ISSN 0233-6723

ИТОГИ НАУКИ И ТЕХНИКИ

СОВРЕМЕННАЯ МАТЕМАТИКА И ЕЕ ПРИЛОЖЕНИЯ

Тематические обзоры

Том 138

Москва 2017

ISSN 0233–6723

РОССИЙСКАЯ АКАДЕМИЯ НАУК

ВСЕРОССИЙСКИЙ ИНСТИТУТ
НАУЧНОЙ И ТЕХНИЧЕСКОЙ ИНФОРМАЦИИ
(ВИНИТИ РАН)

ИТОГИ НАУКИ И ТЕХНИКИ

СЕРИЯ
СОВРЕМЕННАЯ МАТЕМАТИКА
И ЕЕ ПРИЛОЖЕНИЯ

ТЕМАТИЧЕСКИЕ ОБЗОРЫ

Том 138

КВАНТОВЫЕ ВЫЧИСЛЕНИЯ

Москва 2017

СОДЕРЖАНИЕ

ИТОГИ НАУКИ И ТЕХНИКИ.
Современная математика и ее приложения.
Тематические обзоры.
Том 138 (2017). С. 3–10

УДК 519.722, 519.724, 517.983

ОБ АЛГЕБРАИЧЕСКИХ МЕТОДАХ ИССЛЕДОВАНИЯ КВАНТОВЫХ КАНАЛОВ ПЕРЕДАЧИ ИНФОРМАЦИИ

© 2017 г. **Г. Г. АМОСОВ**

Аннотация. Представление Крауса квантового канала передачи информации широко используется на практике. Мы приводим примеры разложений Крауса для каналов, обладающих свойством ковариантности относительно максимальной коммутативной группы унитарных операторов. Показано, что в таких задачах, как оценка минимальной выходной энтропии канала, важно подбирать представление Крауса с неминимальным числом операторов Крауса. Также приведены некоторые алгебраические свойства некоммутативных операторных графов, порожденных операторами Крауса, для случая квантовых каналов, демонстрирующих явление суперактивации.

***Ключевые слова*:** квантовый канал, разложение Крауса, минимальная выходная энтропия, некоммутативный операторный граф, квантовая пропускная способность с нулевой ошибкой.

***AMS Subject Classification*:** 94A17, 94A40, 47C05

1. Введение. Создание в 1970-х гг. квантовой теории статистических решений (см. [4]) привлекло внимание к изучению структурных свойств вполне положительных отображений (см. [10]) и операторных систем (см. [11]). Новая волна интереса к таким вопросам возникла после доказательства квантовой теоремы кодирования (см. [14, 5]) и появления концепции квантовых кодов, исправляющих ошибки (см. [24]). Для конечномерных пространств формулы для пропускной способности были получены в важных частных случаях (см. [18, 19, 15]). Также был получен ряд результатов, проясняющих структуру квантовых каналов (см. [22, 21, 6]). В [17] было определено выпуклое замыкание выходной энтропии квантового канала и доказано, что такая функция обладает свойством сильной супераддитивности для тождественного канала и канала, разрушающего сцепленность. В дальнейшем это свойство было доказано для деполяризующего квантового канала в [7] с некоторой неточностью, которая была исправлена в [1]. Структура некоммутативных графов, порожденных операторами Крауса, имеет также важное значение в теории квантовых кодов исправляющих ошибки (см. [16]). Данная тематика близка к проблеме о передаче квантовой информации через квантовый канал с нулевой ошибкой (см. [23]). Недавно были также обнаружены связи таких исследований с алгебраической геометрией (см. [8]).

2. Ключевые обозначения и определения. Всюду в этой работе мы будем использовать следующие стандартные обозначения:

$B(H,K)$ — алгебра всех ограниченных операторов, действующих из гильбертова пространства H в гильбертово пространство K, $B(H)=B(H,H)$, элементы $B(H,K)$ и $B(H)$ будут обозначаться заглавными латинскими буквами $A,B,C,\dots$, тождественный оператор будет обозначаться I или I_H, если нужно уточнить, в каком пространстве он действует;

$\mathfrak{S}(H)$ — выпуклое множество состояний (положительных ядерных операторов с единичным следом) в гильбертовом пространстве H, элементы $\mathfrak{S}(H)$ будут обозначаться греческими буквами $\rho,\sigma,\dots$;

$S(\rho)=-Tr\rho\log\rho$ — энтропия фон Неймана состояния $\rho\in\mathfrak{S}(H)$;

$\mathrm{Mat}_n(\mathbb{C})$ — алгебра всех квадратных матриц размера $n\times n$;

$\mathrm{Hom}(A,\mathrm{Mat}_n(\mathbb{C}))$ — множество всех гомоморфизмов из алгебры A в алгебру $\mathrm{Mat}_n(\mathbb{C})$;

$GL_n(\mathbb{C})$ — главная линейная группа, состоящая из обратимых матриц из $\mathrm{Mat}_n(\mathbb{C})$.

Рассмотрим аффинное отображение $\Phi : \mathfrak{S}(H) \to \mathfrak{S}(K)$. Линейное отображение $\Phi^* : B(K) \to B(H)$ называется *сопряженным* к Φ, если

$$\mathrm{Tr}(\rho\Phi^*(A)) = \mathrm{Tr}(\Phi(\rho)A) \quad \text{для любых } \rho \in \mathfrak{S}(H) \text{ и } A \in B(K).$$

Аффинное отображение $\Phi : \mathfrak{S}(H) \to \mathfrak{S}(K)$ называется *квантовым каналом*, если отображение Φ^* является вполне положительным, т.е. положительны все отображения вида $\Phi^* \otimes \mathrm{Id}_n$, где Id_n — тождественное отображение алгебры $B(H_n)$, $\dim H_n = n$.

Выберем в гильбертовом пространстве H, $\dim H = d$, ортонормированный базис

$$\{e_j,\ 0 \leqslant j \leqslant d-1\}$$

и определим пару унитарных операторов U и V по формуле

$$Ue_j = e_{j+1 \mod d}, \quad Ve_j = e^{2\pi ij/n}e_j, \quad 0 \leqslant j \leqslant d-1. \tag{1}$$

Элементы семейства унитарных операторов $\{U^kV^m,\ 0 \leqslant k,m \leqslant d-1\}$ называются *обобщенными матрицами Паули*. Обобщенные матрицы Паули $W_{k,m} = U^kV^m$ иногда называют также *операторами Вейля*, поскольку они удовлетворяют соотношениям Гейзенберга—Вейля вида

$$W_{k,m}W_{k',m'} = e^{\frac{2\pi i}{d}(k'm-km')}W_{k',m'}W_{k,m}, \quad 0 \leqslant k,m \leqslant d-1.$$

Пусть

$$\pi_{k,m} \geqslant 0, \quad \sum_{k=0}^{d-1}\sum_{m=0}^{d-1}\pi_{k,m} = 1,$$

— некоторое распределение вероятностей. Тогда формула

$$\Phi(\rho) = \sum_{k=0}^{d-1}\sum_{m=0}^{d-1}\pi_{k,m}W_{k,m}\rho W_{k,m}^*, \quad \rho \in \mathfrak{S}(H), \tag{2}$$

определяет квантовый канал, который мы будем называть *каналом Вейля*.

3. Разложение Крауса и некоммутативный операторный граф. В [10] было показано, что любое вполне положительное отображение $\Phi^* : B(K) \to B(H)$ имеет вид

$$\Phi^*(A) = \sum_{n=1}^{N} V_n^*AV_n, \quad A \in B(H), \tag{3}$$

где $V_n \in B(H,K)$, $N \leqslant +\infty$. Из представления (3) немедленно вытекает, что любой квантовый канал $\Phi : \mathfrak{S}(H) \to \mathfrak{S}(K)$ имеет вид

$$\Phi(\rho) = \sum_{n=1}^{N} V_n\rho V_n^*, \quad \rho \in \mathfrak{S}(H), \quad N \leqslant +\infty; \tag{4}$$

при этом сохранение следа приводит к условию

$$\sum_{n=1}^{N} V_n^*V_n = I_K.$$

Формула (4) называется *разложением Крауса* квантового канала Φ, а V_n — операторами Крауса. Операторы Крауса определены неоднозначно, но однозначно задано их минимальное число N, называемое *рангом Чоя* (см. [10]). Тем не менее, более полезным часто бывает использование представления (4) с числом операторов Крауса, превышающим ранг Чоя. Определим линейное пространство $\mathcal{G}(\Phi)$, состоящее из операторов из $B(K)$, по формуле

$$\mathcal{G}(\Phi) = \overline{\mathrm{Lin}(V_j^*V_k,\ 1 \leqslant j,k \leqslant N)}. \tag{5}$$

Пространство (5) называется *некоммутативным операторным графом, ассоциированным с каналом* Φ. В отличие от операторов Крауса, некоммутативный операторный граф однозначно определяется каналом Φ (см. [11]). Линейное пространство $\mathcal{V} = \mathcal{G}(\Phi)$ обладает свойством

$$I \in \mathcal{V},\ A \in \mathcal{V} \Rightarrow A^* \in \mathcal{V}. \tag{6}$$

Линейные пространства операторов $\mathcal{V}$, обладающие свойством (6), принято называть *некоммутативными операторными системами*. В [12, 13] было показано, что любая некоммутативная операторная система $\mathcal{V}$ является графом $\mathcal{G}(\Phi)$, ассоциированным с некоторым квантовым каналом Φ. При этом канал Φ неоднозначно восстанавливается по $\mathcal{V}$.

Пример 1. *Канал Вейля, инвариантный относительно максимальной коммутативной группы унитарных операторов.* Пусть гильбертово пространство H имеет размерность $\dim H = d$. Воспользовавшись обобщенными матрицами Паули (1), определим квантовый канал по формуле

$$\Phi(\rho) = \sum_{k=0}^{d-1} r_k U^k \rho U^{*k} + \frac{p}{d} \sum_{k=0}^{d-1} \sum_{m=1}^{d-1} U^k V^m \rho V^{*m} U^{*k}, \quad \rho \in \mathfrak{S}(H), \tag{7}$$

где $r_k \geqslant 0$, $p \geqslant 0$, $\sum\limits_{k=0}^{d-1} r_k + p = 1$. Канал (7) является частным случаем канала Вейля (2).

С другой стороны, если в пространстве произвольной конечной размерности d положить $p = 0$, получим

$$\Phi(\rho) = \sum_{k=0}^{d-1} r_k U^k \rho U^{*k}. \tag{8}$$

Каналы (8) называются каналами, демпфирующими фазу; они были подробно изучены в [1, 2]. Отметим, что каналами, демпфирующих фазу, являются каналы Φ_k следующего вида:

$$\Phi_k(\rho) = \left(1 - \frac{d-1}{d} p\right) \rho + \frac{p}{d} \sum_{s=1}^{d-1} (U^k V)^s \rho (V^* U^{k*})^s, \quad \rho \in \mathfrak{S}(H), \tag{9}$$

где $\dim H = d$, $0 \leqslant k \leqslant d-1$.

Обозначим $\mathcal{U}$ максимальную коммутативную группу унитарных операторов, порожденную обобщенными матрицами Паули $\{U^n,\ 0 \leqslant n \leqslant d-1\}$.

Предложение 1. *Канал* (7) *является ковариантным относительно максимальной коммутативной группы унитарных операторов* $\mathcal{U}$ *в том смысле, что*

$$\Phi(T\rho T^*) = T\Phi(\rho)T^*, \quad \rho \in \mathfrak{S}(H), \quad T \in \mathcal{U}.$$

Доказательство. Заметим, что

$$\Phi(U^k V^m) = \lambda_m U^k V^m, \quad (k,m) \neq (0,0),$$

где

$$\lambda_m = \sum_{s=0}^{d-1} r_s e^{-\frac{2\pi i m s}{d}} \quad \text{при } m \neq 0, \qquad \lambda_0 = \sum_{s=0}^{d-1} r_s - p, \qquad \Phi(U^0 V^0) = \Phi(I) = I.$$

Каждый $T \in \mathcal{U}$ является полиномом:

$$T = \sum_{r=0}^{d-1} c_r U^r.$$

Следовательно,

$$T f(U) V^m T^* = g(U) V^m,$$

где f и g — полиномы от U. С другой стороны, для любого полинома

$$h(U) = \sum_{r=0}^{d-1} a_r U^r$$

получаем

$$\Phi(h(U)V^m) = \Phi\left(\sum_{r=0}^{d-1} a_r U^r V^m\right) = \lambda_m \sum_{r=0}^{d-1} a_r U^r V^m = \lambda_m h(U) V^m, \quad m \neq 0.$$

Таким образом, для унитарного $f(U) \in \mathcal{U}$ получаем

$$\begin{aligned}\Phi(f(U)g(U)V^m f(U)^*) &= \Phi(h(U)V^m) = \lambda_m h(U)V^m = \lambda_m f(U)g(U)V^m f(U)^* \\ &= f(U)\Phi(g(U)V^m)f(U)^*, \quad m \neq 0, \\ \Phi(f(U)g(U)f(U)^*) &= \Phi(g(U)) = h(U) = f(U)h(U)f(U)^* = f(U)\Phi(g(U))f(U)^*.\end{aligned}$$

Предложение доказано. □

Пример 2. *Канал с двумя матрицами Паули.* Для случая размерности $d = 2$ можно отождествить обобщенные матрицы Паули с обычными согласно правилу

$$U \equiv \sigma_x, \quad V \equiv \sigma_y, \quad UV = i\sigma_z.$$

Если положить $r_1 = 0$, действие канала (7) принимает вид

$$\Phi(\rho) = (1-p)\rho + \frac{p}{2}\sigma_y\rho\sigma_y + \frac{p}{2}\sigma_z\rho\sigma_z. \tag{10}$$

Канал (10) с двумя матрицами Паули был введен в [9]. Он ковариантен относительно максимальной коммутативной группы унитарных операторов $\mathcal{U}$, порождённой спектральными проекторами матрицы Паули σ_x. Иными словами,

$$\mathcal{U} = \left\{e^{it\sigma_x},\ t \in [0, 2\pi]\right\}.$$

Для $p \leqslant 1/3$ можно подобрать для (10) другие операторы Крауса, так что он примет вид (см. [18])

$$\Phi(\rho) = \frac{1-3p}{1-p}\left((1-p)\rho + p\sigma_y\rho\sigma_y\right) + \frac{2p}{1-p}\left(\frac{1-p}{2}\sigma_y\rho\sigma_y + \frac{1-p}{2}\sigma_x\rho\sigma_x + p\rho\right). \tag{11}$$

Представление (11) играет ключевую роль в доказательстве аддитивности минимальной выходной энтропии унитальных кубитных каналов (см. [18]).

Пример 3. *Квантовый деполяризующий канал.* Определим аффинное отображение Φ формулой

$$\Phi(\rho) = (1-p)\rho + \frac{p}{d}I, \quad \rho \in \mathfrak{S}(H), \quad \dim H = d. \tag{12}$$

Как известно, если $0 \leqslant p \leqslant d^2/(d^2-1)$, то Φ является квантовым каналом, называемым *деполяризующим*. Используя обобщенные матрицы Паули (1), можно представить действие канала (12) в виде

$$\Phi(\rho) = \left(1 - \frac{d^2-1}{d^2}p\right)\rho + \frac{p}{d^2}\sum_{(m,n)\neq(0,0)} U^m V^n \rho V^{*n} U^{*m}.$$

Таким образом, квантовый деполяризующий канал является частным случаем канала (7) для $r_k = p = p/d^2$, $k \neq 0$, $r_0 = 1 - \dfrac{d^2-1}{d^2}p$.

Предложение 2. *Если размерность пространства d является простым числом, то квантовый деполяризующий канал можно представить в следующем виде*:

$$\Phi(\rho) = \frac{1 - \frac{d^2-1}{d^2}p}{1 - \frac{d-1}{d}p}\sum_{k=0}^{d-1}\Phi_k(\rho) + \frac{\frac{p}{d^2}}{1 - \frac{d-1}{d}p}\sum_{l=1}^{d-1}\sum_{k=0}^{d-1} U^l \Phi_k(\rho) U^{*l}, \tag{13}$$

где Φ_k определены формулой (9).

Доказательство. Рассмотрим правую часть равенства (13). Коэффициент при ρ равен

$$\frac{1 - \frac{d^2-1}{d^2}p}{1 - \frac{d-1}{d}p} \cdot \left(1 - \frac{d-1}{d}p\right) = 1 - \frac{d^2-1}{d^2}p,$$

а коэффициент при $U^m\rho U^{*m}$, $m>0$, —

$$\frac{\frac{p}{d^2}}{1-\frac{d-1}{d}p}\cdot\left(1-\frac{d-1}{d}p\right)=\frac{p}{d^2}.$$

Для вычисления коэффициента при $U^mV^n\rho V^{*n}U^{*m}$, $n>0$, заметим, что если d — простое число, то уравнение $l+kn=m \mod d$ имеет единственное решение $l=(m-kn) \mod d$. Следовательно, данный коэффициент равен

$$\frac{\frac{p}{d^2}}{1-\frac{d-1}{d}p}\cdot(d-1)\frac{p}{d}=\frac{p}{d^2}.$$

Предложение доказано. □

4. Минимум выходной энтропии канала. Следуя [17], определим выпуклое замыкание выходной энтропии фон Неймана квантового канала по формуле

$$\hat{S}_\Phi(\rho)=\min_{\rho=\sum\limits_k \pi_k\rho_k}\sum_k \pi_k S(\Phi(\rho_k)),\quad \rho\in\mathfrak{S}(H),$$

где минимум берется по всем таким анасамблям (π_k,ρ_k), что

$$\rho_k\in\mathfrak{S}(H),\quad 0\leqslant\pi_k\leqslant 1,\quad \sum_k\pi_k=1.$$

Поскольку деполяризующий квантовый канал (12) характеризуется свойством ковариантности относительно группы всех унитарных операторов $\mathcal{U}(H)$, т.е.

$$\Phi(U\rho U^*)=U\Phi(\rho)U^*,\quad \rho\in\mathfrak{S}(H),\quad U\in\mathcal{U}(H), \tag{14}$$

для него получаем

$$\hat{S}_\Phi(\rho)=-\left(1-\frac{d-1}{d}p\right)\log\left(1-\frac{d-1}{d}p\right)-(d-1)\frac{p}{d}\log\frac{p}{d}=\mathrm{const}\,.$$

Говорят, что канал Φ обладает *свойством сильной супераддитивности* (см. [17]), если

$$\hat{S}_{\Phi\otimes\Omega}(\rho)\geqslant\hat{S}_\Phi(Tr_k(\rho))+\hat{S}_\Omega(Tr_H(\rho))$$

для любого квантового канала Ω, действующего на состояния $\mathfrak{S}(K)$ в гильбертовом пространстве K.

Пусть (f_j) и (g_k) — два произвольных ортонормированных базиса в гильбертовых пространствах H и K соответственно. Тогда единичный вектор $e\in H\otimes K$ можно следующими двумя способами:

$$e=\sum_j\lambda_j f_j\otimes h_j,\quad e=\sum_k\tilde{\lambda}_k\tilde{h}_k\otimes g_k,$$

где $h_j\in K$, $\tilde{h}_j\in H$ — некоторые единичные векторы и

$$\sum_j|\lambda_j|^2=\sum_k|\tilde{\lambda}_k|^2=1.$$

Для каналов, демпфирующих фазу (8), справедлива следующая оценка (см. [1]).

Предложение 3. *Для произвольного квантового канала Ω имеет место неравенство*

$$S\Big((\Phi\otimes\Omega)(|e\rangle\langle e|)\Big)\geqslant\sum_k|\tilde{\lambda}_k|^2S\Big(\Phi(|\tilde{h}_k\rangle\langle\tilde{h}_k|)\Big)+\sum_j|\lambda_j|^2S\Big(\Omega(|h_j\rangle\langle h_j|)\Big). \tag{15}$$

Из предложения 3 немедленно вытекает, что свойство сильной супераддитивности выполняется для каналов, демпфирующих фазу. Для деполяризующего канала (14) доказательство свойства сильной супераддитивности (см. [7, 1]) опирается на тот факт, что его можно представить в виде выпуклой комбинации каналов, демпфирующих фазу, и на оценку (15). В пространствах простой размерности существование такой выпуклой комбинации следует из предложения 2; для произвольной размерности доказательство существенно сложнее (см. [19]).

5. Некоммутативный операторный граф, приводящий к явлению суперактивации. Под передачей квантовой информации через квантовый канал Φ понимается следующая схема (см. [16]). Сначала происходит кодирование состояний из $\mathfrak{S}(K)$ квантовым каналом $\mathcal{E}:\mathfrak{S}(K)\to\mathfrak{S}(H)$, далее передача $\Phi:\mathfrak{S}(H)\to\mathfrak{S}(H)$ и, наконец, декодирование квантовым каналом $\mathcal{D}:\mathfrak{S}(H)\to\mathfrak{S}(K)$. Говорят, что квантовую информацию можно передать через квантовый канал Φ с нулевой ошибкой, если существуют такие состояния $\{\rho_k,\ 1\leqslant k\leqslant N,\ N\geqslant 2\}$ и пара $(\mathcal{E},\mathcal{D})$, что

$$\mathcal{D}\circ\Phi\circ\mathcal{E}(\rho_k)=\rho_k,\quad 1\leqslant k\leqslant N.$$

В [23] было показано, что некоммутативный операторный граф (5), порожденный матрицами вида

$$\begin{pmatrix} a & b & c\theta & d\\ b & a & d & c/\theta\\ c/\theta & d & a & b\\ d & c\theta & b & a\end{pmatrix} \tag{16}$$

приводит к явлению суперактивации для значения параметра $\theta=e^{i\pi/2n}$, т.е. для квантового канала Φ, ассоциированного с графом (16), невозможна передача квантовой информации с нулевой ошибкой, в то время как для n-ой тензорной степени $\Phi^{\otimes n}$ такая передача становится возможной.

Здесь мы хотели бы проанализировать структуру (16) с точки зрения базовых понятий алгебраической геометрии (см. [20]). Пусть A — конечно порожденная ассоциативная алгебру. Рассмотрим многообразие представлений

$$\mathbf{Rep}_n(A)=\mathrm{Hom}(A,\mathrm{Mat}_n(\mathbb{C})).$$

Главная линейна группа $GL_n(\mathbb{C})$ естественным образом действует на алгебре $\mathrm{Mat}_n(\mathbb{C})$ по формуле

$$x\to gxg^{-1},\quad x\in\mathrm{Mat}_n(\mathbb{C}),\quad g\in GL_n(\mathbb{C}).$$

Фактор-множество

$$\mathbf{Rep}_n(A)/GL_n(\mathbb{C})$$

называется *многообразием модулей* алгебры A.

Рассмотрим группу G, порожденную элементами x, y и z и соотношениями

$$x^2=y^2=z^2=1,\quad xz=zx,\quad yz=zy. \tag{17}$$

Отметим, что если к соотношениям (17) добавить $xy=yx$, мы получим четверную группу Клейна K_4.

Обозначим A алгебру над полем $\mathbb{C}$, порождённую группой G. Нас будет интересовать многообразие модулей $\mathbf{Rep}_4(A)/GL_4(\mathbb{C})$. Рассмотрим следующие три элемента $\mathrm{Mat}_4(\mathbb{C})$:

$$X=\begin{pmatrix}0&1&0&0\\1&0&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix},\quad Y=\begin{pmatrix}0&0&\theta&0\\0&0&0&1/\theta\\1/\theta&0&0&0\\0&\theta&0&0\end{pmatrix},\quad Z=\begin{pmatrix}0&0&0&1\\0&0&1&0\\0&1&0&0\\1&0&0&0\end{pmatrix}.$$

В [8] было показано, что для каждого ненулевого $\theta\in\mathbb{C}$ отображение $\pi_\theta:A\to\mathrm{Mat}_4(\mathbb{C})$, заданное формулой

$$\pi_\theta(x)=X,\quad \pi_\theta(y)=Y,\quad \pi_\theta(z)=Z,$$

определяет представление алгебры A.

Предложение 4. *Однопараметрическое семейство представлений (π_θ) определяет кривую $[\pi_\theta]\in\mathbf{Rep}_4(A)/GL_4(\mathbb{C})$.*

Доказательство. Следуя [3], заметим, что при $\theta\neq\pm1$ образ A при отображении π_θ изоморфен алгебре $\mathcal{M}_\theta$, $\dim\mathcal{M}_\theta=8$, с образующими x, y, z, удовлетворяющими (17) и дополнительному соотношению

$$xy+yx=(\theta+\theta^{-1})z.$$

Для $\theta = \pm 1$ образ A изоморфен групповой алгебре $\mathbb{C}K_4$ группы Клейна K_4 с образующими x, y, z, удовлетворяющими (17) и дополнительному соотношению $xy = yx$. Данные соотношения не меняются при естественном действии группы $GL_4(\mathbb{C})$. □

Принимая во внимание, что $\pi_{\pm 1}(A)$ — коммутативная алгебра, изоморфная $\mathbb{C}K_4$, мы будем называть кривую $[\pi_\theta]$ *некоммутативной деформацией* алгебры $\mathbb{C}K_4$. Предельный случай $\theta = \pm i$ отвечает квантовому каналу, по которому можно передать квантовую информацию с нулевой ошибкой.

Аналогичную ситуацию получаем, рассматривая многообразие модулей $\mathbf{Rep}_{4^n}(A^{\otimes n})/GL_{4^n}(\mathbb{C})$. Здесь некоммутативная деформация $[\pi_{\theta_1} \otimes \cdots \otimes \pi_{\theta_n}] \in \mathbf{Rep}_{4^n}(A^{\otimes n})/GL_{4^n}(\mathbb{C})$ алгебры $\mathbb{C}K_4^{\otimes n}$ описывает явление суперактивации для квантовых каналов на языке алгебраической геометрии. Пропускная способность с нулевой ошибкой появляется для значений параметров $\prod\limits_k \theta_k = \pm i$.

СПИСОК ЛИТЕРАТУРЫ

1. *Амосов Г. Г.* Об оценке выходной энтропии тензорного произведения канала, демпфирующего фазу, на произвольный канал// Пробл. передачи информ. — 2013. — *49*, № 3. — С. 32–39.
2. *Амосов Г. Г.* Оценка выходной энтропии тензорного произведения двух квантовых каналов// Теор. мат. физ. — 2015. *182*, № 3. — С. 453–464.
3. *Амосов Г. Г., Ждановский И. Ю.* О структуре алгебры, порожденной некоммутативным операторным графом, демонстрирующим явление суперактивации для пропускной способности с нулевой ошибкой// Мат. заметки. — 2016. — *99*, № 6. — С. 929–932.
4. *Холево А. С.* Вероятностные и статистические аспекты квантовой теории. — М.: Наука, 1980.
5. *Холево А. С.* Квантовые теоремы кодирования// Усп. мат. наук. — 1998. — *53*, № 6. — С. 193–230.
6. *Amosov G. G.* On Weyl channels being covariant with respect to the maximum commutative group of unitaries// J. Math. Phys. — 2007. — 48, № 1. — С. 2104–2117.
7. *Amosov G. G.* The strong superadditivity conjecture holds for the quantum depolarizing channel in any dimension// Phys. Rev. A. — 2007. — *75*, № 6. — С. 060304.
8. *Amosov G. G., Zhdanovskiy I. Yu.* On the noncommutative deformation of the operator graph corresponding to the Klein group// J. Math. Sci. — 2016. — *215*, № 6. — С. 659–676.
9. *Bennett C. H., Fuchs C. A., Smolin J. A.* Entanglement-enhanced classical communication on a noisy quantum channel// in: Quantum Communication, Computing and Measurement. — New York: Plenum Press, 1997. — С. 79–88.
10. *Choi M. D.* Completely positive linear maps on complex matrices// Linear Algebra Appl. — 1975. — *10*. — С. 285–290.
11. *Choi M. D., Effros E. G.* Injectivity and operator spaces// J. Funct. Anal. — 1977. — *24*, № 2. — С. 156–209.
12. *Cubitt T. S., Chen J., Harrow A. W.* Superactivation of the asymptotic zero-error classical capacity of a quantum channel// IEEE Trans. Inform. Theory. — 2011. — *57*, № 12. — С. 8114–8126; `arXiv:0906.2547`.
13. *Duan R.* Super-activation of zero-error capacity of noisy quantum channels// `arXiv:0906.2527` (2009).
14. *Holevo A. S.* The capacity of the quantum channel with general signal states// IEEE Trans. Inform. Theory. — 1998. — *44*, № 1. — С. 269–273.
15. *Holevo A. S.* On complementary channels and the additivity problem// Probab. Theory Appl. — 2005. — *51*. — С. 133–143.
16. *Holevo A. S.* Quantum channel, system, information. — Berlin–Boston: De Gryuter, 2012.
17. *Holevo A. S., Shirokov M. E.* On Shor's channel extension and constrained channels// Commun. Math. Phys. — 2004. — 249. — С. 417–430.
18. *King C.* Additivity for unital qubit channels// J. Math. Phys. — 2002. — *43*, № 10. — С. 4641–4653.
19. *King C.* The capacity of the quantum depolarizing channel// IEEE Trans. Inform. Theory. — 2003. *49*, № 1. — С. 221–229.
20. *Kontsevich M., Rosenberg A.* Noncommutative smooth spaces// in: The Gelfand Mathematical Seminars, 1996–1999. — Boston: Birkhäuser, 2000. — С. 85–108.
21. *Nathanson M., Ruskai M. B.* Pauli diagonal channels constant on axes// J. Phys. A: Math. Theor. — 2007. — *40*. — С. 8171–8204.
22. *Ruskai M. B., Szarek S., Werner E.* An analysis of completely positive trace-preserving paps on 2×2 matrices// Lin. Alg. Appl. — 2002. — *347*. — С. 159–187.
23. *Shirokov M. E.* On channels with positive quantum zero-error apaity having vanishing n-shot capacity// Quantum Inf. Process. — 2015. — *14*, № 8. — С. 3057–3074.

24. *Shor P. W.* Scheme for reducing decoherence in quantum computer memory// Phys. Rev. A. — 1995. — *52*. — C. R2493–R2496.

Г. Г. Амосов
Математический институт им. В. А. Стеклова РАН, Москва;
Санкт-Петербургский государственный университет;
Московский физико-технический институт
E-mail: gramos@mi.ras.ru

ИТОГИ НАУКИ И ТЕХНИКИ.
Современная математика и ее приложения.
Тематические обзоры.
Том 138 (2017). С. 11–18

УДК 519.7

АНАЛИЗ СВОЙСТВ КВАНТОВОГО ХЕШИРОВАНИЯ

© 2017 г. **А. В. ВАСИЛЬЕВ, А. Р. ВАСИЛОВ, М. А. ЛАТЫПОВ**

Аннотация. В работе анализируется метод двоичного квантового хеширования, позволяющий представлять двоичные наборы в виде квантового состояния. Показана высокая устойчивость данного метода к восстановлению прообраза. Предложены эвристические подходы к построению множеств с малым отклонениям, лежащих в основе построения квантовой хеш-функции и обеспечивающих ее устойчивость к коллизиям.

Ключевые слова: квантовые вычисления, квантовая криптография, квантовое хеширование, линейные двоичные коды, случайный поиск, алгоритм роя частиц.

AMS Subject Classification: 81P94

1. Введение. Хеширование является широко известным приемом в информатике и имеет массу полезных приложений. В области квантовых вычислений идеи хеширования применялись в [6, 11, 7, 2]. Однако в явно формализованном виде квантовое хеширование появилось в [3]. Затем последовали исследования, связанные с применением квантового хеширования для эффективного вычисления некоторого класса булевых функций в модели квантовых ветвящихся программ (см. [4]) и приложение данной техники для вычисления булевых функций в квантовой коммуникационной модели (см. [20]).

Одновременно были предложены обобщения метода квантового хеширования и исследование его свойств. Так, например, в [1] рассмотрено обобщение предложенной ранее функции, позволяющее строить новые квантовые хеш-функции на основе комбинации произвольных классических универсальных хеш-семейств и некоторого специального семейства функций, называемого квантовым хеш-генератором. Известно, что классические универсальные хеш-семейства тесно связаны с кодами с исправлением ошибок: одно можно получить из другого (см. [19]). Это дает возможность использования произвольных кодов с исправлением ошибок для получения новых квантовых хеш-функций.

В [21] был предложен обобщенный подход к построению квантовых хеш-функций для произвольных конечных абелевых групп. Данный подход основан на понятии множеств с малым отклонением, которые находят разнообразные применения в информатике (см. [17, 9, 12]).

Одним из наиболее интересных частных случаев такого подхода является задача хеширования двоичных данных, рассмотренная в [22]. Описанный вариант двоичного квантового хеширования является по существу эквивалентным квантовой функции отпечатков, использующей представление входных данных в относительной фазе квантового состояния (см. [24]). В данной работе для функции двоичного квантового хеширования мы доказываем усиленное свойство устойчивости к восстановлению прообраза на основе подхода из [14], а также предлагаем различные алгоритмы построения множеств с малым отклонением, которые определяют параметры квантового хеширования.

2. Предварительные сведения. Данная работа основывается на определении квантовой хеш-функции и ее свойств из [22]. Для полноты изложения приведем в данном разделе необходимые определения.

Работа субсидирована программой государственной поддержки Казанского (Приволжского) федерального университета в целях повышения его конкурентоспособности среди ведущих мировых научно-образовательных центров, а также Российским фондом фундаментальных исследований (проекты №№ 14-07-00878, 15-37-21160).

2.1. Квантовые хеш-функции.

Определение 1. *Квантовой функцией будем называть функцию вида*

$$\psi : \{0,1\}^n \to (\mathcal{H}^2)^{\otimes s},$$

где

$$(\mathcal{H}^2)^{\otimes s} = \mathcal{H}^2 \otimes \cdots \otimes \mathcal{H}^2 = \mathcal{H}^{2^s}$$

— 2^s-мерное гильбертово пространство, описывающее состояния s кубит.

Согласно [15] квантовая функция ψ называется квантовой односторонней функцией, если

(i) ее легко вычислять, т.е. существует полиномиальный алгоритм, который на входном наборе w выдает значение $|\psi(w)\rangle$;
(ii) тяжело обратить, т.е., имея лишь $|\psi(w)\rangle$, невозможно достоверно получить w.

Свойство 1. *Если $n \gg s$, то, имея лишь $|\psi(w)\rangle$, невозможно достоверно получить w.*

В определении квантовых односторонних функций явно не требуется наличие еще одного важного свойства, которое требуется для их практически значимых применений. Речь идет о возможности с высокой вероятностью различать образы квантовой односторонней функции. Как было показано в [3], это свойство можно определить следующим образом.

Определение 2. *Квантовая функция $\psi : \{0,1\}^n \to (\mathcal{H}^2)^{\otimes s}$ называется δ-устойчивой, если*

$$|\langle \psi(w_1) \,|\, \psi(w_2) \rangle| < \delta$$

для любой пары входных наборов w_1, w_2, $w_1 \neq w_2$.

Объединением приведенных выше определений стало понятие квантовой хеш-функции.

Определение 3. *Назовем квантовую функцию*

$$\psi : \{0,1\}^n \to (\mathcal{H}^2)^{\otimes s}$$

квантовой хеш-функцией, если она является квантовой односторонней и δ-устойчивой функцией.

2.2. Множества с ε-отклонением. Предлагаемый подход основан на важном комбинаторном объекте, называемом *множества с ε-отклонением* (в англоязычной литературе — ε-biased set). Приведем его определение в следующем виде.

Определение 4. *Множество $B \subseteq \{0,1\}^n$ называется множеством с ε-отклонением, если для любого $x \in \{0,1\}^n$, $x \neq 0$ имеем*

$$\frac{1}{|B|} \left| \sum_{b \in B} (-1)^{\sum_{i=1}^{n} b_i x_i} \right| \leqslant \varepsilon;$$

здесь суммирование в показателе степени ведется по модулю 2.

Как было доказано в [5], такое множество существует, если его размер не меньше $O(n/\varepsilon^2)$, а в [8] приводится явная конструкция размера $O(n/(\varepsilon^2 \log(1/\varepsilon)))^{5/4}$, основанная на алгебраических кодах. Данная конструкция основывается на тесной связи между множествами с ε-отклонением и так называемыми ε-сбалансированными линейными кодами с исправлением ошибок.

Определение 5. *Линейный код $C : \{0,1\}^n \to \{0,1\}^m$ для сообщений длины n и блоков длины m называется ε-сбалансированным, если вес любого ненулевого кодового слова $C(x)$ находится в диапазоне $(\frac{1}{2} - \epsilon)m$ и $(\frac{1}{2} + \epsilon)m$.*

Поскольку C является двоичным линейным кодом, его порождающая матрица A элементов $\mathbb{F}_2$ имеет размер $(n \times m)$ и $C(x) = x \cdot A$.

Известно (см. [8]), что мультимножество $B \subset \{0,1\}^n$ является множеством с ε-отклонением тогда и только тогда, когда ε-сбалансированным является линейный код C_B, порождающая матрица которого состоит из элементов B.

2.3. Двоичное квантовое хеширование. Для определения квантовой хеш-функции зафиксируем $\varepsilon \in (0,1)$ и условимся, что $B = \{b_1, b_2, \ldots\} \subseteq \{0,1\}^n$ является множеством с ε-отклонением.

Определение 6. *Определим квантовую функцию* $\psi_B : \{0,1\}^n \to (\mathcal{H}^2)^{\otimes(\log|B|)}$ *следующим образом. Для входного набора* $w \in \{0,1\}^n$ *положим*

$$|\psi_B(w)\rangle = \frac{1}{\sqrt{|B|}} \sum_{i=1}^{|B|} (-1)^{\sum_{j=1}^n b_{ij} w_j} |i\rangle,$$

где b_{ij} *— j-й элемент двоичного набора* $b_i \in B$*, а суммирование в показателе степени ведется по модулю 2.*

В [22] было доказано, что функция ψ_B является ε-устойчивой квантовой хеш-функцией.

3. Анализ устойчивости к восстановлению прообраза. В данном разделе мы проанализируем квантовую хеш-функцию над $\mathbb{Z}_2^n$ и докажем усиленные криптографические свойства по сравнению с [22].

В [14] авторы дали определение квантовой схемы, которая переводит бинарную строку в квантовое состояние на основе квазилинейных кодов. Если схема использует чистые состояния, то количество доступной информации не превышает $O(1)$ бит. В этом разделе перечислены и доказаны аналогичные свойства для схемы двоичного квантового хеширования.

Рассмотрим двоичную квантовую хеш-функцию ψ_B, основанную на множестве с ε-отклонением B. По построению размер этого множества является степенью 2, поэтому обозначим его $|B| = 2^d$. Соответственно, 2^d также является размерностью ассоциированного с функцией ψ_B гильбертова пространства.

Для $a \in \{0,1\}^n$ определим оператор плотности нормализованного состояния $\rho_a = |\psi_B(a)\rangle\langle\psi_B(a)|$ и ненормализованного состояния $\rho'_a = 2^{d-n}\rho_a$. Кроме того, для произвольного $|\nu\rangle \in \mathcal{H}^{2^d}$ определим распределение вероятности $\mu_\nu(a) = \langle\nu|\rho'_a|\nu\rangle$, что соответствует измерению с исходом $|\nu\rangle\langle\nu|$.

Следующая лемма аналогична [14, лемма 3.4] и позволяет оценить относительную энтропию между распределением вероятности $\mu_\nu(a)$ и равномерным распределением на $\{0,1\}^n$.

Лемма 1. *Пусть* $|\nu\rangle \in \mathcal{H}^{2^d}$ *— некоторый единичный вектор, вектор a выбран случайно согласно равномерному распределению на* $\{0,1\}^n$*. Тогда*

$$\mathbf{E}[\max\{0, \mu_\nu(a)\ln(2^n\mu_\nu(a))\}] < \frac{23}{2^n}.$$

Доказательство. Определим для $i \in \{1, \ldots, 2^d\}$ случайные величины

$$X_i = (-1)^{(b_i,a)}\nu_i,$$

где (b_i, a) — скалярное произведение векторов b_i и a.

Очевидно,

$$\mu_\nu(a) = 1/2^n \left(\sum_{i=1}^{2^d} X_i\right)^2, \quad \mathbf{E}[X_i] = 0, \quad |X_i| \leqslant 1.$$

Тогда для любого $t > 0$ имеем

$$\Pr\left[\mu_\nu(a) \geqslant \frac{t}{2^n}\right] = \Pr\left[\left|\sum_{i=1}^{2^d} X_i\right| \geqslant \left|\sqrt{t}\right|\right] \leqslant 4\exp\left(-\frac{t}{4}\right),$$

где последнее неравенство следует из [14, лемма 2.2].

Определим $g(x) = \max\{0, x\ln(x)\}$, и пусть $\tilde{\mu}$ — случайная величина, распределение вероятности которой имеет вид

$$\Pr[\tilde{\mu} \geqslant t] = 4\exp(-\frac{t}{4}) = f(t), \quad t > 8\ln 2.$$

Тогда

$$\mathbf{E}\Big[\max\Big\{0, \mu_\nu(a)\ln(2^n\mu_\nu(a))\Big\}\Big] \geqslant \frac{1}{2^n}\mathbf{E}\Big[g(2^n\mu_\nu(a))\Big] \geqslant \frac{1}{2^n}\mathbf{E}\Big[g(\tilde{\mu})\Big],$$

где первое неравенство следует из определения $g(x)$, а второе — из [14, лемма 2.3]. Следовательно,

$$\mathbf{E}\Big[g(\tilde{\mu})\Big] = \int\limits_{8\ln 2}^{\infty} x\ln(x)\left(-\frac{df}{dx}\right)dx = \int\limits_{8\ln 2}^{\infty} \exp\left(\ln(x) + \ln(\ln(x)) - \frac{x}{4}\right)dx < 23.$$

что и требовалось доказать. □

Определение 7. *Для случайных величин P и Q, имеющих дискретное распределение вероятности, расстояние Кульбака—Лейблера между величинами задается следующим образом:*

$$D_{KL}(P \parallel Q) = \sum_i P(i)\ln\frac{P(i)}{Q(i)}.$$

Следующая лемма показывает, что при использовании множеств с ε-отклонением в схемах квантового хеширования расстояние между $\mu_\nu(a)$ и случайной величиной x, равномерно распределенной на $\{0,1\}^n$, выражается как $D_{KL}(\mu_\nu(a) \parallel x)$ и принимает малые значения.

Лемма 2. *Пусть $|\nu\rangle \in \mathcal{H}^{2^d}$ – единичный вектор. Тогда*

$$\sum_{a\in\{0,1\}^n} \mu_\nu(a)\ln(2^n\mu_\nu(a)) < 23.$$

Доказательство. Определим случайную величину

$$\tilde{\mu}(a) = \max\{0, \mu_\nu(a)\ln(2^n\mu_\nu(a))\}.$$

По лемме 1

$$\mathbf{E}[\tilde{\mu}(a)] < \frac{23}{2^n}.$$

Следовательно,

$$\sum_{a\in\{0,1\}^n} \mu_\nu(a)\ln(2^n\mu_\nu(a)) < \sum_{a\in\{0,1\}^n} \tilde{\mu}(a) = 2^n\mathbf{E}[\tilde{\mu}(a)] < 23.$$

Лемма доказана. □

В [14] рассматривалась величина I_{acc}, характеризующая количество доступной информации о входных данных на основе измерения квантового состояния, представляющего эти данные. Данная величина определяется как $I_{acc} = H(J) - H(J|A)$, где A случайная величина, характеризующая выбор входных данных, а J случайная величина, характеризующая результат измерения квантового состояния.

Лемма 3. *Пусть x выбрано случайно согласно равномерному распределению на $\{0,1\}^n$. Тогда доступная информация I_{acc} ансамбля (ρ_x) не превышает*

$$\max_{|\nu\rangle} \sum_{a\in\{0,1\}^n} \mu_\nu(a)\ln\left(2^n\mu_\nu(a)\right) < 23.$$

Эта лемма перефразирует [14, лемма 3.12] с использованием множества с ε-отклонением и приводится без доказательства.

Таким образом, приведенные выше утверждения доказывают следующую теорему.

Теорема 1. *Пусть множество $B \subset \mathbb{Z}_2^n$ является множеством с ε-отклонением, а функция ψ_B является квантовой хеш-функцией, основанной на B. Тогда количество доступной информации о прообразе ψ_B имеет порядок $O(1)$.*

4. Алгоритмы построения множеств с малым отклонением. Известно, что для любого $\varepsilon \in (0,1)$ существует множество с ε отклонением размера $O(n/\varepsilon^2)$. Однако явные конструкции такого множества дают результаты, превышающие указанную оценку (см., например, [8]). Кроме того, получаемые решения имеют *асимптотически* хорошую оценку, что означает их применимость на входных данных достаточно большого размера. В данном разделе предлагаются эвристические подходы к построению множества с малым отклонением, которые можно использовать в дополнение к конструктивным алгоритмам.

4.1. Алгоритмы случайного поиска. При изучении поведения функции на различных входных параметрах было замечено, что многие хорошие решения для задачи определения параметров квантовой хеш-функции распределены в пространстве поиска достаточно равномерно. Такой результат позволяет нам использовать алгоритмы случайного поиска.

Наиболее простой вариант алгоритма случайного поиска был описан в [23]. Мы можем генерировать случайное множество и проверять, является ли оно множеством с ε-отклонением, то есть будет ли квантовая хеш-функция с параметрами из этого множества ε-устойчивой к коллизиям. Для не слишком малых значений ε такой алгоритм может быстро найти неплохое решение. Конечно, этот алгоритм является тривиальным, и при этом он даже не может дать никаких гарантий, что нужное решение будет найдено. Поэтому нужно модифицировать этот алгоритм.

Случайный поиск. В тривиальном варианте случайного поиска мы никак не учитывали результаты предыдущих итераций, что, разумеется, неправильно. В случае, когда мы знаем поведение функции в определенных точках, мы можем выбирать дальнейшую стратегию поиска решения, используя эти знания и какой-либо алгоритм выбора следующей точки.

Поэтому мы можем немного улучшить простой алгоритм случайного поиска следующим образом (см. [18]).

(1) Выбираем случайную точку из пространства поиска.
(2) Для выбранной точки (для множества, которое состоит из координат точки) вычисляем отклонение и, если оно не превышает заданное отклонение ε, то останавливаемся. Иначе создаем гиперсферу фиксированного радиуса и выбираем случайную точку на этой гиперсфере. После этого:
    (a) если выбранное множество обладает меньшим отклонением, то оно становится новым текущим решением, и мы повторяем шаг (2);
    (b) d противном случае выбираем другую случайную точку на гиперсфере.
(3) Алгоритм можно продолжать либо фиксированное число итераций, либо пока не будет достигнут приемлемый результат.

Здесь нужно также добавить, что для задачи поиска параметров квантовой хеш-функции мы используем гиперкуб вместо гиперсферы, так как все параметры функции интерпретируются как целые числа.

Рассмотренный алгоритм является более эффективным, и он лучше подходит для решения нашей задачи. Однако легко видеть, что в силу конструкции алгоритма, он может часто «застревать» в локальном минимуме, так как гиперсфера или гиперкуб имеют фиксированные размеры. Существует немало других алгоритмов, которые направлены на решение данной проблемы, например, это *алгоритм адаптивного случайного поиска* (см. [25]).

Адаптивный случайный поиск. Вместо того, чтобы всегда использовать фиксированный размер гиперкуба, предлагается увеличивать его при необходимости. Тогда алгоритм будет выглядеть следующим образом.

(1) Выбираем случайную точку из пространства поиска.
(2) Для выбранной точки вычисляем отклонение и, если оно не превышает заданное отклонение ε, останавливаемся. Иначе мы создаем две гиперсферы: первую с текущим радиусом r и вторую с радиусом r', при этом $r' > r$. На каждой гиперсфере мы случайный образом выбираем точку, и, если точка на сфере с большим радиусом дает более значимое улучшение результата, мы увеличиваем текущий радиус: $r = r'$.

