|\alpha|^2\right)$$

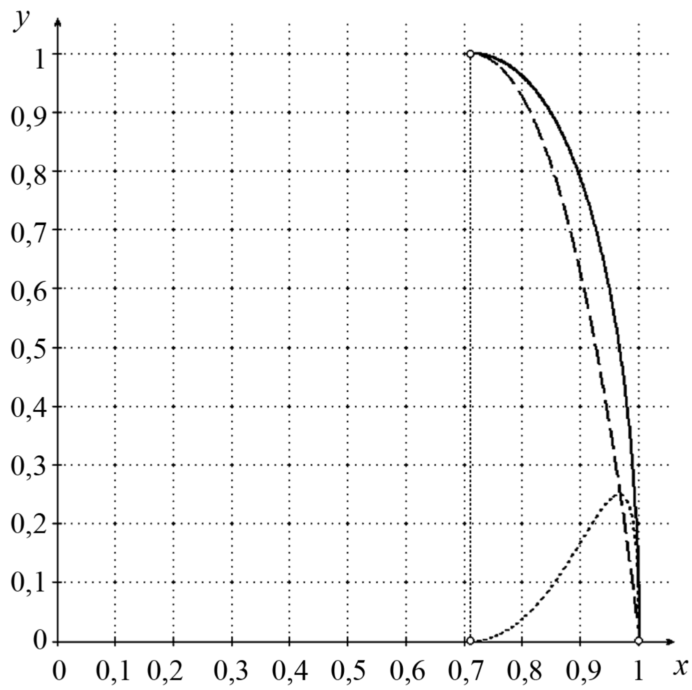

Рисунок 6.2.4. Графики функций $y = 2x\sqrt{1-x^2}$ (сплошная линия), $y = 4x^2\left(1-x^2\right)$ (пунктирная линия) и $y = 2x\sqrt{1-x^2} - 4x^2\left(1-x^2\right)$ (график, составленный из точек) на интервале $\left(\frac{1}{\sqrt{2}};\, 1\right)$

(пунктирная линия) в зависимости от значения $x=|\alpha|\in\left(\frac{1}{\sqrt{2}};\,1\right)$; на интервале $\left(\frac{1}{\sqrt{2}};\,1\right)$ функция $y=2x\sqrt{1-x^2}-4x^2\left(1-x^2\right)$ (график, составленный из точек), являющаяся разностью предыдущих функций, достигает своего максимального значения при $x=|\alpha|=\frac{\sqrt{3}+1}{2\sqrt{2}}$.

Изложим теперь последовательность действий Алисы, осуществляемых ею по отношению к своим двум кубитам D и A, то есть приведем **алгоритм A**.

Алгоритм A (алгоритм Александр)

На входе алгоритма имеется состояние

$$\left|\psi_0^{(4)}\right\rangle=\left|\psi^{(1)}\right\rangle\left|\psi^{(3)}\right\rangle=\left(\alpha|0\rangle+\beta|1\rangle\right)\left(\alpha|001\rangle+\beta|110\rangle\right)=$$
$$=\alpha|0\rangle\left(\alpha|001\rangle+\beta|110\rangle\right)+\beta|1\rangle\left(\alpha|001\rangle+\beta|110\rangle\right)$$

квантовой системы DABC из четырех кубитов D, A, B и C, из которых кубиты D и A принадлежат Алисе, а кубиты B и C принадлежат Бобу.

Шаг 1. Алиса пропускает свои кубиты D и A через элемент **CNOT** [50]. Это равносильно тому, что к состоянию $\left|\psi_0^{(4)}\right\rangle$ применяется линейное преобразование с матрицей $\mathbf{CNOT}\otimes\mathbf{I}_2\otimes\mathbf{I}_2$, где $\otimes$ – знак тензорного произведения, $\mathbf{CNOT}=\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}$, $\mathbf{I}_2=\begin{pmatrix}1&0\\0&1\end{pmatrix}$. В результате получается состояние $\left|\psi_1^{(4)}\right\rangle$ квантовой системы DABC, задаваемое равенством:

$$\left|\psi_1^{(4)}\right\rangle=\alpha|0\rangle\left(\alpha|001\rangle+\beta|110\rangle\right)+\beta|1\rangle\left(\alpha|101\rangle+\beta|010\rangle\right).$$

Шаг 2. Алиса пропускает свой кубит D через элемент Адамара **H** [50], что равносильно применению к состоянию $\left|\psi_1^{(4)}\right\rangle$ линейного преобразования с матрицей $\mathbf{H}\otimes\mathbf{I}_2\otimes\mathbf{I}_2\otimes\mathbf{I}_2$, где $\mathbf{H}=\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$. В результате квантовая система DABC переходит в состояние $\left|\psi_2^{(4)}\right\rangle$, задаваемое равенством:

$$\left|\psi_2^{(4)}\right\rangle=\frac{\alpha}{\sqrt{2}}\big(|0\rangle+|1\rangle\big)\big(\alpha|001\rangle+\beta|110\rangle\big)+\frac{\beta}{\sqrt{2}}\big(|0\rangle-|1\rangle\big)\big(\alpha|101\rangle+\beta|010\rangle\big),$$

что, перегруппировав члены, можно переписать следующим образом:

$$\begin{gathered}\left|\psi_2^{(4)}\right\rangle=\\
=\frac{\sqrt{|\alpha|^4+|\beta|^4}}{\sqrt{2}}|00\rangle\left(\frac{\alpha^2}{\sqrt{|\alpha|^4+|\beta|^4}}|01\rangle+\frac{\beta^2}{\sqrt{|\alpha|^4+|\beta|^4}}|10\rangle\right)+\\
+\alpha\beta|01\rangle\left(\frac{|01\rangle+|10\rangle}{\sqrt{2}}\right)+\\
+\frac{\sqrt{|\alpha|^4+|\beta|^4}}{\sqrt{2}}|10\rangle\left(\frac{\alpha^2}{\sqrt{|\alpha|^4+|\beta|^4}}|01\rangle-\frac{\beta^2}{\sqrt{|\alpha|^4+|\beta|^4}}|10\rangle\right)-\\
-\alpha\beta|11\rangle\left(\frac{|01\rangle-|10\rangle}{\sqrt{2}}\right).\end{gathered}$$

Шаг 3. Алиса проводит измерение над своими двумя кубитами D и A в вычислительном базисе из векторов $|00\rangle$, $|01\rangle$, $|10\rangle$ и $|11\rangle$ [50]. В результате этого измерения квантовая система из четырех кубитов D, A, B и C может иметь следующие состояния своих подсистем:

- с вероятностью $\frac{|\alpha|^4+|\beta|^4}{2}$ подсистема из двух кубитов Алисы D и A в состоянии $|00\rangle$, а подсистема из двух кубитов Боба B и C в состоянии

$$\left|\psi_1^{(2)}\right\rangle = \frac{\alpha^2}{\sqrt{|\alpha|^4+|\beta|^4}}|01\rangle + \frac{\beta^2}{\sqrt{|\alpha|^4+|\beta|^4}}|10\rangle\,;$$

- с вероятностью $|\alpha|^2|\beta|^2$ подсистема из двух кубитов Алисы D и A в состоянии $|01\rangle$, а подсистема из двух кубитов Боба B и C в состоянии

$$\left|\psi_2^{(2)}\right\rangle = \frac{|01\rangle+|10\rangle}{\sqrt{2}}\,;$$

- с вероятностью $\dfrac{|\alpha|^4+|\beta|^4}{2}$ подсистема из двух кубитов Алисы D и A в состоянии $|10\rangle$, а подсистема из двух кубитов Боба B и C в состоянии

$$\left|\psi_3^{(2)}\right\rangle = \frac{\alpha^2}{\sqrt{|\alpha|^4+|\beta|^4}}|01\rangle - \frac{\beta^2}{\sqrt{|\alpha|^4+|\beta|^4}}|10\rangle\,;$$

- с вероятностью $|\alpha|^2|\beta|^2$ подсистема из двух кубитов Алисы D и A в состоянии $|11\rangle$, а подсистема из двух кубитов Боба B и C в состоянии

$$\left|\psi_4^{(2)}\right\rangle = \frac{|01\rangle-|10\rangle}{\sqrt{2}}\,.$$

Таким образом, после применения **алгоритма A** квантовая система BC из кубитов Боба окажется в одном из состояний (6.2.2) с соответствующей вероятностью из (6.2.3).

В данном параграфе были использованы несколько соотношений, представляющих собой неравенства. Доказательства их справедливости изложены в отдельном параграфе 6.3 данной главы.

§ 6.3. Доказательства неравенств, использованных в § 6.2

Данный параграф имеет вспомогательный характер, являясь, как следует из названия параграфа, дополнением к параграфу 6.2.

В параграфе 6.2 утверждалось, что модуль амплитуды

$$\frac{|\alpha|^2}{\sqrt{|\alpha|^4+|\beta|^4}}$$

при компоненте $|01\rangle$ в состояниях $\left|\psi_1^{(2)}\right\rangle$ и $\left|\psi_3^{(2)}\right\rangle$ больше $|\alpha|$ и, кроме того, после выполнения **алгоритма А** возможное значение меры несепарабельности

$$\frac{2|\alpha|^2|\beta|^2}{|\alpha|^4+|\beta|^4}$$

кубита B двухкубитной квантовой системы BC меньше первоначального значения $2|\alpha||\beta|$ меры несепарабельности этого же кубита в трехкубитной квантовой системе ABC, а возможное значение 1 той же меры больше первоначального значения $2|\alpha||\beta|$. При этом математическое ожидание $4|\alpha|^2|\beta|^2$ указанной меры меньше $2|\alpha||\beta|$. Докажем соответствующие неравенства.

Начнем с доказательства неравенства

$$\frac{|\alpha|^2}{\sqrt{|\alpha|^4+|\beta|^4}}>|\alpha|. \tag{6.3.1}$$

Из условий к равенству (6.2.1) следует, что $|\alpha|>|\beta|>0$ и $|\alpha|^2+|\beta|^2=1$. Тогда $|\alpha|^2-|\beta|^2>0$. Значит, $|\alpha|^2|\beta|^2-|\beta|^4>0$, что равносильно неравенству $|\alpha|^2\left(1-|\alpha|^2\right)-|\beta|^4>0$. Отсюда следует, что $|\alpha|^2>|\alpha|^4+|\beta|^4$, что влечет справедливость неравенства

$$|\alpha|>\sqrt{|\alpha|^4+|\beta|^4}\ ,$$

равносильного неравенству (6.3.1).

Докажем неравенство

$$\frac{2|\alpha|^2|\beta|^2}{|\alpha|^4+|\beta|^4}<2|\alpha||\beta|. \tag{6.3.2}$$

Докажем методом от противного. Допустим, что неравенство (6.3.2) неверно. Тогда справедлива следующая цепочка соотношений:

$$1\le\frac{|\alpha||\beta|}{|\alpha|^4+|\beta|^4}=\frac{|\alpha||\beta|\left(|\alpha|^2+|\beta|^2\right)}{|\alpha|^4+|\beta|^4}=\frac{|\alpha|^3|\beta|+|\alpha||\beta|^3}{|\alpha|^4+|\beta|^4}=$$

$$=\frac{|\alpha|^2|\beta|^2\left(\left|\frac{\alpha}{\beta}\right|+\left|\frac{\beta}{\alpha}\right|\right)}{|\alpha|^2|\beta|^2\left(\left|\frac{\alpha}{\beta}\right|^2+\left|\frac{\beta}{\alpha}\right|^2\right)}=\frac{\left|\frac{\alpha}{\beta}\right|+\left|\frac{\beta}{\alpha}\right|}{\left|\frac{\alpha}{\beta}\right|^2+\left|\frac{\beta}{\alpha}\right|^2}. \tag{6.3.3}$$

Так как из (6.2.1) следует, что $|\alpha|>|\beta|>0$, то

$$\left|\frac{\alpha}{\beta}\right|+\left|\frac{\beta}{\alpha}\right|>2\,,$$

что влечет за собой справедливость равенства

$$\left|\frac{\alpha}{\beta}\right|+\left|\frac{\beta}{\alpha}\right|=2+\delta\,,$$

где $\delta\in\mathbb{R}$, $\delta>0$. Отсюда и из (6.3.3) следует справедливость следующей цепочки соотношений:

$$1 \le \frac{2+\delta}{(2+\delta)^2 - 2} = \frac{2+\delta}{4+4\delta+4\delta^2-2} = \frac{2+\delta}{2+\delta+3\delta+4\delta^2} < \frac{2+\delta}{2+\delta} = 1.$$

Получили противоречивое неравенство 1 < 1, и тем самым доказана справедливость неравенства (6.3.2).

Докажем неравенство

$$1 > 2|\alpha||\beta|. \tag{6.3.4}$$

Так как из (6.2.1) следует, что $|\alpha| > |\beta| > 0$ и $|\alpha|^2 + |\beta|^2 = 1$, то верна цепочка соотношений $0 < \left(|\alpha| - |\beta|\right)^2 = |\alpha|^2 + |\beta|^2 - 2|\alpha||\beta| = 1 - 2|\alpha||\beta|$, что влечет за собой справедливость неравенства (6.3.4).

Докажем теперь неравенство

$$4|\alpha|^2|\beta|^2 < 2|\alpha||\beta|. \tag{6.3.5}$$

Из двойного неравенства $|\alpha| > |\beta| > 0$ следует, что $2|\alpha||\beta| > 0$. Поэтому, умножив обе части неравенства (6.3.4) на $2|\alpha||\beta|$, получаем неравенство (6.3.5).

§ 6.4. ATF-технология связи

Протокол детерминированной квантовой связи, или, по-другому, **ATF**-технология связи, представляет собой протокол передачи сообщения из *k* бит (где *k* – произвольное натуральное число) от одного абонента к другому, при условии, что они удалены друг от друга в пространстве и не имеют классического канала связи. Используются только квантовые ресурсы. Этот протокол реализуется путем *k*-кратного применения (передавая каждый раз один бит сообщения) метода **Физули** (кратко – метода **F**), позволяющего при тех же исходных условиях, что и выше, передавать сообщения длиной в один бит. Поэтому **ATF**-технология при своем применении допускает возможности для максимального распараллеливания процесса передачи сообщения.

Аббревиатура **ATF** в названии технологии связи отражает тот факт, что она основана на использовании алгоритма **Александр**, гипотезы **Татьяна** и метода **Физули**.

Алгоритм Александр (**алгоритм A**) и **гипотеза Татьяна** (**гипотеза T**) достаточно подробно изложены соответственно в параграфах 6.2 и 6.1 данной работы. Поэтому остановимся на изложении **метода F**.

Описание **метода F** передачи сообщения, состоящего из одного бита, осуществим (как и ранее **алгоритма A** в параграфе 6.2) в стиле, близком тому, которого придерживаются авторы известной монографии [50] при описании технологии квантовой телепортации.

Когда-то давно Алиса и Боб встречались, но теперь живут далеко друг от друга. Будучи вместе, они приготовили L троек кубитов $A_iB_iC_i$ в состояниях:

$$\left|\psi_i^{(3)}\right\rangle = \alpha\left|001\right\rangle + \beta\left|110\right\rangle,\ \ i \in \{1,\ 2,\ \ldots,\ L\};$$

$$\alpha,\ \beta \in \mathbb{C},\ \ |\alpha| > |\beta| > 0,\ \ |\alpha|^2 + |\beta|^2 = 1.$$

При этом полагаем, что **гипотеза T** верна и двухкубитные квантовые системы B_iC_i из кубитов B_i и C_i, при рассмотрении их в отдельности от A_i (где $i \in \{1,\ 2,\ \ldots,\ L\}$), составляют квантовые системы, удовлетворяющие условиям **гипотезы T** и имеющие одинаковые амплитудные границы **Ксения** (**границы K**, см. параграф 6.1), равные α_{KBC}. Мы также предполагаем, что параметр α подобран таким образом, что выполняется условие

$$\frac{|\alpha|^2}{\sqrt{|\alpha|^4 + |\beta|^4}} > \alpha_{\mathrm{KBC}}\,. \tag{6.4.1}$$

При расставании Алиса взяла из каждой тройки кубитов первый кубит A_i, а Боб взял из каждой тройки кубитов оставшиеся второй и третий кубит B_i и C_i. Кроме этого Алиса сгенерировала для себя еще L кубитов D_i в состояниях

$$\left|\psi_i\right\rangle = \left|\psi_i^{(1)}\right\rangle = \alpha\left|0\right\rangle + \beta\left|1\right\rangle, \;\; i \in \{1,\ 2,\ \ldots,\ L\},$$

соответственно.