В остальных случаях работа алгоритма совпадает с предыдущим алгоритмом с небольшим исключением: если алгоритм «застрял» в локальном минимуме, а число итераций превышено, он не останавливается, а увеличивает шаг и пытается выбраться из этого минимума, чтобы улучшить результат. Такой процесс можно продолжать до тех пор, пока размер шага не станет сравнимым с размером пространства.

Многократный адаптивный случайный поиск. У алгоритма адаптивного случайного поиска есть и свой недостаток: он очень сильно зависит от выбора начальной точки. Если мы выберем неудачную начальную точку, то алгоритм может оказаться в локальном минимуме и выбраться из него только с очень большим шагом, что помешает ему найти хорошее решение. Чтобы избежать этой проблемы и не слишком сильно зависеть от выбора начальной точки, можно запускать работу алгоритма адаптивного случайного поиска из разных точек, которые можно выбирать либо с помощью специального алгоритма, либо случайным образом.

Параллельный адаптивный случайный поиск. Выше мы рассмотрели возможность использования алгоритма адаптивного случайного поиска из разных начальных точек. Этот алгоритм можно тривиальным образом распараллелить, выполняя алгоритм из разных точек в разных потоках.

Жадный адаптивный случайный поиск. Одним из самых популярных алгоритмов, основанных на случайном поиске, является алгоритм *жадного адаптивного случайного поиска* (см. [13]). Этот алгоритм включает в себя следующие общие шаги.

(1) С помощью любого жадного алгоритма находим множество решений-кандидатов.
(2) Используя процедуру локального поиска (см. [16]) находим лучшее решение из этого множества.

Более детальное описание данного подхода и его реализации можно найти в [10].

Повторяющийся случайный поиск. Многие алгоритмы случайного поиска используют процедуру локального поиска (см. [16]). Кроме того, этот алгоритм может использоваться и самостоятельно для решения задач оптимизации, однако он может часто «застревать» в локальном минимуме, не дойдя до глобального. При этом есть алгоритмы, которые позволяют обойти эту проблему. Одним из таких алгоритмов является *алгоритм повторяющегося случайного поиска*.

Когда мы используем процедуру поиска, мы можем «застрять» в локальном оптимуме, когда ни один из ближайших соседей не подходит для перехода. При этом полученное значение может быть далеко от оптимального. Поэтому данный алгоритм реализует принцип повторного запуска поиска. Как только алгоритм завершает работу в каком-либо минимуме и результат не является явно удовлетворительным, начинается новая итерация поиска, т.е. заново выбирается начальная точка и алгоритм поиска повторяется (см. [10]). Важным замечанием является тот факт, что для поиска можно использовать любой алгоритм, в том числе и не стохастический. Обычно используется специфичная для задачи эвристика.

Последовательность действий алгоритма можно описать следующим образом.

(1) Выбирается начальная точка случайным образом или с помощью определенного метода или эвристики. Она становится текущим минимумом.
(2) На основе предыдущих шагов, а также текущего минимума осуществляются различные смещения точек, в результате чего создается множество точек-кандидатов.
(3) Для этого множества точек выполняется процедура локального поиска, в результате чего находится минимальное значение.
(4) В случае, когда найденное минимальное значение удовлетворяет заданному критерию (который зависит от текущего минимального значения и предыдущих шагов), оно становится минимальным.

Алгоритм задания смещения точке может быть различным, но чаще всего используют адаптивные алгоритмы. Также различным может быть и критерий обновления оптимального значения. Вместе алгоритм задания смещения и критерий обновления позволяют избежать остановки алгоритма в локальном минимуме.

Заключение по алгоритмам случайного поиска. Нужно сказать, что алгоритмы случайного поиска работают достаточно хорошо и при этом они наиболее просты в реализации (в отличие, например, от генетического алгоритма). Они не требуют каких-то преобразований задачи или допущений относительно входных данных или размерности задачи.

Однако алгоритмы случайного поиска являются не самыми оптимальными с точки зрения эффективного нахождения решений. В качестве варианта их использования можно предложить либо задачи малой размерности, где они быстро и простым путем придут к нужному ответу, либо напротив задачи очень большой размерности, где никакие другие эвристические алгоритмы не смогут быстро найти приемлемое решение.

Важным фактом является то, что алгоритмы случайного поиска чаще всего могут выполняться параллельно либо с нескольких начальных точек, либо при разбиении пространства решений.

Еще одним преимуществом стохастических алгоритмов является их независимость от способа построения квантовой хеш-функции. Поскольку нет никакой разницы между генерацией случайных чисел и случайных битовых строк, мы можем использовать алгоритмы случайного поиска как над $\mathbb{Z}_2^n$ или $\mathbb{Z}_q$, так и над любой конечной абелевой группой для построения соответствующей квантовой хеш-функции.

4.2. Алгоритм роя частиц для квантового хеширования. Алгоритм роя частиц — это очень известный алгоритм, который основан на идее коллективного разума.

В начале алгоритма частицы случайным образом располагаются в пространстве. После этого они перемещаются по определенным законам, с учетом известной им лучшей позиции, а также с учетом глобальной лучшей позиции. В ходе алгоритма частицы постепенно сближаются и в итоге сосредотачиваются у глобального минимума.

Более детальное описание, а также реализация алгоритма приведены в [10].

По результатам вычислительных экспериментов можно отметить, что алгоритм является достаточно эффективным в плане соотношения результат работы/время, более того, самым эффективным из рассмотренных ранее. Кроме того, алгоритм роя частиц сильно зависит от своих внутренних параметров, и их более аккуратный подбор может значительно улучшить эффективность алгоритма.

СПИСОК ЛИТЕРАТУРЫ

1. *Ablayev F., Ablayev M.* Quantum hashing via ϵ-universal hashing constructions and classical fingerprinting// Lobachevskii J. Math. — 2015. — *36*, № 2. — С. 89–96.
2. *Ablayev F., Vasiliev A.* Algorithms for quantum branching programs based on fingerprinting// Electr. Proc. Theor. Comput. Sci. — 2009. — *9*. — С. 1–11.
3. *Ablayev F. M., Vasiliev A. V.* Cryptographic quantum hashing// Laser Phys. Lett. — 2014. — *11*, № 2. — 025202.
4. *Ablayev F., Vasiliev A.* Computing Boolean functions via quantum hashing// In: Computing with New Resources/ Lect. Notes Comput. Sci. — Springer, 2014. — С. 149–160.
5. *Alon N. and Roichman Y.* Random Cayley graphs and expanders// Random Struct. Algorithms. — 1994. — *5*, № 2. — С. 271–284.
6. *Ambainis A., Freivalds R.* 1-Way quantum finite automata: strengths, weaknesses, and generalizations// Proc. 39th IEEE Conf. on Foundation of Computer Science/ IEEE Comput. Soc. — Washington, 1998. — С. 332–342.
7. *Ambainis A., Nahimovs N.* Improved constructions of quantum automata// In: Theory of Quantum Computation, Communication, and Cryptography/ Lect. Notes Comput. Sci. — Berlin–Heidelberg: Springer-Verlag, 2008. — *5106*. — С. 47–56.
8. *Ben-Aroya A., Ta-Shma A.* Constructing small-bias sets from algebraic-geometric codes// In: Foundations of Computer Science, 2009/ 50th Annual IEEE Symp. — Oct. 2009. — С. 191–197.
9. *Ben-Sasson E. Sudan M., Vadhan S., and Wigderson A.* Randomness-efficient low degree tests and short pcps via epsilon-biased sets// In: Proc. 35 Ann. ACM Symp. on Theory of Computing, New York, 2003. — С. 612–621.
10. *Brownlee J.* Clever algorithms: Nature-inspired programming recipes. — Lulu.com, 2011.
11. *Buhrman H., Cleve R., Watrous J., de Wolf R.* Quantum fingerprinting// Phys. Rev. Lett. — 2001. — *87* (16). — 167902.

12. *Chen S., Moore C., Russell A.* Small-bias sets for nonabelian groups// In: Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques/ Lect. Notes Comput. Sci. — Berlin–Heidelberg: Springer, 2013. — *8096*. — С. 436–451.
13. *Feo T. A., Resende M. G. C.* Greedy randomized adaptive search procedures// J. Global Optim. — 1995. — *6*, № 2. — С. 109–133.
14. *Gavinsky D., Ito T.* Quantum fingerprints that keep secrets/ Technical report, 2010.
15. *Gottesman D., Chuang I.* Quantum digital signatures/ Technical report. — Cornell Univ. Library, Nov. 2001; `arXiv:quant-ph/0105032`
16. *Hoos H. H., Stutzle T.* Stochastic local search: Foundations and applications. — San Francisco: Morgan Kaufmann, 2004.
17. *Naor J., Naor M.* Small-bias probability spaces: Efficient constructions and applications// In: Proc. 22 Ann. ACM Symp. on Theory of Computing. — New York, 1990. — С. 213–223.
18. *Schumer M. A., Steiglitz K.* Adaptive step size random search// IEEE Trans. Automat. Control. — 1968. — *13*, № 3. — С. 270–276.
19. *Stinson D. R.* On the connections between universal hashing, combinatorial designs and error-correcting codes// Proc. Congr. Numer. — 1996. — *114*. — С. 7–27.
20. *Vasiliev A.* Quantum communications based on quantum hashing// Int. J. Appl. Eng. Res. — 2015. — *10 (12)*. — 31415–31426.
21. *Vasiliev A.* Quantum hashing for finite abelian groups// Lobachevskii J. Math. — 2016. — *37*, № 6. — С. 751–754.
22. *Vasiliev A. V.* Binary quantum hashing// Russ. Math. — 2016. — *60*, № 9. — С. 61–65.
23. *Wets R. J.-B., Solis F. J.* Minimization by random search techniques// Math. Oper. Res. — 1981. — *6*, № 1. — С. 19–30.
24. *de Wolf R.* Quantum computing and communication complexity/ Ph.D. thesis. — Univ. of Amsterdam, 2001.
25. *Zabinsky Z. B.* Stochastic adaptive search for global optimization// Nonconvex Optimization and Its Applications. — Springer, 2003. — *72*.

А. В. Васильев
Казанский (Приволжский) федеральный университет
E-mail: `alexander.ksu@gmail.com`

А. Р. Василов
Казанский (Приволжский) федеральный университет
E-mail: `vasilovartur@gmail.com`

М. А. Латыпов
Казанский (Приволжский) федеральный университет
E-mail: `gogen.marat@gmail.com`

ИТОГИ НАУКИ И ТЕХНИКИ.
Современная математика и ее приложения.
Тематические обзоры.
Том 138 (2017). С. 19–49

УДК 519.248.3, 512.552.8

АЛГЕБРЫ ПРОЕКТОРОВ И ВЗАИМНО НЕСМЕЩЕННЫЕ БАЗИСЫ В РАЗМЕРНОСТИ 7

© 2017 г. **И. Ю. ЖДАНОВСКИЙ, А. С. КОЧЕРОВА**

Аннотация. Рассматриваются применения методов теории представлений, комбинаторной алгебры и некоммутативной геометрии к различным задачам квантовой томографии. Для этих целей вводится алгебра проекторов, удовлетворяющих некоторому коммутационному соотношению, которое в данной работе изучается при помощи комбинаторных методов; изложена теория представлений указанной алгебры. Приведено геометрическое описание задачи, и полученные результаты использованы при описании семейства Петреску взаимно несмещенных базисов в размерности 7.

***Ключевые слова*:** взаимно несмещенные базисы, ортогональные пары, коммутационное соотношение, алгебра наблюдаемых.

***AMS Subject Classification*:** 94A40, 16G99

СОДЕРЖАНИЕ

1. Введение

Рассмотрим следующую ситуацию в физике: имеется квантовомеханическая система из двух алгебр наблюдаемых A и B. Предположим, что существуют некоторые линейные комбинации элементов из A и B, которые являются совместно измеримыми. Возникает следующий вопрос: существует ли какое-либо разложение данной квантовомеханической системы в сумму меньших квантовомеханических систем? Более точно сформулируем эту ситуацию в терминах классической алгебры. Именно, имеется свободное произведение алгебр $A * B$ и идеал I, порожденный некоторыми коммутационными соотношениями в следующем виде:

$$[a_i + b_i, a_j + b_j] = 0,$$

где $a_i \in A$, $b_i \in B$. Обозначим символом R фактор-алгебру $A * B/I$. Предположим, что алгебры A и B конечномерны, а набор $\{a_i\}$ — базис в A, а $\{b_i\}$ — набор образующих в B.

В данной работе мы покажем, что если N достаточно велико, то N-мерное представление алгебры R является прямой суммой представлений R меньшей размерности. Более точно, мы

Работа субсидирована программой государственной поддержки ведущих университетов Российской Федерации «5–100». Работа первого автора выполнена при частичной поддержке Российского фонда фундаментальных исследований (проекты №№ 16-01-00113А и 14-01-00416.

докажем, что размерность любого неприводимого представления R не превосходит размерности алгебры B. Далее, предположим, что

$$A \cong \mathbb{C}^{\oplus 3}, \quad B \cong \mathbb{C}^{\oplus 3}$$

с базисами P_1, P_2, $1 - P_1 - P_2$ и Q_1, Q_2, $1 - Q_1 - Q_2$ соответственно. Также предположим, что имеется следующее соотношение для P_1, P_2, Q_1, Q_2:

$$\big[P_1 - Q_2,\ P_2 - Q_1\big] = 0, \tag{1.1}$$

где $[a, b] = ab - ba$. Обозначим через $\mathcal{C}$ фактор $\mathbb{C}^{\oplus 3} * \mathbb{C}^{\oplus 3}$ по идеалу, порожденному соотношением (1.1). Представления этой алгебры допускают естественную геометрическую интерпретацию, которую мы будем изучать в нашей статье.

Также представления алгебры $\mathcal{C}$ имеют отношение и к одному из основнных понятий квантовой томографии — взаимно несмещенным базисам. Напомним понятие взаимно несмещенных базисов в n-мерном комплексном эрмитовом векторном пространстве со скалярным произведением $(\cdot, \cdot)$. Два ортогональных базиса $\{e_i\}$ и $\{f_j\}$ называются взаимно несмещенными, если

$$\big|(e_i, f_j)\big|^2 = \frac{1}{n}. \tag{1.2}$$

Приложения взаимно несмещенных базисов постоянно используются в квантовой теории информации. Одной из причин, почему взаимно несмещенные базисы важны на практике, является то, что они дают мощное математическое средство, позволяющее передавать квантовую информацию с минимальными потерями в канале. Надежные протоколы в квантовых каналах основываются на выборе максимального числа взаимно несмещенных базисов в соответствующем векторном пространстве квантовых состояний передаваемых частиц. Например, протокол BBB4, который использует три таких базиса в двумерном векторном пространстве, позволяет значительно расширить расстояние между источником и приемником квантовой информации. Построение наибольшего числа взаимно несмещенных базисов в векторном пространстве большей размерности важно для создания надежных протоколов в квантовых каналах. Напомним, что задача классификации взаимно несмещенных базисов для произвольной размерности еще далека от решения. Полная классификация известна только в случае размерности <6. Петреску построил одномерное семейство взаимно несмещенных базисов в случае размерности 7 (см. [11]). Рассмотрим фиксированную пару взаимно несмещенных базисов $\{e_i\}$, $\{f_j\}$ из семейства Петреску. Поставим в соответствие векторам $\{e_i\}_{i=1}^7$ и $\{f_j\}_{j=1}^7$ соответственно эрмитовы проекторы π_i и ρ_j ранга 1. Нишоара показал, что можно упорядочить p_i и q_j таким образом, что

$$[\pi_1 + \pi_2, \rho_1 + \rho_2] = [\pi_3 + \pi_4, \rho_3 + \rho_4]$$

(см. [10]). Очевидно, обозначив за P_1, P_2, Q_1 и Q_2 элементы $\pi_1 + \pi_2$, $\pi_3 + \pi_4$, $\rho_1 + \rho_2$ и $\rho_3 + \rho_4$ соответственно, мы получим, что

$$[P_1, Q_1] = [P_2, Q_2]$$

или, что то же самое,

$$[P_1 - Q_2, P_2 - Q_1] = 0,$$

т.е. 7-мерное представление алгебры $\mathcal{C}$. Это дает еще одну мотивировку к изучению алгебры $\mathcal{C}$ в квантовой механике.

Работа организована следующим образом.

В разделе 2 мы рассмотрим две конечномерные алгебры A и B, введем алгебру R и докажем полезные свойства неприводимых R-модулей.

В разделе 3 мы определим алгебру $\mathcal{C}$ как частный случай алгебры R, фактор свободного произведения $A * B$, где $A = \mathbb{C}^{\oplus 3}$, $B = \mathbb{C}^{\oplus 3}$, по соотношению (1.1). Далее, введем на алгебре $\mathcal{C}$ фильтрацию для комбинаторного описания. Ключевой результат в понимании алгебры $\mathcal{C}$ содержится в теореме 3.10, утверждающей, что идеал, порожденный соотношением, является пересечением некоторых трех идеалов, порожденных парами проекторов.

В разделе 4 приведена классификация всех неприводимых $\mathcal{C}$-модулей и дается некоторое геометрическое описание этой классификации. Кроме того, найден 7-мерный $\mathcal{C}$-модуль, соответствующий взаимно несмещенным базисам.

В разделе 5 построено одномерное семейство взаимно несмещенных базисов в размерности 7 с помощью найденного 7-мерного $\mathcal{C}$-модуля и показано, что оно совпадает с семейством Петреску.

Авторы благодарны Г. Г. Амосову, А. И. Бондалу, В. И. Манько за полезные советы, ценные обсуждения и внимание к работе.

2. Конечномерные алгебры с коммутационным соотношением и квантовая механика

В этом разделе мы изучим фактор свободного произведения конечномерных алгебр по идеалу, порожденному некоторыми коммутационными соотношениями.

Прежде всего напомним понятие свободного произведения конечно порожденных ассоциативных алгебр A и B. Обозначим через $F(T)$ свободную ассоциативную алгебру с единицей с набором порождающих S. В этом случае $A = F(T_1)/J_1$ и $B = F(T_2)/J_2$, где T_1 и T_2 — порождающие наборы для A и B, соответственно. J_1 и J_2 — двусторонние идеалы, порожденные соотношениями в алгебрах A и B.

Свободное произведение $A * B$ — это фактор $F(T_1 \sqcup T_2)$ по идеалу J, порожденному идеалами J_1 и J_2. Далее, рассмотрим две конечномерные алгебры A, B и их свободное произведение $A * B$. Предположим, что

$$\dim_{\mathbb{C}} A = n_1, \quad \dim_{\mathbb{C}} B = n_2.$$

Зафиксируем элементы $a_i \in A$, $i = 1, \ldots, n_1$, $b_j \in B$, $j = 1, \ldots, n_1$. Предположим, что a_i — базис в алгебре A как в векторном пространстве, b_i, $i = 1, \ldots, n_1$ — порождающие алгебры B. Рассмотрим идеал I свободного произведения $A * B$, порожденный соотношениями

$$[a_i + b_i, a_j + b_j] = 0, i, j = 1, \ldots, n_1, \tag{2.1}$$

и обозначим через R фактор-алгебру $A * B/I$.

Рассмотрим элементы s_i из $A * B$, определяемые формулами

$$s_i = a_i + b_i, \quad i = 1, \ldots, n_1. \tag{2.2}$$

Тогда соотношения (2.1) означают, что элементы s_i коммутируют. Обозначим через S коммутативную подалгебру в R, порожденную s_i, $i = 1, \ldots, n_1$.

Поскольку a_i, $i = 1, \ldots, n_1$, — базис в A, мы получаем следующее соотношение:

$$a_i a_j = \sum_{k=1}^{n_1} m_{ij}^k a_k, \quad i, j, k = 1, \ldots, n_1, \tag{2.3}$$

где m_{ij}^k — структурные константы алгебры A. Из формул (2.2) получаем, что $a_i = s_i - b_i$. Таким образом, алгебра R порождена элементами s_i, b_j, $i, j = 1, \ldots, n_1$. Также получаем, что

$$(s_i - b_i)(s_j - b_j) = \sum_{k=1}^{n_1} m_{ij}^k (s_k - b_k).$$

Перепишем формулу (2.3) в следующем виде:

$$s_i b_j = -b_i s_j + s_i s_j - \sum_{k=1}^{n_1} m_{ij}^k s_k + b_i b_j + \sum_{k=1}^{n_1} m_{ij}^k b_k, \quad i, j = 1, \ldots, n_1. \tag{2.4}$$

Введем обозначения

$$s_{ij} = s_i s_j - \sum_{k=1}^{n_1} m_{ij}^k s_k, \quad b_{ij} = b_i b_j + \sum_{k=1}^{n_1} m_{ij}^k b_k.$$

Таким образом, мы получаем следующее соотношение:

$$s_i b_j = -b_i s_j + s_{ij} + b_{ij}, \quad i, j = 1, \ldots, n_1. \tag{2.5}$$

Предложение 2.1. *Имеет место сюръективный морфизм правых S-модулей*:

$$f : S^{\oplus n_2} \to R. \tag{2.6}$$

Другими словами, любой элемент из R может быть представлен в виде

$$\sum_{i=1}^{n_2} s'_i b'_i,$$

где $s'_i \in S$, $\{b'_i\}_{i=1}^{n_2}$ — базис в B.

Доказательство. Выберем базис b'_i, $i = 1, \dots, n_2$, в B. Как известно, s_i и b'_i порождают алгебру R. Таким образом, любой элемент из R представляет собой линейную комбинацию мономов следующего вида:

$$s'_1 b'_1 \dots s'_k b'_k, \quad b'_1 s'_1 \dots b'_k s'_k, \quad s'_1 b'_1 \dots s'_k, \quad \text{или} \quad b'_1 s'_1 \dots b'_k$$

для некоторых $s'_i \in S$ и $b'_i \in B$ и любого k. Рассмотрим моном $s'_1 b'_1 \dots s'_k b'_k$. Индукцией по k, примененяя формулу (2.5), можно преобразовать этот моном в сумму двух мономов вида $s''_i b'_i$. Аналогичное утверждение можно доказать для других мономов. Таким образом, любой элемент есть линейная комбинация элементов $s'_i b'_i$, где $s'_i \in S$, $\{b'_i\}$ — базис в B.

Далее, вложение $S \to R$ определяет структуру S-модуля в R. Также рассмотрим свободное произведение S-модуля $S^{\oplus n_2}$ ранга n_2 и базиса e_i, $i = 1, \dots, n_2$. Определим морфизм S-модулей f следующим образом: $f : e_i \mapsto b_i$. Пользуясь первой частью доказательства, получим, что морфизм f сюръективен. □

Следствие 2.2. *Предположим, что V — неприводимый конечномерный R-модуль. В этом случае выполнено следующее неравенство*:

$$\dim_{\mathbb{C}} V \leqslant n_2. \tag{2.7}$$

Доказательство. Пусть V — неприводимый конечномерный R-модуль. Рассмотрим V как S-модуль. Так как S — коммутативная алгебра, то существует одномерный S-подмодуль $\mathbb{C}^\chi$ в V, где $\mathbb{C}^\chi$ — это S-модуль, индуцированный характером $\chi : S \to \mathbb{C}$. Таким образом, $\mathrm{Hom}_S(\mathbb{C}^\chi, V) \neq 0$. Пользуясь сопряженностью функторов, имеем

$$\mathrm{Hom}_R(\mathcal{C} \otimes_S \mathbb{C}^\chi, V) = \mathrm{Hom}_S(\mathbb{C}^\chi, V) \neq 0. \tag{2.8}$$

Таким образом, существует нетривиальный морфизм R-модулей

$$g : R \otimes_S \mathbb{C}^\chi \to V.$$

Пользуясь неприводимостью V, получаем, что g сюръективен. Следовательно,

$$\dim_{\mathbb{C}} V \leqslant \dim_{\mathbb{C}} R \otimes_S \mathbb{C}^\chi. \tag{2.9}$$

Используя предложение 2.1 и умножая тензорно последовательность (2.6) на $\mathbb{C}^\chi$, получим, что морфизм

$$f : S^{\oplus n_2} \otimes_S \mathbb{C}^\chi = \mathbb{C}^{n_2} \to R \otimes_S \mathbb{C}^\chi$$

сюръективен. Следовательно,

$$\dim_{\mathbb{C}} R \otimes_S \mathbb{C}^\chi \leqslant n_2.$$

Используя формулу (2.9), получаем требуемое утверждение. □

Замечание 2.3. Заметим, что при выборе в качестве a_1 и b_1 скалярных элементов в соответствующих алгебрах, получаем что s_1 — скалярный элемент в свободном произведении, который коммутирует со всеми элементами. Тогда в качестве порождающих идеала I достаточно выбрать $n_1 - 1$ таких элементов a_i и b_i, что

$$[a_i + b_i, a_j + b_j] = 0.$$

В конце этого раздела сделаем замечание по поводу применения описанной конструкции в квантовой механике.

Замечание 2.4. Рассмотрим следующую ситуацию: имеются две алгебры наблюдаемых A и B размерностей n_1 и n_2. Зафиксируем базис a_i в A и порождающие b_i в B. Рассмотрим квантовомеханическую систему $\mathcal{Q}$, порожденную алгебрами наблюдаемых A и B. Пусть существуют n_1 совместно измеримых наблюдаемых, представляющих собой линейные комбинации $s_i = a_i + b_i$, $i = 1, \dots, n_1$. В этом случае квантовомеханическая система $\mathcal{Q}$ раскладывается в прямую сумму квантовомеханических систем размерности $\leqslant n_2^2$.

3. Алгебра $\mathcal{C}$

Рассмотрим частный случай алгебры R, когда в качестве A и B выбраны алгебры $\mathbb{C}^{\oplus 3}$; обозначим эту алгебру через $\mathcal{C}$. В этом разделе мы будем изучать комбинаторное строение алгебры $\mathcal{C}$.

3.1. Алгебра $\mathcal{C}$ и связь с квантовой механикой. В этой части мы объясним связь между представлениями построенной алгебры $\mathcal{C}$ и некоторыми понятиями квантовой механики (см. [14]).

Рассмотрим алгебры $A = \mathbb{C}^{\oplus 3}$ и $B = \mathbb{C}^{\oplus 3}$. Зафиксируем базисы $1 - P_1 - P_2$, P_1, P_2 и $1 - Q_1 - Q_2$, Q_1, Q_2 алгебр A и B соответственно, удовлетворяющие соотношениям

$$P_i^2 = P_i, \quad Q_i^2 = Q_i, \quad i = 1, 2, \qquad P_i P_j = Q_i Q_j = 0, \quad i \neq j.$$

Рассмотрим алгебру $\mathcal{C}$, которая является фактор-алгеброй $A * B$ по идеалу, порожденному соотношением

$$[P_1 - Q_2, P_2 - Q_1] = 0, \tag{3.1}$$

т.е.

$$P_1 Q_1 - Q_1 P_1 - P_2 Q_2 + Q_2 P_2 = 0.$$

Как указывалось ранее, алгебра $\mathcal{C}$ является частным случаем алгебры R. Элементы нужно выбирать следующим образом:

$$a_1 = b_1 = 1, \quad a_2 = P_1, \quad b_2 = -Q_2, \quad a_3 = P_2, \quad b_3 = -Q_1.$$

Рассмотрим такое представление $\mathcal{C}$, что порождающие P_1, P_2, Q_1, Q_2 представляют собой эрмитовы матрицы. В этом случае имеются следующие связи с квантовой механикой и квантовой теорией информации.

Во-первых, имеется интерпретация из раздела 2. А именно, проекторы P_1, P_2, Q_1, Q_2 — это наблюдаемые. В этом случае соотношения

$$P_1 P_2 = P_2 P_1, \quad Q_1 Q_2 = Q_2 Q_1$$

означают, что P_1, P_2 и Q_1, Q_2 — пары совместно измеримых наблюдаемых. Поскольку P_i, Q_j — проекторы, получаем следующую интерпретацию: P_i и Q_i — «индикаторные» наблюдаемые, а $P_1 - Q_2$ и $P_2 - Q_1$ — совместно измеримые наблюдаемые.

Во-вторых, имеется есть связь между алгеброй $\mathcal{C}$ и алгеброй Гейзенберга. Напомним, что алгебра Гейзенберга $\mathfrak{h}_2$ — это алгебра Ли с генераторами x_1, x_2, y_1, y_2, z и соотношениями

$$[x_i, y_j] = \delta_{ij} z, \quad [x_i, x_j] = [y_i, y_j] = 0, \quad [x_i, z] = [y_i, z] = 0, \quad i = 1, 2, \tag{3.2}$$

где δ_{ij} — символ Кронекера. Рассмотрим универсальную обертывающую алгебру $U(\mathfrak{h}_2)$ с теми же генераторами. Рассмотрим двусторонний идеал I алгебры $U(\mathfrak{h}_2)$, порожденный соотношениями $x_i^2 - x_i$, $y_i^2 - y_i$, $x_i x_j$, $y_i y_j$. Таким образом, у нас имеется морфизм

$$\psi : \mathcal{C} \to \mathfrak{u} = U(\mathfrak{h}_2)/I,$$

определенный по правилу

$$\psi : P_i \mapsto x_i, \ Q_i \mapsto y_i, \quad z = \psi([P_1, Q_1]).$$

Очевидно, этот морфизм ψ сюръективен, а идеал $\operatorname{Ker}\psi$ порожден элементами $P_1 Q_2 - Q_2 P_1$ и $P_2 Q_1 - Q_1 P_2$. Следовательно,

$$\mathcal{C}/\operatorname{Ker}\psi \cong \mathfrak{u}.$$

Изучим алгебру $\mathfrak{u}$. Имеются следующие соотношения:

$$x_i z = z x_i = y_i z = z y_i = 0, \quad i = 1, 2. \tag{3.3}$$

Покажем, что $x_1 z = 0$. Как известно,

$$z = x_1 y_1 - y_1 x_1 = x_2 y_2 - y_2 x_2.$$

Следовательно, пользуясь коммутативностью x_1 и y_2 и соотношением $x_1 x_2 = 0$, получаем

$$x_1 z = x_1(x_2 y_2 - y_2 x_2) = 0.$$

Аналогично можно получить и остальное.

Кроме того, выведем, что $z = 0$ в алгебре $\mathfrak{u}$. Рассмотрим элементы $x_1 y_1 - y_1 x_1 = z$ и $s = x_1 z + z x_1$. Имеем

$$s = x_1(x_1 y_1 - y_1 x_1) + (x_1 y_1 - y_1 x_1) x_1 = x_1 y_1 - y_1 x_1 = z.$$

Используя соотношения (3.3), получим, что $z = 0$. Таким образом, алгебра $\mathfrak{u}$ коммутативна.

Рассмотрим идеал J алгебры $\mathfrak{u}$, порожденный элементом z. Тождества (3.3) означают, что $J^2 = 0$.

Предложение 3.1.

$$\mathfrak{u} \cong \mathbb{C}^{\oplus 9}.$$

Доказательство. Алгебра $\mathfrak{u}$ коммутативна; она порождена элементами x_1, x_2, y_1, y_2 с соотношениями

$$x_i^2 = x_i, \quad y_i^2 = y_i, \quad x_1 x_2 = y_1 y_2 = 0, \quad x_i y_j = y_j x_i, \quad i, j = 1, 2.$$

Рассмотрим элементы

$$g_1 = (1 - x_1 - x_2) + \epsilon x_1 + \epsilon^2 x_2, \quad g_2 = (1 - y_1 - y_2) + \epsilon y_1 + \epsilon^2 y_2,$$

где ϵ — простой корень из единицы степени 3. Можно показать, что $g_i^3 = 1$, $i = 1, 2$ и $g_1 g_2 = g_2 g_1$. Кроме того, x_i и y_i — линейные комбинации элементов 1, g_1, g_1^2 или элементов 1, g_2, g_2^2 соответственно. Рассмотрим группу $G = \mathbb{Z}_3 \oplus \mathbb{Z}_3$. Легко показать, что $\mathfrak{u} = \mathbb{C}[G]$. Следовательно, получаем требуемый результат. □

Следствие 3.2. *Одномерные представления $\mathcal{C}$ — это одномерные представления $\mathfrak{u}$. Это означает, что для любого $f : \mathcal{C} \to \mathbb{C}$ существует морфизм $g : \mathfrak{u} \to \mathbb{C}$ такой, что $f = g \circ \psi$.*

Доказательство. Рассмотрим $f : \mathcal{C} \to \mathbb{C}$. Морфизм f определен значениями $f(P_i)$, $f(Q_i)$. Понятно, что $f(P_i), f(Q_i) \in \{0, 1\}$, $i = 1, 2$. Непосредственная проверка показывает, что существует только 9 возможностей для $f(P_i)$ и $f(Q_i)$. □

В-третьих, имеется связь с квантовой томографией; мы остановимся на ней более подробно. Пусть $\{e_i\}$, $\{f_j\}$ — взаимно несмещенные базисы (см. (1.2)), а $\{\pi_i\}_{i=1}^n, \{\rho_j\}_{j=1}^n$ — соответствующие этим базисам наборы эрмитовых ортогональных проекторов ранга 1. Условие (1.2) можно записать в виде

$$\operatorname{Tr} \pi_i \rho_j = \frac{1}{n}. \tag{3.4}$$

Так как проекторы имеют ранг 1, то это соотношение можно переписать следующим образом:

$$\pi_i \rho_j \pi_i = \frac{1}{n} \pi_i, \quad \rho_j \pi_i \rho_j = \frac{1}{n} \rho_j, \quad i, j = 1, \ldots, n. \tag{3.5}$$

Обобщением указанных соотношений является редуцированная алгебра Темперли—Либа. Напомним, что редуцированная алгебра Темперли—Либа $B_r(\Gamma)$ для некоторого простого графа Γ — это алгебра над $\mathbb{C}[r]$ с порождающими x_v, индексированными вершинами Γ и соотношениями

$$x_v^2 = x_v, \quad x_v x_w = x_w x_v = 0 \tag{3.6}$$

если вершины v, w не соединены ребром, и

$$x_v x_w x_v = r x_v, \quad x_w x_v x_w = r x_w \tag{3.7}$$

в противном случае.

Взаимно несмещенные базисы приводят нас к представлениям редуцированной алгебры Темперли—Либа $B_{\frac{1}{n}}(\Gamma_{n,n})$ для полного двудольного графа $\Gamma_{n,n}$ с n вершинами в каждом ряду;

при этом порождающие должны быть эрмитовыми проекторами ранга 1. Детали этих представлений, связанные со взаимно несмещенными базисами в $\mathbb{C}^n$, можно найти в [3].

Можно рассмотреть все n-мерные представления алгебры $B_{\frac{1}{n}}(\Gamma_{n,n})$, где порождающие — проекторы ранга 1. Такие представления задают ортогональные пары в алгебре Ли $\mathfrak{sl}(n)$, введенные А. И. Кострикиным и соавторами (см. [1, 8]). Задача классификации ортогональных пар в $\mathfrak{sl}(n)$ является естественной «комплексификацией» соответствующей задачи для взаимно несмещенных базисов в $\mathbb{C}^n$. А именно, если рассмотреть n-мерные представления алгебры $B_{\frac{1}{n}}(\Gamma_{n,n})$, где каждый проектор является эрмитовым, то соответствующее многообразие модулей параметризует взаимно несмещенные базисы в $\mathbb{C}^n$. Естественным образом на многообразиях модулей $\mathbf{Rep}_n B_{n,n}$ и $\mathcal{M}_n B_{n,n}$ определена вещественная инволюция $\dagger$, неподвижные точки $\mathcal{M}_n^{\dagger} B_{n,n}$ которой соответствуют представлениям, в которых порождающие представляются эрмитовыми проекторами (см. подробности в [4]).

Полная классификация ортогональных пар в $\mathfrak{sl}(n)$ и соответственно взаимно несмещенных базисов в $\mathbb{C}^n$ известна только в случае $n \leqslant 5$. Конструкцию 4-мерного семейства в $\mathbb{C}^6$ можно найти в [4]. Кроме того, в [5] имеются приложения симплектической геометрии для изучения взаимно несмещенных базисов.

Отметим также следующий объект, возникающий вместе с ортогональными парами и взаимно несмещенными базисами. Матрица F, при сопряжении на которую из проекторов π_i получаются ρ_i, называются обобщенно-адамаровыми. Условие (3.4) (и соответственно, (1.2)) естественным образом переписывается в терминах уравнений на элементы матрицы. Матрицы перехода между соответствующими базисами называются комплексно-адамаровыми. На множестве обобщенно-адамаровых (и соответственно, комплексно-адамаровых) матриц введено отношение эквивалентности: две обобщенно-адамаровы матрицы F_1 и F_2 эквивалентны, если $F_2 = M_1 F_1 M_2$, где M_i, $i = 1, 2$ — невырожденные мономиальные матрицы. В случае комплексно-адамаровых матриц надо выбрать M_i, $i = 1, 2$, мономиальными унитарными матрицами. Соответственно, принято считать что первая строка и первый столбец обобщенно-адамаровой (и, соответственно, комплексно-адамаровой) матрицы состоят из 1 (то же самое и в случае комплексно-адамаровой: после выноса $1/\sqrt{n}$ за скобку). Несложно проверяется, что задача классификации ортогональных пар в $\mathfrak{sl}(n)$ и взаимно несмещенных базисов в $\mathbb{C}^n$ эквивалентна классификации обобщенно-адамаровых (и комплексно-адамаровых) матриц размера n. В настоящий момент обобщенно-адамаровы и комплексно-адамаровы матрицы являются предметом пристального исследования (см. например, [9, 16, 15]).

В случае размерности 7 Петреску показал (см. [11]), что существует одномерное семейство комплексно-адамаровых матриц:

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & a\epsilon & a\epsilon^4 & \epsilon^5 & -1 & -1 & \epsilon \\ 1 & a\epsilon^4 & a\epsilon & -1 & \epsilon^5 & -1 & \epsilon \\ 1 & \epsilon^5 & -1 & \epsilon/a & \epsilon^4/a & \epsilon & -1 \\ 1 & -1 & \epsilon^5 & \epsilon^4/a & \epsilon/a & \epsilon & -1 \\ 1 & -1 & -1 & \epsilon & \epsilon & \epsilon^4 & \epsilon^5 \\ 1 & \epsilon & \epsilon & -1 & -1 & \epsilon^5 & \epsilon^4 \end{pmatrix};$$

здесь a — комплексное число, по модулю равное 1, ϵ — корень степени 6 из 1. Прямая проверка показывает, что если $a \in \mathbb{C}^*$, то эта матрица является обобщенно-адамаровой. Нишоара (см. [10]) показал, что в размерности 7 проекторы, соответствующие взаимно несмещенным базисам из семейства Петреску, после некоторого упорядочения удовлетворяет следующим соотношениям:

$$\Big[\pi_1 + \pi_2,\ \rho_1 + \rho_2\Big] = \Big[\pi_3 + \pi_4,\ \rho_3 + \rho_4\Big] = 0. \tag{3.8}$$

Обозначим через $I_{7,7}$ двусторонний идеал в $B_{\frac{1}{7}}(\Gamma_{7,7})$, порожденный соотношением (3.8). Обозначим через $A_{7,7}$ фактор алгебры $B_{\frac{1}{7}}(\Gamma_{7,7})$ по соотношениям

$$\sum_{i=1}^{7}\pi_i - 1, \quad \sum_{j=1}^{7}\rho_j - 1.$$

Тогда соответствие

$$P_1 \mapsto \pi_1 + \pi_2, \quad P_2 \mapsto \pi_3 + \pi_4, \quad Q_1 \mapsto \rho_1 + \rho_2, \quad Q_2 \mapsto \rho_3 + \rho_4 \tag{3.9}$$

определяет гомоморфизм $\mathcal{C} \to A_{7,7}$. Таким образом, получаем, что ортогональные пары в $\mathfrak{sl}(7)$ (и, соответственно, взаимно несмещенные базисы в размерности 7) определяют 7-мерное представление алгебры $\mathcal{C}$.

3.2. Алгебра $\mathbf{Pr}(\Gamma)$ и алгебра путей в колчане. В этом разделе мы введем понятие алгебры $\mathbf{Pr}(\Gamma)$ для фиксированного графа Γ, а также объясним связь с алгеброй путей в колчане $\boldsymbol{Q}_\Gamma$, отвечающем графу Γ. Алгебра $\mathbf{Pr}(\Gamma)$ — это алгебра над $\mathbb{C}$ с единичным элементом и генераторами x_v, обозначенными вершинами Γ, с соотношениями

$$\begin{aligned} &x_v^2 = x_v && \text{для каждого } v \in V(\Gamma),\\ &x_v x_w = x_w x_v = 0 && \text{для несмежных вершин } v,\ w. \end{aligned}$$

Существует натуральный морфизм (аргументации) $\epsilon : \mathbf{Pr}(\Gamma) \to \mathbb{C}$, определенный по формуле $\epsilon : x_v \mapsto 0$. Ядро ϵ называется идеалом аргументации; обозначим его $\mathbf{Pr}^+(\Gamma)$. Также определим алгебру путей $\mathbb{C}\boldsymbol{Q}$ для фиксированного колчана $\boldsymbol{Q}$. Пути в $\boldsymbol{Q}$ образуют базис в алгебре $\mathbb{C}\boldsymbol{Q}$. Обозначим через $\boldsymbol{Q}_0$ множество вершин в колчане $\boldsymbol{Q}$, а через $P(\boldsymbol{Q})$ — множество путей в $\boldsymbol{Q}$. Поставим тривиальный путь e_v в соответствие каждой вершине $v \in \boldsymbol{Q}_0$. Определим отображения

$$s : P(\boldsymbol{Q}) \to \boldsymbol{Q}_0, \quad t : P(\boldsymbol{Q}) \to \boldsymbol{Q}_0$$

следующим образом. Для фиксированного $\gamma \in P(\boldsymbol{Q})$ обозначим через $s(\gamma)$ и $t(\gamma)$ начало и конец пути γ соответственно. Определим композицию путей в колчане $\boldsymbol{Q}$ следующим образом. Рассмотрим два пути γ_1 и γ_2. Если $t(\gamma_1) = s(\gamma_2)$, то $\gamma_1\gamma_2$ — это путь, полученный непосредственным соединением путей. В противном случае $\gamma_1\gamma_2 = 0$. Ясно, что единичный элемент в $\mathbb{C}\boldsymbol{Q}$ — это сумма $\sum e_v$, которая берется по всем вершинам $\boldsymbol{Q}$. Таким образом, мы определили алгебру путей $\mathbb{C}\boldsymbol{Q}$.

Построим двойной колчан $\boldsymbol{Q}_\Gamma$, отвечающий фиксированному графу Γ. Множество вершин $\boldsymbol{Q}_\Gamma$ — это множество $V(\Gamma)$. Мы соединяем смежные вершины i, j противоположными стрелками a_{ij} и a_{ji}. Имеется соответствие между множеством путей в $\boldsymbol{Q}_\Gamma$ и множеством элементов $\mathbf{Pr}(\Gamma)$, определенное следующим образом:

$$f : \gamma \mapsto x_\gamma \in \mathbf{Pr}(\Gamma), \tag{3.10}$$

где $x_\gamma = x_{i_1} \dots x_{i_k}$ и $i_1, \dots, i_k$ — последовательные вершины в пути γ.

Предложение 3.3 (см. [4])**.** *Соответствие f является биекцией между $\mathbb{C}\boldsymbol{Q}_\Gamma$ и $\mathbf{Pr}^+(\Gamma)$. Следовательно, алгебра $\mathbf{Pr}(\Gamma)$ имеет $\mathbb{C}$-базис $1, x_\gamma$, где γ пробегает все пути в $\boldsymbol{Q}_\Gamma$.*

Напомним конструкцию гомотопа $\widehat{A}_x$ алгебры A с помощью элемента $x \in A$. Пусть x — фиксированный элемент в алгебре A. Будем рассматривать ассоциативную алгебру A_x (без единицы) с произведением $*_x$, определенным по формуле

$$a_1 *_x a_2 = a_1 x a_2.$$

Формально добавляя единицу, мы получим алгебру $\widehat{A}_x$. Свойства гомотопов изучены в [3]. В частности, имеется морфизм $\phi : \widehat{A}_x \to A$, определенный по правилу $\phi : a \mapsto ax$. Введем обозначение

$$\delta(\boldsymbol{Q}_\Gamma) = 1 + \sum a_{ij},$$

где сумма берется по всем стрелкам в колчане $\boldsymbol{Q}_\Gamma$. Алгебра $\mathbf{Pr}(\Gamma)$ — это гомотоп алгебры $\mathbb{C}\boldsymbol{Q}_\Gamma$ с помощью элемента $\Delta(\boldsymbol{Q}_\Gamma)$ (см. [3]). Пользуясь свойствами гомотопов, имеем морфизм

$$\phi : \mathbf{Pr}(\Gamma) \to \mathbb{C}\boldsymbol{Q}_\Gamma \tag{3.11}$$

определенный по правилу $x_v \mapsto e_v\Delta(\boldsymbol{Q}_\Gamma)$.

Пусть $\Gamma_{k,m}$ — полный двудольный граф с k и m вершинами в верхнем и нижнем ряду соответственно; обозначим их $1, 2, \dots, k$ и $1', 2', \dots, m'$ соответственно.

Рассмотрим случай $\mathbb{C}^{\oplus 3} * \mathbb{C}^{\oplus 3}$; этой алгебре соответствует граф $\Gamma_{3,3}$. Вершины 1, 2, 3 и $1'$, $2'$, $3'$ отвечают P_1, P_2, $P_3 = 1 - P_1 - P_2$ и Q_1, Q_2, $Q_3 = 1 - Q_1 - Q_2$ соответственно. Алгебра $\mathbb{C}^{\oplus 3} * \mathbb{C}^{\oplus 3}$ изоморфна фактору алгебры $\mathbf{Pr}(\Gamma_{3,3})$ по идеалу, порожденному элементами $P_1 + P_2 + P_3 - 1$ и $Q_1 + Q_2 + Q_3 - 1$. Также заметим, что алгебра $\mathbb{C}^{\oplus 3} * \mathbb{C}^{\oplus 3}$ изоморфна алгебре $\mathbf{Pr}(\Gamma_{2,2})$. Для простоты обозначим алгебры $\mathbf{Pr}(\Gamma_{2,2})$ и $\mathbb{C}\boldsymbol{Q}_{\Gamma_{2,2}}$ соответственно через $\mathbf{Pr}$ и $\mathbb{C}\boldsymbol{Q}$. Также имеется гомоморфизм

$$\phi : \mathbf{Pr} \to \mathbb{C}\boldsymbol{Q},$$

определенный по формуле

$$\phi : P_1 \mapsto e_1 + a_{11'} + a_{12'}, \quad P_2 \mapsto e_2 + a_{21'} + a_{22'}, \quad Q_1 \mapsto e_{1'} + a_{1'1} + a_{1'2}, \quad Q_2 \mapsto e_{2'} + a_{2'1} + a_{2'2}.$$

3.3. Фильтрация на $\mathcal{C}$. Напомним, что фильтрация на фиксированной ассоциативной алгебре A — это множество таких конечномерных подпространств F^iA, $i = 0, 1, 2, \dots$, что

(i) $F^0A \subseteq F^1A \subseteq \dots \subseteq F^iA \subseteq F^{i+1}A \dots$;
(ii) $\bigcup_{i=0}^{\infty} F^iA = A$;
(iii) $F^iA \cdot F^jA \subseteq F^{i+j}A$, где $F^iA \cdot F^jA$ — подпространство, порожденное $c' \cdot c''$, $c' \in F^iA$, $c'' \in F^jA$.

Рассмотрим алгебру путей $\mathbb{C}\boldsymbol{Q}$ в фиксированном колчане $\boldsymbol{Q}$. Определим функцию длины $l : P(\boldsymbol{Q}) \to \mathbb{N}_0$ следующим образом. Положим $l(e_v) = 0$ для любой вершины $v \in \boldsymbol{Q}_0$. Можно сказать, что $l(\gamma) = k$ тогда и только тогда, когда γ — произведение k стрелок. Таким образом, существует фильтрация на $\mathbb{C}\boldsymbol{Q}$: $F^i\mathbb{C}\boldsymbol{Q}$ — это пространство, порожденное путями длины $\leqslant i$.