Они договорились, что 3 года спустя в определенный час (например, в 19 часов 00 минут) определенного дня (например, 1 января) Алиса должна передать Бобу один бит классической информации. При этом предполагается, как было оговорено выше, что никакого **классического канала связи** между Алисой и Бобом **не существует**. И один бит классической информации передается исключительно посредством квантовых ресурсов, имеющихся у них.

Разрешима ли сформулированная задача, то есть сможет ли Боб получить сообщение из одного бита, переданного ему Алисой? Если разрешима, то каковы достаточные для этого значения параметров L и α?

Схематически решение выглядит следующим образом: Алиса до указанного выше времени осуществляет следующие действия. Если значение передаваемого однобитового сообщения равно нулю, то она не делает ничего. Если же значение передаваемого однобитового сообщения равно единице, то она осуществляет последовательность действий над всеми своими $2L$ кубитами (эту последовательность действий, предусмотренную для передачи бита со значением 1, опишем ниже) и заканчивает эту работу до 19 часов 00 минут указанного выше дня. А Боб после 19 часов 00 проводит измерение над своими L парами B_iC_i кубитов в вычислительном базисе. При этом, если Алиса не делала ничего, то очевидно, что в результате измерения Боба пара кубитов B_iC_i будет в состоянии $\left|01\right\rangle$ с вероятностью $P\left(\left|01\right\rangle\right) = \left|\alpha\right|^2$. Если же Алиса выполнила действия, предусмотренные для передачи бита со значением 1, то мы полагаем, что в результате измерения Боба пара кубитов B_iC_i будет в состоянии $\left|01\right\rangle$ с вероятностью $P\left(\left|01\right\rangle\right) = \left|\alpha\right|^2 + \left|\beta\right|^4$ (соответствующее обоснование будет изложено ниже, после описания действий Алисы по передаче бита со значением 1). Далее Боб проводит обработку результатов измерений над своими L парами кубитов, которая заключается в решении статистической задачи проверки по L исходам (то есть по выборке объема L) простой гипотезы

$$H_0 : P\left(\left|01\right\rangle\right) = \left|\alpha\right|^2$$

с альтернативой – тоже простой гипотезой

$$H_1 : P\left(\left|01\right\rangle\right) = \left|\alpha\right|^2 + \left|\beta\right|^4 .$$

Если гипотеза H_0 верна, то Боб считает, что бит, переданный Алисой, имеет значение 0. В противном случае, то есть когда H_0 отвергается, бит считается равным 1. При этом ясно, что достаточное значение L будет определяться заданным уровнем значимости и значением амплитуды α.

А теперь опишем действия Алисы при передаче ею Бобу бита со значением 1. Алиса выполняет L итераций и в каждой итерации одну и ту же последовательность действий. Действия Алисы в i-той итерации ($i \in \{1,\ 2,\ \ldots,\ L\}$) заключаются в следующем.

Алиса применяет **алгоритм А**, описанный в параграфе 6.2 данной работы, к своей паре кубитов D_iA_i. В результате этого пара кубитов B_iC_i Боба окажется в одном из четырех несепарабельных состояний (6.2.2) соответственно с вероятностями (6.2.3). Теперь заметим, что каждая пара кубитов B_iC_i Боба представляет собой квантовую систему, подобную квантовым системам, для которых выполняется **гипотеза Т**, и параметр α подобран таким образом, что выполняется условие (6.4.1). Тогда в соответствии с **гипотезой Т** при измерениях в вычислительном базисе можно полагать, что каждая пара кубитов B_iC_i Боба находится в одном из трех состояний

$$\left|01\right\rangle,\ \frac{\left|01\right\rangle + \left|10\right\rangle}{\sqrt{2}},\ \frac{\left|01\right\rangle - \left|10\right\rangle}{\sqrt{2}} \qquad (6.4.2)$$

соответственно с вероятностями

$$|\alpha|^4 + |\beta|^4 \,,\; |\alpha|^2 |\beta|^2 ,\; |\alpha|^2 |\beta|^2 . \qquad (6.4.3)$$

Следовательно, после проведения Бобом измерения в вычислительном базисе пара кубитов B_iC_i окажется в состоянии $|01\rangle$ с вероятностью

$$P(|01\rangle) = |\alpha|^4 + |\beta|^4 + |\alpha|^2 |\beta|^2 = |\alpha|^2 \left(|\alpha|^2 + |\beta|^2\right) + |\beta|^4 = |\alpha|^2 + |\beta|^4 . \qquad (6.4.4)$$

Вопрос о достаточных значениях параметра α для реализации **метода F** рассмотрим в следующем параграфе 6.5, а вопрос определения значения объема выборки L по заданным значениям ошибок первого и второго рода и решение статистической задачи проверки по выборке заданного объема L простой гипотезы $H_0 : P(|01\rangle) = |\alpha|^2$ с альтернативой – тоже простой гипотезой $H_1 : P(|01\rangle) = |\alpha|^2 + |\beta|^4$ будут рассмотрены в параграфе 6.6.

§ 6.5. Ограничения на значения модулей амплитуд состояний трехкубитных квантовых систем в ATF-технологии связи

Согласно равенствам (4.3.9), (4.3.10) и (4.3.11), модули амплитуд состояний

$$\left|\psi_i^{(3)}\right\rangle = \alpha|001\rangle + \beta|110\rangle \,,\; i \in \{1,\, 2,\, \ldots,\, L\} ;$$

$$\alpha, \beta \in \mathbb{C} \,,\; |\alpha| > |\beta| > 0 \,,\; |\alpha|^2 + |\beta|^2 = 1$$

трехкубитных квантовых систем $A_iB_iC_i$ определяют величину меры несепарабельности (в смысле 4.3.4) каждого из кубитов с остальной частью системы, то есть чем ближе значения $|\alpha|$ и $|\beta|$, тем больше значение меры несепарабельности как величины физического ресурса, содержащегося в каждой квантовой системе $A_iB_iC_i$, и тем выше устойчивость к деструктивным явлениям, таким, как, например, декогеренция [21].

Однако выполнение **гипотезы T** и условия (6.4.1) накладывают свои ограничения на значения $|\alpha|$, препятствуя выбору близких значений $|\alpha|$ и $|\beta|$. А именно, если известно значение амплитудной границы **Ксения**

$$\alpha_{\text{КВС}} = \tau > \frac{1}{\sqrt{2}},$$

то из неравенства (6.4.1) следует справедливость следующего ограничения на значения модуля амплитуды $|\alpha|$:

$$|\alpha| \in \left(\sqrt{\frac{\tau^2 - \tau\sqrt{1-\tau^2}}{2\tau^2 - 1}};\ \sqrt{\frac{\tau^2 + \tau\sqrt{1-\tau^2}}{2\tau^2 - 1}} \right). \tag{6.5.1}$$

Так как при $1 > \tau > \dfrac{1}{\sqrt{2}}$ справедливы неравенство

$$\sqrt{\frac{\tau^2 - \tau\sqrt{1-\tau^2}}{2\tau^2 - 1}} > \frac{1}{\sqrt{2}} \tag{6.5.2}$$

и двойное неравенство

$$\sqrt{\frac{\tau^2 - \tau\sqrt{1-\tau^2}}{2\tau^2 - 1}} < \tau \le \sqrt{\frac{\tau^2 + \tau\sqrt{1-\tau^2}}{2\tau^2 - 1}}, \tag{6.5.3}$$

то из (6.5.1) следует, что предпочтительными значениями для $|\alpha|$ оказываются те, которые удовлетворяют условию

$$|\alpha| \in \left(\sqrt{\frac{\tau^2 - \tau\sqrt{1-\tau^2}}{2\tau^2 - 1}};\ \tau \right) \tag{6.5.4}$$

и, по физическим соображениям [7], как можно ближе расположенные к левому краю

$$\sqrt{\frac{\tau^2 - \tau\sqrt{1-\tau^2}}{2\tau^2 - 1}}$$

интервала (6.5.4).