Отметим следующее полезное свойство морфизма ϕ, которое следует из формулы (3.11).

Предложение 3.4. *Морфизм $\phi : \mathbf{Pr}(\Gamma) \to \mathbb{C}\boldsymbol{Q}_\Gamma$ инъективен.*

Доказательство. Рассмотрим элемент $x = \sum c_\gamma x_\gamma$, где $\gamma \in P(\boldsymbol{Q}_\Gamma)$, x_γ — элемент из $\mathbf{Pr}(\Gamma)$, соответствующий пути γ, и $c_\gamma \in \mathbb{C}$. Предположим, что

$$\phi(x) = \phi(\sum c_\gamma x_\gamma) = \sum c_\gamma \gamma\Delta(\boldsymbol{Q}_\Gamma) = 0.$$

Докажем, что $\Delta(\boldsymbol{Q}_\Gamma)$ не является делителем нуля. Пусть существует такой элемент

$$\Theta = \sum_\gamma c_\gamma \gamma \in \mathbb{C}\boldsymbol{Q}_\Gamma$$

что $\Theta\Delta(\boldsymbol{Q}_\Gamma) = 0$. Рассмотрим линейно независимые пути γ в разложении элемента Θ. Умножая на $\Delta(\boldsymbol{Q}_\Gamma)$, получим линейно независимые пути в разложении $\Theta\Delta(\boldsymbol{Q}_\Gamma)$. Таким образом, $\Theta = 0$. □

Следствие 3.5. *Длина пути индуцирует функцию длины L элемента из $\mathbf{Pr}(\Gamma)$, а именно, $L(x_\gamma) = l(\gamma) + 1$, т.е. $L(x_{i_1} \dots x_{i_k}) = k$. Если $x = \sum c_\gamma x_\gamma$, то*

$$L(x) = \max_{\gamma : c_\gamma \neq 0} L(x_\gamma).$$

Также фильтрация на $\mathbb{C}\boldsymbol{Q}_\Gamma$ индуцирует фильтрацию на $\mathbf{Pr}(\Gamma)$: $F^0\mathbf{Pr}(\Gamma) = \mathbb{C} \cdot 1$, $F^i\mathbf{Pr}(\Gamma)$ — пространство, порожденное элементом длины $\leqslant i$.

Вернемся к алгебре $\mathbf{Pr}$. На $\mathbf{Pr}$ имеется фильтрация, индуцированная фильтрацией на $\mathbb{C}\boldsymbol{Q}$. Алгебра $\mathcal{C}$ — это фактор $\mathbf{Pr}$ по идеалу I, порожденному элементом $h = [P_1 - Q_2, P_2 - Q_1]$. Также напомним, что $\mathcal{C}$ — это фактор алгебры $\mathbf{Pr}(\Gamma_{3,3})$ по идеалу $\mathcal{I}$, порожденному элементами $P_1 + P_2 + P_3 - 1$, $Q_1 + Q_2 + Q_3 - 1$, h. Очевидно,

$$\mathbf{Pr}\,/I \cong \mathbf{Pr}(\Gamma_{3,3})/\mathcal{I}.$$

Поскольку $S_3 \times \mathbb{Z}_2$ — это группа автоморфизмов графа $\Gamma_{3,3}$, то определено действие этой группы на группе $\mathbf{Pr}(\Gamma_{3,3})$. Легко проверить, что элементы $P_1+P_2+P_3-1$, $Q_1+Q_2+Q_3-1$ инвариантны относительно действия этой группы. Также заметим, что описанная конструкция определяет действие $S_3 \times \mathbb{Z}_2$ на $\mathbf{Pr}$.

Лемма 3.6. *Существует вполне определенное действие группы $S_3 \times \mathbb{Z}_2$ на идеале $\mathcal{I}$, заданное следующим образом. Действия перестановок определено по формулам*

$$\begin{aligned} \sigma_1 :&\quad P_1 \leftrightarrow P_2, \quad Q_1 \leftrightarrow Q_2, \\ \sigma_2 :&\quad P_1 \leftrightarrow P_3, \quad Q_2 \leftrightarrow Q_3. \end{aligned}$$

Группа $\mathbb{Z}_2$ действует перестановками:

$$P_1 \leftrightarrow Q_2, \quad P_2 \leftrightarrow Q_1.$$

Доказательство. Имеем

$$\begin{aligned} \sigma_2(h) = \big[P_3 - Q_3,\ P_2 - Q_1\big] &= \big[Q_1 + Q_2 - P_1 - P_2,\ P_2 - Q_1\big] \\ &= \big[Q_1,\ P_2\big] + \big[Q_2,\ P_2\big] + \big[P_1,\ Q_1\big] + \big[P_2,\ Q_1\big] = \big[P_1,\ Q_1\big] - \big[P_2,\ Q_2\big] = h. \end{aligned}$$

Дальнейшее доказательство очевидно. □

Обозначим через pr естественную проекцию $\mathbf{Pr} \to \mathcal{C} = \mathbf{Pr}\,/I$, а через $F^i\mathcal{C}$ — образ $\mathrm{pr}(F^i\,\mathbf{Pr})$. Таким образом, алгебра $\mathcal{C}$ имеет фильтрацию, индуцированную фильтрацией на $\mathbf{Pr}$. Далее, морфизм pr индуцирует сюръективный морфизм $\mathrm{pr}^i : F^i\,\mathbf{Pr} \to F^i\mathcal{C}$, $i = 0, 1, 2, \ldots$. Кроме того, обозначим через I^i пространство $\operatorname{Ker} pr^i = I \cap F^i\,\mathbf{Pr}$, $i = 0, 1, 2, \ldots$.

Рассмотрим фактор-пространства $\mathrm{gr}^0\,\mathbf{Pr} = \mathbb{C} \cdot 1$, $\mathrm{gr}^i\,\mathbf{Pr} = F^i\,\mathbf{Pr}\,/F^{i-1}\,\mathbf{Pr}$, $i = 1, 2, \ldots,$. Очевидно, в векторном пространстве $\mathrm{gr}^i\,\mathbf{Pr}$ можно выбрать базис, состоящий из элементов x_γ, $l(\gamma) = i-1$.

Предложение 3.7. *Рассмотрим векторные пространства $\mathrm{gr}^i\,\mathcal{C}$. Имеют место следующие соотношения*:

$$\dim_{\mathbb{C}} \mathrm{gr}^0\,\mathcal{C} = 1, \quad \dim_{\mathbb{C}} \mathrm{gr}^1\,\mathcal{C} = 4, \tag{3.12}$$

$$\dim_{\mathbb{C}} \mathrm{gr}^2\,\mathcal{C} \leqslant 7, \quad \dim_{\mathbb{C}} \mathrm{gr}^i\,\mathcal{C} \leqslant 6, \quad i \geqslant 3. \tag{3.13}$$

Более того, любой элемент $x \in F^l\mathcal{C}$ может быть представлен как линейная комбинация элементов $P_1Q_1P_1\ldots$, $Q_1P_1Q_1\ldots$, $P_1Q_2P_1\ldots$, $Q_2P_1Q_2\ldots$, $P_2Q_1P_2\ldots$ и $Q_1P_2Q_1\ldots$ длины l и элементов длины $<l$.

Доказательство. Случаи $\mathrm{gr}^0\,\mathcal{C}$ и $\mathrm{gr}^1\,\mathcal{C}$ тривиальны. Имеет место следующая коммутативная диаграмма:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & I^{l-1} & \longrightarrow & F^{l-1}\,\mathbf{Pr} & \longrightarrow & F^{l-1}\mathcal{C} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & I^{l} & \longrightarrow & F^{l}\,\mathbf{Pr} & \longrightarrow & F^{l}\mathcal{C} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & I^{l}/I^{l-1} & \longrightarrow & F^{l}\,\mathbf{Pr}\,/F^{l-1}\,\mathbf{Pr} & \longrightarrow & F^{l}\mathcal{C}/F^{l-1}\mathcal{C} & \longrightarrow & 0, \end{array} \tag{3.14}$$

где два верхних ряда и три колонки — это точные последовательности. Используя эти последовательности и непосредственные вычисления, мы получаем, что нижний ряд — это точная последовательность.

Также рассмотрим морфизм

$$f : I^l \to F^l\,\mathbf{Pr} \to F^l\,\mathbf{Pr}\,/F^{l-1}\,\mathbf{Pr},$$

определенный следующим образом. Возьмем элемент $y = \sum\limits_{\gamma} c_\gamma x_\gamma \in I^l$ и рассмотрим разложение

$$y = \sum_{s=0}^{l} y_s, \quad \text{где} \quad y_s = \sum_{\gamma : l(\gamma)=s-1} c_\gamma x_\gamma.$$

Таким образом, морфизм f определен по правилу $f(y) = y_l$. Следовательно, $\operatorname{gr}^l \mathcal{C}$ — это фактор $\operatorname{gr}^l \mathbf{Pr}$ по подпространству I^l/I^{l-1}. Кроме того, I^l/I^{l-1} — это пространство, порожденное «l-частями» элементов из I^l.

Неравенство $\dim_{\mathbb{C}} \operatorname{gr}^2 \mathcal{C} \leqslant 7$ очевидно.

Докажем утверждение по индукции. Во-первых, докажем, что любой элемент $F^3\mathcal{C}$ представляет собой линейную комбинацию $P_1Q_1P_1$, $Q_1P_1Q_1$, $P_1Q_2P_1$, $Q_2P_1Q_2$, $P_2Q_1P_2$, $Q_1P_2Q_1$ и элементов длины <3.

Обозначим через $V \subseteq I^3$ подпространство, порожденное такими элементами вида $x_\gamma h$, $h x_{\gamma'}$ и $x_\gamma h x_{\gamma'}$, что $L(x_\gamma) = L(x_{\gamma'}) = 1$ и $L(x_\gamma h x_{\gamma'}) = 3$. Рассмотрим образ V в $\operatorname{gr}^3 \mathbf{Pr}$ над f. Легко проверить, что фактор $\operatorname{gr}^3 \mathbf{Pr}\,/f(V)$ порождается элементами $P_1Q_1P_1$, $Q_1P_1Q_1$, $P_1Q_2P_1$, $Q_2P_1Q_2$, $P_2Q_1P_2$, $Q_1P_2Q_1$. Также отметим следующее соотношение для остальных $P_iQ_jP_k$:

$$P_iQ_jP_k = \pm P_1Q_1P_1 + x, \tag{3.15}$$

где $L(x) \leqslant 2$. Аналогичное утверждение выполнено для $Q_iP_jQ_k$. Далее, предположим, что утверждение верно для любых $l \leqslant k$ и докажем, что оно верно также для $l = k+1$. Достаточно доказать, что утверждение верно для мономов. Рассмотрим моном $t = P_{i_1}Q_{i_2}\dots Q_{i_{k+1}}$, где $i_{k+1} = 2$. По предположению индукции справедливо соотношение

$$\begin{aligned} t = (c_1P_1Q_1\dots P_1 + c_2Q_1P_1Q_1\dots Q_1 + \dots + c_6Q_1P_2Q_1\dots Q_1)Q_2 \\ = c_1P_1Q_1\dots P_1Q_2 + c_3P_1Q_2P_1\dots Q_2 + c_5P_2Q_1\dots P_2Q_2 + x, \end{aligned}$$

где $L(x) < k+1$. Пользуясь формулой (3.15) и фильтрацией, получаем, что

$$P_1Q_1\dots P_1Q_2 = c''P_1Q_1\dots P_1Q_1 + x, \quad P_2Q_1\dots P_2Q_2 = c'P_1Q_1\dots P_1Q_1 + x',$$

где $c', c'' = \pm 1$, $L(x) < k+1$ и $L(x') < k+1$. Остальные случаи рассматриваются аналогично. □

Используя лемму 3.6, получаем следующее утверждение.

Следствие 3.8. *Действие группы $S_3 \times \mathbb{Z}_2$ на алгебре $\mathcal{C}$ согласовано с фильтрацией. Таким образом, $\operatorname{gr}^l \mathcal{C}$ — это $S_3 \times \mathbb{Z}_2$-модуль для любых $l \in \mathbb{N}_0$.*

3.4. Идеал I алгебры $\mathbf{Pr}$ как пересечение идеалов и базиса в $\mathcal{C}$. В этом разделе будет показано, что идеал I алгебры $\mathbf{Pr}$ представляет собой пересечение трех более простых идеалов алгебры $\mathbf{Pr}$; это позволит вычислить размерность $\operatorname{gr}^i \mathcal{C}$ и базиса в $\mathcal{C}$.

Рассмотрим идеалы

$$I_1 = \langle P_1, Q_2 \rangle, \quad I_2 = \langle P_2, Q_1 \rangle, \quad I_3 = \langle 1 - P_1 - P_2, 1 - Q_1 - Q_2 \rangle$$

алгебры $\mathbf{Pr}$. Ясно, что $I_2 = \sigma_1(I_1)$ и $I_3 = \sigma_2(I_1)$. Фактор-алгебры $\mathcal{C}_j = \mathbf{Pr}\,/I_j$, $j = 1, 2, 3$, изоморфны свободному произведению $\mathbb{C}^{\oplus 2} * \mathbb{C}^{\oplus 2}$. Обозначим через ψ_j естественные проекции $\mathbf{Pr} \to \mathcal{C}_j$, $j = 1, 2, 3$. Ясно, что

$$\psi_2 = \psi_1 \circ \sigma_1, \quad \psi_3 = \psi_1 \circ \sigma_2. \tag{3.16}$$

Рассмотрим случай I_1. Имеются алгебры $\mathbb{C}^{\oplus 3}$ с базисами P_1, P_2, $1 - P_1 - P_2$ и Q_1, Q_2, $1 - Q_1 - Q_2$. Определим морфизмы $\mathbb{C}^{\oplus 3} \to \mathbb{C}^{\oplus 2}$ как естественные проекции с ядрами, порожденными P_1 и Q_2 соответственно. Таким образом, мы можем определить морфизмы $\mathbb{C}^{\oplus 3} \to \mathcal{C}_1 = \mathbb{C}^{\oplus 2} * \mathbb{C}^{\oplus 2}$. Пользуясь универсальностью свободного произведения,

$$\psi_1 : \mathbf{Pr} = \mathbb{C}^{\oplus 3} * \mathbb{C}^{\oplus 3} \to \mathcal{C}_1 = \mathbb{C}^{\oplus 2} * \mathbb{C}^{\oplus 2},$$

заметим, что любой элемент из $\mathbb{C}^{\oplus 2} * \mathbb{C}^{\oplus 2}$ имеет прообраз при таком морфизме. Таким образом, ψ_1 сюръективен. Можно показать, что $\operatorname{Ker} \psi_1 = I_1$. Рассуждая аналогично, получим, что факторы $\mathcal{C}_j$ изоморфны $\mathbb{C}^{\oplus 2} * \mathbb{C}^{\oplus 2}$.

Предложение 3.9. *Рассмотрим алгебру* $\mathbf{Pr}$ *и двусторонние идеалы* $I = \langle h \rangle$, $I_1 = \langle P_1, Q_2 \rangle$, $I_2 = \langle P_2, Q_1 \rangle$ *и* $I_3 = \langle 1 - P_1 - P_2, 1 - Q_1 - Q_2 \rangle$. *Тогда*

$$I \subseteq I_1 \cap I_2 \cap I_2. \tag{3.17}$$

Доказательство. Очевидно, что $I \subset I_j$, $j = 1, 2$. Также нетрудно убедиться, что

$$h = (1 - Q_1 - Q_2)(P_1 + P_2) - (1 - P_1 - P_2)(Q_1 + Q_2).$$

Таким образом, $I \subset I_3$. □

Кроме того, сделаем полезное замечание. Обозначим через x_1, y_1, x_2, y_2 и x_3, y_3 порождающие идемпотенты алгебр $\mathcal{C}_1$, $\mathcal{C}_2$ и $\mathcal{C}_3$ соответственно. В этом случае определен морфизм

$$\psi_1 : P_1 \mapsto 0,\ P_2 \mapsto x_1,\ Q_1 \mapsto y_1,\ Q_2 \mapsto 0;$$

Морфизмы ψ_2 и ψ_3 определяются формулой (3.16). Очевидно, что существует естественная фильтрация на $\mathcal{C}_i$, порожденная функцией длины. Хорошо известно, что элементы $x_i y_i x_i \dots$, $y_i x_i y_i \dots$ образуют базис в $\mathcal{C}_i$, $i = 1, 2, 3$. Кроме того,

$$\dim_{\mathbb{C}} \operatorname{gr}^l \mathcal{C}_i = 2$$

с базисом, состоящим из $x_i y_i \dots$, $y_i x_i \dots$ длины l.

Теорема 3.10. *Выполнено следующее соотношение*:

$$I = I_1 \cap I_2 \cap I_3. \tag{3.18}$$

Доказательство. Для простоты обозначим через I_{123} пересечение $I_1 \cap I_2 \cap I_3$. Используя предложение 3.9, получаем сюръективный морфизм $\pi : \mathcal{C} \to \mathbf{Pr}\,/I_{123}$. Заметим, что идеал I_{123} представляет собой $S_3 \times \mathbb{Z}_2$-инвариант. Этот морфизм определяет фильтрацию на алгебре $\mathbf{Pr}\,/I_{123}$. Также имеем сюръективный морфизм $\pi : \operatorname{gr}^l \mathcal{C} \to \operatorname{gr}^l \mathbf{Pr}\,/I_{123}$. Получается следующая факторизация морфизмов ψ_i, $i = 1, 2, 3$:

$$\begin{array}{ccc} \mathcal{C} & \xrightarrow{\quad\psi_i\quad} & \mathcal{C}_1 \\ & {\scriptstyle\pi}\searrow \quad \nearrow{\scriptstyle\psi_i'} & \\ & \mathbf{Pr}\,/I_{123}. & \end{array} \tag{3.19}$$

Докажем, что

$$\dim_{\mathbb{C}} \operatorname{gr}^l \mathbf{Pr}\,/I_{123} = 6, \quad l \geqslant 3, \qquad \dim_{\mathbb{C}} \operatorname{gr}^2 \mathbf{Pr}\,/I_{123} = 7.$$

Для этого рассмотрим элементы из предложения 3.7 и покажем, что образы этих элементов при действии морфизма π линейно независимы. Зафиксируем $l \geqslant 3$ и введем обозначения

$$\begin{aligned} e_1 &= \pi(P_1 Q_2 P_1 \dots), \quad e_2 = \pi(P_2 Q_1 P_2 \dots), \quad e_3 = \pi(P_1 Q_1 P_1 \dots), \\ f_1 &= \pi(Q_2 P_1 Q_2 \dots), \quad f_2 = \pi(Q_1 P_2 Q_1 \dots), \quad f_3 = \pi(Q_1 P_1 Q_1 \dots). \end{aligned}$$

Предположим, что существует нетривиальная линейная комбинация

$$a_1 e_1 + a_2 e_2 + a_3 e_3 + b_1 f_1 + b_2 f_2 + b_3 f_3 = 0$$

в векторном пространстве $\operatorname{gr}^l \mathbf{Pr}\,/I_{123}$. Рассмотрим

$$\psi_1'\Big(a_1 e_1 + a_2 e_2 + a_3 e_3 + b_1 f_1 + b_2 f_2 + b_3 f_3\Big) = a_2 x_1 y_1 \dots + b_2 y_1 x_1 \dots = 0.$$

Таким образом, $a_2 = b_2 = 0$. Используя действие группы $S_3 \times \mathbb{Z}_2$, получаем, что $a_i = b_i = 0$, $i = 1, 2, 3$.

Группа симметрий дает нам две возможности:

$$P_1 Q_1 - P_2 Q_2 = 0, \quad Q_1 P_1 - Q_2 P_2 = 0$$

или

$$P_1 Q_1 - Q_1 P_1 - P_2 Q_2 + Q_2 P_2 = 0 \tag{3.20}$$

в $\mathrm{gr}^2\,\mathbf{Pr}\,/I_{123}$. Непосредственным вычислением можно убедиться, что не существует такого элемента $x \in I_{123}$, что $L(x) \leqslant 2$ и часть длины 2 — это $P_1Q_1 - Q_1P_1$. Таким образом, остается единственная возможность (3.20).

Это означает, что π — изоморфизм. Объединяя полученные результаты с результатами предложения 3.9, получаем, что $I = I_{123}$. □

Следствие 3.11. *Алгебра $\mathcal{C}$ имеет следующий базис*:

(i) *единичный элемент* 1 *и элементы* P_1, P_2, Q_1, Q_2 *длины* 0 *и* 1 *соответственно;*
(ii) *элементы* P_1Q_1, P_1Q_2, P_2Q_1, P_2Q_2, Q_1P_1, Q_1P_2, Q_2P_1 *длины* 2*;*
(iii) *элементы* $P_1Q_1P_1\ldots$, $Q_1P_1Q_1\ldots$, $P_1Q_2P_1\ldots$, $Q_2P_1Q_2\ldots$, $P_2Q_1P_2\ldots$, $Q_1P_2Q_1\ldots$ *длины* k, $k \geqslant 3$.

Этот набор — бесконечный базис алгебры $\mathcal{C}$. В частности, алгебра $\mathcal{C}$ бесконечномерна.

Следствие 3.12. *Рассмотрим морфизмы $\psi_i : \mathcal{C} \to \mathcal{C}_i$. Тогда*

$$\operatorname{Ker}\psi_1 \cap \operatorname{Ker}\psi_2 \cap \operatorname{Ker}\psi_3 = \{0\}.$$

4. Теория представлений алгебры $\mathcal{C}$

В этом разделе при помощи изучения центра алгебры $\mathcal{C}$ получена классификация всех неприводимых $\mathcal{C}$-модулей и приведено геометрическое описание неприводимых $\mathcal{C}$-модулей.

4.1. Алгебры S_a, $a \in \mathbb{C}^*$. Изучим одномерное семейство коммутативных подалгебр.

Рассмотрим алгебру $\mathcal{C}$. Введем параметр $a = (a_0 : a_1) \in \mathbb{P}^1$ (напомним, что проективная прямая $\mathbb{P}^1$ содержит точки с однородными координатами $(a_0 : a_1)$). Рассмотрим элемент $[a_0P_1 - a_1Q_2,\ a_0P_2 - a_1Q_1]$. Ясно, что

$$\Big[a_0P_1 - a_1Q_2,\ a_0P_2 - a_1Q_1\Big] = -a_0a_1\Big(\big[P_1, Q_1\big] - \big[P_2, Q_2\big]\Big) = -a_0a_1\Big[P_1 - Q_2,\ P_2 - Q_1\Big]. \quad (4.1)$$

Если $a_0, a_1 \neq 0$, то идеалы $\Big\langle\big[a_0P_1 - a_1Q_2,\ a_0P_2 - a_1Q_1\big]\Big\rangle$ и $\Big\langle\big[P_1 - Q_2,\ P_2 - Q_1\big]\Big\rangle$ в $\mathbf{Pr}$ совпадают. Таким образом, мы можем рассмотреть семейство подалгебр S_a, параметризованное $\mathbb{P}^1 \setminus \{(0 : 1), (1 : 0)\} = \mathbb{C}^*$ с координатами $a = a_1/a_0$.

Зафиксируем $a \in \mathbb{C}^*$ и рассмотрим подалгебру $S_a \subset \mathcal{C}$, порожденную элементами $s_1 = P_1 - aQ_2$ и $s_2 = P_2 - aQ_1$. Алгебра S_a коммутативна. Заметим, что S_a инвариантна относительно действий инволюции σ_1 из леммы 3.6. Также, используя предложение 2.1 в случае $A = \mathbb{C}^{\oplus 3}$ и $B = \mathbb{C}^{\oplus 3}$ и теорему 3.11, получаем, что алгебра S_a бесконечномерна.

Кроме того, у нас имеется вполне определенное действие S_3 на алгебре S_a. Действительно, эта группа действует на S_a перестановками элементов s_1, s_2, $s_1 + s_2 + (a - 1)$. Перестановка $P_i \leftrightarrow Q_i$ преобразует подалгебру S_a в $S_{1/a}$. Поэтому, если $a = \pm 1$, мы имеем корректно определенное действие $S_3 \times \mathbb{Z}_2$.

Предложение 4.1. *Выполнено следующее соотношение*:

$$s_1s_2(s_1 + s_2 + (a - 1)) = 0. \quad (4.2)$$

Доказательство. Перепишем левую часть следующим образом:

$$\begin{aligned} s_1s_2\Big(s_1 + s_2 - (a-1)\Big) &= (P_1 - aQ_2)(P_2 - aQ_1)\Big((P_1 + P_2) - a(Q_1 + Q_2) + (a-1)\Big) = \\ &= -a\Big(P_1Q_1 + Q_2P_2\Big)\Big((P_1 + P_2) - a(Q_1 + Q_2) + (a-1)\Big) = \\ &= -a\Big(P_1Q_1P_1 + P_1Q_1P_2 - P_1Q_1\Big) + a^2\Big(Q_2P_2Q_1 + Q_2P_2Q_2 - Q_2P_2\Big). \end{aligned}$$

Покажем, что элементы $P_1Q_1P_1 + P_1Q_1P_2 - P_1Q_1$ и $Q_2P_2Q_1 + Q_2P_2Q_2 - Q_2P_2$ выводятся из коммутационного соотношения. Действительно,

$$P_1\Big[P_1 - Q_2,\ P_2 - Q_1\Big](P_2 - 1) = P_1Q_1P_1 + P_1Q_1P_2 - P_1Q_1.$$

Поэтому

$$P_1Q_1P_1 + P_1Q_1P_2 - P_1Q_1 = 0$$

в алгебре $\mathcal{C}$. Аналогично,

$$Q_2P_2Q_1 + Q_2P_2Q_2 - Q_2P_2 = 0.$$

Утверждение доказано. □

Предложение 4.2. *Зафиксируем $a \in \mathbb{C}^*$. Рассмотрим сюръективный морфизм $\phi : \mathbb{C}[s_1, s_2] \to S_a$. Ядро ϕ порождено элементом $s_1s_2(s_1 + s_2 + (a-1))$, т.е. соотношение (4.2) — единственное определяющее соотношение в алгебре S_a.*

Доказательство. Рассмотрим элемент $h_1 \in \operatorname{Ker}\phi$. Пользуясь бесконечномерностью S_a, получаем $\gcd(h_1, s_1s_2(s_1 + s_2 + (a-1))) \neq 1$. Имеем три возможности:

(i) $h_1 = s_1h_2$ для некоторого h_2,
(ii) $h_1 = s_2h_2$ для некоторого h_2,
(iii) $h_1 = (s_1 + s_2 + (a-1))h_2$ для некоторого h_2.

Применяя действия группы S_3, получаем, что $h = s_1s_2(s_1 + s_2 + (a-1))h'$ для некоторого h'. □

Рассмотрим семейство аффинных многообразий $\operatorname{Spec} S_a = \operatorname{Hom}_{\mathrm{alg}}(S_a, \mathbb{C})$, $a \in \mathbb{C}^*$.

Следствие 4.3. *Имеются следующие две возможности*:

(i) $a \neq 1$, $\operatorname{Spec} S_a$ — *объединение трех прямых, пересекающихся в трех различных точках*;
(ii) $a = 1$, $\operatorname{Spec} S_1$ — *объединение трех прямых, проходящих через одну точку.*

Доказательство. Зафиксируем $a \in \mathbb{C}^*$. Рассмотрим аффинное многообразие $\operatorname{Spec} S_a$. Существует естественное вложение $\operatorname{Spec} S_a$ в аффинное многообразие $\mathbb{C}^2$ с координатами s_1, s_2. При этом подмногообразие $\operatorname{Spec} S_a$ задано уравнением (4.2). □

4.2. Центр алгебры $\mathcal{C}$. Опишем центр алгебры $\mathcal{C}$. Рассмотрим одномерное семейство подалгебр $S_a \subset C$, $a \in \mathbb{C}^*$. Введем обозначения $s_1(a) = P_1 - aQ_2$ и $s_2(a) = P_2 - aQ_1$ для фиксированного $a \in \mathbb{C}^*$. Обозначим через $\mathcal{Z}(\mathcal{C})$ центр алгебры $\mathcal{C}$.

Предложение 4.4. *Верны следующие утверждения*:

(i) *Подалгебры S_{a_1} и S_{a_2} для любых различных $a_1, a_2 \in \mathbb{C}^*$, $a_1 \neq a_2$, порождают алгебру $\mathcal{C}$.*
(ii) *Элементы $s_1^2(a') + (a'-1)s_1(a')$, $s_2^2(a') + (a'-1)s_2(a')$, $s_1(a')s_2(a')$ лежат в пересечении $\bigcap\limits_{a\in\mathbb{C}^*} S_a$ для любого $a' \in \mathbb{C}^*$.*
(iii) *Имеет место вложение*

$$\bigcap_{a\in\mathbb{C}^*} S_a \subseteq \mathcal{Z}(\mathcal{C}).$$

Доказательство. Используя выражения для $s_i(a)$ как линейных комбинаций P_i и Q_j, получаем первое утверждение. Непосредственными вычислениями убеждаемся в справедливости следующих тождеств:

$$a_2(s_1^2(a_1) + (a_1-1)s_1(a_1)) = a_1(s_1^2(a_2) + (a_2-1)s_1(a_2)), \tag{4.3}$$

$$a_2(s_2^2(a_1) + (a_1-1)s_2(a_1)) = a_1(s_2^2(a_2) + (a_2-1)s_2(a_2)), \tag{4.4}$$

$$a_2s_1(a_1)s_2(a_1) = a_1s_1(a_2)s_2(a_2) \tag{4.5}$$

для любых $a_1, a_2 \in \mathbb{C}^*$. Это доказывает второе утверждение. В частности, мы получили, что

$$\bigcap_{a\in\mathbb{C}^*} S_a = S_{a_1} \cap S_{a_2}$$

для любых $a_1, a_2 \in \mathbb{C}^*$, $a_1 \neq a_2$. Рассмотрим $x \in S_{a_1} \cap S_{a_2}$. Получаем, что x коммутирует с $s_i(a_j)$, $i = 1, 2$, $j = 1, 2$. Пользуясь первым утверждением, получаем, что $x \in \mathcal{Z}(\mathcal{C})$. □

Предложение 4.5. *Зафиксируем $a \in \mathbb{C}^*$. Любой элемент из центра $\mathcal{Z}(\mathcal{C})$ может быть представлен как сумма $f_1(t_1) + f_2(t_2) + f_3(t_3)$, где $f_i \in \mathbb{C}[x]$ и*

$$\begin{aligned} t_1 &= \frac{s_2^2(a) + (a-1)s_2(a) + s_1(a)s_2(a)}{a}, \\ t_2 &= \frac{s_1^2(a) + (a-1)s_1(a) + s_1(a)s_2(a)}{a}, \\ t_3 &= \frac{s_1(a)s_2(a)}{a}. \end{aligned} \tag{4.6}$$

Доказательство. Рассмотрим морфизмы $\psi_i : \mathcal{C} \to C_i$, $i = 1, 2, 3$, из п. 3.4. Очевидно,

$$\psi_i(\mathcal{Z}(\mathcal{C})) \subseteq \mathcal{Z}(\mathcal{C}_i), \quad i = 1, 2, 3,$$

где $\mathcal{Z}(\mathcal{C}_i)$ — центр алгебры $\mathcal{C}_i$, $i = 1, 2, 3$. Докажем, что $x \in \mathcal{Z}(\mathcal{C})$ тогда и только тогда, когда $\psi_i(x) \in \mathcal{Z}(\mathcal{C}_i)$, $i = 1, 2, 3$. Легко видеть, что необходимость очевидна. Напомним, что x_i, y_i — генераторы в $\mathcal{C}_i$, $i = 1, 2, 3$. Хорошо известно, что центр $\mathcal{C}_i$ порождается элементом $\theta_i = x_i y_i + y_i x_i - x_i - y_i$ для любых $i = 1, 2, 3$ (см. []). Зафиксируем $a \in \mathbb{C}^*$ и рассмотрим элемент

$$t_3 = \frac{s_1(a)s_2(a)}{a}. \tag{4.7}$$

Ясно, что $\psi_i(t_3) = 0$, $i = 1, 2$, и $\psi_3(t_3) = \theta_3$. Напомним, что на $\mathbb{C}$ действует группа $S_3 \times \mathbb{Z}_2$. Ясно, что эта группа сохраняет центр $\mathcal{Z}(\mathcal{C})$. Рассмотрим различные элементы вида $\sigma(t_3)$, $\sigma \in S_3$; можно найти такие элементы вида t_i, $i = 1, 2$, что $\psi_j(t_i) = 0$ при $i \neq j$ и $\psi_i(t_i) = \theta_i$, $i = 1, 2$. Непосредственные вычисления показывают, что

$$t_1 = -\frac{s_2^2(a) + (a-1)s_2(a) + s_1(a)s_2(a)}{a}, \quad t_2 = -\frac{s_1^2(a) + (a-1)s_1(a) + s_1(a)s_2(a)}{a}. \tag{4.8}$$

Пусть $\psi_i(x) \in \mathcal{Z}(\mathbb{C}_i)$, $i = 1, 2, 3$. Для $\psi_i(x)$ выполнены следующие формулы: $\psi_i(x) = f_i(\theta_i)$, $i = 1, 2, 3$, для некоторых полиномов $f_i \in \mathbb{C}[x]$. Рассмотрим элемент

$$z = f_1(t_1) + f_2(t_2) + f_3(t_3) \in \mathcal{Z}(\mathcal{C}).$$

Далее, имеем формулы

$$\psi_i(z) = \psi_i(x) = f_i(\theta_i), \quad i = 1, 2, 3.$$

Таким образом,

$$x - z \in \operatorname{Ker}\psi_1 \cap \operatorname{Ker}\psi_2 \cap \operatorname{Ker}\psi_3.$$

Как известно (см. следствие 3.12),

$$\operatorname{Ker}\psi_1 \cap \operatorname{Ker}\psi_2 \cap \operatorname{Ker}\psi_3 = \{0\}.$$

Таким образом, $x = z$. □

Заметим, что более удобно выбрать t_i по формулам (4.7) и (4.8), поскольку выражения для t_i в терминах P_i, Q_j не зависят от a.

Следствие 4.6. *Имеют место следующие соотношения*:

$$t_1 t_2 = t_2 t_3 = t_3 t_1 = 0. \tag{4.9}$$

Более того, элементы t_1t_2, t_2t_3, t_3t_1 порождают ядро естественного морфизма $\mathbb{C}[t_1, t_2, t_3] \to \mathcal{Z}(\mathcal{C})$.

Доказательство. Докажем, что $t_1 t_2 = 0$. Ясно, что $\psi_i(t_1t_2) = 0$, $i = 1, 2, 3$. Таким образом, $t_1t_2 = 0$. Аналогично, $t_it_j = 0$ для $i \neq j$.

Далее, рассмотрим некоторый $h(t_1, t_2, t_3) = 0$. Поскольку $t_it_j = 0$ для $i \neq j$, можем записать h как сумму $h_1(t_1) + h_2(t_2) + h_3(t_3)$, где $h_i \in \mathbb{C}[x]$. Используя морфизмы ψ_i, получаем $h_i = 0$. □

Как известно, на $\mathcal{Z}(\mathcal{C})$ группа S_3 действует перестановками t_i. Вычисляя

$$\operatorname{Spec}\mathcal{Z}(\mathcal{C}) = \operatorname{Hom}_{\text{alg}}(\mathcal{Z}(\mathcal{C}), \mathbb{C}),$$

мы получаем следующее утверждение.

Следствие 4.7. *Аффинное многообразие* $\operatorname{Spec}\mathcal{Z}(\mathcal{C})$ *представляет собой совокупность трех прямых в трехмерном пространстве, проходящих через одну точку. Группа* S_3 *действует на* $\operatorname{Spec}\mathcal{Z}(\mathcal{C})$ *перестановками прямых.*

Сделаем замечание о приложении центра $\mathcal{Z}(\mathcal{C})$ к квантовой механике. Как известно, можно рассмотреть квантовомеханическую систему, соответствующую алгебре $\mathcal{C}$. В этом случае элементы центра $\mathcal{Z}(\mathcal{C})$ играют роль законов сохранения энергии системы. Это означает, что если разложить рассматриваемую квантовомеханическую систему в прямую сумму конечномерных неприводимых подсистем, то элементы $\mathcal{Z}(\mathcal{C})$ будут постоянны на неприводимых подсистемах. Обратно, характеры $\mathcal{Z}(\mathcal{C})$ дают разложение квантовомеханической системы в прямую сумму неприводимых подсистем.

Далее, рассмотрим геометрическую интерпретацию подалгебр S_a при различных $a \in \mathbb{C}^*$ и центра $\mathcal{Z}(\mathcal{C})$. Зафиксируем $a \in \mathbb{C}^*$ и рассмотрим естественный морфизм аффинных многообразий

$$p_a : \operatorname{Spec} S_a \to \operatorname{Spec}\mathcal{Z}(\mathcal{C}).$$

Поскольку $\mathcal{Z}(\mathcal{C}) \to S_a$ — вложение, то морфизм p_a доминантный. Обозначим через L_i, $i = 1, 2, 3$, компоненты $\operatorname{Spec} S_a$, определяемые уравнениями $s_1 = 0$, $s_2 = 0$, $s_1+s_2+(a-1) = 0$ соответственно. Напомним, имеется действие S_3 на аффинном многообразии $\operatorname{Spec} S_a$. Рассмотрим инволюции τ_i, $i = 1, 2, 3$, группы S_3, определенные формулами

$$\begin{aligned}
&\tau_1 :\ s_1 \mapsto s_1,\ s_2 \mapsto -(a-1) - s_1 - s_2,\\
&\tau_2 :\ s_1 \mapsto -(a-1) - s_1 - s_2,\ s_2 \mapsto s_2,\\
&\tau_3 :\ s_1 \leftrightarrow s_2.
\end{aligned}$$

Ясно, что $\tau_i(L_i) = L_i$, $i = 1, 2, 3$. Обозначим через l_i компоненты $\operatorname{Spec}\mathcal{Z}(\mathcal{C})$, определяемые уравнениями $t_1 = 0$, $t_2 = 0$ и $t_3 = 0$.

Предложение 4.8. *Зафиксируем* $a \in \mathbb{C}^*$. *Выполнены следующие утверждения.*

(i) $p_a(L_i) = l_i$ *и ограничение* p_a *на* L_i *имеет степень* 2.
(ii) $p_a|_{L_i} \circ \tau_i = p_a$ *и* $L_i/\tau_i \cong l_i$.
(iii) *Рассмотрим такие точки* $x_i \in L_i$, *что* $\tau_i(x_i) = x_i$. *Тогда*

$$x_1 = \left(0,\ -\frac{a-1}{2}\right), \quad x_2 = \left(-\frac{a-1}{2},\ 0\right), \quad x_3 = (0,0).$$

Таким образом, дивизоры ветвления ограничения p_a *на* L_i, $i = 1, 2, 3$, *состоят соответственно из точек*

$$\left(-\frac{(a-1)^2}{4a},\ 0,\ 0\right), \quad \left(0,\ -\frac{(a-1)^2}{4a},\ 0\right), \quad \left(0,\ 0,\ -\frac{(a-1)^2}{4a}\right),$$

лежащих в $\operatorname{Spec}\mathcal{Z}(\mathcal{C})$.
(iv) $p^{-1}(0,0,0) = \{(0,0), (0,1-a), (1-a,0)\}$.

Доказательство. Рассмотрим случай L_1. Точки L_1 имеют координаты $(0, x)$ в координатах s_1, s_2. Ограничение p_a на L_1 задается следующим образом:

$$(0,x) \mapsto \frac{x^2 + ax}{a}.$$

Непосредственная проверка и действие группы S_3 доказывает предположение. □

Следствие 4.9. (i) *Если* $a = 1$ *то дивизор ветвления* $-(0,0,0)$.
(ii) *Если* $a = 1$, *то морфизм* p_a *дает изоморфизм между* $\operatorname{Spec} S_a/\mathbb{Z}_2$ *и* $\operatorname{Spec}\mathcal{Z}(\mathcal{C})$, *где инволюция действует по формуле* $x \mapsto -x$.
(iii) *Если* $a = -1$, *то дивизор ветвления есть набор* $\{(1,0,0), (0,1,0), (0,0,1)\}$.

4.3. Свойства $\mathcal{C}$-модулей. Опишем свойства конечномерных $\mathcal{C}$-модулей, в частности, дадим описание неприводимых $\mathcal{C}$-модулей. Во-первых, рассмотрим множество так называемых характеров, т.е. одномерных $\mathcal{C}$-модулей. Напомним, что мы вычислили его в разделе 3.1.

Зафиксируем $a \in \mathbb{C}^*$. Как известно (см. раздел 2), любой элемент $x \in \mathcal{C}$ может быть выражен следующим образом:

$$x = s + Q_1 s' + Q_2 s'', \quad s, s', s'' \in S_a. \tag{4.10}$$

Рассмотрим алгебру $\mathcal{C}$ как алгебру с генераторами s_i, $i = 1, 2$, и Q_i, $i = 1, 2$. По аналогии с разделом 2 имеем следующие формулы для P_i:

$$P_1 = s_1 + aQ_2, \quad P_2 = s_2 + aQ_1.$$

Используя ортогональность P_i, получаем следующие формулы:

$$(s_1 + aQ_2)(s_2 + aQ_1) = 0, \quad (s_2 + aQ_1)(s_1 + aQ_2) = 0.$$

Таким образом, получаем следующее соотношение:

$$s_1 s_2 + aQ_2 s_2 + a s_1 Q_1 = 0, \quad s_2 s_1 + aQ_1 s_1 + a s_2 Q_2 = 0. \tag{4.11}$$

При помощи формул

$$(s_1 + aQ_2)^2 = s_1 + aQ_2, \quad (s_2 + aQ_1)^2 = s_2 + aQ_1,$$

получаем соотношения

$$a(Q_1 s_2 + s_2 Q_1) = s_2 - s_2^2 + (a - a^2)Q_1, \quad a(Q_2 s_1 + s_1 Q_2) = s_1 - s_1^2 + (a - a^2)Q_2. \tag{4.12}$$

Таким образом, мы можем рассматривать алгебру $\mathcal{C}$ как алгебру с единицей и порождающими Q_1, Q_2, s_1, s_2, удовлетворяющую соотношениям

$$Q_i^2 = Q_i,\ i = 1, 2, \qquad Q_i Q_j = 0,\ i \neq j, \qquad s_1 s_2 = s_2 s_1$$

и соотношениям (4.2), (4.11) и (4.12).

Умножая элемент $aQ_2 s_2$ на $(s_1 + (a - 1))$ слева, из соотношения (4.11) получим

$$(s_1 + (a-1))aQ_2 s_2 = -(s_1 + (a-1))a s_1 Q_1 - (s_1 + (a-1))s_1 s_2.$$

Напомним, что элемент $(s_1 + (a - 1))s_1$ — центральный. Используя соотношение (4.12), получаем

$$\begin{aligned} a s_1 Q_2 s_2 + (a-1)aQ_2 s_2 &= -aQ_2 s_1 s_2 + (s_1 - s_1^2)s_2 + (a - a^2)Q_2 s_2 + (a-1)aQ_2 s_2 \\ &= -aQ_1(s_1 + (a-1))s_1 - (s_1 + (a-1))s_1 s_2. \end{aligned}$$

Окончательно имеем

$$s_1 s_2 - Q_2 s_1 s_2 + Q_1(s_1 + (a-1))s_1 = 0. \tag{4.13}$$

Из симметрии имеем

$$(Q_1 s_1 - Q_2 s_2)((a-1) + s_1 + s_2) = 0 \tag{4.14}$$

и

$$-s_1 s_2 + Q_1 s_1 s_2 - Q_2 s_2((a-1) + s_2) = 0. \tag{4.15}$$

Полученные соотношения будем применять для изучения $\mathcal{C}$-модулей.

Введем понятие сингулярного характера. Будем говорить, что характер χ — *сингулярный*, если $\chi \in \{(0,0), (1-a, 0), (0, 1-a)\}$, т.е. отвечает сингулярным точкам многообразия $\operatorname{Spec} S_a$.

Предложение 4.10. *Зафиксируем $a \neq \pm 1$. Рассмотрим характер $\chi \in \operatorname{Spec} S_a$. Обозначим через $\mathbb{C}^\chi$ одномерный S_a-модуль, соответствующий χ. Справедливы следующие утверждения*:

(i) *если χ не сингулярный, то*

$$\dim_{\mathbb{C}} \mathcal{C} \otimes_{S_a} \mathbb{C}^\chi = 2;$$

(ii) *если χ сингулярный, то*

$$\dim_{\mathbb{C}} \mathcal{C} \otimes_{S_a} \mathbb{C}^\chi = 3.$$

Доказательство. Пусть v — такой вектор, что $s_i v = \chi(s_i)v$. Хорошо известно, что порождающими $\mathcal{C}$-модуль $\mathcal{C} \otimes_{S_a} \mathbb{C}^\chi$ как векторное пространство над $\mathbb{C}$ являются векторы $1 \otimes v$, $Q_1 \otimes v$ и $Q_2 \otimes v$ (они могут быть линейно зависимыми). Умножая тензорно соотношение (4.13) на v, мы получаем следующее соотношение:

$$s_2 s_1 \otimes v - Q_1 s_1 s_2 \otimes v + Q_2((a-1)+s_1)s_1 \otimes v \\ = \chi(s_1 s_2) \cdot 1 \otimes v - \chi(s_1 s_2) \cdot Q_1 \otimes v + ((a-1)+\chi(s_1))\chi(s_1) \cdot Q_2 \otimes v = 0.$$

Это выражение тривиально тогда и только тогда, когда

$$\chi(s_1)\chi(s_2) = 0, \quad \chi(s_1)(\chi(s_1) + (a-1)) = 0,$$

т.е. χ соответствует прямой $s_1 = 0$ и точке $s_1 = -(a-1)$, $s_2 = 0$.

Применяя группу симметрий, мы видим, что (4.13), (4.14) и (4.15) будут тривиальными линейными комбинациями тогда и только тогда, когда $\chi \in \{(0,0), (1-a,0), (0,1-a)\}$. □

Рассмотрим $\mathcal{C}$-модуль W. Обозначим через $\mathrm{Char}(W)$ множество таких характеров $\chi \in \operatorname{Spec} S_a$, что существует вложение $\mathbb{C}^\chi \to W$ как S_a-модулей.

Напомним, что существует три инволюции τ_i, $i = 1, 2, 3$, действующие на $L_i \subset \operatorname{Spec} S_a$.

Предложение 4.11. *Рассмотрим $\mathcal{C}$-модуль W. Предположим, что $\chi \in \mathrm{Char}(W)$, $\chi \in L_i$ и χ — не сингулярный. Тогда $\tau_i(\chi) \in \mathrm{Char}(W)$.*

Доказательство. Предположим, что $\chi \in L_1$. Тогда

$$\chi(s_1) = 0, \quad \chi(s_2) = x, \quad s_2 1 \otimes v = \chi(s_2) 1 \otimes v.$$

Используя соотношение (4.14), получим, что $Q_2 \otimes v = 0$. Вычислим $s_2 Q_1 \otimes v$. Пользуясь соотношением (4.12), находим

$$s_2 Q_1 \otimes v + x Q_1 \otimes v = \frac{x - x^2}{a} 1 \otimes v + (1-a) Q_1 \otimes v.$$

Таким образом,

$$s_2 Q_1 \otimes v = (-(a-1) - x) Q_1 \otimes v + \frac{x - x^2}{a} 1 \otimes v.$$

Аналогично,

$$s_1 Q_1 \otimes v = 0.$$

Следовательно, оператор s_2, действующий на двумерное пространство, порожденное $1 \otimes v$ и $Q_1 \otimes v$, имеет два собственных вектора x и $-(a-1) - x = \tau_1((0,x))$. Аналогично доказывается остальное. □

Следствие 4.12. *Если $a = 1$, то характер сингулярен тогда и только тогда, когда $\chi = (0,0)$. Таким образом, справедливы следующие утверждения*:

(i) *если $\chi = (0,0)$, то*
$$\dim_{\mathbb{C}} \mathcal{C} \otimes_{S_a} \mathbb{C}^\chi = 3;$$

(ii) *если $\chi \neq (0,0)$, то*
$$\dim_{\mathbb{C}} \mathcal{C} \otimes_{S_a} \mathbb{C}^\chi = 2.$$

Далее мы классифицируем неприводимые $\mathcal{C}$-модули.

Предложение 4.13. *Рассмотрим неприводимый $\mathcal{C}$-модуль W.*

(i) *Предположим, что характер $\chi \in L_i \subset \operatorname{Spec} S_a$ не сингулярен, $\tau_i(\chi) \neq \chi$ и $\chi \in \mathrm{Char}(W)$. Имеется следующий изоморфизм $\mathcal{C}$-модулей:*
$$W \cong \mathcal{C} \otimes_{S_a} \mathbb{C}^\chi \cong \mathcal{C} \otimes_{S_a} \mathbb{C}^{\tau_i(\chi)}. \tag{4.16}$$

(ii) *Если $a \neq \pm 1$ и характер χ сингулярен, то $\mathcal{C} \otimes_{S_a} \mathbb{C}^\chi$ является нетривиальным расширением одномерных $\mathcal{C}$-модулей.*

(iii) *Если*

$$a \neq \pm 1, \quad \chi \in L_i \subset \operatorname{Spec} S_a, \quad \tau_i(\chi) = \chi,$$

то $\mathcal{C} \otimes_{S_a} \mathbb{C}^\chi$ *— неприводимый* $\mathcal{C}$*-модуль. Если*

$$a = -1, \quad \chi \in L_i \subset \operatorname{Spec} S_a, \quad \tau_i(\chi) = \chi,$$

то $\mathcal{C} \otimes_{S_a} \mathbb{C}^\chi$ *— сумма одномерных* $\mathcal{C}$*-модулей. Если*

$$a = 1, \quad \chi \in L_i \subset \operatorname{Spec} S_a, \quad \tau_i(\chi) = \chi,$$

то характер χ *сингулярен и* $\chi = (0, 0)$.

Доказательство. Если характер $\chi \in L_i$ не сингулярен и $\tau_i(\chi) \neq \chi$, то

$$\operatorname{Char}(W) = \{\chi,\ \tau_i(\chi)\}, \quad \dim_{\mathbb{C}} W \geqslant 2.$$

Кроме того, $\mathcal{C} \otimes_{S_a} \mathbb{C}^\chi$ имеет размерность 2, и мы имеем нетривиальный морфизм $\mathcal{C} \otimes_{S_a} \mathbb{C}^\chi \to W$. Так как W неприводим, получаем, что $W \cong \mathcal{C} \otimes_{S_a} \mathbb{C}^\chi$. Первое утверждение доказано.

Рассмотрим $\chi = (0, 0) \in \operatorname{Spec} S_a$. В этом случае

$$s_1 1 \otimes v = 0, \quad s_1 Q_1 \otimes v = 0, \quad s_1 Q_2 \otimes v = (1 - a) Q_2 \otimes v$$

для s_1;

$$s_2 1 \otimes v = 0, \quad s_2 Q_1 \otimes v = (1 - a) Q_1 \otimes v, \quad s_2 Q_2 \otimes v = 0$$

для элемента s_2. Ясно, что

$$Q_i 1 \otimes v = Q_i \otimes v, \quad Q_i Q_j \otimes v = \delta_{ij} Q_j \otimes v, \quad i, j = 1, 2.$$

Несложно проверить, что существуют двумерные подмодули W_0 модуля $\mathcal{C} \otimes_{S_a} \mathbb{C}^\chi$, порожденные образами Q_i, s_i, $i = 1, 2$, однако нет другого такого одномерного подмодуля W_1 модуля $\mathcal{C} \otimes_{S_a} \mathbb{C}^\chi$, что $W_0 \oplus W_1 = \mathcal{C} \otimes_{S_a} \mathbb{C}^\chi$.

Рассуждая аналогично и используя непосредственные вычисления, можно доказать остальное. □

Следствие 4.14. *Имеется следующий список неприводимых* $\mathcal{C}$*-модулей*:

(i) 9 *одномерных модулей из предложения* 3.1;

(ii) $\mathcal{C} \otimes_{S_a} \mathbb{C}^\chi$*, если характер* χ *не сингулярен. Заметим, что если* $\chi \in L_i \subset \operatorname{Spec} S_a$*, то*

$$\mathcal{C} \otimes_{S_a} \mathbb{C}^\chi \cong \mathcal{C} \otimes_{S_a} \mathbb{C}^{\tau_i(\chi)}.$$

Это означает, что двумерные неприводимые $\mathcal{C}$*-модули, соответствующие* L_i*, параметризуются кривыми* $l_i = L_i/\tau_i$.

Рассмотрим алгебру $\mathcal{C}$. Напомним, что имеют место морфизмы $\psi_i : \mathcal{C} \to \mathcal{C}_i$ (см. п. 3.4). Очевидно, можно рассматривать неприводимые $\mathcal{C}$-модули как неприводимые $\mathcal{C}_i$-модули, применяя ψ_i.

Следствие 4.15. *Для любого неприводимого* $\mathcal{C}$*-модуля* V *существует такое* i*, что* V *может быть получен из* $\mathcal{C}_i$*-модуля* V_i *применением* ψ_i.

4.4. Алгебры $\mathcal{C}_\vartheta, \vartheta \in \operatorname{Spec} \mathcal{Z}(\mathcal{C})$. Изучим фактор алгебры $\mathcal{C}$ по идеалу, порожденному соотношением $z - \vartheta(z) \cdot 1$, $z \in \mathcal{Z}(\mathcal{C})$, для фиксированного характера $\vartheta \in \operatorname{Spec} \mathcal{Z}(\mathcal{C})$.

Можно рассматривать алгебру $\mathcal{C}$ как алгебру над ее центром $\mathcal{Z}(\mathcal{C})$. Обозначим через $\operatorname{Irr}(\mathcal{C})$ множество неприводимых $\mathcal{C}$-модулей и рассмотрим отображение: $p : \operatorname{Irr}(\mathcal{C}) \to \operatorname{Spec} \mathcal{Z}(\mathcal{C})$, определенное следующим образом. Зафиксируем неприводимый $\mathcal{C}$-модуль V, который можно рассматривать как $\mathcal{Z}(\mathcal{C})$-модуль. По лемме Шура, модуль V, рассматриваемый как $\mathcal{Z}(\mathcal{C})$-модуль, есть прямая сумма $\dim_{\mathbb{C}} V$ копий $\mathbb{C}^\vartheta$ для некоторого характера $\vartheta \in \operatorname{Spec} \mathcal{Z}(\mathcal{C})$. Отображение p определено правилом $V \mapsto \vartheta$.

Зафиксируем характер $\vartheta \in \operatorname{Spec} \mathcal{Z}(\mathcal{C})$. Рассмотрим алгебру $\mathbb{C}_\vartheta$ — фактор алгебры $\mathcal{C}$ по идеалу, порожденному соотношением $z - \vartheta(z) \cdot 1$, $z \in \mathcal{Z}(\mathcal{C})$. Неприводимые $\mathcal{C}$-модули, соответствующие ϑ, являются неприводимыми $\mathcal{C}_\vartheta$-модулями. Поскольку $\mathcal{Z}(\mathcal{C})$ — подалгебра $\mathcal{C}$, заключаем, что $\mathcal{C}$ является $\mathcal{Z}(\mathcal{C})$-модулем. Ясно, что $\mathcal{C}_\vartheta$ как векторное пространство изоморфно $\mathcal{C} \otimes_{\mathcal{Z}(\mathcal{C})} \mathbb{C}^\vartheta$.

Предложение 4.16. *Зафиксируем характер $\vartheta \in \operatorname{Spec} \mathcal{Z}(\mathcal{C})$. Выполнены следующие соотношения для размерностей*:

(i) *если* $\vartheta = (0,0,0)$, *то* $\dim_{\mathbb{C}} \mathcal{C}_\vartheta = 9$;
(ii) *если* $\vartheta \neq (0,0,0)$, *то* $\dim_{\mathbb{C}} \mathcal{C}_\vartheta = 4$.

Доказательство. Напомним, что слой морфизма p_a над $(0,0,0)$ состоит из трех сингулярных характеров. Тогда получаем, что S_a-модуль $S_a \otimes_{\mathcal{Z}(\mathcal{C})} \mathbb{C}^\vartheta$ для $\vartheta = (0,0,0)$ имеет размерность 3 и изоморфен прямой сумме $\bigoplus \mathcal{C}^\chi$, где суммирование ведется по сингулярным характерам S_a. Действительно, в этом случае, имеем изоморфизм

$$\mathcal{C} \otimes_{S_a} S_a \otimes_{\mathcal{Z}(\mathcal{C})} \mathbb{C}^\vartheta = \bigoplus \mathcal{C} \otimes_{S_a} \mathbb{C}^\chi \tag{4.17}$$

где суммирование ведется по сингулярным характерам S_a. Используя предложение 4.10, получим, что

$$\dim_{\mathbb{C}} \mathcal{C} \otimes_{S_a} \mathbb{C}^\chi = 3$$

и, таким образом,

$$\mathcal{C} \otimes_{\mathcal{Z}(\mathcal{C})} \mathbb{C}^\vartheta = 9.$$

Предположим, что $\vartheta \in l_i \subset \operatorname{Spec} \mathcal{Z}(\mathcal{C})$ не является дивизором ветвления p_a и $\vartheta \neq (0,0,0)$. В этом случае можно показать, что S_a-модуль $S_a \otimes_{\mathcal{Z}(\mathcal{C})} \mathbb{C}^\vartheta$ изоморфен прямой сумме $\mathbb{C}^\chi \oplus \mathbb{C}^{\tau_i(\chi)}$, где суммирование ведется по сингулярным характерам $\chi \in L_i$ и $p_a(\chi) = \vartheta$. Таким образом, получаем, что

$$\mathcal{C} \otimes_{\mathcal{Z}(\mathcal{C})} \mathbb{C}^\vartheta = \mathcal{C} \otimes_{S_a} \mathbb{C}^\chi \bigoplus \mathcal{C} \otimes_{S_a} \mathbb{C}^{\tau_i(\chi)}.$$

Используя предложение 4.10, получаем, что

$$\dim_{\mathbb{C}} \mathcal{C} \otimes_{\mathcal{Z}(\mathcal{C})} \mathbb{C}^\vartheta = 4.$$

Пусть ϑ принадлежит дивизору ветвления p_a. Выберем a' так, что ϑ не принадлежит дивизору ветвления $p_{a'}$, и применим рассуждения предыдущего пункта. □

Докажем следующую структурную теорему для алгебры $\mathcal{C}_\vartheta$ для различных $\vartheta \in \operatorname{Spec} \mathcal{Z}(\mathcal{C})$.

Теорема 4.17. *Рассмотрим алгебру $\mathcal{C}_\vartheta$. Справедливы следующие утверждения*:

(i) *если* $\vartheta \notin \{(0,0,0),(-1,0,0),(0,-1,0),(0,0,-1)\}$, *то* $\mathcal{C}_\vartheta \cong \operatorname{Mat}_2(\mathbb{C})$;
(ii) *если* $\vartheta \in \{(-1,0,0),(0,-1,0),(0,0,-1)\}$, *то алгебра $\mathcal{C}_\vartheta$ имеет двумерный радикал J*;
(iii) *если* $\vartheta = (0,0,0)$, *то алгебра $\mathcal{C}_\vartheta$ имеет шестимерный радикал.*

Доказательство. Пусть $\vartheta = (0,0,x)$, $x \neq 0$. В этом случае алгебра $\mathcal{C}_\vartheta$ — это фактор $\mathcal{C}$ по идеалу, порожденному соотношением $t_3 = 1$. Перепишем это соотношение в виде $s_1 s_2 - ax \cdot 1$. Можно показать, что алгебра $\mathcal{C}_\vartheta$ имеет базис 1, s_1, Q_1, $Q_1 s_1$ и соотношениями

$$s_1^2 + (a-1)s_1 + ax = 0, \quad s_1 Q_1 + Q_1 s_1 - s_1 + (1-a)Q_1 + x + 1 - a = 0.$$

Ясно, что в $\mathcal{C}_\vartheta$ существует двумерная коммутативная подалгебра $\mathcal{S}$, порожденная s_1. Зафиксируем характер λ в $\mathcal{S}$. Ясно, что

$$\lambda(s_1)^2 + (a-1)\lambda(s_1) + x = 0.$$

Обозначим через v генератор в одномерном $\mathcal{S}$-модуле $\mathbb{C}^\lambda$, соответствующий характеру λ. Рассмотрим $\mathcal{C}_\vartheta$-модуль $\mathcal{C}_\vartheta \otimes_{\mathcal{S}} \mathbb{C}^\lambda$. Это двумерный модуль имеет базис $1 \otimes v$, $Q_1 \otimes v$. Таким образом, имеем гомоморфизм $\mathcal{C}_\vartheta \to \operatorname{Mat}_2(\mathbb{C})$, определенный формулой

$$s_1 \mapsto \begin{pmatrix} \lambda(s_1) & \lambda(s_1) - x - 1 + a \\ 0 & -\lambda(s_1) + 1 - a \end{pmatrix}, \quad Q_1 \mapsto \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}. \tag{4.18}$$

Докажем, что если $x \neq -1$, то этот гомоморфизм является изоморфизмом. Достаточно показать, что $\mathcal{C}_\vartheta$-модуль $\mathcal{C}_\vartheta \otimes_{\mathcal{S}} \mathbb{C}^\lambda$ неприводим. Пусть существует нетривиальное $\mathcal{C}_\vartheta$-инвариантное подпространство $\mathcal{C}_\vartheta \otimes_{\mathcal{S}} \mathbb{C}^\lambda$. Ясно, что это подпространство является ядром матрицы, соответствующей Q_1 или образу этой матрицы. Непосредственное вычисление показывает, что это подпространство существует тогда и только тогда, когда $x = -1$.

Пусть $x = -1$. Рассмотрим элемент $f = a + s_1 - (a+1)Q_1$. Можно проверить, что $h^2 = 0$. Рассмотрим двусторонний идеал J алгебры $\mathcal{C}_\vartheta$, порожденный f. Непосредственное вычисление показывает, что идеал состоит из двух элементов f и $(s_1 - 1)Q_1$. Легко показать, что $J^2 = 0$. Это означает, что J — радикал $\mathcal{C}_\vartheta$, так что $\mathcal{C}_\vartheta/J \cong \mathbb{C} \oplus \mathbb{C}$. Учитывая симметрию, получаем первое и второе утверждения.

Пусть $\vartheta = (0,0,0)$ и $a \neq 1$. В этом случае алгебра $\mathcal{C}_\vartheta$ девятимерная, ее базис состоит из элементов 1, s_1, s_2, Q_1, s_1Q_1, s_2Q_1, Q_2, s_1Q_2, s_2Q_2, а набор соотношений состоит из

$$s_1s_2 = 0, \quad s_1^2 + (a-1)s_1 = 0, \quad s_2^2 + (a-1)s_2 = 0,$$

а также (4.11) и (4.12). Можно переписать соотношения в виде

$$\begin{gathered} s_1Q_1 + Q_2s_2 = 0, \quad Q_1s_1 + s_2Q_2 = 0, \\ Q_1s_2 + s_2Q_1 = s_2 + (1-a)Q_1, \quad Q_2s_1 + s_1Q_2 = s_1 + (1-a)Q_2. \end{gathered}$$

Рассмотрим элементы

$$f_1 = s_1 + (a-1)Q_2, \quad f_2 = s_2 + (a-1)Q_1.$$

Обозначим через J' двусторонний идеал $\mathcal{C}_\vartheta$, порожденный f_1, f_2. Легко проверить, что

$$f_1^2 = f_2^2 = f_1f_2 = 0, \quad s_2f_1 = (a-1)s_2Q_2.$$

Используя соотношения, получаем

$$s_2Q_2s_2Q_2 = -s_2s_1Q_1Q_2 = 0.$$

Аналогично можно показать, что элементы s_1Q_1, $s_1(1-Q_2)$, $s_2(1-Q_1) \in J'$ являются нильпотентами, а J' — радикал $\mathcal{C}_\vartheta$ и $\mathcal{C}_\vartheta/J' = \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C}$.

В случае $a = 1$, обозначим через J' идеал, порожденный s_1, s_2. Непосредственное вычисление показывает, что J' — 6-мерный идеал и $\mathcal{C}_\vartheta/J' = \mathbb{C} \oplus \mathbb{C} \oplus \mathbb{C}$. □

Следствие 4.18. *Размерность любого неприводимого $\mathcal{C}$-модуля меньше 2. Двумерные неприводимые $\mathcal{C}$-модули параметризованы набором*

$$U = \operatorname{Spec} \mathcal{Z}(\mathcal{C}) \setminus \big\{(0,0,0),\ (-1,0,0),\ (0,-1,0),\ (0,0,-1)\big\}. \tag{4.19}$$

4.5. Представления $\mathcal{C}$, соответствующие представлениям алгебры $A_{7,7}$. Мы построили морфизм $\mathcal{C} \to A_{7,7}$ в разделе 3.1. Сейчас мы изучим ограничение нетривиального 7-мерного представления $A_{7,7}$ на $\mathcal{C}$.

Используя свойства фильтрации $\mathcal{C}$ и в $A_{7,7}$, получим следующее утверждение.

Предложение 4.19. *Морфизм i инъективен.*

Обозначим за θ 7-мерное $A_{7,7}$-представление. Используя соотношение $\operatorname{Tr} \pi_i\rho_j = 1/7$, получим следующие значения для характеров θ:

характер	dim	P_1	P_2	Q_1	Q_2	P_1Q_1	P_1Q_2	P_2Q_1	P_2Q_2
χ	7	2	2	2	2	$\frac{4}{7}$	$\frac{4}{7}$	$\frac{4}{7}$	$\frac{4}{7}$

Во-первых, вычислим следы элементов P_1, P_2, Q_1, Q_2, P_1Q_1, P_1Q_2, P_2Q_1, P_2Q_2 в различных неприводимых $\mathcal{C}$-модулях. Имеем 9 одномерных $\mathcal{C}$-модулей. Следующий список содержит одномерные модули:

характер	dim	P_1	P_2	Q_1	Q_2	P_1Q_1	P_1Q_2	P_2Q_1	P_2Q_2
χ_1	1	0	0	0	0	0	0	0	0
χ_2	1	1	0	0	0	0	0	0	0
χ_3	1	0	1	0	0	0	0	0	0
χ_4	1	0	0	1	0	0	0	0	0
χ_5	1	0	0	0	1	0	0	0	0
χ_6	1	1	0	1	0	1	0	0	0
χ_7	1	1	0	0	1	0	1	0	0
χ_8	1	0	1	1	0	0	0	1	0
χ_9	1	0	1	0	1	0	0	0	1

Во-вторых, рассмотрим двумерные неприводимые $\mathcal{C}$-модули. Как мы знаем, эти модули параметризованы $\operatorname{Spec}\mathcal{Z}(\mathcal{C})$, т.е. точками типа $(x,0,0)$, $(0,y,0)$, $(0,0,z)$, $x,y,z\neq 0,-1$. Получаем следующий список:

характер	dim	P_1	P_2	Q_1	Q_2	P_1Q_1	P_1Q_2	P_2Q_1	P_2Q_2
$\chi_{(x,0,0)}$	2	0	1	1	0	0	0	$x+1$	0
$\chi_{(0,y,0)}$	2	1	0	0	1	0	$y+1$	0	0
$\chi_{(0,0,z)}$	2	1	1	1	1	$-z$	$1+z$	$1+z$	$-z$

Действительно, рассмотрим представления $\mathcal{C}$, соответствующие точке $(0,0,z)$. В этом случае $t_3=z$. Таким образом, $t_3=-P_1Q_1-Q_2P_2=z\cdot 1$. Вычисляя следы, получим, что $-\operatorname{Tr}(P_1Q_1+Q_2P_2)=2z$. Далее, в этом представлении имеются тождества

$$P_2=1-P_1,\quad Q_2=1-Q_1.$$

Таким образом, $-2\operatorname{Tr}P_1Q_1=2z$ и потому $\operatorname{Tr}P_1Q_1=-z$.

Напомним понятие композиционных факторов Жордана—Гельдера и его свойства в теории представлений. Рассмотрим ассоциативную алгебру A. Говорят, что A-модуль V имеет *композиционные факторы Жордана—Гельдера* (коротко, композиционные факторы) $W_1,\dots,W_s$, если существует последовательность A-подмодулей следующего типа:

$$0=M_0\subset M_1\subset M_2\cdots\subset M_{s-1}\subset M_s=V \tag{4.20}$$

и факторы $W_i=M_i/M_{i-1}$, $i=1,\dots,s$, — неприводимые A-модули. Известно, что множество композиционных факторов в A-модуле единственно с точностью до перестановок. Обозначим через $\mathbf{gr}(V)$ прямую сумму $W_1\oplus\cdots\oplus W_s$ для A-модуля V с композиционными факторами $W_1,\dots,W_s$. Два n-мерных A-модуля V_1 и V_2 имеют одинаковые характеры тогда и только тогда, когда $\mathbf{gr}(V_1)\cong\mathbf{gr}(V_2)$.

Рассмотрим $\mathcal{C}$-модуль V, соответствующий θ, а найдем его композиционные факторы. Для этого требуется найти такие числа m_i, $i=1,\dots,9$, $n_1,n_2,n_3\in\mathbb{N}_0$, что

$$\chi=\sum_{i=1}^{9}m_i\chi_i+n_1\chi_{(x,0,0)}+n_2\chi_{(0,x,0)}+n_3\chi_{(0,0,x)}. \tag{4.21}$$

Для любого множества $m_1,\dots,m_9$, n_1,n_2,n_3, удовлетворяющего (4.21), получаем, что $\mathcal{C}$-модуль имеет m_i факторов, изоморфных одномерному $\mathcal{C}$-модулю χ_i, $i=1,\dots,9$, и n_i факторов, изоморфных двумерному $\mathcal{C}$-модулю.

Предложение 4.20. *$\mathcal{C}$-Модуль V имеет следующие композиционные факторы Жордана—Гельдера*:

(i) *одномерный фактор, соответствующий* χ_1;

(ii) *двумерный фактор, соответствующий* $(-6/7,\ 0,\ 0)$;
(iii) *двумерный фактор, соответствующий* $(0,\ -6/7,\ 0)$;
(iv) *двумерный фактор, соответствующий* $(0,\ 0,\ -4/7)$.

Утверждение доказывается непосредственным вычислением.

Рассмотрим $\mathcal{C}$-модуль V. Зафиксируем $a \in \mathbb{C}^*$. Докажем, что эти композиционные факторы образуют прямую сумму в V.

Предложение 4.21. *Обозначим через V_0, V_1, V_2, V_3 $\mathcal{C}$-модули, соответствующие композиционным факторам в V в предложении*
reffacjh. *Имеет место следующий изоморфизм*:

$$V \cong V_0 \oplus V_1 \oplus V_2 \oplus V_3. \tag{4.22}$$

Доказательство. Зафиксируем $a \in \mathbb{C}^*$ и рассмотрим $\mathcal{C}$-модуль V как S_a-модуль. Напомним, что $\mathrm{Char}(V)$ — это множество таких характеров $\lambda \in \operatorname{Spec} S_a$, что существует вложение S_a-модулей $\mathbb{C}^\lambda \to V$. В этом случае имеем следующее разложение V:

$$V = \bigoplus_{\lambda \in \mathrm{Char}(V)} \mathbb{C}^\lambda. \tag{4.23}$$

Можно доказать, что $\mathrm{Char}(V)$ состоит из 7 различных точек в $\operatorname{Spec} S_a$. Множество $\mathrm{Char}(V)$ делится на компоненты следующим образом:

$$\mathrm{Char}(V) = \lambda_0 \cup \big(\lambda_1, \tau_1(\lambda)\big) \cup \big(\lambda_2, \tau_2(\lambda_2)\big) \cup \big(\lambda_3, \tau_3(\lambda_3)\big),$$

где λ_0 — характер, соответствующий точке $(0,0) \in \operatorname{Spec} S_a$, τ_i — инволюции, действующие на компоненту $L_i \subset \operatorname{Spec} S_a$. $\mathcal{C}$-Модуль $\mathbb{C}^{\lambda_0}$ изоморфен V_0. Можно проверить, что $\mathcal{C}$-модуль $\mathcal{C} \otimes_{S_a} \mathbb{C}^{\lambda_i}$, $i = 1,2,3$, неприводим и изоморфен факторам V_i, $i = 1,2,3$, соответственно. Таким образом, имеем вложения $V_i = \mathcal{C} \otimes_{S_a} \mathbb{C}^{\lambda_i} \to V$ $\mathcal{C}$-модулей. Используя стандартные рассуждения, получаем

$$V = V_0 \oplus V_1 \oplus V_2 \oplus V_3. \tag{4.24}$$

Предложение доказано. □

5. Построение одномерного семейства взаимно несмещенных базисов в размерности 7

В этом разделе мы построим одномерное семейство ортогональных пар в $\mathfrak{sl}(7)$ и взаимно несмещенных базисов в 7-мерном эрмитовом пространстве с помощью представлений алгебры $\mathcal{C}$, редуцированных алгебр Темперли—Либа и других похожих на них алгебр. Это семейство было ранее построено Петреску (см. [11].

В этом разделе мы будем использовать различные типы многообразий представлений и модулей алгебр. Для фиксированной алгебры A обозначим через $\mathbf{Rep}_n A$ многообразие всех ее n-мерных представлений и через $\mathcal{M}_n A$ фактор этого многообразия по действию группы $\mathrm{GL}_n(\mathbb{C})$ сопряжениями соответственно.

5.1. Стратегия построения одномерного семейства пар в $\mathfrak{sl}(7)$. Опишем стратегию построения представлений $A_{7,7}$ по представлению алгебры $\mathcal{C}$, описанному в разделе 4.5. Введем несколько новых алгебр и последовательно будем строить представления $A_{7,7}$.

Сначала введем две изоморфные ассоциативные алгебры с единицей B_1 и B_2 следующим образом: порождающие алгебр — π_1, π_2, P_2, Q_1, ρ_3, ρ_4 и π_3, π_4, P_1, Q_2, ρ_1, ρ_2 соответственно; все порождающие в алгебрах B_i, $i = 1,2,$ — идемпотенты. Соотношения на порождающие в алгебре B_1:

$$\begin{gathered} \pi_1\pi_2 = \pi_2\pi_1 = 0, \qquad \pi_i P_2 = P_2\pi_i = 0,\ i = 1,2, \qquad \rho_3\rho_4 = \rho_4\rho_3 = 0, \\ \rho_k Q_1 = Q_1\rho_k = 0,\ k = 3,4, \qquad \big[\pi_1 + \pi_2,\ Q_1\big] = \big[P_2,\ \rho_3 + \rho_4\big], \end{gathered} \tag{5.1}$$

Соотношения в алгебре B_2 из соотношений в B_1 получаются заменой π_1, π_2, P_2, Q_1, ρ_3, ρ_4 на π_3, π_4, P_1, Q_2, ρ_1, ρ_2 соответственно.

Алгебра $B_{1/7}(\Gamma_{4,4})$ — редуцированная алгебра Темперли—Либа с порождающими π_i, ρ_i, $i = 1, \dots, 4$. Идеал $I_{4,4}$ порожден соотношением

$$\big[\pi_1 + \pi_2,\ \rho_1 + \rho_2\big] = \big[\pi_3 + \pi_4,\ \rho_3 + \rho_4\big]. \tag{5.2}$$

Далее, имеем следующую коммутативную диаграмму:

$$\begin{array}{ccc} \mathcal{C} & \xrightarrow{\quad j_1 \quad} & B_1 \\ \big\downarrow{\scriptstyle j_2} & & \big\downarrow{\scriptstyle \phi_1} \\ B_2 & \xrightarrow{\quad \phi_2 \quad} & B_{1/7}(\Gamma_{4,4})/I_{4,4}, \end{array} \tag{5.3}$$

морфизмы j_1, j_2, ϕ_1 определены по формулам

$$\begin{aligned} j_1 &: \ P_1 \mapsto \pi_1 + \pi_2, \quad Q_2 \mapsto \rho_3 + \rho_4, \quad P_2 \mapsto P_2, \quad Q_1 \mapsto Q_1, \\ j_2 &: \ P_2 \mapsto \pi_3 + \pi_4, \quad Q_1 \mapsto \rho_1 + \rho_2, \quad P_1 \mapsto P_1, \quad Q_2 \mapsto Q_2, \\ \phi_1 &: \ \pi_i \mapsto \pi_i, \quad \rho_j \mapsto \rho_j, \quad P_2 \mapsto \pi_3 + \pi_4, \quad Q_1 \mapsto \rho_1 + \rho_2; \end{aligned}$$

морфизм ϕ_2 определен аналогично.

Рассмотрим редуцированные алгебры Темперли—Либа $B_{1/7}(\Gamma_{4,7})$ и $B_{1/7}(\Gamma_{7,4})$ с порождающими π_i, $i = 1, \dots, 7$, ρ_j, $j = 1, \dots, 4$, и π_i, $i = 1, \dots, 4$, ρ_j, $j = 1, \dots, 7$. Далее, введем алгебры $B_{4,7}$ и $B_{7,4}$ как факторы алгебр Темперли—Либа $B_{1/7}(\Gamma_{4,7})$ и $B_{1/7}(\Gamma_{7,4})$ по соотношениям

$$\sum_{i=1}^{7} \pi_i - 1, \quad \sum_{j=1}^{7} \rho_j - 1,$$

соответственно. Рассмотрим идеалы $I_{4,7}$ и $I_{7,4}$ алгебр $B_{4,7}$ и $B_{7,4}$, порожденные соотношением (5.2). Также введем идеал $I_{7,7}$ алгебры $B_{7,7}$, порожденный соотношением (5.2). Обозначим для краткости факторалгебры $B_{1/7}(\Gamma_{4,4})/I_{4,4}$, $B_{4,7}/I_{4,4}$ и $B_{7,4}/I_{7,4}$ через $A_{4,4}$, $A_{4,7}$ и $A_{7,4}$ соответственно. Имеем следующую коммутативную диаграмму:

$$\begin{array}{ccc} A_{4,4} & \xrightarrow{\quad \psi_1 \quad} & A_{4,7} \\ \big\downarrow{\scriptstyle \psi_2} & & \big\downarrow{\scriptstyle \mu_1} \\ A_{7,4} & \xrightarrow{\quad \mu_2 \quad} & A_{7,7}, \end{array} \tag{5.4}$$

где морфизмы ψ_i, μ_i, $i = 1, 2$, определены естественным образом: переводят π_i и ρ_j из одной алгебры в π_i и ρ_j другой алгебры.

Напомним основные определения многообразий представлений и модулей фиксированной размерности конечнопорожденной ассоциативной алгебры A. Обозначим через $\mathbf{Rep}_n A$ аффинное многообразие $\mathrm{Hom}_{\mathrm{alg}}(A, \mathrm{Mat}_n(\mathbb{C}))$. Заметим, что на $\mathrm{Mat}_n(\mathbb{C})$ действует сопряжениями группа $\mathrm{GL}_n(\mathbb{C})$. Следовательно, группа $\mathrm{GL}_n(\mathbb{C})$ действует на $\mathbf{Rep}_n A$. Так как группа $\mathrm{GL}_n(\mathbb{C})$ редуктивна, то категорный фактор $\mathbf{Rep}_n A$ по действию $\mathrm{GL}_n(\mathbb{C})$ является аффинным многообразием. Этот категорный фактор будем обозначать $\mathcal{M}_n A$. Далее, поскольку имеется гомоморфизм алгебр $\zeta : A \to B$, то естественным образом определен морфизм многообразий $\zeta^* : \mathbf{Rep}_n B \to \mathbf{Rep}_n A$. Если морфизм ζ сюръективен, то $zeta^*$ — вложение. Например, естественному гомоморфизму $B_{7,7} \to A_{7,7}$ соответствует вложение многообразий $\mathbf{Rep}_7 A_{7,7} \to \mathbf{Rep}_7 B_{7,7}$.

Рассмотрим многообразия представлений алгебр, входящих в коммутативные диаграммы (5.3), (5.4). Будем рассматривать представления B_i, где π_i, ρ_j — проекторы ранга 1, а P_k, Q_l — ранга 2. В случае алгебр $A_{4,4}$, $A_{4,7}$, $A_{7,4}$ и $A_{7,7}$ порождающие являются проекторами ранга 1. В случае алгебры $\mathcal{C}$ мы в разделе 4.5 рассматривали представления, когда P_i, Q_j — проекторы ранга 2. Будем обозначать рассматриваемые многообразия представлений символом $\mathbf{Rep}_7$ с указанием соответствующей алгебры. Аналогично, многообразия $\mathcal{M}_7$ для соответствующих алгебр являются факторами указанных многообразий $\mathbf{Rep}_7$.

Соответственно, получаем следующие коммутативные диаграммы многообразий представлений:

$$\begin{array}{ccc} \mathbf{Rep}_7\,\mathcal{C} & \xleftarrow{\;j_1^*\;} & \mathbf{Rep}_7\,B_1 \\ {\scriptstyle j_2^*}\uparrow & & \uparrow{\scriptstyle \phi_1^*} \\ \mathbf{Rep}_7\,B_2 & \xleftarrow{\;\phi_2^*\;} & \mathbf{Rep}_7\,A_{4,4} \end{array} \quad \text{and} \quad \begin{array}{ccc} \mathbf{Rep}_7\,A_{4,4} & \xleftarrow{\;\psi_1^*\;} & \mathbf{Rep}_7\,A_{4,7} \\ {\scriptstyle \psi_2^*}\uparrow & & \uparrow{\scriptstyle \mu_1^*} \\ \mathbf{Rep}_7\,A_{7,4} & \xleftarrow{\;\mu_2^*\;} & \mathbf{Rep}_7\,A_{7,7}. \end{array} \tag{5.5}$$

Напомним, что в п. 4.5 мы классифицировали представления алгебры $\mathcal{C}$, соответствующие ортогональным парам в $\mathfrak{sl}(7)$. Такие представления образуют в $\mathbf{Rep}_7\,\mathcal{C}$ одну $\mathrm{GL}_7(\mathbb{C})$-орбиту. С помощью этих коммутативных диаграмм будем изучать слои отображения $\mathbf{Rep}_7\,A_{7,7} \to \mathbf{Rep}_7\,\mathcal{C}$. Многообразие $\mathbf{Rep}_7\,A_{7,7}$ является подмногообразием $\mathbf{Rep}_7\,B_{7,7}$. Таким образом, получаем многообразие представлений $B_{7,7}$, удовлетворяющих соотношению (5.2). Изучая слои в коммутативных диаграммах (5.5), мы получим семейства Петреску обобщенно-адамаровых и комплексно-адамаровых матриц размера 7.

5.2. Алгебры B_1 и B_2. Рассмотрим многообразия $\mathbf{Rep}_7\,B_i$, $i = 1, 2$, вместе с отображениями $\mathbf{Rep}_7\,B_i \to \mathbf{Rep}_7\,\mathcal{C}$, $i = 1, 2$.

Отметим, что морфизмы $j_i : \mathcal{C} \to B_i$, $i = 1, 2$, являются мономорфизмами. Действительно, рассмотрим морфизм j_1. Факторизуя алгебру B_1 по идеалу, порожденному элементами π_1, ρ_3, получим алгебру, изоморфную $\mathcal{C}$. Этот изоморфизм является сечением j_1. Для j_2 ситуация аналогична.

Напомним, что разложения фиксированного проектора ранга 2 в сумму ортогональных проекторов ранга 1 параметризуются многообразием $Y = \mathbb{P}^1 \times \mathbb{P}^1 \setminus \Delta$, где Δ — диагональное подмногообразие. Проектор ранга 1 из разложения фиксированного проектора ранга 2 определяется своим образом и ядром. Как известно, множество одномерных подпространств в образе проектора ранга 2 — это $\mathbb{P}^1$. Ядро и образ соответствуют двум несовпадающим точкам на $\mathbb{P}^1$.

Рассмотрим отображение $j_1^* : \mathbf{Rep}_7\,B_1 \to \mathbf{Rep}_7\,\mathcal{C}$. Несложно заметить, что в слое отображения j_1^* лежит 4-мерное многообразие $Y \times Y$, параметризующее разложение проекторов ранга 2:

$$P_1 = \pi_1 + \pi_2, \quad Q_2 = \rho_3 + \rho_4. \tag{5.6}$$

Далее, рассмотрим подмногообразие $X_1 \subset \mathbf{Rep}_7\,B_1$, задаваемое уравнениями

$$\operatorname{Tr}\pi_1 Q_1 = \operatorname{Tr}\pi_2 Q_1 = \operatorname{Tr} P_2\rho_3 = \operatorname{Tr} P_2\rho_4 = \frac{2}{7}, \tag{5.7}$$

$$\operatorname{Tr}\pi_1\rho_3 = \operatorname{Tr}\pi_2\rho_3 = \operatorname{Tr}\pi_1\rho_4 = \operatorname{Tr}\pi_2\rho_4 = \frac{1}{7}. \tag{5.8}$$

Эти уравнения возникают из условий на следы (3.4). Определим отображение: $j_1^* : X_1 \to \mathbf{Rep}_7\,\mathcal{C}$ как ограничение на подмногообразие. Отметим, что многообразие X_1 является $\mathrm{GL}_7(\mathbb{C})$-инвариантным.

Далее, из представления θ алгебры $\mathcal{C}$ из (4.5) получаем, что $\operatorname{Tr} P_1 Q_1 = 4/7$. Следовательно, из (5.6) получаем, что $\operatorname{Tr}(\pi_1+\pi_2)Q_1 = 4/7$ и, следовательно, $\operatorname{Tr}\pi_1 Q_1 = 2/7$ и $\operatorname{Tr}\pi_2 Q_1 = 2/7$ совпадают. Аналогично, совпадают уравнения $\operatorname{Tr} P_2\rho_3 = 2/7$ и $\operatorname{Tr} P_2\rho_4 = 2/7$. Далее, из представления θ получаем, что $\operatorname{Tr} P_1 Q_2 = 4/7$. Используя разложение (5.6), получаем, что $\operatorname{Tr}(\pi_1+\pi_2)(\rho_3+\rho_4) = 4/7$. Следовательно, вместо четырех уравнений (5.8) достаточно рассматривать три.

Докажем следующую лемму.

Лемма 5.1. *Пусть p_1, q_1 и p_2, q_2 — такие проекторы ранга 1 в 4-мерном пространстве, что*

$$p_i p_j = q_i q_j = 0,\ i \neq j, \qquad p_1 q_2 = q_2 p_1 = p_2 q_1 = q_1 p_2 = 0.$$

Пусть π_1, π_2 — такие ортогональные проекторы ранга 1, что $\pi_1 + \pi_2 = p_1 + p_2$. Тогда

$$\operatorname{Tr} p_2 q_2 \operatorname{Tr}\pi_i q_1 + \operatorname{Tr} p_1 q_1 \operatorname{Tr}\pi_i q_2 = \operatorname{Tr} p_1 q_1 \operatorname{Tr} p_2 q_2, \quad i = 1, 2. \tag{5.9}$$

Доказательство. Пусть W — 4-мерное пространство, в котором действуют проекторы p_1, p_2, q_1, q_2. Обозначим через W_1 и W_2 пространства, порожденные образами проекторов p_1, q_1 и p_2, q_2

соответственно. Тогда из условий леммы получаем, что $W_1 \oplus W_2 = W$. Пусть Pr_1 — проектор на W_1 вдоль W_2 и $\mathrm{Pr}_2 = 1 - \mathrm{Pr}_1$ — проектор на W_2 вдоль W_1. Далее,

$$\mathrm{Pr}_1 \pi_i \mathrm{Pr}_1 = \mathrm{Tr}\, \mathrm{Pr}_1 \pi_i \cdot p_1.$$

Действительно, $\mathrm{Pr}_1 \pi_i \mathrm{Pr}_1$ имеет тоже ядро и образ, что и проектор p_1. Аналогично,

$$\mathrm{Pr}_2 \pi_i \mathrm{Pr}_2 = \mathrm{Tr}\, \mathrm{Pr}_2 \pi_i \cdot p_2.$$

Также отметим, что

$$\mathrm{Tr}\, \pi_i q_1 = \mathrm{Tr}\, \pi_i \mathrm{Pr}_1 q_1 \mathrm{Pr}_1 = \mathrm{Tr}\, \mathrm{Pr}_1 \pi_i \mathrm{Pr}_1 q_1 = \mathrm{Tr}\, \pi_i \mathrm{Pr}_1 \cdot \mathrm{Tr}\, p_1 q_1.$$

и аналогично

$$\mathrm{Tr}\, \pi_i q_2 = \mathrm{Tr}\, \pi_i \mathrm{Pr}_2 \cdot \mathrm{Tr}\, p_2 q_2.$$

Далее,

$$\mathrm{Tr}\, p_2 q_2 \cdot \mathrm{Tr}\, \pi_i q_1 + \mathrm{Tr}\, p_1 q_1 \cdot \mathrm{Tr}\, \pi_i q_2 = \mathrm{Tr}\, p_1 q_1\, \mathrm{Tr}\, p_2 q_2 (\mathrm{Tr}\, \pi_i (\mathrm{Pr}_1 + \mathrm{Pr}_2)) = \mathrm{Tr}\, p_1 q_1 \cdot \mathrm{Tr}\, p_2 q_2$$

так как $\mathrm{Tr}\, \pi_i = 1$, что и требовалось доказать. □

Напомним, что представление θ алгебры $\mathcal{C}$ представляет собой прямую сумму четырех представлений: одного тривиального и трех двумерных. Пространство, в котором реализовано представление θ, раскладывается в прямую сумму

$$V = V_0 \oplus V_1 \oplus V_2 \oplus V_3. \tag{5.10}$$

При этом в V_0 порождающие алгебры $\mathcal{C}$ действуют как нулевые операторы; P_1 и Q_2 действуют в пространстве V_1 нулевым образом; P_2 и Q_1 имеют ранг 1, обозначим эти операторы P_2' и Q_1'. Аналогично, P_2 и Q_1 в пространстве V_2 — нулевые операторы, а проекторы P_1, Q_2 ранга 1 обозначим P_1' и Q_2'. В пространстве V_3 операторы P_1, P_2, Q_1, Q_2, являющиеся проекторами ранга 1, обозначим P_1'', P_2'', Q_1'', и Q_2''.

Теперь рассмотрим разложения

$$P_1' + P_1'' = \pi_1 + \pi_2, \quad Q_2' + Q_2'' = \rho_3 + \rho_4.$$

Рассмотрим 4-мерное пространство $V_2 \oplus V_3$. Имеем

$$P_1' P_1'' = P_1'' P_1' = 0, \qquad P_1' Q_i'' = Q_i'' P_1' = 0,\ i = 1, 2, \qquad P_1'' Q_2' = Q_2' P_1'' = 0.$$

Используя таблицу следов из разделаЁ4.5, получаем, что

$$\mathrm{Tr}\, P_1' Q_2' = \mathrm{Tr}\, P_2' Q_1' = \frac{1}{7}, \quad \mathrm{Tr}\, P_1'' Q_2'' = \frac{3}{7}, \quad \mathrm{Tr}\, P_1'' Q_1'' = \frac{4}{7}.$$

Применяя лемму 5.1 к случаям $p_1 = P_1'$, $p_2 = P_1''$, $q_1 = Q_2'$, $q_2 = Q_1''$ и $p_1 = P_1'$, $p_2 = P_1''$, $q_1 = Q_2'$, $q_2 = Q_2''$, получим следующие соотношения:

$$\frac{1}{7} \mathrm{Tr}\, \pi_1 Q_1'' + \frac{4}{7} \mathrm{Tr}\, \pi_i Q_2' = \frac{4}{49}, \quad \frac{1}{7} \mathrm{Tr}\, \pi_i Q_2'' + \frac{3}{7} \mathrm{Tr}\, \pi_i Q_2' = \frac{3}{49}. \tag{5.11}$$

Так как образы проекторов P_1', P_1'' содержатся в ядре Q_1' и наоборот, получаем, что

$$P_1' Q_1' = Q_1' P_1' = 0.$$

Раскладывая $P_1' + P_1''$ в сумму ортогональных проекторов ранга 1,

$$P_1' + P_1'' = \pi_1 + \pi_2,$$

получаем

$$\pi_i Q_1' = Q_1' \pi_i = 0, \quad i = 1, 2.$$

Тогда

$$\mathrm{Tr}\, \pi_i Q_1 = \mathrm{Tr}\, \pi_i (Q_1' + Q_1'') = \mathrm{Tr}\, \pi_i Q_1''. \tag{5.12}$$

Далее, вернемся к уравнениям (5.7) и (5.8). Используя (5.12), имеем

$$\mathrm{Tr}\, \pi_i Q_1'' = \frac{2}{7}. \tag{5.13}$$

Соотношения (5.11) переписываются следующим образом:

$$\operatorname{Tr}\pi_i Q_2' = \frac{1}{14}, \quad \operatorname{Tr}\pi_i Q_2'' = \frac{3}{14}.$$

Соответственно, получаем, что

$$\operatorname{Tr}\pi_i Q_2 = \operatorname{Tr}\pi_i (Q_2' + Q_2'') = \frac{2}{7}, \quad i = 1, 2.$$

Аналогично, рассматривая разложение $Q_2 = \rho_3 + \rho_4$, находим

$$\operatorname{Tr}\rho_j P_1 = \frac{2}{7}, \quad j = 3, 4.$$

Таким образом, рассматривая разложения (5.6), получаем, что если $\operatorname{Tr}\pi_1\rho_3 = 1/7$, то $\operatorname{Tr}\pi_i\rho_j = 1/7$ для всех $i = 1, 2$ и $j = 3, 4$. Следовательно, многообразие X_1 задается тремя уравнениями:

$$\operatorname{Tr}\pi_1 Q_2 = \frac{2}{7}, \quad \operatorname{Tr}\rho_3 P_1 = \frac{2}{7}, \quad \operatorname{Tr}\pi_1\rho_3 = \frac{1}{7}. \tag{5.14}$$

Выписывая в подходящих координатах эти уравнения, получаем следующее утверждение.

Предложение 5.2. *Многообразие X_1 имеет 2 компоненты. Слой при отображении j_1^* каждой из них представляет собой $\mathbb{C}^*$.*

Определим многообразие $X_2 \subset \mathbf{Rep}_7 B_2$ уравнениями (5.7) и (5.8) с заменой π_1, π_2 на π_3, π_4, заменой ρ_3, ρ_4 на ρ_1, ρ_2 и заменой P_2, Q_1 на P_1, Q_2 соответственно. Так же, как и в случае с X_1, многообразие X_2 является $\mathrm{GL}_7(\mathbb{C})$-инвариантным, и определено отображение $j_2^* : X_2 \to \mathbf{Rep}_7 \mathcal{C}$. Получаем следующее утверждение.

Предложение 5.3. *Многообразие X_2 имеет 2 компоненты. Слой при отображении j_2^* каждой из них представляет собой $\mathbb{C}^*$.*

Отметим также, что 7-мерные представления алгебры B_1, соответствующие точкам многообразия X_1, имеют разложение в прямую сумму одного одномерного, одного двумерного и одного 4-мерного. Эти представления можно реализовать эндоморфизмами пространства V представления θ алгебры $\mathcal{C}$. В частности, на пространстве V_0 порождающие алгебры B_1 действуют нулевыми операторами, на V_1 элементы P_2, Q_1 действуют одномерными проекторами, на $V_2 \oplus V_3$ элементы π_i, ρ_j, P_2, Q_1 действуют одномерными проекторами. Обозначим последнее представление алгебры B_1 через η и докажем, что это 4-мерное представление алгебры B_1 неприводимо. Действительно, так как тройки проекторов π_1, π_2, P_2 и ρ_3, ρ_4, Q_1 ортогональны и представляются одномерными проекторами, то $\eta(1 - \pi_1 - \pi_2 - P_2)$ и $\varrho(1 - \rho_3 - \rho_4 - Q_1)$ — тоже одномерные проекторы. Получаем две четверки ортогональных проекторов. Для доказательства неприводимости достаточно доказать, что образ алгебры B_1 при представлении η совпадает с $\mathrm{Mat}_4(\mathbb{C})$. Учитывая, что следы всех попарных произведений проекторов из разных четверок не равны 0, получаем что попарные произведения линейно независимы. Следовательно, попарные упорядоченные произведения проекторов из первой четверки и второй образуют базис в $\mathrm{Mat}_4(\mathbb{C})$. Следовательно, η неприводимо. Таким образом, мы получили следующее утверждение.