В дальнейшей части данного параграфа приведем доказательства использованных в данном параграфе математических соотношений.

Докажем, что из неравенства (6.4.1) при $\alpha_{\text{КВС}} = \tau > \frac{1}{\sqrt{2}}$ вытекает справедливость включения (6.5.1). Из (6.4.1) следует, что справедливо неравенство

$$\frac{|\alpha|^2}{\sqrt{|\alpha|^4 + |\beta|^4}} > \tau ,$$

которое равносильно неравенству

$$|\alpha|^4 > \tau^2 \left(|\alpha|^4 + \left(1 - |\alpha|^2\right)^2 \right).$$

Отсюда, обозначив $x = |\alpha|^2$, получаем неравенство

$$x^2 > \tau^2 \left(x^2 + (1-x)^2 \right),$$

эквивалентное неравенству

$$\left(2\tau^2 - 1\right) x^2 - 2\tau^2 x + \tau^2 < 0 .$$

Решив последнее неравенство, получаем

$$x \in \left(\frac{\tau^2 - \tau\sqrt{1-\tau^2}}{2\tau^2 - 1} ; \ \frac{\tau^2 + \tau\sqrt{1-\tau^2}}{2\tau^2 - 1} \right),$$

откуда, учитывая, что $|\alpha| = \sqrt{x}$, имеем

$$|\alpha| \in \left(\sqrt{\frac{\tau^2 - \tau\sqrt{1-\tau^2}}{2\tau^2 - 1}} ; \ \sqrt{\frac{\tau^2 + \tau\sqrt{1-\tau^2}}{2\tau^2 - 1}} \right),$$

что совпадает с (6.5.1).

Докажем теперь методом от противного, что при $\tau > \frac{1}{\sqrt{2}}$ справедливо неравенство (6.5.2), то есть неравенство

$$\sqrt{\frac{\tau^2-\tau\sqrt{1-\tau^2}}{2\tau^2-1}} > \frac{1}{\sqrt{2}}.$$

Допустим, что данное неравенство неверно, то есть допустим, что справедливо неравенство

$$\sqrt{\frac{\tau^2-\tau\sqrt{1-\tau^2}}{2\tau^2-1}} \le \frac{1}{\sqrt{2}}.$$

Отсюда следует, что

$$\frac{\tau^2-\tau\sqrt{1-\tau^2}}{2\tau^2-1} \le \frac{1}{2}.$$

Это неравенство равносильно неравенству

$$2\tau^2-2\tau\sqrt{1-\tau^2} \le 2\tau^2-1,$$

откуда следует, что

$$2\tau\sqrt{1-\tau^2} \ge 1.$$

Возводя в квадрат обе части последнего неравенства, имеем

$$4\tau^2\left(1-\tau^2\right) \ge 1.$$

Данное неравенство равносильно неравенству

$$4\tau^4-4\tau^2+1 \le 0.$$

Представив последнее неравенство в виде

$$\left(2\tau^2-1\right)^2 \le 0,$$

получаем $\tau=\frac{1}{\sqrt{2}}$, что противоречит условию $\tau>\frac{1}{\sqrt{2}}$. Следовательно, допущение неверно, что равносильно справедливости неравенства (6.5.2).

Докажем теперь справедливость двойного неравенства (6.5.3) при условии, что $1>\tau>\frac{1}{\sqrt{2}}$. Докажем сперва методом от противного, что

$$\sqrt{\frac{\tau^2+\tau\sqrt{1-\tau^2}}{2\tau^2-1}}>\tau\,.$$

Допустим, что справедливо неравенство

$$\sqrt{\frac{\tau^2+\tau\sqrt{1-\tau^2}}{2\tau^2-1}}\le\tau\,.$$

Из последнего неравенства получаем

$$\tau^2+\tau\sqrt{1-\tau^2}\le\tau^2\left(2\tau^2-1\right),$$

что равносильно неравенству

$$\sqrt{1-\tau^2}\le-2\tau\left(1-\tau^2\right).$$

Отсюда следует, что

$$\sqrt{1-\tau^2}\le 0\,,$$

что, в свою очередь, влечет равенство $\tau = 1$, которое противоречит условию $\tau < 1$. Следовательно, допущение неверно, а верно неравенство

$$\sqrt{\frac{\tau^2+\tau\sqrt{1-\tau^2}}{2\tau^2-1}}>\tau\,,$$

и тем самым доказана справедливость правой части двойного неравенства (6.5.3).

Теперь докажем методом от противного, что

$$\sqrt{\frac{\tau^2-\tau\sqrt{1-\tau^2}}{2\tau^2-1}}<\tau\,.$$

Допустим, что справедливо неравенство

$$\sqrt{\frac{\tau^2-\tau\sqrt{1-\tau^2}}{2\tau^2-1}}\ge\tau\,.$$

Из последнего неравенства получаем

$$\tau^2 - \tau\sqrt{1-\tau^2} \geq \tau^2\left(2\tau^2 - 1\right),$$

что равносильно неравенству

$$\sqrt{1-\tau^2} \leq 2\tau\left(1-\tau^2\right).$$

Отсюда следует, что

$$2\tau\sqrt{1-\tau^2} \geq 1.$$

Возведем обе части последнего равенства в квадрат и получим

$$4\tau^2\left(1-\tau^2\right) \geq 1.$$

Это неравенство равносильно неравенству

$$4\tau^4 - 4\tau^2 + 1 \leq 0,$$

то есть

$$\left(2\tau^2 - 1\right)^2 \leq 0,$$

что противоречит условию $\tau > \dfrac{1}{\sqrt{2}}$. Следовательно, допущение неверно, а верно неравенство

$$\sqrt{\frac{\tau^2 - \tau\sqrt{1-\tau^2}}{2\tau^2 - 1}} < \tau,$$

и тем самым доказана справедливость и левой части двойного неравенства (6.5.3).

§ 6.6. Решение статистической задачи в ATF-технологии связи

В **методе F** (составной части **ATF-**технологии связи), представленном в параграфе 6.4, действия Боба – стороны, принимающей сообщение – для определения каждого очередного бита принимаемого сообщения были сведены к измерению пар кубитов из массива из L пар кубитов и решению статистической задачи проверки по выборке заданного объема L простой гипотезы

$$H_0 : P(|01\rangle) = p_0 = |\alpha|^2$$

с альтернативой – тоже простой гипотезой

$$H_1 : P(|01\rangle) = p_1 = |\alpha|^2 + |\beta|^4,$$

где

$$\alpha, \beta \in \mathbb{C},\ |\alpha| > |\beta| > 0,\ |\alpha|^2 + |\beta|^2 = 1,\ \frac{|\alpha|^2}{\sqrt{|\alpha|^4 + |\beta|^4}} > \alpha_{\text{K}},$$

α_{K} – **амплитудная граница Ксения** (см. параграф 6.1).

Статистическая задача выбора из двух простых гипотез, то есть статистическая задача проверки простой гипотезы против альтернативы (также простой гипотезы) в математическом плане является известной решенной задачей. Это решение основано на лемме Неймана–Пирсона [35] и в определенном смысле является наилучшим (точнее, оптимальным) решением. В нашем случае в силу малости значения величины $|\beta|^4$ и, следовательно, близости (близки, но не равны) значений вероятностей p_0 и p_1, оправдано применение асимптотической версии указанного решения [35]. В соответствии с этим в данном параграфе по наперед заданным ошибкам первого рода δ_1 и второго рода δ_2 определим сперва необходимый объем L выборки и критическую границу $r_{\text{кр}}$.