Предложение 5.4. *Представления алгебры B_1, соответствующие точкам многообразия X_1, являются прямыми суммами одномерного, двумерного и 4-мерного неприводимых представлений B_1. В частности, при действии группы $\mathrm{GL}_7(\mathbb{C})$ сопряжениями получаем, что стабилизатор $\mathrm{St}_{\mathrm{GL}_7(\mathbb{C})}(x)$ любой точки $x \in X_1$ является трехмерным тором $(\mathbb{C}^*)^{\times 3}$.*

Далее, рассмотрим отображение $j_1^* : X_1 \to \mathbf{Rep}_7 \mathcal{C}$. Правая часть, как мы знаем, является одной $\mathrm{GL}_7(\mathbb{C})$-орбитой представления θ. При этом $\mathrm{St}_{\mathrm{GL}_7(\mathbb{C})}(\theta) = (\mathbb{C}^*)^{\times 4}$ (торы соответствуют неприводимым подпредставлениям θ). Для любой точки $x \in X_1$ и любого $g \in \mathrm{GL}_7(\mathbb{C})$ имеем

$$j_1^*(g \cdot x) = g \cdot \theta, \quad \text{где} \quad g \cdot x = gxg^{-1}.$$

Соответственно, определено действие факторгруппы $\mathrm{St}_{\mathrm{GL}_7(\mathbb{C})}(\theta)/\mathrm{St}_{\mathrm{GL}_7(\mathbb{C})}(x) = \mathbb{C}^*$ в слое $(j_1^*)^{-1}(\theta)$. Несложно проверить, что слой представляет собой две орбиты относительно действия $\mathbb{C}^*$. Таким образом, получаем следующее утверждение.

Предложение 5.5. *Каждое многообразие X_i, $i = 1, 2$, представляет собой объединение двух* $\mathrm{GL}_7(\mathbb{C})$*-орбит. Таким образом, каждый фактор $X_i/\mathrm{GL}_7(\mathbb{C})$, $i = 1, 2$, состоит из двух точек.*

Отметим, что на каждом X_i, $i = 1, 2$, группа $\mathbb{Z}_2 \times \mathbb{Z}_2$ действует перестановками π_i, $i = 1, 2$, и ρ_j, $j = 3, 4$ в случае X_1 и π_i, $i = 3, 4$, и ρ_j, $j = 1, 2$ в случае X_2. Прямым вычислением можно показать, что компоненты инварианты относительно одновременной перестановки π_i и ρ_j.

5.3. Алгебры $A_{4,4}$, $A_{4,7}$, $A_{7,4}$ и $A_{7,7}$. Рассмотрим многообразие представлений алгебр $A_{4,4}$, $A_{4,7}$, $A_{7,4}$ и $A_{7,7}$, соответствующих представлению θ алгебры $\mathcal{C}$.

Имеем коммутативную диаграмму

$$\begin{array}{ccc} \mathcal{C} & \xrightarrow{\quad j_1 \quad} & B_1 \\ \downarrow{\scriptstyle j_2} & & \downarrow{\scriptstyle \overline{\phi_1}} \\ B_2 & \xrightarrow{\quad \overline{\phi_2} \quad} & B_1 *_{\mathcal{C}} B_2, \end{array} \tag{5.15}$$

где $B_1 *_{\mathcal{C}} B_2$ — свободное произведение B_i, $i = 1, 2$, над $\mathcal{C}$. Используя универсальное свойство свободного произведения, определим морфизм алгебр

$$\psi : B_1 *_{\mathcal{C}} B_2 \to A_{4,4}$$

причем $\phi_i = \psi \circ \overline{\phi_i}$, $i = 1, 2$. Так как $\phi_i(B_i)$, $i = 1, 2$ порождают всю алгебру $A_{4,4}$, получаем, что естественный гомоморфизм $\psi : B_1 *_{\mathcal{C}} B_2 \to A_{4,4}$ сюръективен. Далее, имеем вложение

$$\psi^* : \mathbf{Rep}_7 A_{4,4} \to \mathbf{Rep}_7 B_1 *_{\mathcal{C}} B_2 = \mathbf{Rep}_7 B_1 \times_{\mathbf{Rep}_7 \mathcal{C}} \mathbf{Rep}_7 B_2. \tag{5.16}$$

Напомним, что $\mathbf{Rep}_7 A_{4,4}$ — представления алгебры $A_{4,4}$, при которых порождающие π_i, ρ_i, $i = 1, \ldots, 4$, являются проекторами ранга 1, а следы произведений равны $1/7$. Таким образом, $\mathbf{Rep}_7 A_{4,4}$ вкладывается в расслоенное произведение $X_1 \times_{\mathbf{Rep}_7 \mathcal{C}} X_2$. Покажем, что

$$\operatorname{Tr} \pi_i \rho_j = \frac{1}{7}, \quad i, j \in \{1, 2\},\ i, j \in \{3, 4\}$$

(для других i, j это следует из уравнений, определяющих многообразия X_1 и X_2). Докажем, что $\operatorname{Tr} \pi_1 \rho_1 = 1/7$; остальное доказывается аналогично.

Рассмотрим разложение (5.10) пространства V. Введем соответствующие проекторы Π_i, $i = 0, \ldots, 3$, на пространства V_i вдоль $\bigoplus\limits_{j \neq i} V_j$. Сравнивая образы и ядра, получаем, что

$$\Pi_3 \pi_i P i_3 = x_i P_1'',\ i = 1, 2, \qquad \Pi_3 \rho_1 \Pi_3 = y_i Q_1'',\ i = 1, 2.$$

Учитывая (5.13), находим

$$\operatorname{Tr} \Pi_3 \pi_1 \Pi_3 Q_1'' = \frac{2}{7} = x_1 \operatorname{Tr} P_1'' Q_1'' = \frac{4}{7} x_1.$$

Следовательно, $x_1 = 1/2$. Аналогично, $x_2 = y_1 = y_2 = 1/2$. Так как образы π_1 и ρ_1 лежат в $V_2 \oplus V_3$ и $V_1 \oplus V_3$, а ядра содержат $V_0 \oplus V_1$ и $V_0 \oplus V_2$ соответственно, то получаем, что

$$\operatorname{Tr} \pi_1 \rho_1 = \operatorname{Tr} \Pi_3 \pi_1 \Pi_3 \rho_1 \Pi_3 = \frac{1}{4} \operatorname{Tr} P_1'' Q_1'' = \frac{1}{7}.$$

С остальными проекторами ситуация аналогична. Таким образом, доказано следующее утверждение.

Предложение 5.6. *ψ^* является изоморфизмом многообразий $\mathbf{Rep}_7 A_{4,4}$ и $X_1 \times_{\mathbf{Rep}_7 \mathcal{C}} X_2$.*

Несложно показать, что 7-мерные представления алгебры $A_{4,4}$ приводимы и являются суммой 6-мерного неприводимого и одномерного тривиального. В частности, стабилизатор точки $x' \in \mathbf{Rep}_7 A_{4,4}$ есть $(\mathbb{C}^*)^{\times 2}$. В слое $j_1^* \circ \phi_1^*$ действует факторгруппа $\mathrm{St}_{\mathrm{GL}_7(\mathbb{C})}(\theta)/\mathrm{St}_{\mathrm{GL}_7(\mathbb{C})}(x') = (\mathbb{C}^*)^{\times 2}$. Получаем следующее утверждение.

Следствие 5.7. *Многообразие* $\mathbf{Rep}_7 A_{4,4}$ *является объединением четырех* $\mathrm{GL}_7(\mathbb{C})$*-орбит. Слой отображения*

$$(j_1^* \circ \phi_1^*)^{-1}(\theta) = (j_1^* \circ \phi_1^*)^{-1}(\theta)$$

является объединением четырех алгебраических торов $(\mathbb{C}^*)^{\times 2}$. *Многообразие* $\mathcal{M}_7 A_{4,4} = \mathbf{Rep}_7 A_{4,4}/\mathrm{GL}_7(\mathbb{C})$ *состоит из* 4 *точек.*

Зафиксируем произвольное 7-мерное представление Ω алгебры $A_{4,4}$ из следствия 5.7. Рассмотрим алгебру $A_{4,7}$ и многообразие представлений $Z \subset \mathbf{Rep}_7 A_{4,7}$, соответствующих Ω. Для описания Z рассмотрим множество разложений проектора ранга 3 в 7-мерном пространстве в сумму трех ортогональных проекторов ранга 1. Как известно, эти разложения параметризуются точками многообразия $(\mathbb{P}^2)^{\times 3} \setminus \mathcal{D}$, где $\mathcal{D}$ — подмногообразие таких троек (pt_1, pt_2, pt_3), $pt_i \in \mathbb{P}^2$, что pt_i, $i = 1, 2, 3$, не лежат на одной прямой. Таким образом, $\mathcal{D}$ — дивизор $(\mathbb{P}^2)^{\times 3}$, и открытое многообразие $(\mathbb{P}^2)^{\times 3} \setminus \mathcal{D}$ имеет размерность 6.

Будем обозначать матрицы проекторов π_i, ρ_j, $i, j = 1, \ldots, 4$, теми же буквами. Построим по этим матрицам 7-мерное представление алгебры $A_{4,7}$. Для этого разложим матрицу $1 - \sum\limits_{i=1}^{4} \pi_i$ в сумму

$$1 - \sum_{i=1}^{4} \pi_i = \pi_5 + \pi_6 + \pi_7 \tag{5.17}$$

матриц таких ортогональных проекторов, что $\operatorname{Tr} \pi_i \rho_j = 1/7$, $i = 5, 6, 7$, $j = 1, \ldots, 4$. Отметим, что с учетом соотношений в алгебре $A_{4,7}$, уравнения на следы с π_7 следуют из уравнений на следы с π_5 и π_6. Таким образом, имеем 8 уравнений на $(\mathbb{P}^2)^{\times 3} \setminus \mathcal{D}$, задающих многообразие Z. Докажем, что эти уравнения зависимы и выводятся из четырех.

Заметим что $\Pi_2 \pi_5 \Pi_2$ и $\Pi_2 - P_1'$ имеют одни и те же ядро и образ и, следовательно, $\Pi_2 \pi_5 \Pi_2 = x(\Pi_2 - P_1')$ для некоторого $x \in \mathbb{C}^*$. Сначала покажем, что из соотношения $\operatorname{Tr} \pi_5 Q_2' = 2/7$ следует, что

$$\Pi_2 \pi_5 \Pi_2 = \frac{1}{3}(\Pi_2 - P_1').$$

Действительно,

$$\frac{2}{7} = \operatorname{Tr} \Pi_2 \pi_5 \Pi_2 Q_2 = \operatorname{Tr} \Pi_2 \pi_5 \Pi_2 Q_2' = x \operatorname{Tr}(\Pi_2 - P_1') Q_1' = \frac{6}{7} x,$$

т.е. $x = 1/3$. Далее, несложно проверить, что

$$\operatorname{Tr} \pi_5 \rho_1 = \operatorname{Tr} \Pi_2 \pi_5 \Pi_2 \rho_1 \Pi_2.$$

Тогда получаем, что

$$\operatorname{Tr} \Pi_2 \pi_5 \Pi_2 \rho_1 = \frac{1}{3} \cdot \frac{1}{2} \operatorname{Tr}(\Pi_2 - P_1') Q_2' = \frac{1}{7},$$

так как ранее было показано, что

$$\Pi_2 \rho_1 \Pi_2 = \frac{1}{2} \rho 1.$$

Аналогично рассматриваются остальные случаи. Таким образом, можно вместо 8 уравнений выбрать четыре:

$$\operatorname{Tr} \pi_j Q_k = \frac{2}{7}, \quad j = 5, 6, \ k = 1, 2. \tag{5.18}$$

Отметим, что у нас имеются две тройки ортогональных проекторов ранга 1: Π_0, $\Pi_1 - P_2'$, $\Pi_2 - P_1'$, π_5, π_6, π_7. Для этих проекторов выполнены соотношения

$$\Pi_0 + \Pi_1 - P_2' + \Pi_2 - P_1' = \pi_5 + \pi_6 + \pi_7$$

и условие, что следы произведений проекторов из разных троек равны $1/3$. Более того, это условие на следы эквивалентно уравнениям (5.18). При заданных Π_0, $\Pi_1 - P_2'$, $\Pi_2 - P_1'$ классификация π_5, π_6, π_7 известна: она возникает из классификации ортогональных пар в $\mathfrak{sl}(3)$. Классификация π_5, π_6, π_7 дает полное описание многообразия Z.

Предложение 5.8. *Многообразие Z является объединением шести двумерных торов $(\mathbb{C}^*)^{\times 2}$. На множестве двумерных торов действует симметрическая группа S_3, переставляющая π_5, π_6, π_7.*

Несложно показать, что представления алгебры $A_{4,7}$ в 7-мерном пространстве, параметризованные точками многообразия Z, неприводимы. Используя стабилизаторы, получаем, что на Z действует одномерный тор. Вспоминая, что для построения Z мы фиксировали одно из четырех возможных представлений $A_{4,4}$, получаем следующее утверждение.

Предложение 5.9. *Многообразие $\mathcal{M}_7 A_{4,7} = \mathbf{Rep}_7 A_{4,7}/\operatorname{GL}_7(\mathbb{C})$ есть объединение четырех копий $Z/\mathbb{C}^*$. Следовательно, $\mathcal{M}_7 A_{4,7}$ является объединением 24 одномерных торов. Для алгебры $A_{7,4}$ ситуация аналогична.*

Теперь изучим алгебру $A_{7,7}$. Для алгебр $A_{4,4}$, $A_{4,7}$ и $A_{7,4}$ имеем следующую коммутативную диаграмму:

$$\begin{array}{ccc} A_{4,4} & \xrightarrow{\psi_1} & A_{4,7} \\ \downarrow{\scriptstyle \psi_2} & & \downarrow{\scriptstyle \overline{\mu_1}} \\ A_{7,4} & \xrightarrow{\overline{\mu_2}} & A_{4,7} *_{A_{4,4}} A_{7,4}. \end{array} \tag{5.19}$$

В силу того, что образы $A_{4,7}$ и $A_{7,4}$ в $A_{7,7}$ порождают всю алгебру $A_{7,7}$, существует сюръективный гомоморфизм

$$A_{4,7} *_{A_{4,4}} A_{7,4} \to A_{7,7}$$

и, следовательно, имеем вложение многообразий

$$\mathbf{Rep}_7 A_{7,7} \to \mathbf{Rep}_7 A_{4,7} \times_{\mathbf{Rep}_7 A_{4,4}} \mathbf{Rep}_7 A_{7,4}.$$

$\mathbf{Rep}_7 A_{7,7}$ как подмногообразие в $\mathbf{Rep}_7 A_{4,7} \times_{\mathbf{Rep}_7 A_{4,4}} \mathbf{Rep}_7 A_{7,4}$ задано девятью уравнениями

$$\operatorname{Tr} \pi_j \rho_k = \frac{1}{7}, \quad j,k = 5,\dots,7.$$

Заметим, что, как и ранее, из этих девяти уравнений можно выбрать четыре линейно независимых, например,

$$\operatorname{Tr} \pi_j \rho_k = \frac{1}{7}, \quad j,k = 5,6.$$

Зафиксируем представление Ω; тогда представления из слоя

$$(\psi_1^* \circ \mu_1^*)^{-1}(\Omega) = (\psi_2^* \circ \mu_2^*)^{-1}(\Omega)$$

содержатся в произведении $Z \times Z$. Используя тот факт, что Π_0, $\Pi_1 - P_2'$, $\Pi_2 - P_1'$ и π_5, π_6, π_7, а также Π_0, $\Pi_1 - Q_1'$, $\Pi_2 - Q_2'$ и ρ_5, ρ_6, ρ_7 соответствуют ортогональным парам, можно вывести, что эти четыре уравнения выводятся из двух, которые можно выбрать так:

$$\operatorname{Tr} \pi_5 \rho_5 = \frac{1}{7}, \quad \operatorname{Tr} \pi_5 \rho_6 = \frac{1}{7}.$$

Решая эти уравнения, получаем что в слое над Ω лежит объединение конечного числа двумерных торов. Вспомним, что после факторизации по $\operatorname{GL}_7(\mathbb{C})$ в слое над Ω будет действовать фактор стабилизатора Ω по стабилизатору представления $A_{7,7}$, которое неприводимо. Этот фактор является одномерным тором. Прямое вычисление показывает, что факторы двумерных торов в слое по одномерному являются одномерными торами. Таким образом, получаем следующее утверждение.

Предложение 5.10. *Многообразие $\mathbf{Rep}_7 A_{7,7}$ является объединением конечного числа семейств $\operatorname{GL}_7(\mathbb{C})$-орбит. Каждое семейство параметризовано одномерным алгебраическим тором $\mathbb{C}^*$.*

Выписывая матрицы перехода между образами π_i, $i = 1,\dots,7$, и ρ_j, $j = 1,\dots,7$, получаем однопараметрические семейства обобщенно-адамаровых матриц.

Отметим, что инволюция $\dagger$, определенная в п. 3.1, действует на $\mathcal{M}_7 A_{7,7}$. Неподвижные точки $\mathcal{M}_7^\dagger A_{7,7}$ соответствуют комплексно-адамаровым матрицам. В терминах одномерного семейства

Петреску инволюция † действует следующим образом: $a \mapsto \frac{1}{\overline{a}}$, т.е. неподвижные точки соответствуют семейству Петреску комплексно-адамаровых матриц. Таким образом, мы доказали получили следующую теорему.

Теорема 5.11. *Многообразие модулей $\mathcal{M}_7 A_{7,7}$ изоморфно (с точностью до конечных симметрий) одномерному семейству Петреску обобщенно-адамаровых матриц. Многообразие неподвижных точек $\mathcal{M}_7^{\dagger} A_{7,7}$ изоморфно (с точностью до конечных симметрий) одномерному семейству Петреску комплексно-адамаровых матриц.*

СПИСОК ЛИТЕРАТУРЫ

1. *Кострикин А. И., Кострикин И. А., Уфнаровский В. А.* Ортогональные разложения простых алгебр Ли (тип A_n)// Тр. Мат. ин-та им. В. А. Стеклова АН СССР. — 1981. — *158*. — С. 105–120.
2. *фон Нейман И.* Математические основы квантовой механики. — М.: Наука, 1964.
3. *Bondal A., Zhdanovskiy I.* Representation theory for system of projectors and discrete Laplace operator/ Preprint IPMU, IPMU13-0001.
4. *Bondal A., Zhdanovskiy I.* Orthogonal pairs and mutually unbiased bases// J. Math. Sci. — 2016. — *216*, № 1. С. 23–40.
5. *Bondal A., Zhdanovskiy I.* Symplectic geometry of unbiasedness and critical points of a potential// to appear in: Adv. Stud. Pure Math. — Tokyo: Math. Soc. Jpn. — 2016; `arXiv:1507.00081`
6. *Durt T., Englert B.-G., Bengtsson I., Zyczkowski K.* On mutually unbiased bases// Int. J. Quantum Inform. — 2010. — *8*. — С. 535.
7. *Haagerup U.* Orthogonal maximal abelian *-subalgebras of the $(n \times n)$-matrices and cyclic n-roots// in: Operator Algebras and Quantum Field Theory. — Int. Press, 1997. — С. 296–322.
8. *Kostrikin A. I., Pham Huu Tiep*, Orthogonal decompositions and integral lattices. — Walter de Gruyter, 1994.
9. *Matolcsi M., Szollosi F.* Towards a classification of 6×6 complex Hadamard matrices// Open. Syst. Inf. Dyn. — 2008. — *15*, № 2. — С. 93–108.
10. *Nicoara R.* A finiteness result for commuting squares of matrix algebras// J. Operator Theory. — 2006. — *55*, № 2. — С. 295–310; `arXiv:math/0404301`
11. *Petrescu M.* Existence of continuous families of complex Hadamard matrices of certain prime dimensions and related results/ Ph.D. thesis. — Los Angeles: Univ. of California, 1997.
12. *Popa S.* Orthogonal pairs of *-subalgebras in finite von Neumann algebras// J. Operator Theory. — 1983. — *9*. — С. 253–268. (1983)
13. *Ruskai M. B.* Some connections between frames, mutually unbiased bases, and POVM's in quantum information theory// Acta Appl. Math. — 2009. — *108*, № 3. — С. 709–719.
14. *Sakai S.* $C*$-Algebras and $W*$-Algebras. — New York–Heidelberg–Berlin: Springer-Verlag, 1971.
15. *Szollosi F.* Complex Hadamard matrices of order 6: a four-parameter family// J. Lond. Math. Soc. — 2012. — *85*. — С. 616–632; `arXiv:htp.1008.0632`
16. *Tadej W., Zyczkowski K.* Defect of a unitary matrix// Lin. Alg. Appl. — 2008. — *429*. — С. 447–481.

И. Ю. Ждановский
Московский физико-технический институт;
Национальный исследовательский университет «Высшая школа экономики», Москва
E-mail: `ijdanov@mail.ru`

А. С. Кочерова
Московский физико-технический институт
E-mail: `akocherova@yandex.ru`

ИТОГИ НАУКИ И ТЕХНИКИ.
Современная математика и ее приложения.
Тематические обзоры.
Том 138 (2017). С. 50–59

УДК 530.145, 517.977

ДИСКРЕТНЫЕ АППРОКСИМАЦИИ ДИНАМИЧЕСКОГО КВАНТОВОГО ЭФФЕКТА ЗЕНОНА

© 2017 г. **Н. Б. ИЛЬИН, А. Н. ПЕЧЕНЬ**

Аннотация. Обсуждаются аппроксимации динамического квантового эффекта Зенона фиксированным числом неселективных квантовых измерений. Найден широкий класс измерений, эффективность которых в случае двухуровневых систем близка к оптимальной.

Ключевые слова: квантовый эффект Зенона, квантовая теория управления, квантовые измерения, двухуровневая система, кубит.

AMS Subject Classification: 49K15, 81V80

1. Введение. Эволюция квантовой системы под воздействием измерений её состояния замедляется и в предельном случае непрерывной последовательности измерений прекращается. Это явление было названо Сударшаном (E. C. G. Sudarshan) и Б. Мисрой (B. Misra) эффектом Зенона в [14] по аналогии с парадоксом «стрела» Зенона Элейского. Квантовый эффект Зенона был впервые предсказан в работах Л. А. Халфина [4, 5]. Этот эффект лежит в основе возможности управления открытыми квантовыми системами с помощью измерений. В последнее время в связи с развитием квантовых технологий большое значение приобретает управление зацепленными квантовыми состояниями [13], управление с помощью измерений [11,15–18] квантовое управление с обратной связью [12,19] и управление в стохастическом пределе квантовой теории [7,8]. Использование неселективных квантовых измерений для управления квантовыми системами изучалось в [15–17].

2. Квантовый эффект Зенона. Пусть система находится в начальном состоянии с матрицей плотности ρ_0 и через промежутки времени δt_k над системой производятся неселективные измерения состояния, т.е. результат измерения не считывается (см. [6]). Измеряемое состояние задаётся таким проектором P, что $\rho_0 = P\rho_0 P$. При каждом измерении матрица плотности преобразуется по формуле

$$\rho_{t-0} \to \rho_{t+0} = \mathcal{M}_P(\rho_{t-0}) = P\rho_{t-0}P + (\mathbb{I} - P)\rho_{t-0}(\mathbb{I} - P),$$

а между измерениями — по формуле

$$\rho_{t+0} \to \rho_{t+\delta t} = e^{-i\delta t H}\rho_{t+0}e^{i\delta t H}.$$

В [14] доказано, что

$$\lim_{\max \delta t_k \to\, 0} \operatorname{Tr}[\rho_t P] = 1. \tag{1}$$

Таким образом, в пределе непрерывного измерения система с вероятностью единица остаётся в состоянии P на протяжении всего времени.

В [9, 10] рассмотрено обобщение этого результата. Пусть измеряется зависящий от времени проектор $P_t = W_t P W_t^\dagger$, где W_t — унитарный оператор эволюции, удовлетворяющий некоторым условиям гладкости, а эволюция матрицы плотности такая же, как в предыдущем случае. Тогда

$$\lim_{\max \delta t_k \to\, 0} \operatorname{Tr}[\rho_t P_t] = 1. \tag{2}$$

Работа выполнена при поддержке Министерства образования и науки Российской Федерации (проект № 1.669.2016/ФПМ)..

Таким образом, в каждый момент времени система находится в состоянии P_t с вероятностью единица, т.е. система точно следует за изменением величины P_t. Это так называемый динамический эффект (или анти-эффект) Зенона. Его можно интерпретировать как возможность управлять квантовой системой, заставляя её с помощью достаточно частых измерений следовать заданной траектории, определяемой проектором P_t. Более подробное изложение квантового эффекта Зенона и связанных с ним вопросов содержится в [1].

3. Нижняя оценка для максимума вероятности перехода в n-уровневых системах. В лабораторных условиях часто достаточно сложно проводить большое количество измерений за время, в течение которого система хорошо изолирована от внешних воздействий. Возникает вопрос, насколько возможно приблизиться к описанной в [14, 16] идеальной ситуации в пределе непрерывных измерений с помощью конечного числа измерений.

Пусть U — унитарный оператор, $Q = \sum\limits_k^n q_k P_k$ — спектральное разложение наблюдаемой Q, где q_k — собственные значения и P_k — проекторы на её собственные векторы. Неселективное измерение и унитарная эволюция определяют следующие преобразования матрицы плотности:

$$\rho \to \mathcal{M}_Q(\rho) := \sum_k^n P_k \rho P_k, \tag{3}$$

$$\rho \to \mathcal{U}(\rho) := U \rho U^\dagger. \tag{4}$$

Результирующая матрица плотности после измерения наблюдаемых $Q_1, \ldots, Q_N$ с унитарной эволюцией U_i между измерениями i и $i+1$ имеет вид

$$\rho_N = \mathcal{U}_N \circ \mathcal{M}_{Q_N} \circ \mathcal{U}_{N-1} \circ \cdots \circ \mathcal{M}_{Q_1} \circ \mathcal{U}_0 \ (\rho_0). \tag{5}$$

Рассматривается задача максимизации целевого функционала

$$J_N[Q_1, \ldots, Q_N] := \operatorname{Tr}\left[\rho_N O\right], \tag{6}$$

где O — эрмитова матрица, соответствующая целевой наблюдаемой. Этот целевой функционал является квантовомеханическим средним значением целевой наблюдаемой в некоторый фиксированный момент времени. Задача управления состоит в нахождении оптимальных наблюдаемых $Q_1^{\text{opt}}, \ldots, Q_N^{\text{opt}}$, которые максимизируют целевой функционал, т.е. таких, что

$$J_N\Big[Q_1^{\text{opt}}, \ldots, Q_N^{\text{opt}}\Big] = \max_{Q_1 \ldots Q_N} J_N\Big[Q_1, \ldots, Q_N\Big] \equiv J_N^{\max}\Big[\rho_0, O\Big] \tag{7}$$

для данной матрицы плотности ρ_0 и целевого оператора O.

В работе [16] получено явное выражение для $J_N^{\max}\big[\rho_0, O\big]$.

Теорема 1. *Пусть*

$$O = \lambda \cdot \mathbb{I} + \boldsymbol{\lambda} \cdot \boldsymbol{\sigma}, \quad \tilde{\rho} = \mathcal{U}_N \circ \mathcal{U}_{N-1} \circ \cdots \circ \mathcal{U}_0(\rho_0) = \frac{1}{2}[\mathbb{I} + \boldsymbol{a} \cdot \boldsymbol{\sigma}], \quad \Delta\varphi = \angle(\boldsymbol{a}, \boldsymbol{\lambda}) \in [0, \pi].$$

Тогда

$$J_N^{\max}\big[\rho_0, O\big] = \lambda + |\boldsymbol{\lambda}||\boldsymbol{a}| \left[\cos\frac{\Delta\varphi}{N+1}\right]^{N+1}. \tag{8}$$

Рассмотрим задачу максимизации вероятности перехода $P_N[\psi_i, \psi_f]$ из состояния $|\psi_i\rangle$ в состояние $|\psi_f\rangle$ для двухуровневой системы с гамильтонианом $H = \sigma_z$. Начальная матрица плотности есть $\rho_0 = |\psi_i\rangle\langle\psi_i|$ и целевой оператор есть $O = |\psi_f\rangle\langle\psi_f|$, что соответствует

$$\lambda = \frac{1}{2}, \quad \boldsymbol{\lambda} = \frac{1}{2}\langle\psi_f|\boldsymbol{\sigma}|\psi_f\rangle, \quad \boldsymbol{a} = \langle\psi_i|e^{iT\sigma_z}\boldsymbol{\sigma}e^{-iT\sigma_z}|\psi_i\rangle, \quad \Delta\varphi_{i\to f} = \angle(\boldsymbol{\lambda}, \boldsymbol{a}).$$

Отметим, что

$$|\boldsymbol{\lambda}| = \frac{1}{2}, \quad |\boldsymbol{a}| = 1, \quad \cos\Delta\varphi_{i\to f} = 2|\langle\psi_f|e^{-iT\sigma_z}|\psi_i\rangle|^2 - 1.$$

Асимптотика выражения (8) будет иметь вид

$$P_N^{\max}\big[\psi_i,\psi_f\big]=1-\frac{\Delta\varphi_{i\to f}^2}{4N}+O\left(\frac{1}{N^2}\right). \tag{9}$$

Имеем

$$\lim_{N\to\infty}P_N^{\max}\big[\psi_i,\psi_f\big]=1,$$

что согласуется с динамическим эффектом Зенона. С помощью (9) можно, например, по заданной величине населённости уровня $P_N^{\max}\big[\psi_i,\psi_f\big]=1-\varepsilon$, $\varepsilon\ll 1$, которую мы желаем получить, найти минимальное необходимое для этого число измерений

$$N\approx\frac{\Delta\varphi_{i\to f}^2}{4\varepsilon}. \tag{10}$$

Задача максимизации вероятности перехода в n-уровневой системе рассматривалась в [3]. Определим матрицы

$$\sigma_x=|\psi_i\rangle\langle\psi_i^\perp|+|\psi_i^\perp\rangle\langle\psi_i|,\quad \sigma_y=i\Big(|\psi_i\rangle\langle\psi_i^\perp|-|\psi_i^\perp\rangle\langle\psi_i|\Big),\quad \sigma_z=\mathbb{I}-2|\psi_i\rangle\langle\psi_i|.$$

Здесь

$$|\psi_i^\perp\rangle=\frac{\psi}{\|\psi\|},\quad \psi=|\psi_f\rangle-\langle\psi_i|\psi_f\rangle|\psi_i\rangle$$

для невырожденного случая $|\psi_f\rangle\neq|\psi_i\rangle$. Эти матрицы являются матрицами Паули в двумерном пространстве, натянутом на векторы $|\psi_f\rangle$ и $|\psi_i\rangle$. Обозначим $\boldsymbol{\sigma}=(\sigma_x,\sigma_y,\sigma_z)$. Справедлива следующая теорема (см. [3]).

Теорема 2. *Пусть $|\psi_i\rangle$ и $|\psi_f\rangle$ — начальное и целевое состояния системы. Положим*

$$\boldsymbol{\lambda}=\langle\psi_f|\boldsymbol{\sigma}|\psi_f\rangle,\quad \boldsymbol{a}=\langle\psi_i|\boldsymbol{\sigma}|\psi_i\rangle.$$

Тогда для максимума вероятности перехода $P_N^{\max}\big[\psi_i,\psi_f\big]$ под воздействием N неселективных измерений имеет место оценка

$$P_N^{\max}\big[\psi_i,\psi_f\big]\geqslant\frac{1}{2}\left(1+\left[\cos\frac{\Delta\varphi}{N+1}\right]^{N+1}\right), \tag{11}$$

где

$$\Delta\varphi=\angle(\boldsymbol{a},\boldsymbol{\lambda})=\arccos\Big[2\big|\langle\psi_f|e^{-iTH}|\psi_i\rangle\big|^2-1\Big]. \tag{12}$$

Здесь $\angle(\boldsymbol{a},\boldsymbol{\lambda})$ — угол между векторами $\boldsymbol{a}$ и $\boldsymbol{\lambda}$. Выражения для наблюдаемых Q_k, на которых $P_N\big[\psi_i,\psi_f\big]$ достигает значения в правой части неравенства (11)*, имеют вид*

$$Q_k=\alpha P_k+\beta(\mathbb{I}-P_k),\quad \alpha,\beta\in\mathbb{R},\quad \alpha\neq\beta, \tag{13}$$

где

$$P_k=\frac{1}{2}e^{iH(T-t_k)}\Big[\mathbb{I}+\boldsymbol{a}_k\cdot\boldsymbol{\sigma}\Big]e^{-iH(T-t_k)}. \tag{14}$$

Если $\Delta\varphi\in(0,\pi)$, то вектор $\boldsymbol{a}_k$ получается вращением единичного вектора $\boldsymbol{a}$ на угол $k\Delta\varphi/(N+1)$ в плоскости векторов $\boldsymbol{a}$ и $\boldsymbol{\lambda}$:

$$\boldsymbol{a}_k=\boldsymbol{a}\frac{\sin\left[\frac{N-k+1}{N+1}\Delta\varphi\right]}{\sin\Delta\varphi}+\boldsymbol{\lambda}\frac{\sin\left[\frac{k}{N+1}\Delta\varphi\right]}{\sin\Delta\varphi},\quad k=1,\ldots,N. \tag{15}$$

Если $\Delta\varphi=0$, то

$$\boldsymbol{a}_k=\boldsymbol{a},\quad k=1,\ldots,N. \tag{16}$$

Если $\Delta\varphi=\pi$, то вектор $\boldsymbol{a}_k$ получается вращением единичного вектора $\boldsymbol{a}$ на угол $\pi k/(N+1)$ в плоскости векторов $\boldsymbol{a}$ и $\tilde{\boldsymbol{a}}$, где $\tilde{\boldsymbol{a}}$ — любой единичный вектор, ортогональный вектору $\boldsymbol{a}$,

$$\boldsymbol{a}_k=\boldsymbol{a}\cos\left[\frac{k}{N+1}\pi\right]+\tilde{\boldsymbol{a}}\sin\left[\frac{k}{N+1}\pi\right],\quad k=1,\ldots,N. \tag{17}$$

Отметим, что в двухуровневых системах наблюдаемые (13) доставляют глобальный максимум.

4. Вариация целевого функционала при наличии измерений и когерентного управления. В задаче квантового управления представляет интерес процесс управления с помощью совместного использования неселективных измерений и внешнего импульса модулированной формы, описывающего взаимодействие системы с внешним электромагнитным полем. В этом случае унитарная эволюция будет функционалом от интенсивности внешнего поля $f(t) \in L^1([t_1, t_2]; \mathbb{R})$, $\mathcal{U}_t^f(\rho) := U_t^f \rho U_t^{f\dagger}$, $t \in [t_1, t_2]$, где унитарный оператор U_t^f является решением уравнения Шрёдингера

$$i\frac{dU_t^f}{dt} = \big(H_0 + f(t)V\big)U_t^f, \quad U_{t=t_1}^f = \mathbb{I}. \tag{18}$$

Здесь H_0 и V — эрмитовы матрицы. Для того, чтобы задача была нетривиальной, предполагается $[H_0, V] \neq 0$. В фиксированные моменты времени $t_1 \dots t_i \dots t_N$ производятся измерения наблюдаемых $Q_1, \dots, Q_i, \dots, Q_N$. Результирующее преобразование матрица плотности примет вид

$$\rho_N^f = \mathcal{U}_{T-t_N}^f \circ \mathcal{M}_{Q_N} \circ \dots \mathcal{M}_{Q_i} \circ \mathcal{U}_{t_i - t_{i-1}}^f \circ \dots \circ \mathcal{M}_{Q_1} \circ \mathcal{U}_{t_1}^f(\rho_0). \tag{19}$$

Соответственно и целевой функционал будет определяться помимо измеряемых величин $Q_1, \dots, Q_i, \dots, Q_N$ также и управлением $f(t)$:

$$J_N\Big[Q_1, \dots, Q_N; f\Big] := \mathrm{Tr}\left[\rho_N^f O\right]. \tag{20}$$

Поскольку формула (19) имеет вид произведения супероператоров, действующих на начальную матрицу плотности ρ_0, то вариация $\delta\rho_N^f$ будет суммой вариаций отдельных сомножителей:

$$\delta\rho_N^f = \sum_i \Big[\dots \delta\mathcal{M}_{Q_i} \circ \mathcal{U}_{t_i - t_{i-1}}^f \dots (\rho_0) + \dots \mathcal{M}_{Q_i} \circ \delta\mathcal{U}_{t_i - t_{i-1}}^f \dots (\rho_0)\Big]. \tag{21}$$

Поскольку

$$\delta U_{t_i - t_{i-1}}^f = -i \int\limits_{t_{i-1}}^{t_i} U_{t_i - t_{i-1}}^f V_t \delta f(t) dt,$$

где $V_t = U_t^{f\dagger} V U_t^f$, $t \in [t_i, t_{i-1}]$, то

$$\delta\mathcal{U}_{t_i - t_{i-1}}^f(\rho) = -i \int\limits_{t_{i-1}}^{t_i} U_{t_i - t_{i-1}}^f [V_t, \rho] U_{t_i - t_{i-1}}^{f\dagger} \delta f(t) dt. \tag{22}$$

Для вариации $\delta\mathcal{M}_{Q_i}$, учитывая равенство

$$\sum_k^n \delta P_k = 0,$$

получим выражение

$$\delta\mathcal{M}_{Q_i}(\rho) = \sum_k^{n-1} \Big[\delta P_k \rho (P_k - P_n) + (P_k - P_n)\rho\delta P_k\Big]. \tag{23}$$

Вариация целевого функционала выражается через вариацию результирующей матрицы плотности ρ_N^f:

$$\delta J_N = \mathrm{Tr}\left[\delta\rho_N^f O\right]. \tag{24}$$

5. Оценка эффективности некоторого класса измерений, не зависящих от динамики. В [16] найдено максимально возможное значение функционала $J_N^{\max}$ по всем допустимым измерениям. При этом измерения, на которых достигается максимум, зависят от решения рассматриваемой динамической задачи (см. теорему 2). Поэтому осуществлять их на практике может быть неудобно. В связи с этим представляет интерес оценка для максимального значения целевого функционала $J^{\max}$, которое может быть получено при использовании не зависящей от гамильтониана системы последовательности измерений. В доказываемом ниже результате рассматриваются естественно возникающие в данной задаче измерения, зависящие только от начального и целевого состояний управляемой системы. Подобная последовательность измерений была впервые рассмотрена Дж. фон Нейманом (см. [2]) при обсуждении определения энтропии квантовой системы (см. также [9]). В [2,9] рассматривались измерения в квантовой системе без собственной динамики, т.е. с нулевым гамильтонианом. Мы рассматриваем эту последовательность измерений в системе с произвольным гамильтонианом. Получена оценка снизу для вероятности перехода из начального состояния в заданное целевое состояние для произвольных n-уровневых квантовых систем. В формулировке теоремы 3 и далее выражение $f(x) \geqslant o(x)$ означает, что

$$f_-(x) = \frac{|f(x)| - f(x)}{2} = o(x).$$

Теорема 3. *Пусть $U_t = e^{-itH}$, $W_t = e^{-it\Lambda}$, где H, Λ — эрмитовы $(m\times m)$-матрицы, начальное состояние есть*

$$\rho_0 = |\phi_0\rangle\langle\phi_0|,$$

целевое состояние в момент времени T есть

$$\rho_{target} = |\phi_N\rangle\langle\phi_N|,$$

где $|\phi_N\rangle = W_T|\phi_0\rangle$. Пусть A — такая эрмитова $(m \times m)$-матрица с невырожденным спектром, что $|\phi_0\rangle$ есть её собственное значение. Если в моменты времени Tk/N производятся измерения величины

$$A^{(k)} = W_{Tk/N} A W_{Tk/N}^\dagger, \quad k = 1, \ldots, N-1,$$

и если $\rho_N = \rho_N(\rho_0)$ (см. (4), (5)), то

$$\langle\phi_N|\rho_N|\phi_N\rangle \geqslant 1 - \frac{T^2\|H-\Lambda\|^2}{N} + o\left(\frac{T^2}{N}\right). \tag{25}$$

Доказательство. Пусть ϕ_i являются собственными векторами наблюдаемой A, $\phi_1 = |\phi_0\rangle$. Пусть $\phi_i^{(k)}$ — такой ортонормальный базис в $\mathbb{C}^m$, что $\phi_i^{(k)} = W_{Tk/N}\phi_i$. Векторы $\phi_i^{(k)}$ являются собственными векторами наблюдаемой $A^{(k)} = W_{Tk/N} A W_{Tk/N}^\dagger$. После последовательности неселективных измерений величин $A^{(k)}$ в моменты времени Tk/N вероятность перехода из состояния $|\phi_0\rangle$ в состояние $|\phi_N\rangle$ будет описываться выражением

$$\langle\phi_N|\rho_N|\phi_N\rangle = \sum_{i_{N-1},\ldots,i_1=1}^{m} \left|\langle\phi_N|U_{T/N}\phi_{i_{N-1}}^{(N-1)}\rangle\right|^2 \ldots \left|\langle\phi_{i_2}^{(2)}|U_{T/N}\phi_{i_1}^{(1)}\rangle\right|^2 \left|\langle\phi_{i_1}^{(1)}|U_{T/N}\phi_0\rangle\right|^2. \tag{26}$$

Пусть

$$P = \left|\langle\phi_N|U_{T/N}\phi_{N-1}\rangle\right|^2 \ldots \left|\langle\phi_2|U_{T/N}\phi_1\rangle\right|^2 \left|\langle\phi_1|U_{T/N}\phi_0\rangle\right|^2, \tag{27}$$

где $\phi_1^{(k)} = |\phi_k\rangle$. Величина P описывает вероятность перехода из состояния $|\phi_0\rangle$ в состояние $|\phi_N\rangle$ в результате последовательности селективных измерений. Имеем

$$\langle\phi_N|\rho_N|\phi_N\rangle \geqslant P \tag{28}$$

Пусть

$$P_k = \left|\langle\phi_{k+1}|U_{T/N}\phi_k\rangle\right|^2 = \left|\langle W_{T/N}\phi_k|U_{T/N}\phi_k\rangle\right|^2 = \left|\langle\phi_k|e^{i\Lambda T/N}e^{-iHT/N}|\phi_k\rangle\right|^2, \quad k = 0, \ldots, N-1.$$

Тогда $P = P_0 P_1 \dots P_{N-1}$. С точностью до второго порядка по T/N получаем

$$P_k = \left[1 - \frac{1}{2}\frac{T^2}{N^2}\Big(\langle\Lambda^2\rangle_k - \langle\{\Lambda, H\}\rangle_k + \langle H^2\rangle_k\Big)\right]^2 + \\ + \left[\frac{T}{N}\Big(\langle\Lambda\rangle_k - \langle H\rangle_k\Big) - \frac{1}{2}\frac{T^2}{N^2}\langle i[\Lambda, H]\rangle_k\right]^2 + o\left(\frac{T^2}{N^2}\right), \quad (29)$$

где

$$\langle A\rangle_k = \langle\phi_k|A|\phi_k\rangle, \quad [A, B] = AB - BA, \quad \{A, B\} = AB + BA.$$

С помощью элементарных преобразований получаем

$$P_k = 1 - \frac{T^2}{N^2}\Big\langle\Big(H - \Lambda - \langle H - \Lambda\rangle_k\Big)^2\Big\rangle_k + o\left(\frac{T^2}{N^2}\right). \quad (30)$$

Используя неравенство

$$\langle(A - \langle A\rangle)^2\rangle \leqslant \|A\|^2,$$

получаем

$$P_k \geqslant 1 - \frac{T^2\|H - \Lambda\|^2}{N^2} + o\left(\frac{T^2}{N^2}\right).$$

Тогда

$$P = P_0 P_1 \dots P_{N-1} \geqslant 1 - \frac{T^2\|H - \Lambda\|^2}{N} + o\left(\frac{T^2}{N}\right).$$

Теорема доказана. □

В задаче о перевороте спина можно выбрать $\Lambda = \sigma_y$. Тогда нужно положить $T = \pi/2$, так как $|2\rangle = e^{i\pi\sigma_y/2}|1\rangle$. Гамильтониан есть $H = \sigma_z$, причем $\|\sigma_z - \sigma_y\| = \sqrt{2}$. Оценка для населённости уровня $|2\rangle$, аналогичная формуле (9), имеет вид

$$\rho_{22}(N) \geqslant 1 - \frac{\pi^2}{2N} + o\left(\frac{1}{N}\right). \quad (31)$$

Разница между вариантами порядка $1/N$.