Объем выборки L определяется из приблизительного равенства

$$L \approx \frac{\left(u(\delta_1)\sqrt{p_0(1-p_0)} + u(\delta_2)\sqrt{p_1(1-p_1)}\right)^2}{(p_0 - p_1)^2}, \tag{6.6.1}$$

а граница критерия $r_{\text{кр}}$ определяется из приблизительного равенства

$$r_{\text{кр}} \approx Lp_0 + u(\delta_1)\sqrt{Lp_0(1-p_0)}, \tag{6.6.2}$$

где $u(\delta_1)$, $u(\delta_2)$ определяются соответственно по заданным ошибкам первого и второго рода δ_1, δ_2 с использованием таблицы функции Лапласа $\Phi(x)$ [28] из равенств

$$\Phi\left(u(\delta_1)\right)=1-\delta_1,\ \Phi\left(u(\delta_2)\right)=1-\delta_2.$$

Используя равенства $p_0=|\alpha|^2$ и $p_1=|\alpha|^2+|\beta|^4$ для значений вероятностей p_0 и p_1, из равенств (6.6.1) и (6.6.2) получаем приблизительное равенство для определения значения объема выборки

$$L\approx\frac{|\alpha|}{|\beta|^7}\left(u(\delta_1)+u(\delta_2)\sqrt{|\alpha|^2+|\beta|^4}\right) \qquad (6.6.3)$$

и приблизительное равенство для определения значения критической границы

$$r_{\text{кр}}\approx L|\alpha|^2+u(\delta_1)\sqrt{L|\alpha|^2|\beta|^2}\,. \qquad (6.6.4)$$

Пусть L_1 – число пар кубитов, оказавшихся в состоянии $|01\rangle$ после измерения, проведенного Бобом над каждой парой кубитов из массива из L пар кубитов, для определения значения очередного бита сообщения.

Если

$$L_1<r_{\text{кр}}, \qquad (6.6.5)$$

то принимается гипотеза

$$H_0:P\left(|01\rangle\right)=p_0=|\alpha|^2$$

и Боб полагает, что значение принятого бита сообщения равно 0. Если же неравенство (6.6.5) не выполняется, то гипотеза H_0 отвергается и Боб полагает, что значение принятого бита равно 1.

Выводы по главе 6

1. Сформулирована **гипотеза Татьяна**, которая является краеугольным камнем **ATF**-технологии связи на основе квантовых ресурсов.

Проведено научное обоснование этой гипотезы. Показано, что она находится в согласии с известными теоретическими и экспериментальными результатами, связанными с физическим явлением квантового фазового перехода. Граница, после которой осуществляется квантовый фазовый переход, названа **границей Ксения**.

2. Разработан эффективный **алгоритм А** дистанционного изменения меры несепарабельности двухкубитных квантовых систем, изначально являющихся подсистемами трехкубитных квантовых систем в определенном несепарабельном состоянии. Это позволяет сделать вывод о том, что ресурс несепарабельности можно дистанционно как уменьшить, так и увеличить без непосредственного воздействия на двухкубитную подсистему на месте его нахождения.

3. Если уменьшение меры несепарабельности каждого из кубитов в указанных выше двухкубитных подсистемах в какой-то мере ожидаемо и объясняется тем, что ресурс несепарабельности уменьшается в результате разрушения (из-за действий Алисы при реализации **алгоритма А**) связи одного из кубитов исходной трехкубитной подсистемы с остальной частью трехкубитной квантовой системы, то увеличение меры несепарабельности является удивительной неожиданностью (так как по сути дела получаем технологию передачи физического ресурса в удаленную точку без использования среды передачи и без классического канала связи), что вселяет определенные надежды на возможные в будущем продуктивные практические приложения.

4. С допущением предположения о справедливости **гипотезы Т** разработан эффективный протокол детерминированной квантовой связи (**ATF-**технология связи), который при своей практической реализации позволяет передавать побитно сообщение, представленное в двоичном виде, от одного абонента к другому абоненту, удаленному в пространстве от первого. При этом для передачи сообщения не используется никакая среда и отсутствует классический канал связи.

Заключение

В заключение приведем в сжатой форме, путем перечисления, некоторые важные, на наш взгляд, результаты по разработке элементов теории несепарабельности многосоставных систем, изложенные в данной работе.

1. Описание физического явления несепарабельности для многосоставных квантовых систем, осуществленное на основе расширения описания Николя Жизана [33] для двухсоставных систем.

В соответствии с положениями квантовой физики вполне возможно и даже обычно для двух или более разделенных пространством объектов образовывать в действительности единое целое в том смысле, что если мы потревожим один из этих объектов, то среагируют <u>все</u>. Это и называется **несепарабельностью**. Состояние такой единой целой квантовой системы называется **несепарабельным состоянием**, а сама квантовая система называется **несепарабельной квантовой системой**.

При этом выражение «разделенных пространством» по отношению к объектам, составляющим квантовую систему, надо понимать прежде всего как **отсутствие между ними любого вида классической коммуникации**. И, как следствие, несепарабельность «вводит в физику нелокальные корреляции» [33], и этим она, в частности, отличается от всех известных физических ресурсов.

2. Строгое математическое определение несепарабельности многокубитных квантовых систем, совпадающее в случае двухкубитных квантовых систем с известным определением несепарабельности двухкубитных систем [56; 59].

Состояние $|\psi\rangle$ n-кубитной квантовой системы $A_1A_2\ldots A_n$ называется **сепарабельным состоянием**, если найдется подстановка $s \in \mathbb{S}_n$, такая, что состояние $\left|\psi^{(s)}\right\rangle$ квантовой системы $A_{s(1)}A_{s(2)}\ldots A_{s(n)}$ разлагается в тензорное произведение состояний размерности меньшей, чем 2^n.

Состояние $|\psi\rangle$ n-кубитной квантовой системы $A_1A_2\ldots A_n$ называется **несепарабельным состоянием**, если оно не является сепарабельным состоянием.

3. Разработан аналитический аппарат для исследования свойств несепарабельных многокубитных квантовых систем в составе следующих позиций:

- сформулирован набор определений различных типов сепарабельности и несепарабельности состояний многокубитных квантовых систем;
- установлены взаимосвязи между различными типами сепарабельности и несепарабельности состояний многокубитных квантовых систем, пригодные для исследования вопроса несепарабельности произвольного состояния многокубитной квантовой системы;
- проработаны направления вплоть до возможности получения решения задачи бинарной классификации состояний (определения, сепарабельно или несепарабельно) многокубитных квантовых систем для произвольного числа кубитов в квантовой системе; проработанность данных направлений характеризуется доведением до возможности получения критерия $\mathbf{K}_n$ (критерий **Константин**$_n$) несепарабельности и алгоритма $\mathbf{K}_n$ (алгоритм **Константин**$_n$) определения несепарабельности состояния n-кубитной квантовой системы при фиксированном числе кубитов n в квантовой системе;
- введено понятие **булевой маски** состояния n-кубитной квантовой системы; исследованы свойства булевых масок состояний многокубитных квантовых систем; доказано, что несепарабельность булевой маски квантового состояния является достаточным условием несепарабельности самого состояния; установлено, что булевы маски служат эффективным инструментом для решения задачи выяснения несепарабельности состояний многокубитных квантовых систем;
- введено понятие **нумератора весов** состояния n-кубитной квантовой системы; исследованы свойства нумераторов весов состояний

многокубитной квантовой системы; доказано, что если нумератор весов состояния не разлагается в произведение нумераторов двух состояний меньшей размерности, чем размерность исходного состояния, то исходное состояние является несепарабельным состоянием; установлено, что нумераторы весов служат эффективным инструментом для решения задачи выяснения несепарабельности состояний многокубитных квантовых систем.

4. Сформулирован и доказан критерий **K₃** (критерий **Константин₃**) несепарабельности состояний трехкубитных квантовых систем. В силу особой важности (по нашим представлениям) этого критерия приведем его формулировку. В этих целях напомним соответствующие обозначения.

Пусть $|\psi\rangle = (a_0,\ a_1,\ a_2,\ a_3,\ a_4,\ a_5,\ a_6,\ a_7)^{\mathrm{T}}$ – произвольное состояние трехкубитной квантовой системы, где $a_k \in \mathbb{C}$, $k \in \{0,\ 1,\ \ldots,\ 7\}$,

$$|a_0|^2 + |a_1|^2 + |a_2|^2 + |a_3|^2 + |a_4|^2 + |a_5|^2 + |a_6|^2 + |a_7|^2 = 1\,.$$

Положим

$$V_{21}^{(0)} = \{a_0a_5 - a_1a_4,\ a_0a_6 - a_2a_4,\ a_0a_7 - a_3a_4,\\ a_1a_6 - a_2a_5,\ a_1a_7 - a_3a_5,\ a_2a_7 - a_3a_6\},$$

$$V_{21}^{(1)} = \{a_0a_3 - a_1a_2,\ a_0a_6 - a_2a_4,\ a_0a_7 - a_2a_5,\\ a_1a_6 - a_3a_4,\ a_1a_7 - a_3a_5,\ a_4a_7 - a_5a_6\},$$

$$V_{21}^{(2)} = \{a_0a_5 - a_1a_4,\ a_0a_3 - a_1a_2,\ a_0a_7 - a_1a_6,\\ a_3a_4 - a_2a_5,\ a_4a_7 - a_5a_6,\ a_2a_7 - a_3a_6\}.$$

Критерий K₃. Состояние $|\psi\rangle$ трехкубитной квантовой системы является несепарабельным состоянием тогда и только тогда, когда каждый из наборов величин $V_{21}^{(0)}$, $V_{21}^{(1)}$ и $V_{21}^{(2)}$ содержит ненулевой элемент.

Аналогичный критерий получен и для состояний четырехкубитной квантовой системы, то есть получен критерий **К$_4$** (критерий **Константин$_4$**).

5. Полностью решена задача бинарной классификации состояний трехкубитной и четырехкубитной квантовых систем.

6. Определена количественная характеристика $V\left(|\psi\rangle\right)$ несепарабельности произвольного состояния $|\psi\rangle$ многокубитной квантовой системы, так называемая **V-мера** (**мера Виолетта**); $V\left(|\psi\rangle\right)$ – мера несепарабельности состояния $|\psi\rangle$. Исследованы свойства этой меры. **V-мера** является адекватной (по нашим представлениям) количественной характеристикой ресурса несепарабельности состояний многокубитных квантовых систем, позволяющей получить значение несепарабельности состояния многокубитной системы с позиции наименее «надежного» звена (подсистемы исходной системы) по несепарабельности во всей исходной квантовой системе.

7. Для произвольного состояния $|\psi\rangle = \left(a_0,\ a_1,\ a_2,\ a_3\right)^{\mathrm{T}}$ двухкубитной квантовой системы, где $a_k \in \mathbb{C}$, $k \in \{0,\ 1,\ 2,\ 3\}$,

$$|a_0|^2 + |a_1|^2 + |a_2|^2 + |a_3|^2 = 1,$$

значение **V-меры** совпадает со значением меры **согласованность** (concurrence), то есть, справедливо равенство

$$V\left(|\psi\rangle\right) = 2\left|a_0 a_3 - a_1 a_2\right|.$$

8. Для произвольного состояния $|\psi\rangle = \left(a_0,\ a_1,\ \ldots,\ a_7\right)^{\mathrm{T}}$ трехкубитной квантовой системы, где $a_k \in \mathbb{C}$, $k \in \{0,\ 1,\ \ldots,\ 7\}$,

$$|a_0|^2 + |a_1|^2 + |a_2|^2 + |a_3|^2 + |a_4|^2 + |a_5|^2 + |a_6|^2 + |a_7|^2 = 1,$$

значение **V-меры** определяется равенством

$$V(|\psi\rangle) = 2\cdot\min\Big\{\Big(|a_0a_5 - a_1a_4|^2 + |a_0a_6 - a_2a_4|^2 + |a_0a_7 - a_3a_4|^2 +$$

$$+|a_1a_6 - a_2a_5|^2 + |a_1a_7 - a_3a_5|^2 + |a_2a_7 - a_3a_6|^2\Big)^{\frac{1}{2}},$$

$$\Big(|a_0a_3 - a_1a_2|^2 + |a_0a_6 - a_2a_4|^2 + |a_0a_7 - a_2a_5|^2 +$$

$$+|a_1a_6 - a_3a_4|^2 + |a_1a_7 - a_3a_5|^2 + |a_4a_7 - a_5a_6|^2\Big)^{\frac{1}{2}},$$

$$\Big(|a_0a_5 - a_1a_4|^2 + |a_0a_3 - a_1a_2|^2 + |a_0a_7 - a_1a_6|^2 +$$

$$+|a_3a_4 - a_2a_5|^2 + |a_4a_7 - a_5a_6|^2 + |a_2a_7 - a_3a_6|^2\Big)^{\frac{1}{2}}\Big\}.$$

9. Для произвольного состояния четырехкубитной квантовой системы получено выражение значения **V-меры** через амплитуды состояния в вычислительном базисе.

10. Исследовано проявление ресурса несепарабельности на стационарных состояниях двухкубитных, трехкубитных и четырехкубитных квантовых систем, состоящих из кубитов-спинов-½ с одним и тем же гиромагнитным отношением и находящихся в постоянном магнитном поле.

11. Разработаны новая квантовая **ATF**-технология связи и ее научные основы.

Основные качественные характеристики этой технологии связи следующие:

- передача информации осуществляется без использования ныне известных видов материи (без физической среды);
- невозможность установления факта передачи и невозможность перехвата или искажения передаваемой информации;
- передача информации на любое (неограниченное) расстояние;

- передача информации без значительных энергетических затрат;
- время передачи информации не зависит от величины расстояния между абонентами (фиксировано в реальном масштабе);
- физические свойства среды, в которой находятся абоненты, не влияют на качество связи.

Научные основы **ATF-**технологии связи представляют собой результаты исследований свойств ресурса несепарабельных состояний квантовых систем, определения его количественной характеристики и установления связи между количественной характеристикой и координатами соответствующего состояния в вычислительном базисе.

Однако мы должны заметить, что результаты по **ATF-**технологии связи являются модельными. Данное обстоятельство связано с тем, что пока еще не получены в необходимом количестве убедительные экспериментальные подтверждения гипотезы **T**, справедливость которой предполагается в **ATF-**технологии связи.

Литература

1. Алиев Ф.К., Бородин А.М., Клюев А.В. К вопросу о сепарабельности состояний трёхкубитных квантовых систем // Обозрение прикладной и промышленной математики. Т. 16. вып. 4. М.: ТВП, 2009.

2. Алиев Ф.К., Бородин А.М., Клюев А.В. О состояниях с максимальной мерой несепарабельности двухкубитных квантовых систем // Обозрение прикладной и промышленной математики. Т. 16. Вып. 4. М.: ТВП. 2009.

3. Алиев Ф.К. Бородин А.М., Клюев А.В. К вопросу о сепарабельности состояний многокубитных квантовых систем // Обозрение прикладной и промышленной математики. Т. 17. Вып. 5. М.: ТВП. 2010.

4. Алиев Ф.К. Бородин А.М. О возможности применения квантового механизма телепортации для представления произвольной двоичной последовательности в виде суммы двух случайных равновероятных двоичных последовательностей // Обозрение прикладной и промышленной математики. Т. 17. Вып. 5. М.: ТВП. 2010.

5. Алиев Ф.К., Бородин А.М., Корольков А.В. О связи свойств несепарабельности состояния многокубитной квантовой системы и его булевой проекции // Материалы XI науч.-техн. конф. Секция № 13. М., 2011.

6. Алиев Ф.К., Бородин А.М. Достаточные условия несепарабельности состояний трёхкубитной квантовой системы // Материалы XI науч.-техн. конф. Секция № 13. М., 2011.

7. Алиев Ф.К. О состояниях квантовой системы из двух частиц со спиновым числом 1/2 и разными гиромагнитными отношениями // Материалы XI Науч.-техн. конф. по криптографии. Секция «Проблемы квантовой криптографии». М., 2011.

8. Алиев Ф.К. О новом способе передачи информации // Материалы XI науч.-техн. конф. Секция № 13. М., 2011.

9. Алиев Ф.К., Бородин А.М., Вассенков А.В., Матвеев Е.А. О несепарабельных состояниях многочастичных квантовых систем // В сб. научных трудов по итогам работы VI–VII Всеросс. науч.-техн. конф. шко-

лы-семинара «Информационная безопасность – актуальная проблема современности». Краснодар: ФВАС (г. Краснодар). 2013. Т. 1. С. 77–80.