Теорема 4. *Пусть двухуровневая квантовая система описывается гамильтонианом и начальным состоянием*

$$H = h_0 \cdot \mathbb{I} + \boldsymbol{h}\cdot\boldsymbol{\sigma}, \quad \rho_0 = \frac{1}{2}[\mathbb{I} + \boldsymbol{a}\cdot\boldsymbol{\sigma}]$$

соответственно. Пусть в моменты времени t_k, $k = 1 \dots N$ производятся неселективные измерения проекторов $P_k = \frac{1}{2}\big[\mathbb{I} + \boldsymbol{\lambda}_k\cdot\boldsymbol{\sigma}\big]$ на состояния, описываемые векторами $\boldsymbol{\lambda}_k$, а между измерениями эволюция системы определяется гамильтонианом H. Рассмотрим целевой функционал $J_O = \operatorname{Tr}\big[\rho_T O\big]$, где ρ_T — матрица плотности в конечный момент времени T и $O = \lambda\cdot\mathbb{I} + \boldsymbol{\lambda}\cdot\boldsymbol{\sigma}$ — целевая наблюдаемая (H, ρ_0 и O — эрмитовы (2×2)-матрицы, а $\boldsymbol{\sigma}$ — вектор матриц Паули). Тогда значение целевого функционала J_O после N измерений равно

$$J_O = \lambda + \big(\boldsymbol{\lambda}\cdot R_{\boldsymbol{h},\varphi_N}\boldsymbol{\lambda}_N\big)\prod_{k=1}^{N-1}\big(\boldsymbol{\lambda}_{k+1}\cdot R_{\boldsymbol{h},\varphi_k}\boldsymbol{\lambda}_k\big)\big(\boldsymbol{\lambda}_1\cdot R_{\boldsymbol{h},\varphi_0}\boldsymbol{a}\big). \quad (32)$$

Здесь $R_{\boldsymbol{h},\varphi}$ — оператор вращения вокруг оси $\boldsymbol{h}$ на угол φ против часовой стрелки,

$$\varphi_k = 2(t_{k+1} - t_k)|\boldsymbol{h}|, \quad t_{N+1} = T, \quad t_0 = 0.$$

Доказательство. Произвольная (2×2)-матрица плотности $\rho = \frac{1}{2}\big[\mathbb{I} + \boldsymbol{a}\cdot\boldsymbol{\sigma}\big]$ при измерении наблюдаемой величины, описываемой проектором $P = \frac{1}{2}\big[\mathbb{I} + \boldsymbol{\lambda}\cdot\boldsymbol{\sigma}\big]$ преобразуется по формуле (см. [16])

$$\rho \to \rho' = \frac{1}{2}\Big[\mathbb{I} + (\boldsymbol{a}\cdot\boldsymbol{\lambda})\boldsymbol{\lambda}\cdot\boldsymbol{\sigma}\Big] \quad (33)$$

Между измерениями матрица ρ преобразуется с помощью оператора унитарной эволюции

$$U_k = e^{-i(t_{k+1}-t_k)H} = e^{-i(t_{k+1}-t_k)h_0}e^{-i\boldsymbol{n}\cdot\boldsymbol{\sigma}\varphi_k/2} \quad (34)$$

по формуле

$$\rho \to \rho'' = U_k \rho {U_k}^\dagger = \frac{1}{2}\Big[\mathbb{I} + e^{-i\boldsymbol{n}\cdot\boldsymbol{\sigma}\varphi_k/2}\ \boldsymbol{a}\cdot\boldsymbol{\sigma}\ e^{i\boldsymbol{n}\cdot\boldsymbol{\sigma}\varphi_k/2}\Big], \tag{35}$$

где $\boldsymbol{n} = \boldsymbol{h}/|\boldsymbol{h}|$. Для того, чтобы преобразовать правую часть равенства (35), используем соотношение

$$e^{-i\boldsymbol{n}\cdot\boldsymbol{\sigma}\varphi/2}\ \boldsymbol{a}\cdot\boldsymbol{\sigma}\ e^{i\boldsymbol{n}\cdot\boldsymbol{\sigma}\varphi/2} = (R_{\boldsymbol{n},\varphi}\boldsymbol{a})\cdot\boldsymbol{\sigma}, \quad |\boldsymbol{n}| = 1, \tag{36}$$

где $R_{\boldsymbol{n},\varphi}$ — оператор вращения вокруг оси $\boldsymbol{n}$ на угол φ против часовой стрелки. Тогда соотношение (35) перейдет в

$$\rho \to \rho'' = U_k \rho {U_k}^\dagger = \frac{1}{2}\Big[\mathbb{I} + (R_{\boldsymbol{h},\varphi_k}\boldsymbol{a})\cdot\boldsymbol{\sigma}\Big]. \tag{37}$$

Последовательно применяя преобразования (37) и (33) к начальной матрице плотности ρ_0, получим матрицу плотности в конечный момент времени T:

$$\rho_T = \frac{1}{2}\left[\mathbb{I} + \prod_{k=1}^{N-1}\big(\boldsymbol{\lambda}_{k+1}\cdot R_{\boldsymbol{h},\varphi_k}\boldsymbol{\lambda}_k\big)\big(\boldsymbol{\lambda}_1\cdot R_{\boldsymbol{h},\varphi_0}\boldsymbol{a}\big)R_{\boldsymbol{h},\varphi_N}\boldsymbol{\lambda}_N\cdot\boldsymbol{\sigma}\right]. \tag{38}$$

Отсюда для функционала $J_O = \mathrm{Tr}[\rho_T O]$ получим формулу (32). □

6. Сравнение эффективности измерений в двухуровневой системе. Представляет интерес сравнение глобально оптимальных управлений, описываемых формулой (13), и управлений, которые описываются в формулировке теоремы 3. В качестве примеров рассмотрим задачи о повороте спина на 180° и на 90° градусов в двухуровневой квантовой системе с гамильтонианом $H = \sigma_z$. Цель управления состоит в том, чтобы в первом случае перевести систему из состояния $|1\rangle$ в состояние $|2\rangle$, а во втором случае из состояния $|1\rangle$ в состояние $(|1\rangle + |2\rangle)/\sqrt{2}$.

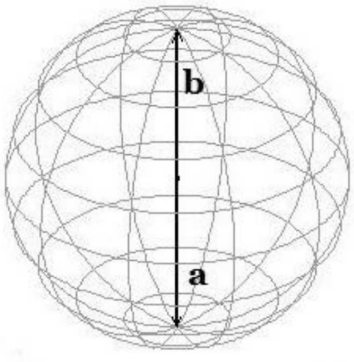

Рис. 1. Вектор $\boldsymbol{a}$, соответствующий состоянию $|1\rangle$, и вектор $\boldsymbol{b}$, соответствующий состоянию $|2\rangle$.

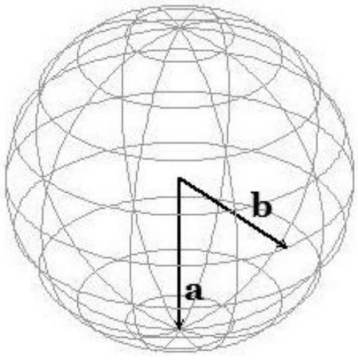

Рис. 2. Вектор $\boldsymbol{a}$, соответствующий состоянию $|1\rangle$, и вектор $\boldsymbol{b}$, соответствующий состоянию $(|1\rangle + |2\rangle)/\sqrt{2}$.

На рис. 1 показаны начальный вектор $\boldsymbol{a}$, соответствующий состоянию $|1\rangle$, и конечный вектор $\boldsymbol{b}$, соответствующий состоянию $|2\rangle$, в задаче о перевороте спина на 180° градусов. На рис. 2 показаны начальный вектор $\boldsymbol{a}$, соответствующий состоянию $|1\rangle$, и конечный вектор $\boldsymbol{b}$, соответствующий состоянию $(|1\rangle + |2\rangle)/\sqrt{2}$, в задаче о перевороте спина на 90° градусов.

В соответствии с теоремой 3 управление осуществляется с помощью измерения величин $A^{(k)} = e^{-i\varphi k\sigma_y/2} A e^{i\varphi k\sigma_y/2}$ в моменты времени $t_k = \varphi k/2$, где $\varphi = \pi/(N+1)$ для переворота спина на 180° градусов из состояния $|1\rangle$ в состояние $|2\rangle$ и $\varphi = \pi/2(N+1)$ для поворота спина на 90° градусов из состояния $|1\rangle$ в состояние $(|1\rangle + |2\rangle)/\sqrt{2}$. В соответствии с теоремой 3 величина A должна быть выбрана в виде проектора на состояние $|1\rangle$, так что $A = (\mathbb{I} - \sigma_z)/2$. Тогда

$$A^{(k)} = \frac{1}{2}(\mathbb{I} + \boldsymbol{\lambda}_k\cdot\boldsymbol{\sigma}) \tag{39}$$

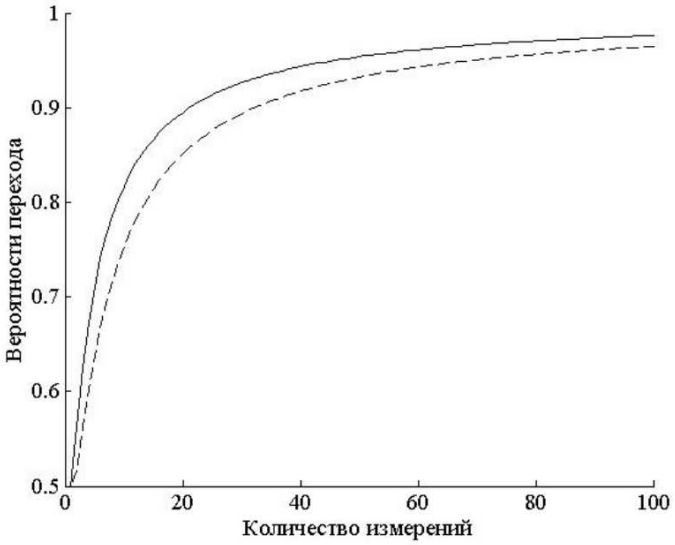

Рис. 3. Вероятности перехода из состояния $|1\rangle$ в состояние $|2\rangle$ в зависимости от количества измерений. Сплошная линия — вероятность для оптимальной последовательности измерений, даваемая формулой (8), пунктирная — вероятность (43) для измерений, определяемых величинами (39).

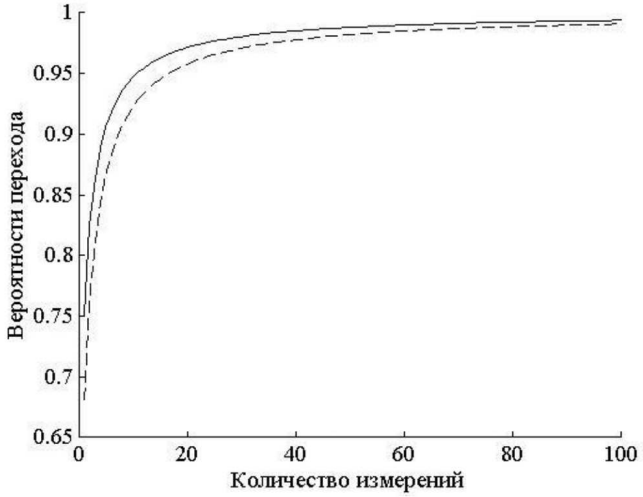

Рис. 4. Вероятности перехода из состояния $|1\rangle$ в состояние $(|1\rangle + |2\rangle)/\sqrt{2}$ в зависимости от количества измерений. Сплошная линия — вероятность для оптимальной последовательности измерений, даваемая формулой (8), пунктирная — вероятность (43) для измерений, определяемых величинами (39).

где

$$\boldsymbol{\lambda}_k = \sin(\varphi k)\boldsymbol{e}_x - \cos(\varphi k)\boldsymbol{e}_z. \tag{40}$$

Используя формулу (32), для вероятностей перехода $P_{i\to f}$ получим

$$P_{i\to f} = \frac{1}{2}\left(1 + \prod_{k=0}^{N}\left(\boldsymbol{\lambda}_{k+1}\cdot R_{z,\varphi}\boldsymbol{\lambda}_k\right)\right), \tag{41}$$

где

$$R_{z,\varphi}\boldsymbol{\lambda}_k = \sin(\varphi k)\cos\varphi\boldsymbol{e}_x + \sin(\varphi k)\sin\varphi\boldsymbol{e}_y - \cos(\varphi k)\boldsymbol{e}_z; \tag{42}$$

тогда выражение (41) для вероятности перехода $P_{i\to f}$ примет вид

$$P_{i\to f} = \frac{1}{2}\left(1 + \prod_{k=0}^{N}\Big\{\sin\varphi(k+1)\sin(\varphi k)\cos\varphi + \cos\varphi(k+1)\cos(\varphi k)\Big\}\right). \tag{43}$$

На рис. 3 показаны графики вероятностей перехода в двухуровневой системе из состояния $|1\rangle$ в состояние $|2\rangle$. На рис. 4 показаны аналогичные графики для перехода из состояния $|1\rangle$ в состояние $(|1\rangle + |2\rangle)/\sqrt{2}$. Сплошными линиями показаны графики вероятностей перехода для максимально эффективного управления (13), а пунктирными линиями — для измерений, определяемых величинами (39).

7. Заключение. В работе рассматривается задача максимизации целевого функционала, описывающего квантовое среднее заданной наблюдаемой в фиксированный момент времени. Проводится сравнение эффективности управления с помощью различных последовательностей неселективных измерений. Приводится выражение для вариации целевого функционала в задаче комбинированного управления, использующего воздействие на систему модулированного электромагнитного импульса и неселективные измерения.

СПИСОК ЛИТЕРАТУРЫ

1. *Иванов М. Г.* Как понимать квантовую механику. — Ижевск: РХД, 2012.
2. *фон Нейман Дж.* Математические основы квантовой механики. — М.: Наука, 1964.
3. *Печень А. Н., Ильин Н. Б.* О задаче максимизации вероятности перехода в n-уровневой квантовой системе с помощью неселективных измерений// Тр. Мат. ин-та им. В. А. Стеклова РАН. — 2011. — *294*. — С. 248–255.
4. *Халфин Л. А.* К теории распада квазистационарного состояния// Докл. АН СССР. — 1957. — *115*. — С. 277–280.
5. *Халфин Л. А.* К квантовой теории нестабильных элементарных частиц// Докл. АН СССР. — 1961. — *141*. — С. 599.
6. *Холево А. С.* Квантовые системы, каналы, информация. — М.: МЦНМО, 2010.
7. *Accardi L., Kozyrev S. V., Pechen A. N.* Coherent quantum control of Λ-atoms through the stochastic limit// in: *Quantum Information and Computing* (eds. Accardi L., Ohya M., Watanabe N.)/ QP–PQ: Quantum Probab. White Noise Anal. — Hackensack, New Jersey: World Scientific, 2006. — *19*. — С. 1–17.
8. *Accardi L., Lu Yun Gang, Volovich I. V.* Quantum theory and its stochastic limit. — Berlin: Springer-Verlag, 2002.
9. *Balachandran A. P., Roy S. M.* Quantum anti-Zeno paradox// Phys. Rev. Lett. — 2000. — *84*. — С. 4019.
10. *Balachandran A. P., Roy S. M.* Continuous time-dependent measurements: quantum anti-Zeno paradox with applications// Int. J. Mod. Phys. A. — 2002. — *17*. — С. 4007–4024.
11. *Belavkin V. P.* On the theory of controlling observable quantum systems// Automat. Remote Control. — 1983. — *44*, № 2. — С. 178.
12. *Fu S., Shi G., Proutiere A., James M. R.* Feedback policies for measurement-based quantum state manipulation// Phys. Rev. A. — 2014. — *90*. — С. 062328.
13. *Grishanin B. A., Zadkov V. N.* Entangling quantum measurements// Opt. Spectrosc. — 2004. — *96*. — С. 751–759.
14. *Misra B., Sudarshan E. C. G.* The Zeno's paradox in quantum theory// J. Math. Phys. — 1977. — *18*, № 4. — С. 756–763.
15. *Pechen A., Brif C., Wu R., Chakrabarti R., Rabitz H.* General unifying features of controlled quantum phenomena// Phys. Rev. A. — 2010. — *82*. — С. 030101.
16. *Pechen A. N., Il'in N. B., Shuang F., Rabitz H.* Quantum control by von Neumann measurements// Phys. Rev. A. — 2006. — *74*. — С. 052102.
17. *Shuang F., Pechen A., Ho T.-S., Rabitz H.* Observation-assisted optimal control of quantum dynamics// J. Chem. Phys. — 2007. — *126 (13)*. — С. 134303.

18. *Vilela Mendes R., Man'ko V. I.* Quantum control and Strocci map// Phys. Rev. A. — 2003. *67*. — С. 053404.
19. *Wiseman H. M., Milburn G. J.* Quantum theory of optical feedback via homodyne detection// Phys. Rev. Lett. — 1993. — *70*. — С. 548.

Ильин Николай Борисович
Математический институт им. В. А. Стеклова РАН
E-mail: ilyn@mi.ras.ru

Печень Александр Николаевич
Национальный исследовательский технологический университет «МИСиС», Москва;
Математический институт им. В. А. Стеклова РАН
E-mail: pechen@mi.ras.ru

ИТОГИ НАУКИ И ТЕХНИКИ.
Современная математика и ее приложения.
Тематические обзоры.
Том 138 (2017). С. 60–75

УДК 517.958:530.145, 519.85

КВАНТОВЫЙ АЛГОРИТМ ВЕТВЕЙ И ГРАНИЦ И ЕГО ПРИМЕНЕНИЕ К ЗАДАЧЕ КОММИВОЯЖЕРА

© 2017 г. **Е. А. МАРКЕВИЧ, А. С. ТРУШЕЧКИН**

Аннотация. Предложен квантовый алгоритм ветвей и границ на основе сочетания общей схемы метода ветвей и границ с квантовым алгоритмом вложенного поиска. Исследуется его вычислительная эффективность в сравнении с аналогичным классическим алгоритмом на примере задачи коммивояжера. Показывается, что в подавляющем большинстве задач классический алгоритм превосходит по скорости квантовый за счет большей адаптивности. Тем не менее, время работы квантового алгоритма постоянно для всех задач, тогда как классический алгоритм на некоторых задачах работает очень медленно. В результате для наихудшего случая квантовый алгоритм ветвей и границ оказался в несколько раз эффективнее классического алгоритма.

Ключевые слова: квантовые вычисления, квантовый компьютер, квантовый поиск, алгоритм Гровера, метод ветвей и границ, задача коммивояжера.

AMS Subject Classification: 81P68, 68Q12

СОДЕРЖАНИЕ

1. Введение

Алгоритм Гровера (см. [19]) является одним из наиболее известных квантовых алгоритмов. Он осуществляет поиск в неупорядоченной базе данных, обеспечивая квадратичное ускорение по сравнению с классическим (т.е. неквантовым, выполненным в традиционной парадигме вычислений) перебором. А именно, если база данных имеет размер N и содержит M объектов, удовлетворяющих условиям поиска, то алгоритм Гровера позволяет найти один из таких объектов за время порядка $O(\sqrt{N/M})$, тогда как классический перебор требует время порядка $O(N/M)$. Недавно был предложен обобщенный алгоритм Гровера (см. [26]), который обеспечивает тот же результат даже в том случае, когда число искомых объектов M заранее не известно, при этом он не использует промежуточных измерений, т.е. работает, не нарушая когерентность.

В [7] в качестве обобщения алгоритма Гровера предложен алгоритм решения более общей задачи — так называемой задачи усиления амплитуды квантового состояния. На основе алгоритма поиска Гровера и алгоритма усиления амплитуды были разработаны квантовые алгоритмы решения ряда задач, которые эффективнее классических алгоритмов (см. обзор [4]).

Однако на практике задача поиска в неупорядоченной базе данных встречается довольно редко. Обычно мы имеем дело с данными, упорядоченными в той или иной форме, что позволяет

Исследование выполнено при поддержке гранта Президента Российской Федерации (проект МК-2815.2017.1).

ускорить поиск. Представляет интерес разработка квантовых алгоритмов поиска в упорядоченных структурах данных и исследование преимущества, которое они могут дать по сравнению с классическими алгоритмами поиска в упорядоченных структурах. Так, в [20, 17, 10] разработаны квантовые алгоритмы поиска в упорядоченном списке.

В ряде случаев множество поиска можно представить в виде дерева. Такой случай рассматривается в [8] на примере задачи удовлетворения ограничений. Пусть даны n переменных, каждая из которых может принимать l различных значений, и конечное множество ограничений, в каждом из которых участвуют m переменных, $m < n$. Требуется найти одну такую комбинацию значений переменных, которая удовлетворяет всем ограничениям, или сделать вывод об отсутствии такой комбинации (отсутствии решения). Множество поиска в этом случае можно представить в виде дерева глубины n, в котором каждая вершина (кроме вершин последнего уровня n) имеет l непосредственных потомков: l вершин дерева первого уровня (корень дерева считается вершиной нулевого уровня) соответствуют l значениям, назначаемым первой переменной (считаем, что переменные упорядоченны), каждый из l потомков этих вершин соответствуют значениям, назначаемым второй переменной и т. д. На каждом уровне дерева $k < n$ часть ветвей может отсекаться. Это происходит, если комбинация значений первых k переменных, соответствующая вершине уровня k дерева, нарушает одно или несколько ограничений, включающих эти переменные. Частичными решениями уровня $k < n$ называются такие комбинации значений первых k переменных, которые не нарушают никакое из ограничений.

Характерным примером задачи такого вида является задача раскраски графа. Она заключается в том, чтобы поставить в соответствие каждой вершине графа один из l цветов так, чтобы никакие смежные вершины не имели одинаковый цвет. Если граф имеет n вершин, то n переменных задачи соответствуют цвету каждой вершины. Переменная может принимать l значений. Ограничений в задаче столько, сколько ребер в графе, и каждое ограничение включает в себя $m = 2$ переменные.

Представление множества поиска в виде дерева позволяет ускорить как классический поиск, так и квантовый. В [8] предложен алгоритм квантового вложенного поиска. Первоначально производится поиск частичных решений среди всех вариантов раскраски некоторого количества $k < n$ вершин. Затем производится поиск полных решений (которым соответствуют листья дерева поиска) только среди потомков частичных решений. Эта процедура обобщается и на случай многократных вложений. В [8] показывается, что квантовый вложенный поиск обеспечивает ускорение по сравнению с аналогичным классическим вложенным поиском.

В настоящей работе рассматривается другой метод структурированного поиска, который также использует представление множества поиска в виде дерева. Речь идет о методе ветвей и границ, широко применяемом в линейном целочисленном программировании и комбинаторной оптимизации (см. [1, 2, 27]).

В данной работе представлено обобщение метода ветвей и границ на квантовый случай на основе сочетания общей схемы метода ветвей и границ с алгоритмом квантового вложенного поиска. В развитие работы [8] предлагается, во-первых, расширение применение алгоритма квантового вложенного поиска на класс задач, решаемых методом ветвей и границ, а во-вторых, более тщательный анализ самого алгоритма вложенного поиска: оптимизация его параметров и его сравнение с классическими алгоритмами метода ветвей и границ по эффективности.

В качестве задачи, на примере которой мы рассматриваем квантовый метод ветвей и границ, мы взяли евклидову задачу коммивояжера, которая, как известно, является NP-полной задачей. Известный результат в области квантовых вычислений гласит, что не существует эффективного (полиномиального) квантового алгоритма решения NP-полных задач, который не использует структуру множества поиска задачи (см. [5]). Поэтому данную работу можно рассматривать как продвижение в направлении разработки квантовых алгоритмов решения NP-полных задач, использующих структуру множества поиска. Однако полиномиального времени решения достичь пока все еще не удается.

К настоящему моменту известны несколько квантовых алгоритмов решения NP-полных задач, превосходящих в эффективности классические алгоритмы: задачи выполнимости булевых формул (в ее различных вариациях) и задачи поиска гамильтонова цикла в графе (см. [4, 23]). Также отметим широкую деятельность по квантовым алгоритмам вычисления логических формул, в которых задача также представляется в виде дерева (см. [16, 11, 24, 9]).

Дальнейший текст организован следующим образом. В разделе 2 описывается общая схема метода ветвей и границ. В разделе 3 приводятся основные сведения об обобщенном алгоритме Гровера. В разделе 4 обсуждается схема квантового алгоритма ветвей и границ на основе алгоритма квантового вложенного поиска. В разделе 5 проводится сравнение вычислительной сложности работы квантового и классического алгоритмов ветвей и границ на примере евклидовой задачи коммивояжера, обсуждаются недостатки и преимущества квантового алгоритма ветвей и границ. Раздел 6 содержит выводы.

2. Метод ветвей и границ

Задачи поиска, решаемые методом ветвей и границ, имеют следующий общий вид (см. [27]). Пусть $\mathscr{X}$ — (конечное) множество поиска. Пусть дана функция $f : \mathscr{X} \to \mathbb{R}$, которая ставит в соответствие каждому элементу x его «стоимость» $f(x)$. Для заданного L требуется найти такой элемент x, что $f(x) \leqslant L$, или сделать вывод об отсутствии такого элемента (отсутствии решения). Таким образом, задача может быть формально записана в виде тройки $(\mathscr{X}, f, L)$. Примерами таких задач являются задача линейного целочисленного программирования, задача коммивояжера, задача об укладке рюкзака и многие другие.

Для того чтобы определить конкретный алгоритм, реализующий метод ветвей и границ, необходимо определить следующие элементы.

(a) Правило ветвления, определяющее разбиение произвольного подмножества поиска $\mathscr{X}' \subset \mathscr{X}$ на более мелкие подмножества: $\mathscr{X}' = \mathscr{X}'_1 \sqcup \ldots \sqcup X'_l$. Рекурсивное применение данного правила, начиная со всего множества $\mathscr{X}$, представляет множество поиска в виде дерева. Вершинами дерева являются подмножества множества решений. Условием прекращения ветвления является наличие решения подзадачи $(\mathscr{X}', f, L)$ либо доказательство отсутствия решения этой подзадачи. Примером является ситуация, когда $\mathscr{X}'$ состоит из одного элемента x. Если $f(x) \leqslant L$, то x является решением, в противном случае решение этой подзадачи отсутствует. Другим примером доказательства отсутствия решения, является оценка $f^*(\mathscr{X}') > L$ (см. следующий пункт). Наконец, решение задачи может быть получено в ходе алгоритма вычисления $f^*(\mathscr{X}')$, пример будет приведен ниже при рассмотрении конкретной реализации метода.

(b) Функцию $f^* : 2^{\mathscr{X}} \to \mathbb{R}$ оценки снизу минимального элемента подмножества-аргумента $\mathscr{X}' \subset X$ (вершины дерева):

$$f^*(\mathscr{X}') \leqslant \min_{x \in \mathscr{X}'} f(x).$$

Если $\mathscr{X}'$ состоит из одного элемента x, то $f^*(\{x\}) = f(x)$. Применение данной функции позволяет отсечь бесперспективные ветви дерева: если $f^*(\mathscr{X}') > L$, то дальнейшее рассмотрение данной ветви бессмысленно. Подмножества (вершины дерева), нижние оценки которых не превосходят L, будем называть *частичными решениями*.

(c) Стратегию поиска, которая определяет порядок, в котором производится исследование вершин построенного на текущий момент дерева. Под исследованием вершины подразумевается ее ветвление и получение оценок f^* для сгенерированных потомков. Наиболее известны три стратегии: стратегия «лучший — первый», стратегия поиска в глубину и стратегия поиска в ширину, а также их комбинации и расширения. В стратегии «лучший — первый» на каждом шаге исследуется вершина с минимальным значением нижней оценки. В поиске в глубину исследуется один из потомков только что исследованной вершины (с целью как можно быстрее добраться до терминальной вершины дерева). В поиске в ширину последовательно исследуются все вершины определенного уровня, после чего происходит переход к следующему уровню.

За счет отсечения бесперспективных ветвей алгоритмы ветвей и границ работают обычно намного быстрее, чем алгоритмы полного перебора.

Квантовый алгоритм ветвей и границ мы будем сравнивать по эффективности с классическим алгоритмом ветвей и границ со стратегией поиска в глубину. Причина выбора стратегии поиска в глубину состоит в том, что она широко используется на практике, поскольку позволяет быстро находить субоптимальные решения. Так, в [27] показывается, что метод ветвей и границ с поиском в глубину позволяет за то же время находить лучшие субоптимальные решения задачи коммивояжера, нежели алгоритмы локального поиска, также широко используемые для решении этой задачи. В задачах разрешимости, где нет необходимости искать оптимальное решение (см. далее замечание 1), использование поиска в глубину тем более оправданно.

Алгоритм ветвей и границ решения задачи разрешимости с поиском в глубину реализуется как вычисление функции $S(\mathscr{X})$, где $S : 2^{\mathscr{X}} \to \mathscr{X} \cup \{\varnothing\}$ — функция, задаваемая рекурсивно в виде следующего алгоритма (для произвольного аргумента $\mathscr{X}' \subset \mathscr{X}$):

(1) В соответствии с заданным правилом ветвления выполняется разбиение множества $\mathscr{X}'$ на подмножества: $\mathscr{X}' = \mathscr{X}'_1 \sqcup \ldots \sqcup X'_l$.
(2) В соответствии с заданной функцией нижней оценки f^* вычисляются значения $f^*(\mathscr{X}'_1), \ldots, f^*(\mathscr{X}'_l)$. Подмножества $\mathscr{X}'_1, \ldots, \mathscr{X}'_l$ сортируются по возрастанию их нижних оценок. Обозначим отсортированный таким образом набор множеств как $\mathscr{X}^{(1)}, \ldots, \mathscr{X}^{(l)}$.
(3) Введем переменную i с начальным значением $i = 1$.
(4) Если $f^*(\mathscr{X}^{(i)}) > L$, то $S(\mathscr{X}') := \varnothing$. В противном случае проверяется следующее условие: если $\mathscr{X}^{(i)}$ состоит из одного элемента x, то $S(\mathscr{X}') := x$. В противном случае вычисляется функция $S(\mathscr{X}^{(i)})$. Если $S(\mathscr{X}^{(i)}) = x \in \mathscr{X}$, то $S(\mathscr{X}') := x$. Если $S(\mathscr{X}^{(i)}) = \varnothing$, то увеличиваем значение i на единицу и повторяем действия этого шага. Если $i = l$ (т.е. $S(\mathscr{X}^{(i)}) = \varnothing$ для всех $i = 1, \ldots, l$), то $S(\mathscr{X}') := \varnothing$.

Таким образом, функция $S(\mathscr{X})$ выдает решение $x \in \mathscr{X}$, удовлетворяющее условию $f(x) \leqslant L$, либо значение $\varnothing$ в случае отсутствия решения.

В данной работе мы будем рассматривать применение метода ветвей и границ к евклидовой задаче коммивояжера. Пусть в единичном квадрате даны n точек («городов»). Задача заключается в том, чтобы найти циклический обход всех городов с суммарной длиной пути, не превышающей заданное значение L.

Существуют различные способы представления множества поиска в виде дерева: как различные способы ветвления, так и различные способы нижней оценки (см. [1, 27]). Приведем здесь один из таких способов, который мы будем использовать в данной работе.

Опишем правило ветвления. Город начала обхода считаем фиксированным. Ему соответствует корневая вершина дерева. Далее необходимо выбрать первый город, который мы посещаем. Выбор можно осуществить $n-1$ способами. Им соответствуют $n-1$ вершин дерева первого уровня. Далее выбирается второй город из $n-2$ оставшихся. Вариантам выбора соответствуют $n-2$ потомков каждой вершины дерева первого уровня. И так далее. Дерево имеет глубину $n-2$ (когда выбраны $n-2$ последовательных пункта маршрута, то окончание маршрута фиксированно: посещение последнего оставшегося города и возвращение в исходный город), вершины дерева на уровне k имеют $n-k-1$ потомков каждая. Отметим, что мы здесь описали дерево при отсутствии отсечений ветвей с помощью функции нижней оценки.

Пусть определена часть маршрута. Тогда функция нижней оценки определяется как сумма следующих величин:

(1) длина уже сформированной части маршрута;
(2) вес минимального остовного (покрывающего) дерева, построенного на непосещенных городах;
(3) минимальное расстояние от первой точки сформированной части маршрута до одного из непосещенных городов;
(4) минимальное расстояние от последней точки сформированной части маршрута до одного из непосещенных городов.

Отметим, что если объединение сформированной части маршрута, минимального остовного дерева и отрезков, соединяющих начальную и конечную точки с ближайшими непосещенными городами, дает замкнутый маршрут длины, меньшей L, то это означает, что получено решение рассматриваемой задачи $(\mathcal{X}', f, L)$ и дальнейшее ветвление можно не производить. О возможности такой ситуации говорилось выше при описании метода ветвей и границ.

Также заметим, что данная реализация метода ветвей и границ сближает задачу с задачами удовлетворения ограничений, описанных во введении: каждая ветвь здесь также соответствует вариантам значений очередной переменной (номеру следующего города). Отличие заключается в том, что ограничение здесь одно, но включает все переменные сразу. Поэтому для отсечения бесперспективных ветвей используется не простая проверка ограничения, а более нетривиальный метод — метод нижней оценки.

Замечание 1. Подчеркнем, что в данной работе мы рассматриваем не задачи оптимизации, в которых требуется найти элемент x с минимальным значением $f(x)$, а задачи разрешимости (поиска), в которой достаточно найти x, для которого значение $f(x)$ не превышает L, но не обязательно минимальное. Это сделано потому, что задачу разрешимости такого вида можно представить в виде задачи вложенного поиска, для которого разработан квантовый алгоритм. Если имеется эффективный алгоритм решения задачи разрешимости, то можно эффективно решить и задачу оптимизации. В самом деле, если последовательно решать задачи разрешимости при различных значениях L (понижая это значение, если на предыдущем этапе решение было получено, и повышая его в противном случае), то можно получить минимальное значение $f(x)$ и соответствующее значение x.

Квантовый алгоритм минимизации/максимизации (для неструктурированного пространства поиска) также существует (см. [15, 3, 22]), однако он основан именно на последовательном решении задач разрешимости (поиска).

Более того, для многих практических ситуаций задача разрешимости может быть предпочтительнее задачи оптимизации. Так, например, задача нахождение оптимального маршрута коммивояжера является NP-трудной и при большой размерности не может быть решена за разумное время. В то же время, можно поставить задачу поиска маршрута, длина которого не превышает некоторое разумное значение L. При определенных L задача может быть решена быстро (см. [18]). Также можно привести пример следующей ситуации (взят из [18]), когда первична именно задача разрешимости: если почтовая служба обнаруживает, что не существует такого пути обхода домов, который позволяет пройти его одному человеку за один рабочий день, то почтовую корреспонденцию должны разносить два или более человек.

3. Обобщенный алгоритм Гровера

В данном разделе мы напомним оценку сложности поиска, которую обеспечивает вариант алгоритма Гровера, предложенный в [26] (будем называть его обобщенным алгоритмом Гровера). Пусть $\mathscr{H}$ — некоторое конечномерное гильбертово пространство, $|s\rangle \in \mathscr{H}$ — начальное состояние квантовой системы, $|t\rangle \in \mathscr{H}$ — некоторое целевое состояние. Алгоритм, предложенный в [26], обеспечивает преобразование $|s\rangle$ в суперпозицию

$$|s\rangle \to A\,|t\rangle + B\,|t^{\perp}\rangle\,,$$

где $|t^{\perp}\rangle$ — некоторый вектор, ортогональный $|t\rangle$. Величина $|A|^2$ есть вероятность успеха (при измерении проекции на вектор $|t\rangle$ мы получим положительный результат с данной вероятностью), $|B|^2 = 1 - |A|^2$ — вероятность ошибки. Для того чтобы обеспечить вероятность ошибки $|B|^2 \leqslant \varepsilon$, алгоритм должен осуществить

$$T = \frac{1}{\sqrt{\lambda}} \ln \frac{4}{\varepsilon} \tag{1}$$

или более вычислений функции проверки условий поиска (т.е. функции, аргументом которой является объект множества поиска, а результатом — двоичная переменная, указывающая, удовлетворяет ли объект условиям поиска) и столько же выполнений процедуры создания начального состояния $|s\rangle$. Здесь $\lambda = |\,\langle t|s\rangle\,|^2$.

С точки зрения задачи поиска данный результат интерпретируется следующим образом. Пусть базисные векторы $\mathscr{H}$ соответствуют объектам из некоторого множества поиска мощности N. Соответственно, $\dim \mathscr{H} = N$. Вектор

$$|s\rangle = \frac{1}{\sqrt{N}} \sum_{x=1}^{N} |x\rangle$$

представляет собой равномерную суперпозицию всех элементов поиска, $\{|x\rangle\}_{x=1}^{N}$ — ортонормированный базис. Пусть, далее, среди элементов x существуют $M \leqslant N$ элементов, которые удовлетворяют условиям поиска. Данное подмножество будем называть множеством решений. Будем обозначать их $|y\rangle$, $y = 1, \ldots, M$ (т.е., мы пронумеровали элементы множества поиска таким образом, что искомые объекты имеют номера от 1 до M). Тогда целевой вектор имеет вид равномерной суперпозиции элементов множества решений:

$$|t\rangle = \frac{1}{\sqrt{M}} \sum_{y=1}^{M} |y\rangle \,.$$

В этом случае $\lambda = M/N$ и алгоритм обеспечивает вероятность ошибки не более ε при количестве проверок условий поиска

$$T = \sqrt{\frac{N}{M}} \ln \frac{4}{\varepsilon} \tag{2}$$

или более. Сложность классического перебора (которую также можно определить как количество проверок условий поиска) составляет $O(N/M)$, т.е. квантовый алгоритм поиска обеспечивает квадратичное ускорение по сравнению с классическим.

Если мы не знаем мощность множества решений M, то мы можем оценить ее снизу тривиальным образом, т.е. единицей, что дает формулу

$$T = \sqrt{N} \ln \frac{4}{\varepsilon}. \tag{3}$$

В исходном варианте алгоритма Гровера (см. [19]) слишком большое количество итераций, например, применение формулы (3) вместо формулы (2) при $M > 1$, влечет за собой уменьшение вероятности успеха вплоть до величин, близких к нулю. В обобщенном алгоритме Гровера нет такой проблемы: при неизвестном M можно использовать и формулу (3). Тем не менее, нетривиальная оценка снизу величины M (или, в более общем случае, λ) позволяет воспользоваться формулой (2) (соответственно, (1)) и тем самым понизить сложность вычислений.

4. Квантовый метод ветвей и границ

Перейдем теперь к описанию квантового алгоритма ветвей и границ. В его основе лежит общая схема метода ветвей и границ, описанная в разделе 2, в сочетании с квантовым алгоритмом вложенного поиска. Конкретную реализацию описанной ниже схемы квантового вложенного поиска в виде квантовых последовательности унитарных операторов см. в [8] со следующей поправкой: унитарные операторы, реализующие базовый алгоритм Гровера (как часть алгоритма вложенного поиска) следует заменить на обобщенный алгоритм Гровера из [26].

Пусть нам дана задача $(\mathscr{X}, f, L)$. В соответствии с общей схемой метода ветвей и границ пусть нам даны правило ветвления и функция нижней оценки. Они определяют представление множества поиска в виде дерева. В дальнейшем под деревом поиска будем понимать полное дерево, которое образуется в результате рекурсивного применения правила ветвления, т.е. без учета отсечений ветвей. Для простоты будем предполагать, что дерево поиска однородно в том смысле, что все терминальные вершины находятся на одной глубине n и что количество непосредственных потомков одинаково для всех вершин одного уровня (но может отличаться для вершин разных уровней). Это предположение выполнено для реализации метода ветвей и границ для задачи коммивояжера, описанной в разделе 2. Однако оно не является принципиальным, и представленный ниже алгоритм можно адаптировать и для общего случая.

В соответствии со схемой квантового алгоритма вложенного поиска необходимо задать уровни дерева $1 \leqslant k_1 < k_2 < \ldots < k_m < n \equiv k_{m+1}$ (напомним, что корень дерева считается нулевым уровнем), на которых алгоритм будет искать частичные решения. Частичные решения уровня k_i, $i \geqslant 2$, ищутся среди потомков частичных решений уровня k_{i-1}. В отличие от классического метода ветвей и границ в квантовом случае не всегда оптимально производить поиск частичных решений последовательно на каждом уровне. Как число промежуточных уровней поиска m, так и сами номера уровней $k_1, \ldots, k_m$ представляют собой параметры задачи и, вообще говоря, подлежат оптимизации.

Введем также следующие обозначения. Обозначим через N_i количество вершин дерева поиска на уровне k_i, через N_n — количество вершин на последнем уровне (мощность полного множества поиска), через M_i — количество частичных решений на уровне k_i. Соответственно, M_n — количество полных решений задачи. Далее, N'_i — количество потомков на уровне k_i у одной вершины на уровне k_{i-1} (т.е. $N_i = N_{i-1}N'_i$), N'_n — количество потомков на уровне n у одной вершины на уровне k_m (т.е. $N_n = N_m N'_n$). Наконец, $M'_i \leqslant M_i$ — количество частичных решений на уровне k_i, которые имеют потомков среди частичных решений на уровне k_{i+1}. Например, в задаче коммивояжера нижняя граница пути маршрута, соответствующему некоторой вершине уровня k_i может не превышать L, но уточнение нижней оценки для всех потомков этой вершины до уровня k_j может дать значения выше L, в результате чего все потомки этой вершины отсекаются, т.е. $M'_i \leqslant M_i$.

Гильбертово пространство, в котором производится вычисление, есть

$$\mathscr{H} = \mathscr{H}_1 \otimes \mathscr{H}'_2 \otimes \ldots \otimes \mathscr{H}'_m \otimes \mathscr{H}'_n,$$

где $\dim \mathscr{H}_1 = N_1$, $\dim \mathscr{H}'_i = N'_i$, $i = 2, \ldots, m$, $\dim \mathscr{H}'_n = N'_n$. Введем также обозначение

$$\mathscr{H}_i = \mathscr{H}_1 \otimes \mathscr{H}'_2 \otimes \ldots \otimes \mathscr{H}'_i,$$

$\dim \mathscr{H}_i = N_i$. Первым шагом алгоритма является создание равномерной суперпозиции состояний

$$|\psi\rangle = |\psi_1\rangle\,|\psi_2\rangle \cdots |\psi_m\rangle\,|\psi_n\rangle = \frac{1}{\sqrt{N_n}} \sum_{x_1=1}^{N_1} \sum_{x_2=1}^{N'_2} \ldots \sum_{x_m=1}^{N'_m} \sum_{x_n=1}^{N'_n} |x_1\rangle\,|x_2\rangle \cdots |x_m\rangle\,|x_n\rangle\,,$$

где

$$|\psi_i\rangle = \frac{1}{\sqrt{N'_i}} \sum_{x_i=1}^{N'_i} |x_i\rangle \in \mathscr{H}'_i, \tag{4}$$

x_i нумерует потомков на уровне k_i одной вершины уровня k_{i-1}. Листья дерева и наборы чисел $(x_1, \ldots, x_n)$ находятся во взаимооднозначном соответствии: x_1 задает вершину уровня k_1, x_2 Э— ее потомка на уровне k_2 и т. д.

Вычисление нижней оценки в методе ветвей и границ может быть достаточно трудоемкой задачей, которая вносит основной вклад в сложность алгоритма. По этой причине под сложностью алгоритма мы будем понимать количество вычислений функции нижней оценки (см. [27, 18]).

Алгоритм квантового вложенного поиска может быть описан рекурсивным образом. Опишем рекурсивный алгоритм «поиск частичных решений на уровне дерева k_i»:

(1) Если $i = 1$, то в пространстве $\mathscr{H}_1$ выполняется обобщенный алгоритм Гровера для поиска частичных решений на уровне k_1. А именно, начальная суперпозиция имеет вид $|\psi_1\rangle \in \mathscr{H}_1$ (см. (4)), а целевой вектор является равномерной суперпозицией частичных решений (обозначим их y_1):

$$|\varphi_1\rangle = \frac{1}{\sqrt{M_1}} \sum_{y_1=1}^{M_1} |y_1\rangle \in \mathscr{H}_1.$$

Поскольку $\langle\varphi_1|\psi_1\rangle = \sqrt{M_1/N_1}$, то этот этап требует

$$T_1 = \sqrt{\frac{N_1}{M_1}} \ln \frac{4}{\varepsilon} \tag{5}$$

вычислений функции нижней оценки при вероятности ошибки не более ε. Выполнение функции «поиск частичных решений на уровне дерева k_1» завершается, на выходе имеем суперпозицию

$$|\widetilde{\psi}_1\rangle = A_1\,|\varphi_1\rangle + B_1\,|\varphi_1^{\perp}\rangle\,.$$

Здесь и далее верхний индекс $^{\perp}$ означает, что вектор ортогонален соответствующему вектору без данного индекса и тоже нормирован на единицу. Также здесь и далее подразумевается, что коэффициенты вида A_j и B_j удовлетворяют условиям $|A_j|^2 + |B_j|^2 = 1$, $|B_j|^2 \leqslant \varepsilon$.

Если $i \geqslant 2$, то в пространстве $\mathscr{H}_{i-1}$ выполняется алгоритм «поиск частичных решений на уровне дерева k_{i-1}». На выходе имеем суперпозицию

$$|\widetilde{\psi}_{i-1}\rangle = A_{i-1}\,|\varphi_{i-1}\rangle + B_{i-1}\,|\varphi_{i-1}^{\perp}\rangle\,, \tag{6}$$

$$|\varphi_{i-1}\rangle = \frac{1}{\sqrt{M_{i-1}}}\sum_{y_{i-1}=1}^{M_{i-1}} |y_{i-1}\rangle\,,$$

y_{i-1} нумеруют частичные решения уровня k_{i-1}. Обозначим вычислительную сложность этой процедуры через T_{i-1}. После чего переходим к этапу (2).

(2) Перед началом данного этапа состояние в пространстве $\mathscr{H}_i$ имеет вид

$$|\widetilde{\psi}_{i-1}\rangle\,|\psi_i\rangle = \frac{A_{i-1}}{\sqrt{M_{i-1}}}\sum_{y_{i-1}=1}^{M_{i-1}} |y_{i-1}\rangle\,|\psi_i\rangle + B_{i-1}\,|\varphi_{i-1}^{\perp}\rangle\,|\psi_i\rangle\,. \tag{7}$$

На данном этапе к $|\psi_i\rangle$ применяется последовательность унитарных преобразований, осуществляющих алгоритм Гровера в пространстве $\mathscr{H}_i'$, зависящая от y_{i-1}:

$$\frac{A_{i-1}}{\sqrt{M_{i-1}}}\sum_{y_{i-1}=1}^{M_{i-1}} |y_{i-1}\rangle\,|\psi_i\rangle \to \frac{A_{i-1}}{\sqrt{M_{i-1}}}\sum_{y_{i-1}=1}^{M_{i-1}} |y_{i-1}\rangle\,U(y_{i-1})\,|\psi_i\rangle\,.$$

Более формально, можно говорить об унитарных операторах $\widetilde{U}$ действующих в пространстве $\mathscr{H}_i$ по правилу

$$\widetilde{U}\,|y_{i-1}\rangle\,|\psi_i\rangle = |y_{i-1}\rangle\,U(y_{i-1})\,|\psi_i\rangle\,,$$

однако фактически речь идет о параллельном применении различных унитарных преобразований $U(y_{i-1})$ из пространства $\mathscr{H}_i'$ к каждому элементу суперпозиции. Поэтому «эффективное» начальное состояние есть $|\psi_i\rangle$, а целевое — равномерная суперпозиция потомков вершин уровня k_{i-1} на уровне k_i, соответствующих частичным решениям этого уровня (обозначим их y_i'):

$$|\varphi_i'(y_{i-1})\rangle = \frac{1}{\sqrt{M_i(y_{i-1})}}\sum_{y_i'=1}^{M_i(y_{i-1})} |y_i'\rangle\,,$$

где $M_i(y_{i-1})$ — количество потомков частичного решения y_{i-1} среди частичных решений уровня k_i. Скалярное произведение целевого состояния на начальное составляет $\sqrt{M_i(y_{i-1})/N_i'}$. Оценим снизу мощность множества решений $M_i(y_{i-1})$ тривиальным образом, т.е. единицей (некоторые вершины уровня k_{i-1} могут иметь только одного потомка — частичное решение уровня k_i), поэтому этот этап требует $\sqrt{N_i'}\ln(4/\varepsilon)$ функции нижней оценки при вероятности ошибки ε.

Последние рассуждения проведены для случая, когда $M_i(y_{i-1})$ положительно, т.е. вершина имеет по крайней мере одного потомка среди частичных решений на уровне k_i. Если это не так, т.е. $M_i(y_{i-1}) = 0$, то в результате применения обобщенного алгоритма Гровера начальное состояние не изменяется, равно как и в результате применения алгоритма к состоянию

$|\varphi_{i-1}^{\perp}\rangle\,|\psi_i\rangle$. Поэтому после этого этапа суперпозиция (7) преобразуется в

$$|\Psi_i\rangle = \frac{A_{i-1}}{\sqrt{M_{i-1}}} \sum_{y_{i-1}\in\mathscr{Y}_{i-1}} |y_{i-1}\rangle \left[A'_i\,|\varphi'_i(y_{i-1})\rangle + B'_i\,|\varphi'_i(y_{i-1})^{\perp}\rangle\right] + \frac{A_{i-1}}{\sqrt{M_{i-1}}} \sum_{y_{i-1}\notin\mathscr{Y}_{i-1}} |y_{i-1}\rangle\,|\psi_i\rangle + B_{i-1}\,|\varphi_{i-1}^{\perp}\rangle\,|\psi_i\rangle\,, \tag{8}$$

где $\mathscr{Y}_{i-1}$ — подмножество частичных решений уровня k_{i-1}, которые имеют потомков среди частичных решений уровня k_i, $|\mathscr{Y}_i| = M'_{i-1}$.