10. Алиев Ф.К., Бородин А.М., Вассенков А.В., Матвеев Е.А., Царьков А.Н., Шеремет И.А. О способе дистанционного изменения меры несепарабельности квантовых систем и возможности его применения в области связи. Серпухов: Изв. Института инженерной физики. 2014. № 3(33). С. 30–38.

11. Алиев Ф.К., Бородин А.М., Вассенков А.В., Матвеев Е.А., Царьков А.Н., Шеремет И.А. ATF-технология связи, основанная на использовании ресурса несепарабельных состояний квантовых систем // Наукоемкие технологии. 2015. № 1. С. 65–78.

12. Алиев Ф.К., Матвеев Е.А., Шеремет И.А. Критерий несепарабельности состояния трехкубитной квантовой системы // Материалы XII науч.-техн. конф. по криптографии. Секция № 12. М., 2016.

13. Алиев Ф.К., Бородин А.М., Матвеев Е.А., Шеремет И.А. Двухкубитные состояния А.В. Клюева // В сб. науч. трудов по итогам работы XII–XIII Всеросс. науч.-техн. конф. школы-семинара «Информационная безопасность – актуальная проблема современности». Краснодар, 2016.

14. Алиев Ф.К., Бородин А.М., Матвеев Е.А., Шеремет И.А. О количественной характеристике ресурса несепарабельности многокубитных квантовых систем // В сб. научных трудов по итогам работы XII–XIII Всеросс. науч.-техн. конф. школы-семинара «Информационная безопасность – актуальная проблема современности». Краснодар, 2016.

15. Алиев Ф.К., Матвеев Е.А., Шеремет И.А. О характеристиках критерия принятия решения в ATF-технологии связи // В сб. научных трудов по итогам работы XII–XIII Всерос. науч.-техн. конф. школы-семинара «Информационная безопасность – актуальная проблема современности». Краснодар, 2016.

16. Алиев Ф.К., Матвеев Е.А., Шеремет И.А. К вопросу о бинарной классификации состояний спиновых квантовых систем // В сб. научных трудов по итогам работы XII–XIII Всеросс. науч.-техн. конф. школы-семинара «Информационная безопасность – актуальная проблема современности». Краснодар, 2016.

17. Балашов В.В., Долинов В.К. Курс квантовой механики. Ижевск: НИЦ «Регулярная и хаотическая динамика». 2001. 336 с.

18. Барсуков О.А., Ельяшевич М.А. Основы атомной физики. М.: Научный мир. 2006. 648 с.

19. Баумастер Д., Экерт А., Цайлингер А. Физика квантовой информации. М.: Постмаркет. 2002. 376 с.

20. Белинский А.В. Квантовые измерения: учебное пособие. М.: БИНОМ. 2008. 182 с.

21. Берман Г.П., Дулен Г.Д., Майньери Р., Цифринович В.И. Введение в квантовые компьютеры. Москва–Ижевск: НИЦ «Регулярная и хаотическая динамика». 2004. 188 с.

22. Боровков А.А. Теория вероятностей. М.: Наука. 1976. 352 с.

23. Будкер Д., Кимбелл Д., ДеМиль Д. Атомная физика. Освоение через задачи: Пер. с англ. М.: Физматлит. 2009. 400 с.

24. Валиев К.А., Кокин А.А. Квантовые компьютеры: надежда и реальность. Москва–Ижевск: НИЦ «Регулярная и хаотическая динамика». 2004. 320 с.

25. Воеводин В.В., Кузнецов Ю.А. Матрицы и вычисления. М.: Наука. 1984. 320 с.

26. Гантмахер Ф.Р. Теория матриц. Изд. 4-е. М.: Наука. 1988. 560 с.

27. Глухов М.М., Елизаров В.П., Нечаев А.А. Алгебра. Т. 1, 2. М.: Гелиос–АРВ. 2003. 336 с., 416 с.

28. Гмурман В.Е. Теория вероятностей и математическая статистика. М.: Высшая Школа. 2000. 479 с.

29. Гринштейн Дж., Зайонц А. Квантовый вызов. Современные исследования оснований квантовой механики. М.: ИД «Интеллект». 2008. 400 с.

30. Делоне Н.Б. Квантовая природа вещества. М.: Физматлит. 2008. 208 с.

31. Дориченко С.А., Ященко В.В. 25 этюдов о шифрах. М.: ТЕИС. 1994. 69 с.

32. Емельянов В.И., Владимирова Ю.В. Квантовая физика. Биты и кубиты: Учеб. пособие. М.: Физический факультет МГУ. 2012. 176 с.

33. Жизан Н. Квантовая случайность: Пер. с англ. М.: Альпина нон-фикшн. 2016. 202 с.

34. Иванов М.Г. Как понимать квантовую механику. М.–Ижевск: НИЦ «Регулярная и хаотическая динамика». 2012. 516 с.

35. Ивченко Г.И., Медведев Ю.И. Математическая статистика. М.: ЛИБРОКОМ. 2014. 352 с.

36. Имре Ш., Балаж Ф. Квантовые вычисления и связь. Инженерный подход. М.: Физматлит. 2008. 320 с.

37. Кайе Ф., Лафлам Р., Моска М. Введение в квантовые вычисления. М.–Ижевск: НИЦ «Регулярная и хаотическая динамика». 2009. 360 с.

38. Кашурников В.А., Красавин А.В. Численные методы квантовой статистики. М.: Физматлит. 2010. 628 с.

39. Килин С.Я. и др. Квантовая криптография: идеи и практика. Минск: Белорусская наука. 2007. 391 с.

40. Клышко Д.Н. Фотоны и нелинейная оптика. М.: Наука. 1980. 302 с.

41. Клышко Д.Н. Физические основы квантовой электроники. М.: Наука. 1986. 280 с.

42. Кокин А.А. Твердотельные квантовые компьютеры на ядерных спинах. М.–Ижевск: Институт компьютерных исследований. 2004. 204 с.

43. Корн Г., Корн Т. Справочник по математике для научных работников и инженеров. М.: Наука. 1984. 833 с.

44. Кудрявцев Л.Д. Курс математического анализа. Т. 1, 2. М.: Высшая школа. 1981. 687 с., 584 с.

45. Ланкастер П. Теория матриц. М.: Наука. 1982. 272 с.

46. Мальцев А.И. Основы линейной алгебры. М.: Наука. 1970. 400 с.

47. Матвеев А.Н. Атомная физика: учебное пособие для вузов. М.: Мир и образование. 2007. 432 с.

48. Матвеев Е.А. Нумераторы весов состояний квантовых систем // Материалы XII науч.-техн. конф. Секция № 12. М., 2016.

49. Никитин Н.В., Шарапова П.Р., Колотинский Н.В. Сборник задач по квантовой физике: учебное пособие. М.: КДУ. 2015. 144 с.

50. Нильсен М., Чанг И. Квантовые вычисления и квантовая информация. М.: Мир. 2006. 824 с.

51. Перри Р. Элементарное введение в квантовые вычисления: Пер. с англ. Учеб. пособие. Долгопрудный: Интеллект. 2015. 208 с.

52. Прескилл Дж. Квантовая информация и квантовые вычисления. Т. 1. М.–Ижевск: НИЦ «Регулярная и хаотическая динамика». 2008. 464 с.

53. Самарцев В.В. Коррелированные фотоны и их применение. М.: Физматлит. 2014. 168 с.

54. Сергеев Н.А., Рябушкин Д.С. Основы квантовой теории ядерного магнитного резонанса. М.: Логос. 2013. 272 с.

55. Сокольников И. С. Тензорный анализ. М.: КомКнига. 2007. 376 с.

56. Стиб В.-Х., Харди Й. Задачи и их решения в квантовых вычислениях и квантовой теории информации. Ижевск: НИЦ «Регулярная и хаотическая динамика». 2007. 296 с.

57. Фейнман Р.Ф., Лейтон Р.Б., Сэндс М. Фейнмановские лекции по физике. Вып. 8, 9 // Квантовая механика: учебное пособие. М.: ЛКИ. 2008. 528 с.

58. Фриш С.Э. Оптические спектры атомов. СПб.: Лань. 2010. 656 с.