(3) Подавление в суперпозиции (8) вершин, не имеющих потомков среди частичных решений уровня k_i и приведение к равномерной суперпозиции оставшихся состояний, т.е. целевое состояние имеет вид

$$|\varphi_i\rangle = \frac{1}{\sqrt{M_i}} \sum_{y_i=1}^{M_i} |y_i\rangle\,, \tag{9}$$

где y_i — частичные решения уровня k_i. В обозначениях (8) каждое такое решение представимо в виде пары (y_{i-1}, y'_i), где $y_{i-1} \in \mathscr{Y}_{i-1}$. Соответственно, $|y_i\rangle = |y_{i-1}\rangle\,|y'_i\rangle$, поэтому (9) можно переписать в виде

$$|\varphi_i\rangle = \frac{1}{\sqrt{M_i}} \sum_{y_{i-1}\in\mathscr{Y}_{i-1}} \sum_{y'_i=1}^{M_i(y_{i-1})} |y_{i-1}\rangle\,|y'_i\rangle\,.$$

Тогда скалярное произведение начальной суперпозиции и целевого состояния по абсолютной величине составит

$$|\,\langle\varphi_i|\Psi_i\rangle\,| = |A_{i-1}A'_i| \sum_{y_{i-1}\in\mathscr{Y}_i} \sqrt{\frac{M_i(y_{i-1})}{M_i M_{i-1}}} \geqslant (1-\varepsilon) \sum_{y_{i-1}\in\mathscr{Y}_i} \sqrt{\frac{M_i(y_{i-1})}{M_i M_{i-1}}}.$$

Предположим дополнительно, что все положительные $M_i(y_{i-1})$ (при разных $y_{i-1} \in \mathscr{Y}_{i-1}$) приблизительно равны друг другу, т.е. $M_i(y_{i-1}) \approx M_i/M'_{i-1}$. Например, это выполнено тогда, когда максимальное значение $M_i(y_{i-1})$ равно единице (такое предположение сделано в [8]), более высокие значения маловероятны. Тогда

$$|\,\langle\varphi_i|\Psi_i\rangle\,| \geqslant (1-\varepsilon)\sqrt{\frac{M'_{i-1}}{M_{i-1}}},$$

и этот этап требует

$$\frac{1}{1-\varepsilon}\sqrt{\frac{M_{i-1}}{M'_{i-1}}}\ln\frac{4}{\varepsilon}$$

запусков этапов (1) и (2), т.е. выполнения процедуры создания начальной суперпозиции (8). Также этот этап требует такого же количество вычислений функции нижней оценки, но эта величина является пренебрежимо малой в сравнении с предыдущей: выполнение этапов (1) и (2) включает в себя множество вычислений функции нижней оценки. В результате данного этапа получается суперпозиция (6).

Таким образом, сложность алгоритма «поиск частичных решений на уровне дерева k_i» (количество вычислений функции нижней оценки) равна

$$T_i = \frac{1}{1-\varepsilon}\sqrt{\frac{M_{i-1}}{M'_{i-1}}}\ln\frac{4}{\varepsilon}\left[T_{i-1} + \sqrt{N'_i}\ln\frac{4}{\varepsilon}\right] \tag{10}$$

при общей вероятности ошибки не более ε.

Решение задачи может быть получено в результате выполнения алгоритма «поиск частичных решений на уровне дерева $k_{m+1} = n$» (т.е. это уже не частичные, а полные решения). Рекуррентное уравнение (10) с начальным условием (5) позволяют определить итоговую сложность алгоритма.

Замечание 2. Невыполнение условия приблизительного равенства друг другу всех положительных $M_i(y_{i-1})$ (при фиксированном i, см. обсуждение этапа (3)) не делает алгоритм полностью непригодным, но ослабляет амплитуды потомков вершин со значениями $M_i(y_{i-1})$ сильно выше среднего (которое равно M_i/M'_{i-1}). Если решение задачи находится только среди потомков именно таких вершин, то это, конечно, может привести к неверному выводу об отсутствии решения у задачи (амплитуда этих решений в конце будет существенно меньше единицы).

Поясним это утверждение. После окончания этапа (2), как видно из (8), если у некоторого частичного решения y_{i-1} уровня k_{i-1} имеется много потомков среди частичных решений уровня k_i, то все они имеют малую амплитуду (обратно пропорциональную $\sqrt{M_i(y_{i-1})}$). На этапе (3) мы должны выровнять амплитуды вероятностей частичных решений уровня k_i, являющихся потомками разных вершин уровня k_{i-1}. Если же мы рассчитываем количество итераций на этом этапе исходя из среднего значения $M_i(y_{i-1})$, то амплитуды потомков тех y_{i-1}, для которых $M_i(y_{i-1})$ сильно выше среднего, не успевают выровняться с общим уровнем при расчитанном количестве итераций.

Разумным предположением может быть то, что $M_i(y_{i-1})$ не может превышать среднее в определенное число K раз, т.е. $M_i(y_{i-1}) \leqslant KM_i/M'_{i-1}$. Это ведет к увеличению итераций на этапе (3) в $\sqrt{K}$ раз. В соответствии с рекуррентной формулой (10) общая сложность возрастет тогда в $\sqrt{K^{m+1}}$ раз по порядку величины.

Замечание 3. При вычислении сложности мы предполагали, что само построение дерева поиска не вносит вклад в сложность алгоритма, поскольку не обращается к функции вычисления нижней оценки. Для способа ветвления вершин в задаче коммивояжера, описанном в разделе 2, это в самом деле так. Однако в общем случае ветвление вершины может зависеть от результатов вычисления нижней оценки вершины (помимо собственно нижней оценки данная функция дает и другую информацию, в нашем случае — минимальное остовное дерево и отрезки, соединяющие начальную и конечную точку маршрута с ближайшими точками, не входящими в него). В этом случае при переходе от уровня k_{i-1} к уровню k_i необходимо построить участок дерева от уровня k_{i-1} к уровню k_i, вычислив нижние оценки в каждой вершине на этом участке. Поскольку это вычисление можно провести параллельно, одновременно для всех ветвей (в суперпозиции (4), (6)), то это увеличит сложность на $k_i - k_{i-1}$, а суммарно — на n.

Замечание 4. При описании классического метода ветвей и границ говорилось о выборе стратегии поиска («лучший — первый», поиск в глубину или в ширину) как одной из составляющих алгоритма. Представленный квантовый алгоритм реализует поиск одновременно в глубину и в ширину. В квантовой реализации различие между этими стратегиями стирается: квантовый параллелизм приводит к одновременному разветвлению всех вершин одного уровня, что соответствует поиску в ширину, но при этом на каждом шаге мы продвигаемся в глубину, т.е. расширение поиска по дереву не стоит нам задержки в углублении по нему.

Замечание 5. Отметим, что существует квантовый алгоритм вычисления веса минимального остовного дерева (см. [14]), который можно было бы использовать для дополнительного ускорения вычислений (помимо квантового поиска), однако он требует проведения измерений, что разрушает когерентность между различными ветвями поиска.

Ключевой проблемой при применении данного алгоритма является оценка неизвестных значений M_i и M'_i для определения необходимого количества итераций. Рассмотрим случай $m = 1$. Тогда сложность алгоритма составит

$$T_2 = \frac{1}{1-\varepsilon}\sqrt{\frac{M_1}{M'_1}}\ln\frac{4}{\varepsilon}\left[\sqrt{\frac{N_1}{M_1}}\ln\frac{4}{\varepsilon} + \sqrt{N'_n}\ln\frac{4}{\varepsilon}\right] = \frac{1}{1-\varepsilon}\left(\ln\frac{4}{\varepsilon}\right)^2\frac{\sqrt{N_1}+\sqrt{M_1N'_n}}{\sqrt{M'_1}}.$$

Для того чтобы надежно определить достаточное количество итераций для обеспечения заданной вероятности успеха, необходимо оценить M_1 сверху, а M'_1 — снизу. Если мы применим тривиальные оценки $M_1 \leqslant N_1$ и $M'_1 \geqslant 1$, то, с учетом $N_1N'_n = N_n$, сложность квантового алгоритма вложенного поиска превысит сложность квантового полного перебора всех вариантов, которая

составляет $\sqrt{N_n}\ln(4/\varepsilon)$ и, соответственно, превысит сложность классического структурированного поиска (который не требует априорного знания величин M_1 и M_1').

Итак, для того чтобы квантовый алгоритм вложенного поиска работал более эффективно, нежели квантовый алгоритм полного перебора и классические алгоритмы структурированного поиска (например, классические алгоритмы ветвей и границ), необходимы нетривиальные оценки величин M_i и M_i'. Для многих задач получение этих оценок может представлять существенные трудности.

5. Применение квантового метода ветвей и границ к решению задачи коммивояжера

В этом разделе мы сравним эффективность предложенного квантового алгоритма ветвей и границ с классическим алгоритмом ветвей и границ с поиском в глубину на примере евклидовой задачи коммивояжера. Описание классического алгоритма ветвей и границ, с которым будет производится сравнение, приведено в разделе 2. Для квантового алгоритмы мы будем использовать те же способ ветвления и функцию нижней оценки.

Будем рассматривать случайные евклидовы задачи коммивояжера: для каждой задачи генерируются n случайных точек («городов») в единичном квадрате в соответствии с равномерным распределением, независимо друг от друга.

Как сказано в конце предыдущего раздела, для эффективной работы квантового алгоритма необходимо получить нетривиальные оценки величин M_i и M_i'.

Решим более простую задачу. Рассмотрим случайную евклидову задачу коммивояжера и случайную вершину на уровне k в дереве поиска для этой задачи. Определим вероятность $p_k(L)$ того, что нижняя оценка для нее не превышает L, в пределе больших n. Отметим, что аналогичная анализ проводится и в [8]: вместо оценки доли частичных решений на определенном уровне дерева для фиксированной случайной задачи там тоже рассматривается вероятность того, что случайная вершина в случайной задаче является частичным решением.

Обратимся к слагаемым нижней оценки, перечисленным в разделе 2. Если k мало, то основной вклад в нижнюю оценку вносит вес минимального остовного дерева, построенного на $n-k$ непосещенных городах, поскольку число $n-k$ велико. Если, напротив, $n-k$ мало, то это означает, что велико k и основной вклад в нижнюю оценку вносит длина уже сформированной части маршрута. Если обе величины k и $n-k$ велики, то вклады в нижнюю оценку длины уже сформированной части маршрута и веса минимального остовного дерева могут быть сопоставимы.

Во всех случаях минимальные расстояния от первой и последней точек сформированного частичного маршрута до непосещенных городов является либо малым (при больших k), либо остается конечным (при малых k), тогда как слагаемое, дающее основной вклад, стремится к бесконечности при больших n. Следовательно, этими слагаемыми можно пренебречь.

Выясним сначала распределение длины частичного маршрута через k городов при больших k. Поскольку мы рассматриваем случайную вершину дерева в случайной задаче, то речь идет о распределении длины маршрута через k случайных точек $\{(x_i, y_i)\}_{i=1}^k$ в единичном квадрате (иными словами, длины случайной ломаной). Длина равна

$$R_k = l_1 + \ldots + l_{k-1},$$

где

$$l_i^2 = (x_{i+1} - x_i)^2 + (y_{i+1} - y_i)^2.$$

Поскольку случайные величины l_i и l_{i+2} являются независимыми, то к последовательности $l_1, l_2, \ldots$ применима центральная предельная теорема для слабо зависимых случайных величин (см. [6]): при больших k длину R_k можно считать нормально распределенной случайной величиной с

$$\mathsf{M}R_k \approx (k-1)\mathsf{M}l_1,$$
$$\mathsf{D}R_k \approx (k-1)[\mathsf{D}l_1 + \operatorname{cov}(l_1, l_2)],$$

где M, D и cov обозначают математическое ожидание, дисперсию и ковариацию соответственно. Вычисляя величины, стоящие в правых частях, получаем $\mathsf{M}R_k \approx 0{,}521(k-1)$, $\mathsf{D}R_k \approx 0{,}075(k-1)$.

Определим теперь распределение веса W_{n-k} остовного дерева, построенного на случайных $n-k$ точках в единичном квадрате, предполагая, что $n-k$ велико (иначе, как сказано выше, этим слагаемым можно пренебречь по сравнению с длиной частичного маршрута). Для веса минимального остовного дерева, построенного на случайных точках в единичном квадрате, также доказана центральная предельная теорема (см. [21]), причем дисперсия веса минимального остовного дерева не зависит от числа точек $n-k$. Численно нами было получено приблизительное значение для дисперсии 0,05. В [25] доказано, что $\sqrt{n}W_{n-k}$ сходится по вероятности к некоторой константе $c(2)$ (число 2 здесь означает размерность). В [12] численно получено значение этой константы: $c(2) = 0{,}6331 \pm 0{,}0013$. Поэтому в качестве приблизительного значения математического ожидания W_{n-k} можно принять число $c(2)\sqrt{n-k} \approx 0{,}633\sqrt{n-k}$.

Длина частичного маршрута и вес минимального остовного дерева являются независимыми случайными величинами, поскольку эти объекты строятся на непересекающихся множествах случайных точек, которые генерируются независимо друг от друга. Поэтому нижнюю оценку B при больших n для случайной вершины уровня k в случайной задаче можно нормально распределенной случайной величиной со средним и дисперсией

$$\mathsf{M}B \approx 0{,}521(k-1) + 0{,}633\sqrt{n-k}, \quad \mathsf{D}B \approx 0{,}075(k-1) + 0{,}050.$$

Следовательно,

$$p_k(L) = \frac{1}{2} + \frac{1}{2}\Phi\left(\frac{L - \mathsf{M}B}{\sqrt{2\mathsf{D}B}}\right), \tag{11}$$

где

$$\Phi(x) = \frac{2}{\sqrt{\pi}} \int\limits_0^x e^{-t^2}\,dt$$

— фунция Лапласа.

Численные расчеты показывают, что формула (11) дает почти идеальное совпадение с эмпирическими значениями $p_k(L)$. Однако напомним, что мы оценили не среднюю долю частичных решений на уровне дерева k для случайной задачи, которая нам необходима, а другую величину — вероятность того, что случайная вершина дерева уровня k для случайной задачи окажется частичным решением. Расчеты показывают, что эти величины могут отличаться на несколько порядков (см. таблицу 1). Происходит это оттого, что нижние оценки вершин одного дерева не являются независимыми случайными величинами. Таким образом, $p_{k_i}(L)N_i$ не может использоваться в качестве приближенной оценки M_i.

По причине отсутствия аналитических оценок для M_i и M_i' мы получали эти оценки эмпирическим путем: через прямой подсчет частичных решений и усреднение по нескольким случайным задачам. Эта процедура очень трудоемка, и с практической точки зрения полный перебор дерева, разумеется, неприемлем. Однако нашей целью является исследование сложности квантового алгоритма ветвей и границ как такового, при наличии оценок для M_i и M_i'.

Было проведено сравнение квантового алгоритма ветвей и границ с классическим (описанным в разделе 2) для числа городов $n = 20$ (для бóльших количеств получение эмпирических оценок для M_i и M_i' занимает слишком много времени) и для следующих значений максимально допустимых длин маршрутов: $L_1 = 3{,}648$, $L_2 = 3{,}852$ и $L_3 = 4{,}057$.

Отметим, почему были выбраны именно эти значения максимально допустимых длин. В [18] численно показано, что вероятность существования маршрута коммивояжера длины не более L при наших условиях (равномерно и независимо генерируемые точки в единичном квадрате) равна

$$P(L) = \frac{1}{2} + \frac{1}{2}\Phi\left(\frac{\gamma(L) - 0{,}6}{\sqrt{0{,}5}}\right),$$

где

$$\gamma(L) = \left(\frac{L}{\sqrt{n}} - 0{,}78\right) n^{1/1{,}5}.$$

i	k_i	M_i/N_i	$p(k_i)$	M'_i/N_i
$L_1 = 3{,}648$				
1	4	$1{,}85 \times 10^{-3}$	0,066	$4{,}75 \times 10^{-4}$
2	6	$1{,}13 \times 10^{-5}$	$6{,}20 \times 10^{-3}$	$1{,}63 \times 10^{-6}$
3	10	$3{,}60 \times 10^{-10}$	$5{,}10 \times 10^{-5}$	$2{,}42 \times 10^{-11}$
4	18	$2{,}42 \times 10^{-16}$	$3{,}33 \times 10^{-8}$	—
$L_2 = 3{,}852$				
1	4	$5{,}10 \times 10^{-3}$	0,122	$2{,}55 \times 10^{-3}$
2	6	$3{,}15 \times 10^{-5}$	0,014	$1{,}15 \times 10^{-5}$
3	10	$2{,}44 \times 10^{-8}$	$4{,}08 \times 10^{-4}$	$4{,}62 \times 10^{-9}$
4	18	$8{,}43 \times 10^{-15}$	$8{,}63 \times 10^{-8}$	—
$L_3 = 4{,}057$				
1	7	$1{,}13 \times 10^{-4}$	0,009	$3{,}43 \times 10^{-5}$
2	10	$5{,}74 \times 10^{-8}$	$3{,}05 \times 10^{-4}$	$1{,}73 \times 10^{-9}$
3	18	$1{,}35 \times 10^{-14}$	$2{,}17 \times 10^{-7}$	—

Таблица 1. Статистика частичных решений на различных уровнях дерева поиска. Для каждой максимальной длины приведена статистика по тем уровням, которые оказались оптимальными для алгоритма квантового многоуровневого поиска. Столбцы M_i/N_i и M'_i/N_i соответствуют эмпирическим значениям (для L_1 — усреднение по 100 задачам, для L_2 — по 10 задачам, для L_3 — по 3 задачам), столбец $p(k_i)$ соответствует значению, рассчитанному по формуле (11). Очевидно, данные теоретические значения не могут служить адекватной оценкой эмпирических значений, поскольку нижние оценки разных вершин одного дерева не являются независимыми.

Выбранные длины соответствуют вероятностям $P(L_1) = 0{,}25$, $P(L_2) = 0{,}50$ и $P(L_3) = 0{,}75$.

Для получения эмпирических оценок M_i и M'_i производилось усреднение по нескольким случайным задачам при данном значении L: для L_1 усреднение проводилось по 100 задачам, для L_2 — по 10 задачам, для L_3 — по 3 задачам (ввиду возрастания сложности перебора дерева для получения этих оценок с ростом L).

Для L_1 и L_2 оптимальным количеством m промежуточных уровней поиска оказалось $m = 3$, а для L_3 — $m = 2$. В таблице 1 приведены уровни поиска k_i, оказавшиеся оптимальными для каждой задачи, и эмпирические оценки M_i/N_i и M'_i/N_i для них.

Результаты работы классического и квантового алгоритма ветвей и границ приведены в таблице 2 для вероятности ошибки квантового алгоритма $\varepsilon \approx \pm 0{,}1$.

Из таблицы 2 видно, что во всех случаях сложность квантового алгоритма намного превышает среднюю и медианную сложности классического алгоритма. Во всех случаях доля задач, в которых сложность классического алгоритма превышает сложность квантового алгоритма, не превышала 5%.

Тем не менее, сложность квантового алгоритма в несколько раз меньше максимальной сложности классического алгоритма, т.е. с некоторой небольшой вероятностью возникают такие задачи, на решение которых классический алгоритм тратит аномально много времени, тогда как

Сложность	$L_1 = 3{,}648$	$L_2 = 3{,}852$	$L_3 = 4{,}057$
Классического алгоритма, минимум	1	1	190
Классического алгоритма, максимум	1 047 274	609 459	690 584
Классического алгоритма, среднее	15 015	15 158	18 861
Классического алгоритма, медиана	572	499	365
Квантового алгоритма	275 815	88 566	157 164

Таблица 2. Сравнение работы классического и квантового алгоритмов ветвей и границ. Статистика, относящаяся к классическому алгоритму, построена по результатам решения 100 задач для каждой максимально допустимой длины маршрута L_1, L_2, L_3. Квантовый алгоритм имеет не зависящую от задачи сложность. Вероятность ошибки квантового алгоритма $\varepsilon = 0{,}1$. Оптимальные уровни поиска приведены в таблице 1.

сложность квантового алгоритма постоянна. Если оценивать сложность алгоритма по худшему случаю, то квантовый алгоритм ветвей и границ эффективнее классического.

Также можно заключить, что на практике было бы выгодно запускать одновременно классический и квантовый алгоритмы: с большой вероятностью задачу решит быстрее классический компьютер, но квантовый компьютер будет справляться быстрее в тех редких случаях, когда будут возникать «плохие» задачи.

Для уменьшения сложности квантового алгоритма мы также разработали следующую его модификацию. До сих пор мы запускали квантовый алгоритм сразу для поиска полных решений. Однако если в дереве на некотором промежуточном уровне уже не остается решений, то квантовый алгоритм напрасно тратит время, анализируя последующие уровни, тогда как классический алгоритм просто прекращает работу. Для снижения времени работы квантового алгоритма в этой ситуации можно запустить сначала квантовый алгоритм поиска частичных решений на уровне k_1; он имеет сложность T_1. Может так оказаться, что уже на этом уровне нет частичных решений. В этом случае делается вывод о том, что решения задачи не существует и вычисление останавливается. Если частичные решения на уровне k_1 существуют, то запускается квантовый алгоритм поиска частичных решений на уровне k_2; он имеет сложность T_2. Если частичных решений не обнаруживается, то также делается вывод о том, что решения задачи не существует и т.д. В этом случае средняя сложность квантового алгоритма определяется выражением

$$T_1 + q_1(L)T_2 + \ldots + q_m(L)T_{m+1},$$

где $q_i(L)$ — вероятность того, что на уровне k_i дерева поиска существует хотя бы одно частичное решение.

Можно предположить, что данный вариант использования квантового алгоритма является более выигрышным в том случае, когда с большой вероятностью на одном из промежуточных уровней частичных решений не существует. Напротив, если решение задачи с большой вероятностью существует, то этот вариант приводит к дополнительным временным затратам: многократным запускам квантового алгоритма для частей дерева, тогда как более оптимально запустить квантовый алгоритм ветвей и границ сразу до конца дерева.

Однако следует учитывать, что многократные запуски квантового алгоритма увеличивают вероятность ошибки. Если вероятность ошибки квантового алгоритма установлена в значении ε, то при $m + 1$ запуске алгоритма вероятность ошибки хотя бы одного запуска (что приведет к ошибочному завершению всего вычисления) составит уже $1 - (1 - \varepsilon)^{m+1} \approx (m + 1)\varepsilon$. Чтобы скомпенсировать это, следует соответствующим образом уменьшить ε.

Мы вычислили сложность данного варианта квантового алгоритма для тех же значений максимальных длин L_1, L_2, L_3. Значения $q_i(L)$ были получены путем усреднения по 100 задачам.

Вероятность ошибки квантового алгоритма ε была в каждом случае установлена таким образом, чтобы $1-(1-\varepsilon)^{m+1} = 0{,}1$. Во всех случаях данный вариант реализации алгоритма дал худшие результаты, нежели прежний вариант, в котором квантовый алгоритм запускается сразу для всего дерева. Произошло это главным образом потому, что пришлось уменьшить значение ε из-за многократных запусков алгоритма. Поэтому была также протестирована следующая модификация алгоритма: запускать алгоритм проверки промежуточных частичных решений только на последнем промежуточном уровне поиска m. Тогда сложность определяется формулой $T_m + q_m(L)T_{m+1}$. Значение ε было установлено в значении 0,05, поскольку $1-(1-0{,}05)^2 \approx 0{,}1$. Тогда для длины L_1 (что, напомним, соответствует вероятности существования маршрута $P(L_1) = 0{,}25$) были получены несколько лучшие результаты, чем в основном варианте алгоритма. А именно, минимальная сложность оказалась равной 253 198 (ср. с таблицей 2), при параметрах $m = 2$, $k_1 = 5$, $k_2 = 9$.

Замечание 6. Другое возможное улучшение квантового алгоритма, также в сторону его большей адаптивности, заключается в следующем. Классический алгоритм при нахождении решения прекращает работу и не перебирает оставшиеся не рассмотренными частичные решения. В противоположность этому, количество итераций квантового алгоритма заранее рассчитывается исходя из необходимости хоть и параллельного, но полного перебора всех частичных решений. Можно ограничить область квантового поиска на дереве не глубиной, а шириной: квантовый алгоритм исследует определенное поддерево и переходит к другому поддереву только в случае ненахождения решения. Однако, во-первых, это потребует дополнительных настраиваемых параметров, связанных с ограничениями по ширине поиска, а во-вторых, квантовый алгоритм потеряет преимущество, о котором сказано выше: фиксированная, не зависимая от задачи сложность. Такой вариант будет означать меньшую степень параллелизма, но большую адаптивность.

6. Заключение

Исходя из сравнения сложности предложенного в данной работе квантового алгоритма ветвей и границ и сложности соответствующего классического алгоритма можно сделать вывод, что в большинстве случаев классический алгоритм намного превосходит квантовый вследствие большей адаптивности. В самом деле, во-первых, для работы квантового алгоритма необходимо иметь оценки количеств частичных решений M_i и M'_i на промежуточных уровнях. Во вторых, необходимо провести оптимизацию по количеству уровней поиска и по выбору самих уровней. Для классического алгоритма ни первого, ни второго не требуется, его работа сама подстраивается под конкретную задачу. В-третьих, классический алгоритм при нахождении решения прекращает работу и не перебирает оставшиеся не рассмотренными частичные решения, тогда как количество итераций квантового алгоритма заранее рассчитывается исходя из необходимости хоть и параллельного, но полного перебора всех частичных решений. В подавляющем большинстве задач квантовый параллелизм не компенсирует отсутствие адаптивности.

Отметим, что проблемы, обнаруженные нами при разработке квантового метода ветвей и границ, известны также и в разработке классических параллельных реализаций этого метода (см. [13]).

Тем не менее, время работы квантового алгоритма постоянно для всех задач, тогда как классический алгоритм на некоторых задачах работает очень медленно. В результате для наихудшего случая квантовый алгоритм ветвей и границ оказался в несколько раз эффективнее классического алгоритма (при условии наличия адекватных оценок количеств частичных решений). При бóльших размерностях задачи эта разница может вырасти еще сильнее. Представляет интерес дальнейшее исследование квантового метода ветвей и границ и оценка сложности решения NP-полных задач с его помощью.

Благодарность. Авторы признательны Д. А. Жолобову за ценные консультации по вопросам практического использования алгоритмов решения задачи коммивояжера.

СПИСОК ЛИТЕРАТУРЫ

1. *Вагнер Г.* Основы исследования операций. Т. 2. — М.: Мир, 1973.

2. *Жолобов Д. А.* Введение в математическое программирование. — М.: МИФИ, 2008.
3. *Ahuja A., Kapoor S.* A quantum algorithm for finding the maximum/ arxiv.org/abs/quant-ph/9911082
4. *Ambainis A.* Quantum search algorithms// SIGACT News. — 2004. — *35*, № 2. — С. 22–35.
5. *Bennett C., Bernstein E., Brassard G., Vazirani U.* Strengths and weaknesses of quantum computing// SIAM J. Comput. — 1997. — *26*, № 5. — С. 1510–1523.
6. *Billingsley P.* Probability and measure. — New York: Wiley, 1995.
7. *Brassard G., Høyer P., Mosca M., Tapp A.* Quantum amplitude amplification and estimation// Quantum Comput. Quantum Inform. Sci. — AMS Contemp. Math. Ser. — 2002. *305*. — С. 53–74.
8. *Cerf N. J., Grover L., Williams C. P.* Nested quantum search and structured problems// Phys. Rev. A. — 2000. — *61*, № 3. — С. 032303.
9. *Childs A., Kimmel S., Kothari R.* The quantum query complexity of read-many formulas// Lect. Notes Comput. Sci. — Springer, 2012. — *7501*. — С. 336–348.
10. *Childs A. M., Landahl A. J., Parrilo P. A.* Improved quantum algorithms for the ordered search problem via semidefinite programming// Phys. Rev. A. — 2007. — *75*, № 3. — С. 032335.
11. *Cleve R., Gavinsky D., Yonge-Mallo D. L.* Quantum algorithms for evaluating min-max trees// In: Theory of Quantum Computation, Communication, and Cryptography/ Lect. Notes Comput. Sci. — Springer, 2008. — *5106*. — С. 11–15.
12. *Cortina-Borja M., Robinson T.* Estimating the asymptotic constants of the total length of Euclidean minimal spanning trees with power-weighted edges// Stat. Probab. Lett. — 2000. — *47*, № 2. — С. 125–128.
13. *Crainic T. G., Le Cun B., Roucairol C.* Parallel branch-and-bound algorithms// In: Parallel Combin. Optim. — New York: Wiley, 2006. — С. 1–28.
14. *Dürr C., Heiligman M., Høyer P., Mhalla M.* Quantum query complexity of some graph problems// SIAM J. Comput. — 2006. — *35*, № 6. — С. 1310–1328.
15. *Dürr C., Høyer P.* A quantum algorithm for finding the minimum/ arxiv.org/abs/quant-ph/9607014
16. *Farhi E., Goldstone J., Gutmann S.* A quantum algorithm for the Hamiltonian NAND tree// Theory Comput. — 2008. — *4*. — С. 169–190.
17. *Farhi E., Goldstone J., Gutmann S., Sipser M.* Invariant quantum algorithms for insertion into an ordered list/ arxiv.org/abs/quant-ph/9901059
18. *Gent I. P., Walsh T.* The TSP phase transition// Artificial Intelligence. — 1996. — *88*, № 1. — С. 349–358.
19. *Grover L. K.* A fast quantum mechanical algorithm for database search// Proc. 28 Ann. Symp. on the Theory of Computing. — New York: ACM Press, 1996. — С. 212–219.
20. *Høyer P., Neerbek J., Shi Y.* Quantum complexities of ordered searching, sorting, and element distinctness// Algorithmica. — 2002. — *34*, № 4. — С. 429–448.
21. *Kesten H., Lee S.* The central limit theorem for weighted minimal spanning trees on random points// Ann. Probab. — 1996. — *6*, № 2. — С. 495–527.
22. *Kowada L. A. B., Lavor C., Portugal R., de Figueiredo C. M. H.* A new quantum algorithm for solving the minimum searching problem// Int. J. Quantum Inform. — 2008. — *6*, № 3. — С. 427–436.
23. *Mandrà S., Guerreschi G. G., Aspuru-Guzik A.* Faster than classical quantum algorithm for dense formulas of exact satisfiability and occupation problems// New J. Phys. — 2016. — *18*, № 7. — С. 073003.
24. *Reichardt B. W.* Reflections for quantum query algorithms// Proc. 22 ACM-SIAM Symp. on Discrete Algorithms. — 2011. — С. 560–569; arxiv.org/abs/1005.1601
25. *Steele M.* Growth rates of Euclidean minimal spanning trees with power weighted edges// Annals Probab. — 1988. — *16*, № 4. — С. 1767–1787.
26. *Yoder T. J., Low G. H., Chuang I. L.* Fixed-point quantum search with an optimal number of queries// Phys. Rev. Lett. — 2014. — *113*. — С. 210501.
27. *Zhang W.* State-space search: Algorithms, complexity, extensions, and applications. — Springer, 1999.

Е. А. Маркевич
Национальный исследовательский ядерный университет «МИФИ», Москва
E-mail: eva-markevich@mail.ru

А. С. Трушечкин
Математический институт им. В. А. Стеклова РАН;
Национальный исследовательский ядерный университет «МИФИ», Москва;
Национальный исследовательский технологический университет «МИСиС», Москва
E-mail: trushechkin@mi.ras.ru

ИТОГИ НАУКИ И ТЕХНИКИ.
Современная математика и ее приложения.
Тематические обзоры.
Том 138 (2017). С. 76–81

УДК 517.977.5

НЕКОТОРЫЕ МАТЕМАТИЧЕСКИЕ ЗАДАЧИ УПРАВЛЕНИЯ КВАНТОВЫМИ СИСТЕМАМИ

© 2017 г. **А. Н. ПЕЧЕНЬ**

Аннотация. В настоящее время активно развиваются квантовые технологии — технологии, в основе которых лежит использование квантовых эффектов и индивидуальных квантовых систем, отдельных атомов или молекул. В этой связи приобретает важность математическое исследование задач по управлению квантовыми системами. В данной работе рассматриваются такие задачи, связанные с управлением квантовыми системами, как исследование экстремумов целевых функционалов для задач переноса населенности и генерации унитарных процессов, а также некогерентное управление и генерация произвольных матриц плотности для открытых квантовых систем.

Ключевые слова: управление квантовыми системами, открытые квантовые системы.

AMS Subject Classification: 81Q93

1. Введение. Квантовые технологии — технологии, в основе которых лежит использование квантовых эффектов и индивидуальных квантовых систем, т.е. отдельных атомов или молекул. Одним из направлений квантовых технологий являются квантовые компьютеры и квантовые вычисления, в основе которых лежит использование законов квантовой физики для ускорения вычислений (см. [1]). Широко известными алгоритмами, которые могут быть реализованы с помощью квантовых компьютеров, являются алгоритм Шора и алгоритм Гровера. Алгоритм Шора позволяет с помощью квантовых эффектов осуществить разложение числа на простые сомножители за полиномиальное время, в то время как полиномиальных классических алгоритмов для решения этой задачи не известно. Алгоритм Гровера позволяет осуществить поиск в неупорядоченной базе данных, состоящей из N элементов, за $\sim \sqrt{N}$ операций, в то время как классические алгоритмы требуют $\sim N$ операций. Создание универсальных квантовых компьютеров испытывает трудности, в том числе из-за невозможности достаточно хорошо изолировать физические системы, выполняющие роль кубитов (квантовых битов), от окружения. Однако существуют прототипы адиабатических квантовых компьютеров, предназначенные для решения некоторого класса задач дискретной оптимизации, известные как D-Wave Systems. Модель D-Wave One была создана в 2011 г. и состояла из 128 кубит, D-Wave Two — в 2013 г. и состояла из 512 кубит. В 2015 г. была разработана модель D-Wave 2X, имеющая 1152 кубит (однако не все кубиты рабочие). Ведутся дискуссии о том, насколько существенны в этих вычислительных устройствах квантовые эффекты и сравнивается их эффективность с классическими вычислительными устройствами (см. [10]).

Другой пример квантовых технологий — квантовая криптография, методы защиты коммуникаций с помощью законов квантовой физики (см. [2]). Простейший алгоритм генерации секретного ключа с использованием квантовой физики, известный как протокол BB84, был разработан Ч. Беннетом (C. Bennett) и Ж. Брассардом (G. Brassard) в 1984 г. В то время как квантовые компьютеры далеки до практической реализации, квантовая криптография уже вступает в практическую фазу. В октябре 2007 г. на выборах в Швейцарии широко использовались квантовые сети, разработанные на основе техники Н. Жизена (N. Gisin). В 2011 г. в Токио во время демонстрации

Работа выполнена при поддержке Министерства образования и науки Российской Федерации (проект №1.669.2016/ФПМ)..

проекта «Tokyo QKD Network», в ходе которого разрабатывается квантовое шифрование телекоммуникационных сетей, была проведена пробная телеконференция на расстоянии в 45 км. В 2016 г. квантовый канал длиной порядка 30 км был запущен в Москве под руководством А. И. Львовского и Ю. В. Курочкина. Получены и важные математические результаты в области квантовой информации. Так, в 2015 г. А. С. Холево в соавторстве с В. Джованетти (V. Giovannetti) и Р. Гарсиа-Патроном (R. García-Patrón) была решена чрезвычайно значимая проблема гауссовских максимизаторов, связанная с оценкой ограничений, накладываемых квантовыми эффектами на пропускную способность линий оптоволоконной связи (см. [14]). Активно развивается лазерное управление химическими реакциями, контроль вращения молекул, фотохимия, другие области технологий, в которых существенны квантовые эффекты.

Развитие квантовых технологий требует в том числе разработки способов управления квантовыми системами. В настоящее время эта область приобретает высокий интерес (см. [5,8,11,16,24, 26]). В данной работе обсуждаются полученные ранее результаты в таких математических задачах управления квантовыми системами, как исследование экстремумов целевых функционалов для задач переноса населенности и генерации унитарных процессов для квантовых систем, некогерентное управление и генерация произвольных матриц плотности для открытых квантовых систем.

2. Формулировка задачи управления квантовой системой. Для того чтобы математически сформулировать задачу управления квантовой системой, необходимо определить множество состояний системы, задать уравнение, которое описывает эволюцию системы под воздействием управления, и определить целевой функционал, максимизация которого обеспечивает достижение цели управления.

Каждой квантовой системе соответствует некоторое комплексное сепарабельное гильбертово пространство $\mathcal{H}$. Например, частице с n состояниями соответствует гильбертово пространство $\mathcal{H} = \mathbb{C}^n$, причем кубиту соответствует простейший нетривиальный случай $n = 2$. Частице, двигающейся в трехмерном пространстве, соответствует гильбертово пространство $\mathcal{H} = L^2(\mathbb{R}^3)$. Гильбертово пространство позволяет определить состояния квантовой системы. Различают чистые и смешанные состояния. Чистыми состояниями являются векторы $\psi \in \mathcal{H}$ единичной длины. Смешанные состояния описываются матрицами плотности, т.е. неотрицательными операторами $\rho : \mathcal{H} \to \mathcal{H}$, $\rho \geqslant 0$, имеющими единичный след, $\operatorname{Tr}\rho = 1$. Чистым состояниям соответствуют матрицы плотности, которые являются проекторами, т.е. такие, что $\rho^2 = \rho$.

Если квантовая система изолирована от влияния окружения и находится под воздействием когерентного управления $u(t)$, например лазерного импульса, то ее эволюция описывается уравнением Шрёдингера для унитарного оператора эволюции U_t:

$$\frac{dU_t}{dt} = -i\Big(H_0 + Vu(t)\Big)U_t, \quad U_{t=0} = \mathbb{I}. \tag{1}$$

Здесь H_0 и V — свободный гамильтониан системы и гамильтониан взаимодействия системы с когерентным управлением (самосопряженные операторы в $\mathcal{H}$); при этом матрица плотности преобразуется по формуле

$$\rho_t = U_t \rho_0 U_t^\dagger.$$

Система является управляемой, если размерность алгебры, порожденной коммутаторами H_0 и V, равна n^2. Если квантовая система взаимодействует с резервуаром, то ее эволюция описывается мастер-уравнением для матрицы плотности

$$\frac{d\rho_t}{dt} = -i\big[H_0 + Vu(t), \rho_t\big] + \mathscr{L}(\rho_t)$$

Если резервуар марковский, то диссипативный генератор имеет следующий вид:

$$\mathscr{L}(\rho_t) = \sum\Big(2L_i\rho_t L_i^\dagger - L_i^\dagger L_i\rho_t - \rho_t L_i^\dagger L_i\Big);$$

здесь L_i — операторы в $\mathcal{H}$. Существуют различные методы вывода мастер-уравнений (см. [7, 12, 27]). В случае произвольного резервуара эволюция матрицы плотности описывается вполне положительным сохраняющим след отображением Φ (см. [6]). Такое отображение для n-уровневой

квантовой системы задается преобразованием

$$\rho_t = \Phi(\rho_0) = \sum_{i=1}^{n^2} K_i \rho_0 K_i^\dagger.$$

Широкий класс задач управления квантовыми системами можно сформулировать в виде задачи максимизации некоторого класса целевых функционалов. Важным примером являются целевые функционалы вида

$$\mathscr{F}_O(u) = \operatorname{Tr}\Big[U_T \rho_0 U_T^\dagger O\Big];$$

такие функционалы описывают задачу максимизации среднего значения наблюдаемой O (самосопряженного оператора в гильбертовом пространстве $\mathcal{H}$) в момент времени $T > 0$ при условии, что в начальный момент $t = 0$ система находится в состоянии с матрицей плотности ρ_0. Другим примером является задача генерации квантовой унитарной операции $W \in SU(n)$, т.е. задача отыскания такого управления, что индуцируемый этим управлением оператор эволюции U_T как можно точнее аппроксимирует W. Эта задача для n-уровневой квантовой системы может быть сформулирована как задача максимизации целевого функционала

$$\mathscr{F}_W(u) = \frac{1}{n^2}\Big|\operatorname{Tr}\big(W^\dagger U_T\big)\Big|^2.$$

3. Ландшафты задач управления. В перечисленных выше задачах необходимо отыскать управление, на котором реализуется глобальный максимум целевого функционала. Локальные, но не глобальные максимумы, если они существуют, могут служить препятствием на пути к поиску глобально оптимальных управлений. Данное обстоятельство определяет важность исследования всех максимумов целевого функционала (см. [13, 15, 17, 21, 23]).

Ландшафтом задачи управления называется график целевого функционала. Локальные, но не глобальные максимумы, если они есть, называются ловушками. Ловушками второго порядка называются критические точки целевого функционала, $\delta\mathscr{F}/\delta u = 0$, в которых гессиан целевого функционала отрицательно полуопределен, $\delta^2\mathscr{F}/\delta u^2 \leqslant 0$, при том, что $\mathscr{F}(u) < \mathscr{F}_{\max}$.

Отсутствие ловушек доказано для $n = 2$ при достаточно больших T (см. [3, 19]). Определим специальное управление u_0 и время T_0:

$$u_0 := \frac{-\operatorname{Tr} H_0 \operatorname{Tr} V + 2\operatorname{Tr}(H_0 V)}{(\operatorname{Tr} V)^2 - 2\operatorname{Tr} V^2}, \tag{2}$$

$$T_0 := \frac{\pi}{\|H_0 - \mathbb{I}\operatorname{Tr} H_0/2 + f_0 V\|}. \tag{3}$$

Теорема 1. *Рассмотрим двухуровневую квантовую систему с эволюцией*

$$i\frac{dU_t}{dt} = \Big(H_0 + u(t)V\Big)U_t.$$

Пусть $[H_0, V] \neq 0$, $\operatorname{Tr} V = 0$ *и* $T \geqslant T_0$. *Тогда все максимумы целевых функционалов* $\mathscr{F}_O(u)$ *и* $\mathscr{F}_W(u)$ *— глобальные.*

В связи с развитием фемто- и аттосекундного управления необходимо исследовать экстремумы целевых функционалов при малых T. Теорема 2 утверждает отсутствие ловушек у $\mathscr{F}_W$ для почти всех W при малых T (см. [4]). Пусть

$$d = \left\| H_0 + u_0 V - \mathbb{I}\frac{\operatorname{Tr} H_0}{2} - u_0 \mathbb{I}\frac{\operatorname{Tr} V}{2} \right\|.$$

Каждая матрица W, удовлетворяющая условию $[H_0 + u_0 V, W] = 0$, имеет вид

$$W = e^{i\alpha_W (H_0 + u_0 V) + i\beta_W}, \quad \text{где} \quad \alpha_W \in \Big(0, \frac{\pi}{d}\Big], \quad \beta_W \in [0, 2\pi). \tag{4}$$

Теорема 2. *Пусть $n = 2$ и $[H_0, V] \neq 0$ в уравнении (1). Если $[H_0 + u_0 V, W] \neq 0$, то для любого $T > 0$ все максимумы целевого функционала $\mathscr{F}_W$ — глобальные. Пусть $[H_0 + u_0 V, W] = 0$. Если $\alpha_W \in (0, \pi/(2d))$, то все максимумы целевого функционала $\mathscr{F}_W$ — глобальные для любого $T > 0$; если же $\alpha_W \in [\pi/(2d), \pi/d]$, то все максимумы целевого функционала $\mathscr{F}_W$ — глобальные для любого $T > \pi/d - \alpha_W$.*

Доказано также отсутствие ловушек в задаче управления коэффициентом прохождения частицы через одномерный потенциальный барьер (см. [22]). В этой задаче рассматривается стационарное уравнение Шредингера для волновой функции $\psi(x)$ частицы с энергией $E = k^2 > 0$, движущейся в поле одномерного потенциала $V(x) \in L^1(\mathbb{R}) \cap C_c(\mathbb{R})$:

$$\Big[\frac{d^2}{dx^2} + V(x)\Big]\psi = E\psi.$$

Асимптотика решения на бесконечности соответствует падающей слева волне, которая частично отражается обратно, частично проходит через потенциальный барьер:

$$x \to -\infty: \quad \psi(x) = e^{ikx} + A(k)e^{-ikx},$$
$$x \to +\infty: \quad \psi(x) = B(k)e^{ikx}.$$

Коэффициенты $A(k)$ и $B(k)$ определяют амплитуды отраженной и прошедшей волны. Коэффициент прохождения частицы есть вероятность того, что частица будет обнаружена справа от барьера,

$$T_E(V) = |B(k)|^2, \quad 0 < T_E \leqslant 1$$

Теорема об отсутствии ловушек в этой задаче имеет следующий вид (см. [22]).

Теорема 3. *Все критические точки коэффициента прохождения — глобальные максимумы, так что*

$$\frac{\delta T_E(V)}{\delta V} = 0 \Rightarrow T_E(V) = 1.$$

Таким образом, в задаче управления туннелированием частицы ловушки также отсутствуют. Однако для квантовых систем с $n \geqslant 3$ в некоторых случаях существуют ловушки второго порядка (см. [21]).

Теорема 4. *Рассмотрим n-уровневую квантовую систему ($n \geqslant 3$), динамика которой определяется уравнением (1). Пусть система управляема. Если $V_{ij} = 0$ для некоторого $i \neq j$ в базисе $|i\rangle$ собственных векторов оператора H_0, то существует (бесконечно много) таких пар (ρ_0, O), что соответствующий целевой функционал $\mathscr{F}_O$ имеет по крайней мере одну ловушку второго порядка.*

Построены также некоторые примеры ловушек для систем с $n = 4$ (см. [13]).

4. Некогерентное управление и приближенная генерация произвольных матриц плотности. Часто управляемые квантовые системы не могут быть достаточно хорошо изолированы от влияния окружения. В некоторых случаях влияние окружения является деструктивным и его необходимо минимизировать. В других ситуациях окружение можно использовать для управления системой. Различные способы такого использования известны под терминами «reservoir engineering» или некогерентное управление (см. [9,20,25]). В данном разделе рассматривается некогерентное управление с использованием некогерентного и в общем случае нетеплового излучения.

Рассмотрим n-уровневый атом, взаимодействующий с когерентным излучением (лазерный импульс) $u(t)$ и с некогерентным излучением спектральной плотности $n_\omega(t)$ (см. [20]). Динамика матрицы плотности атома в этом случае описывается следующим мастер-уравнением:

$$\dot\rho_t = -i\Big[H_0 + H_{n_\omega} + u(t)V,\ \rho_t\Big] + \mathcal{L}_{n_\omega}(\rho_t); \tag{5}$$

здесь генератор $\mathcal{L}_{n_\omega}$ имеет вид

$$\mathcal{L}_{n_\omega}(\rho) = \sum_{i<j} A_{ij}\Big[(n_{\omega_{ij}}+1)L_{Q_{ij}}(\rho) + n_{\omega_{ij}}L_{Q_{ji}}(\rho)\Big],$$

где $A_{ij} \geqslant 0$ — коэффициенты Эйнштейна, $\omega_{ij} = \varepsilon_i - \varepsilon_j$ — частоты перехода в атоме, $Q_{ij} = |i\rangle\langle j|$ — оператор перехода между состояниями $|j\rangle$ и $|i\rangle$ и

$$L_Q(\rho) = 2Q\rho Q^\dagger - Q^\dagger Q\rho - \rho Q^\dagger Q.$$

Интенсивности когерентного и некогерентного излучений $u(t)$ и n_ω рассматриваются как управляющие воздействия. Возникает вопрос, в какой степени такое воздействие позволяет управлять системой? Оказывается, при достаточно общих предположениях такое управление позволяет переводить произвольную начальную матрицу плотности системы сколь угодно близко к произвольной заданной матрице плотности, тем самым приближенно реализуя полную управляемость системы на множестве всех ее матриц плотности (см. [18]). Условия, обеспечивающие такую управляемость, — отличие от нуля всех коэффициентов Эйнштейна и возможность унитарной управляемости системы на временах, на которых влиянием декогеренции в системе можно пренебречь.

5. Заключение. Обсуждаются некоторые полученные ранее результаты в таких областях управления квантовыми системами, как исследование экстремумов целевых функционалов на больших и на малых временах, некогерентное управление и генерация произвольных матриц плотности для квантовых систем, взаимодействующих с когерентым и некогерентным излучением.