59. Холево А.С. Квантовые системы, каналы, информация. М.: МЦНМО. 2010. 328 с.

60. Хренников А.Ю. Введение в квантовую теорию информации. М.: Физматлит. 2008. 284 с.

61. Ципенюк Ю.М. Квантовая микро- и макрофизика. М.: Физматкнига. 2006. 640 с.

62. Чернявский А.Ю. Минимум энтропии измерений как вычислимая мера запутанности многочастичных квантовых состояний: Дисс. ... канд. техн. наук. М.: Физико-технологический институт РАН. 2010. 130 с.

63. Шляйх В.П. Квантовая оптика в фазовом пространстве: Пер. с англ. М.: Физматлит. 2005. 760 с.

64. Эндрюс Г. Теория разбиений: Пер. с англ. М.: Наука. 1982. 256 с.

65. Aliev F.K., Borodin A.M., Vassenkov A.V., Matveev E.A., Tzarkov A.N., Sheremet I.A. ATF-technology of communication based on using the

resource of entangled states of quantum systems // Electromagnetic Waves and Electronic Systems. 2015. V. 20. № 3. P. 60–72.

66. Aspect A., Grangier Ph., Roger G. // Phys. Rev. Lett. 49. 91. 1982.

67. Aspect A., Dalibard J., Roger G. // Phys. Rev. Lett. 49. 1804. 1982.

68. Bell J.S. Physics 1. 195. 1964.

69. Bennett C.H., Brassard G. Quantum cryptography: Public key distribution and coin tossing // In Proceedings of IEEE International Conference on Computers, Systems and Signal Processing. IEEE, New York. 1984. Bangalore, India, December 1984. P. 175–179.

70. Bennett C.H. Quantum cryptography using any two nonorthogonal states // Phys. Rev. Lett. 1992. 68(21). P. 3121–3124.

71. Bennett C.H., Brassard G., Crépeau C., Jozsa R., Peres A., Wootters W.K. Teleporting an Unknown Quantum State via Dual Classical and Einstein-Podolsky-Rosen Channel // Phys. Rev. Lett. 1993. V. 70. № 13. P. 1895–1899.

72. Bennett C.H., Bernstein H.J., Popescu S., Schumacher B. // Phys. Rev. 1996. A 53. 2046.

73. Bennett C.H., DiVincenzo D.P., Smolin J.A., Wootters W.K. // Phys. Rev. 1996. A 54. 3824.

74. Dieks D. Communication by EPR devices // Phys. Lett. 1982. A. 92(6). P. 271–272.

75. Dur W., Vidal G., Cirac J.I. Phys. Rev. 2000. A 62. 062314.

76. Einstein A., Podolsky B. Rosen N. Phys. Rev. 1935. 47 777.

77. Greenberger D.M., Horne M.A., Shimony A., Zeilinger A. Bell's theorem without inequalities // Amer. J. Phys. 1990. V. 58. P. 1131–1143.

78. Hanson R. et al. Unconditional quantum teleportation between distant solid-state qubits, arXiv: 1404.4369v3 [quant-ph] 3Jun 2014.

79. Hanson R. et al. Experimental loophole-free violation of a Bell inequality using entangled electron spins separated by 1.3 km, arXiv: 1508.05949v1 [quant-ph] 24 Aug 2015.

80. Hill S., Wootters W.K. Phys. Rev. Lett. 1997. 78, 5022.

81. Meyer D., Wallach N. Global entanglement in multiparticle systems // Journal of Mathematical Physics. 2002. V. 43. P. 4273.

82. Neumann P., Mizuochi N., Rempp F., Hemmer P., Watanabe H., Yamasaki S., Jacques V., Gaebel T., Jelezko F., Wrachtrup J. Multipartite entanglement among single spins in diamond, Science 320, 1326. 2008.

83. Nielsen M. Quantum Information Theory. Ph. D. thesis. University of New Mexico. 1998.

84. O'Connor K.M., Wootters W.K. Entangled Rings. Department of Physics, Williams College. Williamstown. MA 01267. USA. 2000.

85. Pan J.–W., Bouwmeester D., Daniell H., Wienfurter H., Zeilinger A. Experimental test of quantum nonlocality in three-photon Greenberger-Horne-Zeilinger entanglement. Nature. 2000. V. 403. P. 515–519.

86. Rungta P., Buzer V., Caves C.M., Hillery M., Milburn G.J. Universal state inversion and concurrence in arbitrary dimensions // Phys. Rev. 2001. A 64. 042315.

87. Schmidt E. Zur Theorie der linearen und nichtlinearen Integralgleichungen. Math. Annalen. 1906. 63: 433–476.

88. Schrödinger E. Naturwissenschaften 23 807, 823, 844. 1935.

89. Subir Sachdev. Quantum Phase Transitions. Encyclopedia of Mathematical Physics. USA. 2004.

90. Wootters W.K., Zurek W.H. A single quantum cannot be cloned // Nature. 1982. 299: 802–803.

91. Wootters W.K. Entanglement of Formation of an Arbitrary State of Two Qubits. Department of Physics, Williams College, Williamstown MA 01267. USA. 1997.

92. Wootters W.K. Entangled chains. Department of Physics, Williams College, Williamstown MA 01267. USA. 2003.

Предметный указатель

Fizuli K. Aliev, Andrey V. Korolkov, Evgeniy A. Matveev

ENTANGLED STATES OF MULTI-QUBIT QUANTUM SYSTEMS

Monograph

Edited by F. K. Aliev

R e v i e w e r s:

Barkovsky S.S. – Dr. Sc. (Eng.), lecturer of Public Administration
and National Security Department of Military Academy of General Staff
of Armed Forces of Russian Federation (Moscow)

Rozhkov M.I. – Dr. Sc. (Eng.), professor of Information Security Department
of School of Applied Mathematics at Moscow Institute of Electronics
and Mathematics of National Research University «Higher School of Economics»
(Moscow)

Aliev F.K., Korolkov A.V., Matveev E.A.

Entangled States of Multi-Qubit Quantum Systems. Monograph / Edited by *F.K. Aliev*. – M.: Radiotekhnika. 2017. – 320 s.

The monograph considers development of basic elements of theory of entangled states of multi-qubit quantum systems. Presented results refine the understanding of entanglement – one of the main resources of modern quantum technologies of data storage, processing and transfer, which does not have classical analogues; these results expand the possibilities of developing quantum algorithms and building quantum cryptography and communication systems. One of the models of communication technology based on using the quantum physical resource of entanglement is given in the book.

Aimed at a wide range of readers interested in new tendencies of development of information and telecommunication technologies.

CONTENTS

About the authors

ALIEV Fizuli K. – Dr. Sc. (Phys.-Math.), principal adviser of Main Directorate of Information and Telecommunication Technologies Development of Ministry of Defence of the Russian Federation (Moscow)

KOROLKOV Andrey V. – Ph. D. (Eng.), docent, corresponding member of Academy of Cryptography of Russian Federation, chairholder at Moscow Technical University (MIREA), head of laboratory at Academy of Cryptography of Russian Federation (Moscow)

MATVEEV Evgeniy A. – director of scientific and technical enterprise «Cryptosoft» (Penza, Russian Federation)

Для новых идей

Для новых идей

Для новых идей

Для новых идей

Для новых идей

Научное издание

Авторы:

Физули Камилович Алиев

Андрей Вячеславович Корольков

Евгений Анатольевич Матвеев

НЕСЕПАРАБЕЛЬНЫЕ СОСТОЯНИЯ МНОГОКУБИТНЫХ КВАНТОВЫХ СИСТЕМ

Монография

Под редакцией *Ф. К. Алиева*

Изд. № 103. Сдано в набор 10.03.2017.
Подписано в печать 5.04.2017. Формат 70×100 1/16
Бумага офсетная. Гарнитура Таймс
Печать офсетная
Уч.изд.л. 26. Тираж 1000 экз. Зак. №

Издательство «Радиотехника»
107031, Москва, К-31, Кузнецкий мост, д. 20/6
Тел./факс: (495)621-48-37; 625-78-72, 625-92-41
E-mail: info@radiotec.ru; www.radiotec.ru

Отпечатано в типографии «ПАБЛИТ»