СПИСОК ЛИТЕРАТУРЫ

1. *Валиев К. А., Кокин А. А.* Квантовые компьютеры: надежды и реальность. — Ижевск: РХД, 2004.
2. *Кронберг Д. А., Ожигов Ю. И., Чернявский А. Ю.* Квантовая криптография. — М.: МАКС Пресс, 2011.
3. *Печень А. Н., Ильин Н. Б.* Когерентное управление кубитом свободно от ловушек// Тр. Мат. ин-та им. В. А. Стеклова. — 2014. — *285*. — С. 244–252.
4. *Печень А. Н., Ильин Н. Б.* Об экстремумах целевого функционала в задаче генерации однокубитных квантовых вентилей на малых временах// Изв. РАН. Сер. мат. — 2016. — *80*, № 6. — С. 217–229.
5. *Фрадков Л. А., Якубовский О. А.* (ред.). Управление молекулярными и квантовыми системами. — М.–Ижевск: Институт компьютерных исследований, 2003.
6. *Холево А. С.* Квантовые системы, каналы, информация. — М.: МЦНМО, 2010.
7. *Accardi L., Lu Y. G., Volovich I. V.* Quantum theory and its stohastic limit. — Springer-Verlag, 2002.
8. *D'Alessandro D.* Introduction to quantum control and dynamics. — Boca Raton: Chapman & Hall, 2007.
9. *Barreiro J. T., Schindler P., Gühne O., Monz T., Chwalla M., Roos C. F., Hennrich M., Blatt R.* Experimental multiparticle entanglement dynamics induced by decoherence// Nature Phys. — 2010. — *6*. — С. 943–946.
10. *Boixo S., Rønnow T. F., Isakov S. V., Wang Zh., Wecker D., Lidar D. A., Martinis J. M., Troyer M.* Quantum annealing with more than one hundred qubits// Nature Phys. — 2013. — *10*, № 3. — С. 218–224.
11. *Brumer P. W., Shapiro M.* Principles of the quantum control of molecular processes. — Wiley-Interscience, 2003.
12. *Davis E. B.* Quantum theory of open systems. — Academic Press, 1976.
13. *de Fouquieres P., Schirmer S. G.* Quantum control landscapes: A closer look// Infin. Dimen. Anal. Quantum Probab. Rel. Topics. — 2013. — *16*, № 3. — С. 1350021.
14. *Giovannetti V., Holevo A. S., García-Patrón R.* A solution of Gaussian optimizer conjecture for quantum channels// Commun. Math. Phys. — 2015. — *334*, № 3. — С. 1553–1571.
15. *Hsieh M., Wu R., Rabitz H., Lidar D.* Optimal control landscape for the generation of unitary transformations with constrained dynamics// Phys. Rev. A. — 2010. — *81*. — С. 062352.
16. *Letokhov V. S.* Laser control of atoms and molecules. — Oxford Univ. Press, 2007.
17. *Moore K. W., Rabitz H.* Exploring quantum control landscapes: Topology, features and optimization scaling// Phys. Rev. A. — 2011. — *84*. — С. 012109.

18. *Pechen A.* Engineering arbitrary pure and mixed quantum states// Phys. Rev. A. — 2011. — *84*. — C. 042106.
19. *Pechen A., Il'in N.* Trap-free manipulation in the Landau–Zener system// Phys. Rev. A. — 2012. — *86*. — C. 052117.
20. *Pechen A., Rabitz H.* Teaching the environment to control quantum systems// Phys. Rev. A. — 2006. — *73*. — C. 062102.
21. *Pechen A., Tannor D.* Are there traps in quantum control landscapes?// Phys. Rev. Lett. — 2011. — *106*. — C. 120402.
22. *Pechen A. N., Tannor D. J.* Control of quantum transmission is trap-free// Can. J. Chem. — 2014. — *92*, № 2. — C. 157–159.
23. *Rabitz H., Hsieh M., Rosenthal C.* Quantum optimally controlled transition landscapes// Science. — 2004. — *303*. — C. 1998–2001.
24. *Rice S. A., Zhao M.* Optical control of molecular dynamics. — N.Y.: Wiley, 2000.
25. *Rossini D., Calarco T., Giovannetti V., Montangero S., Fazio R.* Decoherence induced by interacting quantum spin baths// Phys. Rev. A. — 2007. — *75*. — C. 032333.
26. *Tannor D. J.* Introduction to quantum mechanics: A time dependent perspective. — Sausalito: Univ. Science Press, 2007.
27. *Trushechkin A. S., Volovich I. V.* Perturbative treatment of inter-site couplings in the local description of open quantum networks// Europhys. Lett. — 2016. — *113*. — C. 30005.

Печень Александр Николаевич
Национальный исследовательский технологический университет «МИСиС», Москва;
Математический институт им. В. А. Стеклова РАН, Москва
E-mail: pechen@mi.ras.ru

ИТОГИ НАУКИ И ТЕХНИКИ.
Современная математика и ее приложения.
Тематические обзоры.
Том 138 (2017). С. 82–98

УДК 517.958:530.145, 536.73, 536.75

ОБ ОБЩЕМ ОПРЕДЕЛЕНИИ ПРОИЗВОДСТВА ЭНТРОПИИ В МАРКОВСКИХ ОТКРЫТЫХ КВАНТОВЫХ СИСТЕМАХ

© 2017 г. **А. С. ТРУШЕЧКИН**

Аннотация. Рассматривается вопрос об общем определении производства энтропии в единицу времени для квантовой системы, подчиняющейся уравнению Линдблада. Сложность состоит в том, что для определения полного производства энтропии необходимо знать поток энтропии из системы в окружение. Для этого необходимо иметь некоторую информацию об окружении и о том, как оно взаимодействует с системой. Эта информация не содержится в уравнении Линдблада для приведенной матрицы плотности системы. Поэтому уместно поставить следующий вопрос: какой минимальной информацией об окружении необходимо дополнить уравнение Линдблада, чтобы определить поток энтропии в окружение и, затем, производство энтропии полное производство энтропии. Для ответа на этот вопрос мы используем концепцию комплементарного квантового канала, известную в квантовой теории информации. Также доказывается теорема о неотрицательности производства энтропии, а также, при некоторых предположениях, адиабатического и неадиабатического вкладов в него.

***Ключевые слова*:** открытые квантовые системы, уравнение Линдблада, производство энтропии, второй закон термодинамики.

***AMS Subject Classification*:** 81S22, 82C10

СОДЕРЖАНИЕ

1. Введение

Пусть дана открытая квантовая система, которой соответствует конечномерное гильбертово пространство $\mathscr{H}_S$. Состояние системы в произвольный момент времени описывается ее оператором плотности ρ_t (т.е. положительным оператором в $\mathscr{H}_S$ с единичным следом). Уравнение Линдблада (или Горини—Коссаковски—Сударшана—Линдблада, ГКСЛ), описывающее динамику оператора плотности системы, имеет вид (см. [15, 21, 2])

$$\frac{d}{dt}\rho_t = -i[H(\lambda_t), \rho_t] + \sum_{k=1}^{K}\left(L_k(\lambda_t)\rho_t L_k(\lambda_t)^\dagger - \frac{1}{2}\{L_k(\lambda_t)^\dagger L_k(\lambda_t), \rho_t\}\right) \equiv \mathcal{L}(\lambda_t)\rho_t, \tag{1}$$

Исследование выполнено при поддержке гранта Президента Российской Федерации (проект МК-2815.2017.1).

где λ_t — зависящие от времени внешние параметры, $H(\lambda_t)$ — самосопряженный оператор на $\mathscr{H}_S$ (гамильтониан), $L_k(\lambda_t)$ — линейные операторы на $\mathscr{H}_S$, $[A,B] = AB - BA$, $\{A,B\} = AB + BA$. Уравнение Линдблада является наиболее общим уравнением динамики открытой квантовой системы в том случае, когда динамика марковская (т.е. знание состояния ρ_t квантовой системы в текущий момент времени позволяет предсказать дальнейшую эволюцию состояния).

Рассматривается вопрос об определении производства энтропии для открытой квантовой системы, описываемой уравнением (1). Она определяется исходя из уравнения баланса

$$\sigma(\rho_t, \lambda_t) = \frac{d}{dt} S(\rho_t) + J(\rho_t, \lambda_t), \tag{2}$$

где $S(\rho) = -\operatorname{Tr} \rho \ln \rho$ — энтропия фон Неймана, а $J(t)$ — поток энтропии из системы в окружение («резервуар»), $\sigma(\rho_t, \lambda_t)$ — полное производство энтропии. Для фиксированного момента времени мы часто будем опускать зависимость от λ_t и писать просто $\sigma(\rho)$ и $J(\rho)$ — функционалы, определенные на матрицах плотности при фиксированных параметрах λ.

Уравнение (2) можно трактовать следующим образом. Рассмотрим полный гамильтониан системы и окружения («большой» системы):

$$H(\lambda_t) = H_S(\lambda_t) + H_E(\lambda_t) + H_I(\lambda_t), \tag{3}$$

где слагаемые правой части соответствуют гамильтониану системы, гамильтониану окружения и гамильтониану их взаимодействия соответственно. Поскольку динамика большой системы унитарна, то энтропия фон Неймана большой системы неизменна. Как показано в [13], представление о производстве энтропии возникает, когда мы пренебрегаем корреляцией между системой и окружением. Таким образом, производство энтропии есть

$$\sigma(t) = \frac{d}{dt}[S(\rho_t) + S(\rho_t^E)],$$

где через ρ_t и ρ_t^E обозначены приведенные операторы плотности системы и окружения. Величина $\frac{d}{dt} S(\rho_t^E)$ и интерпретируется как поток $J(\rho_t, \lambda_t)$ энтропии из системы в окружение в уравнении (2).

Как видим, в общем случае для определения величины потока $J(t)$ и, следовательно, производства энтропии $\sigma(t)$ недостаточно знания приведенного оператора плотности системы и уравнения Линдблада. Необходима также некоторая информация об окружении и о том, как оно взаимодействует с системой.

В классических работах [31, 32] рассматривается случай, когда, во-первых, уравнение Линдблада выведено в пределе слабой связи, а во-вторых, окружение — это один или несколько тепловых (равновесных) резервуаров.

В этом случае уравнения Линдблада оказывается достаточно для вывода выражения потока энтропии в окружение и, следовательно, производства энтропии, которое в этом случае выражается через квантовую относительную энтропию. Монотонность квантовой относительной энтропии гарантирует неотрицательность производства энтропии, в согласии со вторым законом термодинамики.

Тем не менее, в режимах связи системы с резервуаром, отличных от режима слабой связи, например, в модели непрерывных измерений, выражение для потока и производства энтропии имеет другой вид (см. [9]). Кроме того, важную роль в квантовой теории управления играют неравновесные (нетемпературные) резервуары (см. [27, 25]).

В [18, 19] вводится определение производства энтропии, а также адиабатического и неадиабатического вклада в производство энтропии на основе концепции квантовых траекторий. Определение квантовой траектории возможно при условии проведения частых измерений резервуара. Однако для этого необходимо обеспечить, чтобы постоянные измерения резервуара не влияли на динамику системы (см. [2]). В общем случае это неверно и динамика системы может даже не иметь полугруппового свойства (см. [22]).

Разумеется, если мы знаем полный гамильтониан (3), из которого уравнение Линдблада было выведено в результате некоторого предельного перехода, то можно вывести выражение для производства энтропии, непосредственно найдя предел выражения $\frac{d}{dt} S(\rho_t^E)$. Однако уместно поставить

следующей вопрос: какой *минимальной* информацией об окружении и его взаимодействием с системой необходимо дополнить уравнение Линдблада, чтобы определить поток энтропии $J(t)$ и, затем, производство энтропии $\sigma(t)$.

В данной работе мы отвечаем на этот вопрос, обращаясь к концепции комплементарного канала, известной в квантовой теории информации (см. [11, 5, 6]). Динамика Линдблада $\rho_0 \mapsto \rho_t$ может быть описана как действие некоторого квантового канала. Комплементарный квантовый канал как раз и содержит минимальную информацию об окружении для системы, которая поступает на вход первичного квантового канала.

Также мы доказываем неотрицательность по отдельности адиабатического и неадиабатического вкладов в производство энтропии, расширяя по сравнению с [18, 19] условия, при которых это справедливо. Адиабатический вклад в производство энтропии обусловлен необходимостью поддержания неравновесного стационарного состояния и потому не зависит от внешнего управления, тогда как неадиабатический вклад связан с внешним управлением. Поэтому выделение этого вклада и установление его свойств важно для определения термодинамический цены внешнего управления открытой квантовой системой.

Дальнейший текст организован следующим образом. В разделе 2 приводится классическое определение производства энтропии, справедливое в режиме слабого взаимодействия системы с одним или несколькими равновесными резервуарами. В разделе 3 мы даем общее определение потока энтропии из системы в окружение и производства энтропии, отвечая на приведенный выше вопрос. В разделе 5 приводятся примеры. В разделе 4 доказывается теорема о неотрицательности производства энтропии при определенных условиях. Раздел 6 посвящен сравнению предлагаемого здесь подхода к определению производства энтропии с подходом, предложенным в [18, 19], основанным на квантовых траекториях. В разделе 7 рассматриваются адиабатический и неадиабатический вклады в производство энтропии, доказывается теорема об их неотрицательности при определенных условиях. Наконец, в разделе 8 выводятся некоторые формулы для случая, когда окружение состоит из нескольких тепловых резервуаров.

2. Случай режима слабого взаимодействия с тепловыми резервуарами

Пусть система слабо взаимодействует с одним тепловым резервуаром с обратной температурой β. Тогда увеличение энтропии резервуара можно представить в виде

$$J(\rho_t, \lambda_t) = \beta Q(\rho_t, \lambda_t),$$

где $Q(\rho_t, \lambda_t)$ — поток тепла, т.е. энергии из системы в резервуар. Имеем

$$Q(\rho_t, \lambda_t) = \frac{d}{dt}\langle H_E\rangle = -\frac{d}{dt}\langle H_S(\lambda_t) + H_I(\lambda_t)\rangle \approx -\frac{d}{dt}\langle H_S(\lambda_t)\rangle = -\operatorname{Tr}\Big\{\big[\mathcal{L}(\lambda_t)\rho_t\big]H_S(\lambda_t)\Big\}.$$

Здесь во втором равенстве мы воспользовались законом сохранения полной энергии большой системы, во втором равенстве мы пренебрегли членом взаимодействия H_I, поскольку в режиме слабой связи он мал. Вводя гиббсовское состояние системы по формуле

$$\rho^\beta(\lambda_t) = Z(\lambda_t)^{-1}\exp\big[-\beta H_S(\lambda_t)\big], \tag{4}$$

где

$$Z(\lambda_t) = \operatorname{Tr}\exp\big[-\beta H_S(\lambda_t)\big],$$

можем выразить

$$J(\rho_t, \lambda_t) = \operatorname{Tr}\dot\rho_t \ln\rho^\beta(\lambda_t).$$

Тогда по формуле (2)

$$\sigma(\rho_t, \lambda_t) = -\operatorname{Tr}\Big[\mathcal{L}(\lambda_t)\rho_t\ln\rho_t\Big] + \operatorname{Tr}\Big[\mathcal{L}(\lambda_t)\rho_t\ln\rho^\beta(\lambda_t)\Big] = -\frac{d}{d\tau}S\Big(e^{\mathcal{L}(\lambda_t)\tau}\rho_t\|\rho^\beta(\lambda_t)\Big)\Big|_{\tau=0}, \tag{5}$$

где

$$S(\rho_1\|\rho_2) = \operatorname{Tr}\rho_1\ln\rho_1 - \operatorname{Tr}\rho_1\ln\rho_2$$

— квантовая относительная энтропия.

Теорема 1 (см. [31, 32]). *Если $\mathcal{L}(\lambda)\rho^\beta(\lambda) = 0$ при всех λ, т.е. гиббсовское состояние является стационарным для уравнения Линдблада при фиксированных управляющих параметрах λ, то $\sigma(\rho) \geqslant 0$.*

Доказательство. Доказательство основано на свойстве монотонности относительной энтропии (см. [6, 23]): для любой пары состояний ρ_1 и ρ_2 и любого вполне положительного и сохраняющего след отображения операторов плотности (квантового канала) Φ выполнено неравенство

$$S(\Phi\rho_1\|\Phi\rho_2) \leqslant S(\rho_1\|\rho_2).$$

Тогда, поскольку $\mathcal{L}(\lambda)$ при фиксированном λ является генератором квантовой динамической полугруппы и по условию $e^{\mathcal{L}(\lambda)\tau}\rho^\beta(\lambda) = \rho^\beta(\lambda)$,

$$\sigma(\rho) = -\frac{d}{d\tau}\, S\Big(e^{\mathcal{L}(\lambda)\tau}\rho \,\|\, \rho^\beta(\lambda)\Big)\Big|_{\tau=0} = -\lim_{\tau\to 0}\frac{1}{\tau}\left[S\Big(e^{\mathcal{L}(\lambda)\tau}\rho \,\|\, e^{\mathcal{L}(\lambda)\tau}\rho^\beta(\lambda)\Big) - S\big(\rho\|\rho^\beta(\lambda)\big)\right] \geqslant 0. \quad \square$$

Пусть теперь система связана с n тепловыми резервуарами с обратными температурами $\beta_1, \ldots, \beta_n$ и генератор Линдблада $\mathcal{L}(\lambda_t)$ имеет вид

$$\mathcal{L}(\lambda_t) = \sum_{r=1}^{n} \mathcal{L}_r(\lambda_t),$$

где генератор $\mathcal{L}_r(\lambda_t)$ соответствует взаимодействию системы с r-м резервуаром. Тогда

$$J(\rho,\lambda) = -\sum_r \beta_r \operatorname{Tr}\Big\{\big[\mathcal{L}_r(\lambda)\rho\big]\, H_S\Big\} = \sum_r \operatorname{Tr}\Big\{\big[\mathcal{L}_r(\lambda)\rho\big]\ln\rho^{\beta_r}(\lambda)\Big\}, \tag{6}$$

$$\sigma(\rho,\lambda) = -\sum_r \operatorname{Tr}\Big\{\big[\mathcal{L}_r(\lambda)\rho\big]\ln\rho\Big\} + J(\rho,\lambda) = -\frac{d}{d\tau}\sum_{r=1}^{n} S\Big(e^{\mathcal{L}_r(\lambda)\tau}\rho\|\, \rho^{\beta_r}(\lambda)\Big)\Big|_{\tau=0}. \tag{7}$$

В этом случае достаточным условием неотрицательности производства энтропии, очевидно, является

$$\mathcal{L}_r(\lambda)\rho^{\beta_r}(\lambda) = 0$$

для всех $r = 1, \ldots, n$ и для всех λ, т.е. гиббсовское состояние с обратной температурой β_r, должно быть стационарным для соответствующего генератора.

3. Общее определение производства энтропии

В данном разделе мы дадим общее определение производства энтропии для открытой квантовой системы, динамика которой описывается уравнением Линдблада (1). Как сказано во введении, для этого необходимо определить поток энтропии $J(\rho,\lambda)$ из системы в окружение.

Рассмотрим бесконечно малый интервал времени dt. Тогда действие динамика системы на этом интервале может быть представлено в виде действия некоторого квантового канала Φ:

$$\rho_{t+dt} = \rho_t + \mathcal{L}(\lambda_t)\rho_t dt + o(dt) \equiv \Phi(\rho_t) = V_0\rho_t V_0^\dagger + \sum_{k=1}^{K} V_k\rho_t V_k^\dagger + o(dt),$$

где

$$V_0 = V_0(\lambda_t) = 1 - iH(\lambda_t)dt - \frac{1}{2}\sum_{k=1}^{K} L_k(\lambda_t)^\dagger L_k(\lambda_t)dt,$$

$$V_k = V_k(\lambda_t) = L_k(\lambda_t)\sqrt{dt}, \quad k = 1, \ldots, K.$$

Легко видеть, что

$$V_0^\dagger V_0 + \sum_{k=1}^{K} V_k^\dagger V_k = I + o(dt),$$

где I — тождественный оператор, т.е. мы получили представление Крауса для квантового канала Φ.

Для того чтобы определить поток энтропии, надо иметь некоторые сведения об окружении и о его взаимодействии с системой. В квантовой теории информации для минимального описания окружения используется концепция комплементарного канала (см. [11, 5, 6]). Канал Φ отображает множество операторов плотности на $\mathscr{H}_S$ в себя. Он может быть представлен как

$$\Phi(\rho) = \operatorname{Tr}_E U\Big(\rho \otimes |0\rangle\langle 0|\Big)U^\dagger, \tag{8}$$

где $|0\rangle$ — единичный вектор в некотором конечномерном гильбертовом пространстве $\mathscr{H}_E$, U — унитарный оператор в $\mathscr{H}_S \otimes \mathscr{H}_E$ и Tr_E — частичный след по пространству $\mathscr{H}_E$.

Представление (8) канала Φ определено неоднозначно: одна и та же динамика системы может порождаться разными моделями взаимодействия с окружением. Если мы зафиксируем представление (8), то комплементарный канал определяется как

$$\widetilde{\Phi}(\rho) = \operatorname{Tr}_S U\big(\rho \otimes |0\rangle\langle 0|\big)U^\dagger,$$

Tr_S — частичный след по пространству $\mathscr{H}_S$. Таким образом, комплементарный канал переводит состояние системы в состояние («эффективного») окружения. В нашем случае $\mathscr{H}_E$ — это $(K+1)$-мерное пространство и

$$\begin{aligned}\widetilde{\Phi}(\rho_t) = \left(1 - \sum_{k=1}^{K} \operatorname{Tr}[L_k^\dagger(\lambda_t)L_k(\lambda_t)\rho_t]dt\right)|0\rangle\langle 0| \\ + \sum_{k=1}^{K}\Big(\operatorname{Tr}[L_k(\lambda_t)\rho_t]\,|k\rangle\langle 0| + \operatorname{Tr}\Big[L_k^\dagger(\lambda_t)\rho_t\Big]|0\rangle\langle k|\Big)\sqrt{dt} \\ + \sum_{j,k=1}^{K}\operatorname{Tr}\Big[L_k^\dagger(\lambda_t)L_j(\lambda_t)\rho_t\Big]|j\rangle\langle k|\,dt,\end{aligned} \tag{9}$$

где $\{|0\rangle, |1\rangle, \ldots, |K\rangle\}$ — ортонормированный базис в $\mathscr{H}_E$.

Произвол в выборе ортонормированного базиса соответствует произволу в выборе операторов L_k в уравнении Линдблада (1). Известно, что уравнение Линдблада инвариантно относительно следующих преобразований (см. [2]):

(1) унитарных преобразований

$$L_k \to L'_k = \sum_{j=1}^{K} u_{kj}L_j,$$

где $\{u_{kj}\}$ — произвольная унитарная матрица размерности $K \times K$;

(2) неоднородных преобразований

$$\begin{aligned}L_k &\to L'_k = L_k + a_k, \\ H &\to H' = H + \frac{1}{2i}\sum_{k=1}^{K}(a_k^* L_k - a_k L_k^\dagger) + b,\end{aligned}$$

где a_k — произвольные комплексные числа, а b — произвольное вещественное число. Можно показать, что эти преобразования соответствуют унитарным преобразованиям ортонормированного базиса $\{|0\rangle, |1\rangle, \ldots, |K\rangle\}$ пространства $\mathscr{H}_E$.

Пусть теперь элементы базиса $|0\rangle, |1\rangle, \ldots, |K\rangle$ соответствуют определенным приращениям энтропии окружения за интервал dt. Стоит отметить, что, вообще говоря, энтропия окружения, как правило, бесконечна. Тем не менее, именно приращение энтропии может быть конечным. В представлении (8) состояние $|0\rangle$ является начальным состоянием эффективного окружения. Поэтому оно соответствует нулевому приращению энтропии окружения. Обозначим приращения энтропии, которым соответствуют состояния $|k\rangle$, $k = 1, \ldots, K$, через $\Delta s_k(\lambda_t)$. Например, если

мы имеем дело с тепловым резервуаром с обратной температурой β, то приращение энтропии резервуара связано с приращением энергии резервуара $\Delta E_k(\lambda_t)$ формулой

$$\Delta s_k(\lambda_t) = \beta \Delta E_k(\lambda_t).$$

В этом случае среднее приращение энтропии окружения $J(\rho_t, \lambda_t)dt$ составляет

$$J(\rho_t, \lambda_t)dt = \operatorname{Tr} \widetilde{\Phi}(\rho_t)\Delta S(\lambda_t) = \sum_{k=1}^{K} \operatorname{Tr}\left[L_k^\dagger(\lambda_t)L_k(\lambda_t)\rho_t\right]\Delta s_k(\lambda_t)dt, \tag{10}$$

где мы ввели оператор приращения энтропии

$$\Delta S(\lambda_t) = \sum_{k=1}^{K} \Delta s_k(\lambda_t) \left|k\right\rangle \left\langle k\right|.$$

Соответственно, выражения для потока энтропии из системы в окружение и производства энтропии имеют вид

$$J(\rho_t, \lambda_t) = \sum_k \operatorname{Tr}\left[L_k^\dagger(\lambda_t)L_k(\lambda_t)\rho_t\right]\Delta s_k(\lambda_t), \tag{11}$$

$$\sigma(\rho_t, \lambda_t) = -\operatorname{Tr}\left[\big(\mathcal{L}(\lambda_t)\rho_t\big)\ln\rho_t\right] + \sum_k \operatorname{Tr}\left[L_k^\dagger(\lambda_t)L_k(\lambda_t)\rho_t\right]\Delta s_k(\lambda_t). \tag{12}$$

Во введении был поставлен вопрос о минимальной информации об окружении и его взаимодействии с системой, которой должно быть дополнено уравнение Линдблада, для того чтобы определить поток энтропии из системы в окружение и, затем, производство энтропии. Теперь мы можем ответить на этот вопрос: такой информацией является

(a) специальный выбор операторов L_k, которые соответствуют переходам в окружении $|0\rangle \to |k\rangle$ с определенными приращениями энтропии, и
(b) б) величины этих приращений $\Delta s_k(\lambda)$.

Эти сведения могут быть получены исходя из физических соображений. В большинстве случаев те операторы Линдблада, с которыми обычно выписывается уравнение Линдблада для конкретной системы и конкретного режима взаимодействия с резервуаром, и являются подходящими операторами. Величины приращений энтропии также можно вывести исходя из физической модели взаимодействия системы с резервуаром. Некоторые примеры будут рассмотрены в разделе 5, после того как (в следующем разделе) будет доказана теорема о неотрицательности производства энтропии.

Замечание. Отметим, что пространство $\mathscr{H}_E$, хоть и имеет отношение к реальному окружению, но не тождественно «настоящему» гильбертовому пространству окружения (пространству, где действует оператор H_E из (3)). В частности, $\mathscr{H}_E$ конечномерно, тогда как «настоящее» пространство окружения бесконечномерно. Пространство $\mathscr{H}_E$ — это математическая конструкция, которую в данном контексте можно назвать пространством переходов в окружении, вызванных взаимодействием с системой.

4. Неотрицательность производства энтропии

Определение. Будем говорить, что уравнение Линдблада (1) является *термодинамически состоятельным*, если оно удовлетворяет двум следующим свойствам:

(a) Если возможен переход k, то возможен и обратный переход, обозначаемый $\tilde{k}$, для которого $\Delta s_{\tilde{k}} = -\Delta s_k$. Данное отображение есть инволюция, т.е. $\tilde{\tilde{k}} = k$.
(b) Более того, соответствующие операторы перехода связаны соотношением

$$L_k(\lambda) = L_{\tilde{k}}^\dagger(\lambda) e^{\Delta s_k(\lambda)/2}. \tag{13}$$

Это определение введено в [19, 18] наряду с двумя другими свойствами, которых мы коснемся далее (условие (20) и условия (25)–(26)), в которых при нашем подходе в общем случае нет необходимости.

Теорема 2. *Если уравнение Линдблада термодинамически состоятельно, то производство энтропии* (12) *неотрицательно.*

Доказательство. Подстановка (1) в (12) дает

$$\sigma(\rho) = \sum_k \operatorname{Tr}\left(L_k\rho L_k^\dagger(\Delta s_k - \ln\rho) + \rho L_k \rho \ln\rho L_k^\dagger\right) =$$
$$= \sum_k \operatorname{Tr} L_k\rho\left(L_k^\dagger \Delta s_k - [L_k^\dagger, \ln\rho]\right).$$

Пусть спектральное разложение ρ имеет вид

$$\rho = \sum_{i=1}^{d} p_i \left|e_i\right\rangle \left\langle e_i\right|,$$

где d — размерность $\mathscr{H}_S$. Введем обозначение $\langle e_i|L_k|e_j\rangle = L_k^{ij}$. Тогда, представляя след в виде

$$\operatorname{Tr} A = \sum_i \langle e_i|A|e_i\rangle,$$

получаем

$$\sigma(\rho) = \sum_k \sum_{ij} |L_k^{ij}|^2 p_j \left(\ln\frac{p_j}{p_i} + \Delta s_k\right) =$$
$$= \frac{1}{2}\sum_k\sum_{ij}\left[|L_k^{ij}|^2 p_j\left(\ln\frac{p_j}{p_i}+\Delta s_k\right) + |L_{\tilde{k}}^{ji}|^2 p_i\left(\ln\frac{p_i}{p_j}+\Delta s_{\tilde{k}}\right)\right] =$$
$$= \frac{1}{2}\sum_k\sum_{ij}|L_k^{ij}|^2\left[p_j\left(\ln\frac{p_j}{p_i}+\Delta s_k\right) + p_i e^{-\Delta s_k}\left(\ln\frac{p_i}{p_j}-\Delta s_k\right)\right] =$$
$$= \frac{1}{2}\sum_k\sum_{ij}|L_k^{ij}|^2 p_j\left(\frac{p_i}{p_j}e^{-\Delta s_k}-1\right)\ln\left(\frac{p_i}{p_j}e^{-\Delta s_k}\right).$$

Неотрицательность этого выражения следует из неравенства $(x-1)\ln x \geqslant 0$. □

5. Примеры

Проиллюстрируем использование выражений (11) и (12) на примере конкретной систем при двух различных моделях взаимодействия с окружением. В обоих случаях в качестве систему будем рассматривать пару связанных двухуровневых систем A и B с гамильтонианом

$$H_S = H_0 + \nu V = E_A a^\dagger a + E_B b^\dagger b + \nu(a^\dagger b + a b^\dagger), \tag{14}$$

где $\nu > 0$ — константа взаимодействия двухуровневых систем, a ($a^\dagger$) и b ($b^\dagger$) — операторы уничтожения (рождения) для подсистем A и B соответственно. Они удовлетворяют соотношениям

$$aa^\dagger + a^\dagger a = 1, \quad aa = 0,$$
$$bb^\dagger + b^\dagger b = 1, \quad bb = 0,$$
$$ab - ba = a^\dagger b - ba^\dagger = 0.$$

Пусть подсистема A связана с «теплым» резервуаром с обратной температурой β_h, а подсистема B — с «холодным» резервуаром с обратной температурой $\beta_c > \beta_h$.

В качестве первой модели взаимодействия системы с резервуарами мы рассмотрим режим слабой связи. Пусть гамильтониан большой системы имеет вид

$$H = H_0 + \nu V + H_h + H_c + \lambda H_{Ah} + \lambda H_{Bc}. \tag{15}$$

Здесь H_h и H_c — свободные гамильтонианы резервуаров, $H_{Ah} = (a + a^\dagger)\otimes R_h$ и $H_{Bc} = (b + b^\dagger)\otimes R_c$ — гамильтонианы взаимодействий двухуровневых систем с резервуаром, R_h и R_c — некоторые

операторы, действующие в соответствующих резервуарах, λ — малый безразмерный параметр. Тогда уравнение Линдблада может быть записано в виде (см. [2, 32, 10, 8])

$$\frac{d\rho}{dt} = -i[H_S, \rho] + \mathcal{D}_h(\rho) + \mathcal{D}_c(\rho), \tag{16}$$

где D_h и D_c — диссипаторы, связанные с взаимодействием с теплым и холодным резервуаром соответственно:

$$\mathcal{D}_r(\rho) = \sum_{j=A,B} \gamma_{jr} \left(F_{jr}\rho F_{jr}^\dagger - \frac{1}{2}\{F_{jr}^\dagger F_{jr}, \rho\} + e^{-\beta_r\omega_j} \left(F_{jr}^\dagger \rho F_{jr} - \frac{1}{2}\{F_{jr}F_{jr}^\dagger, \rho\} \right) \right), \tag{17}$$

$r = h, c$, где

$$\begin{aligned}
F_{Ah} &= |e_{01}\rangle \langle e_{01}| (a + a^\dagger) |e_{11}\rangle \langle e_{11}| + |e_{00}\rangle \langle e_{00}| (a + a^\dagger) |e_{10}\rangle \langle e_{10}|, \\
F_{Bh} &= |e_{10}\rangle \langle e_{10}| (a + a^\dagger) |e_{11}\rangle \langle e_{11}| + |e_{00}\rangle \langle e_{00}| (a + a^\dagger) |e_{01}\rangle \langle e_{01}|, \\
F_{Ac} &= |e_{01}\rangle \langle e_{01}| (b + b^\dagger) |e_{11}\rangle \langle e_{11}| + |e_{00}\rangle \langle e_{00}| (b + b^\dagger) |e_{10}\rangle \langle e_{10}|, \\
F_{Bc} &= |e_{10}\rangle \langle e_{10}| (b + b^\dagger) |e_{11}\rangle \langle e_{11}| + |e_{00}\rangle \langle e_{00}| (b + b^\dagger) |e_{01}\rangle \langle e_{01}|.
\end{aligned}$$

Здесь $|e_{00}\rangle, \ldots, |e_{11}\rangle$ — собственные векторы H_S, равные (с соответствующими собственными значениями)

$$\begin{aligned}
&\varepsilon_{00} = 0, \quad |e_{00}\rangle = |00\rangle, \quad \varepsilon_{11} = E_A + E_B, \quad |e_{11}\rangle = |11\rangle, \\
&\varepsilon_{01} = \frac{1}{2}(E_A + E_B - \delta E), \quad |e_{01}\rangle = \sqrt{\frac{\delta E + \Delta E}{2\delta E}}\,|01\rangle - \sqrt{\frac{2\nu^2}{\delta E(\delta E + \Delta E)}}\,|10\rangle, \\
&\varepsilon_{10} = \frac{1}{2}(E_A + E_B + \delta E), \quad |e_{10}\rangle = \sqrt{\frac{\delta E - \Delta E}{2\delta E}}\,|01\rangle + \sqrt{\frac{2\nu^2}{\delta E(\delta E - \Delta E)}}\,|10\rangle,
\end{aligned}$$

$\Delta E = E_A - E_B$, $\delta E = \sqrt{\Delta E^2 + 4\nu^2}$. Базисные векторы $|0\rangle$ и $|1\rangle$ для фиксированной двухуровневой системы обозначают состояния соответственно основное и возбужденное состояния этой системы, $a|1\rangle = |0\rangle$, $a^\dagger|0\rangle = |1\rangle$. Также

$$\begin{aligned}
\omega_A &= \varepsilon_{11} - \varepsilon_{01} = \varepsilon_{10} - \varepsilon_{00} = \varepsilon_{10}, \\
\omega_B &= \varepsilon_{11} - \varepsilon_{10} = \varepsilon_{01} - \varepsilon_{00} = \varepsilon_{01}
\end{aligned}$$

суть боровские частоты (разности между собственными энергиями), участвующие в выражениях для диссипаторов (17). Константы γ_{jr} связаны с корреляционными функциями резервуаров. Они пропорциональны λ^2 и могут быть явно выражены через операторы R_r и H_{jr}, но нам не понадобится их явный вид. Также в (16) мы пренебрегли гамильтонианом лэмбовского сдвига: он ведет к модификации параметров гамильтониана системы (E_A, E_B и ν), что не играет существенной роли в нашем случае.

Выведем выражение для производства энтропии. Для этого из физических соображений необходимо выбрать специальный вид операторов Линдблада, которым соответствуют определенные изменения энтропии в резервуарах (или, эквивалентно, изменения энергии, так как резервуары — тепловые), и величины этих изменений. В данном случае определенным изменениям энергии резервуаров отвечают переходы между энергетическими уровнями всей системы H_S. Операторы F_{Ar} и F_{Br}, участвующие в выражении (17), как раз и соответствуют переходам между энергетическими уровнями всей системы, поэтому именно они и являются подходящими. Пусть, например, двухуровневые системы представляют собой двухуровневые атомы, а резервуары — электромагнитное поле. Тогда переход системы между уровнями энергии с разностью ω_j в результате взаимодействия с резервуаром r соответствует поглощению/испусканию фотона с энергией ω_j и увеличению/уменьшению энтропии резервуара на $\Delta s_{Ar} = \beta_r\omega_j$. Тогда

$$J(\rho) = \sum_{j=A,B} \sum_{r=h,c} \beta_r\omega_j\gamma_{jr}[\operatorname{Tr}(F_{jr}^\dagger F_{jr}\rho) - e^{-\beta_r\omega_j} \operatorname{Tr}(F_{jr}F_{jr}^\dagger\rho)] = -\sum_{r=h,c} \beta_r \operatorname{Tr}[(\mathcal{D}_r\rho)H_S],$$

что совпадает с (6). В справедливости последнего равенства здесь можно убедиться, используя коммутационные соотношения $[F_{jr}, H_S] = \omega_j F_{jr}$ (см. также раздел 8).

Рассмотрим теперь другую модель резервуара (см. [9]). Пусть теплый резервуар состоит из бесконечного числа копий двухуровневой системы с гамильтонианом $E_A h^\dagger h$ (т.е. совпадающим с гамильтонианом подсистемы A), начальное состояние каждой копии — гиббсовское: $\exp(-\beta_h H_A)/\operatorname{Tr}\exp(-\beta_h H_A)$. Каждая из этих копий взаимодействует с подсистемой A на протяжении промежутка времени τ в соответствии с гамильтонианом взаимодействия H_{Ah}, после чего заменяется следующей копией. Аналогично холодный резервуар также состоит из бесконечного числа копий копий двухуровневой системы с гамильтонианом $E_B c^\dagger c$, начальное состояние каждой копии — также гиббсовское: $\exp(-\beta_c H_B)/\operatorname{Tr}\exp(-\beta_c H_B)$. Взаимодействие каждой копии с подсистемой B на протяжении промежутка времени τ определяется гамильтонианом взаимодействия H_{Bc}. Гамильтонианы взаимодействия имеют вид

$$H_{Ah} = \lambda(ha^\dagger + h^\dagger a),$$
$$H_{Bc} = \lambda(cb^\dagger + c^\dagger b),$$

где $h^\dagger$, h, $c^\dagger$, c — операторы рождения и уничтожения в теплом и холодном резервуарах соответственно. В пределе $\tau \to 0$, $\lambda \to \infty$, $\lambda^2\tau = const$ (такой предел называется в [18] моделью непрерывных измерений, в [22] предложено название «стробоскопический предел») динамика приведенной матрицы плотности системы также описывается уравнением Линдблада (16), но с диссипаторами

$$\begin{aligned}\mathcal{D}_h(\rho) &= \gamma_h\left(a\rho a^\dagger - \frac{1}{2}\{a^\dagger a, \rho\} + e^{-\beta_h E_A}\left(a^\dagger \rho a - \frac{1}{2}\{aa^\dagger, \rho\}\right)\right),\\ \mathcal{D}_c(\rho) &= \gamma_c\left(b\rho b^\dagger - \frac{1}{2}\{b^\dagger b, \rho\} + e^{-\beta_h E_B}\left(b^\dagger \rho b - \frac{1}{2}\{bb^\dagger, \rho\}\right)\right),\end{aligned} \tag{18}$$

где $\gamma_h, \gamma_c > 0$ — некоторые константы (пропорциональные λ^2). В данном случае поток тепла в теплый (холодный) резервуар связан с переходом не между уровнями энергии всей системы, а с переходом между уровнями энергии подсистемы A (B). Например, переход из возбужденного состояние в основное в подсистеме A отвечает переходу из основного состояния в возбужденное в двухуровневой системе, относящейся к теплому резервуару, т.е. приращению E_A энергии резервуара и, соответственно, приращению $\Delta s_{Ah} = \beta_h E_A$ энтропии резервуара. Поэтому операторы Линдблада, которые связаны с определенными изменениями энтропии резервуаров, снова совпадают с операторами, использованными в выражении для диссипаторов, в данном случае — в (18). Тогда

$$J(\rho) = \beta_h E_A \gamma_h[\operatorname{Tr}(a^\dagger a\rho) - e^{-\beta_h E_A}\operatorname{Tr}(aa^\dagger\rho)] + \beta_c E_B \gamma_c[\operatorname{Tr}(b^\dagger b\rho) - e^{-\beta_c E_B}\operatorname{Tr}(bb^\dagger\rho)].$$

В обоих примерах условия термодинамической состоятельности выполнены. Так, например, в последнем случае

$$L_1 = \sqrt{\gamma_h}\, a, \quad L_{\tilde{1}} = L_3 = e^{-\beta_h E_A/2}\sqrt{\gamma_h}\, a^\dagger,$$
$$L_2 = \sqrt{\gamma_c}\, b, \quad L_{\tilde{2}} = L_4 = e^{-\beta_c E_B/2}\sqrt{\gamma_c}\, b^\dagger.$$

Замечание. Уравнение (16) с диссипаторами (18) возникает также и в режиме слабой связи, но в так называемом локальном подходе к построению уравнения Линдблада. В самом деле, диссипаторы (17) переходят в диссипаторы (18) при $\nu = 0$, т.е. при пренебрежении влияния взаимодействия частей системы друг с другом на взаимодействие системы с резервуаром. Локальный подход может быть обоснован строго при малых ν в рамках теории возмущений по этому параметру (см. [33]). Локальный подход соответствует нулевому порядку теории возмущений.

Для определения производства энтропии в рамках локального подхода можно воспользоваться формулой (7), которая верна для режима слабой связи, однако первый нетривиальный член разложения этого выражения по ν имеет порядок ν^2. Следовательно, для получения корректного нетривиального выражения для производства энтропии необходимо выписать поправки к

локальным диссипаторам (18) до членов порядка ν^2. Эти поправки и выражение для производства энтропии получены в [33]. Вывод же выражения порядка ν^2 исходя из уравнения Линдблада, выписанного в нулевом порядке по ν, является некорректным и приводит к отрицательным значениям производства энтропии (см. [20]).

6. Сравнение с определением производства энтропии, основанного на концепции квантовых траекторий

Определение производства энтропии, основе концепции квантовых траекторий предложено в [18] для случая модели непрерывных измерений, пример которой был приведен в предыдущем разделе. В [19] оно было распространено на произвольные открытые квантовые системы, описываемые уравнением Линдблада. Решение уравнения Линдблада ρ_t может быть представлено в виде $\rho_t = \mathsf{M}\varrho_t$, где M обозначает математическое ожидание, а ϱ_t — стохастическая матрица плотности, удовлетворяющая уравнению (см. [2])

$$d\varrho_t = -idt\{H_{\text{eff}}(\lambda_t)\varrho_t - \varrho_t H_{\text{eff}}^\dagger(\lambda_t) - \operatorname{Tr}[H_{\text{eff}}(\lambda_t)\varrho_t - \varrho_t H_{\text{eff}}^\dagger(\lambda_t)]\varrho_t\} + \\ + \sum_k dN_k(t)\left[\frac{L_k(\lambda_t)\varrho_t L_k^\dagger(\lambda_t)}{\operatorname{Tr}[L_k^\dagger(\lambda_t)L_k(\lambda_t)\varrho_t]} - \varrho_t\right].$$

Здесь

$$H_{\text{eff}}(\lambda_t) = H(\lambda_t) - \frac{i}{2}\sum_k L_k^\dagger(\lambda_t)L_k(\lambda_t)$$

— эффективный неэрмитов гамильтониан,

$$dN_k(t) = N_k(t+dt) - N_k(t)$$

— приращение k-го процесса Пуассона, который равен единице, если в системе в интервале $[t, t+dt)$ произошел квантовый переход, соответствующий оператору L_k, и равен нулю в противном случае. Эти приращения удовлетворяют следующим свойствам:

$$\begin{aligned} dN_k(t)dN_l(t) &= \delta_{kl}dN_k(t), \\ \mathsf{M}[dN_k(t)] &= \operatorname{Tr}[L_k^\dagger(\lambda_t)L_k(\lambda_t)\rho_t]dt, \end{aligned} \tag{19}$$

где δ_{kl} — символ Кронекера.

Пусть уравнение Линдблада является термодинамически состоятельным и выполнено следующее дополнительное условие (которое в [18, 19] включается в определение термодинамической состоятельности): операторы L_k симметричны относительно обращения времени. Математически это выражается в том, что они коммутируют с оператором обращения времени Θ (см. [29]):

$$L_k(\lambda) = \Theta L_k(\lambda)\Theta. \tag{20}$$

Тогда можно записать стохастический аналог уравнения баланса энтропии (2):

$$ds_{\text{tot}}(t) = ds(t) + ds_E(t), \tag{21}$$

где $ds_{\text{tot}}(t)$ — стохастическое полное приращение энтропии в интервале $[t, t+dt)$,

$$ds_E(t) = \sum_k dN_k(t)\Delta s_k \tag{22}$$

— стохастическое приращение энтропии окружения в этом интервале, и, наконец, ds — стохастическое приращение энтропии системы. Оно имеет вид

$$\begin{aligned} s(t) &= -\operatorname{Tr}\varrho_t \ln\rho_t, \\ \mathsf{M}s(t) &= -\operatorname{Tr}\rho_t\ln\rho_t = S(\rho_t). \end{aligned} \tag{23}$$

Усредненные величины J и σ из (2) тогда имеют вид

$$J(\rho_t, \lambda_t) = \frac{\mathsf{M}[ds_{\mathrm{env}}]}{dt} = \sum_k \operatorname{Tr}\left[L_k^\dagger(\lambda_t) L_k(\lambda_t)\rho_t\right]\Delta s_k(\lambda_t),$$
$$\sigma(\rho_t, \lambda_t) = \frac{\mathsf{M}[ds_{\mathrm{tot}}]}{dt} = -\operatorname{Tr}\left[\big(\mathcal{L}(\lambda_t)\rho_t\big)\ln\rho_t\right] + \sum_k \operatorname{Tr}\left[L_k^\dagger(\lambda_t) L_k(\lambda_t)\rho_t\right]\Delta s_k(\lambda_t).$$

Полученные формулы совпадают с (11) и (12), поэтому подход на основе квантовых траекторий близок к представленному в этой работе подходу на основе комплементарного канала. Так же, как и в нашем подходе, для определения производства энтропии на основе квантовых траекторий необходимо выбрать операторы L_k в пределах произвола, задаваемом уравнением Линдблада, и приращения Δs_k энтропии окружения, соответствующие этим операторам.

Подход на основе квантовых траекторий предполагает бесконечно частые измерения резервуара. Необходимым условием применимости этого подхода является возможность проводить измерения резервуара, которые не влияют на динамику системы. Однако, вообще говоря, изменение состояния резервуара в результате его измерения может повлиять на динамику системы (см. [22]). Условие отсутствия влияния измерений резервуара на динамику системы выполнено в модели непрерывного взаимодействия (см. второй пример в предыдущем разделе). В этом случае мы измеряем каждый раз ту конечномерную часть резервуара, которая только что взаимодействовала с системой и в будущем взаимодействовать уже не будет. Поэтому ее измерение дает информацию о состоянии системы, но не влияет на ее дальнейшую динамику. В общем же случае это условие требует обоснования.

В нашем подходе на основе комплементарного канала и «пространства переходов в окружении» $\mathscr{H}_E$ это обоснование легко получить, если иметь в виду измерения именно в этом пространстве. Достаточное условие того, что измерение слабо влияет на динамику системы, состоит в том, что состояние окружения содержится в базисе, который задает схему измерения [2, п. 6.2]. Вернемся к рассуждениям раздела 3 и допустим, что в конце бесконечно малого промежутка времени dt мы проводим измерение системы $\mathscr{H}_E$ в базисе $|0\rangle, \ldots, |K\rangle$. Базис содержит состояние пространстве переходов окружения $|0\rangle$, что и обеспечивает условие того, что данное измерение не повлияет на динамику системы. Формула (10) не зависит от того, проводим ли мы измерение в пространстве $\mathscr{H}_E$ или нет. Мы можем считать, что в конце каждого интервала dt мы проводим такое измерение, и тогда мы можем определить поток и производство энтропии исходя из концепции квантовых траекторий. Но если измерение не проводится, формула (10) как выражение для среднего от наблюдаемой ΔS (приращения энтропии окружения) по-прежнему справедлива и мы можем не обращаться к концепции квантовых траекторий.

Представляет интерес исследование вопроса, в любом ли случае можно предложить измерение в «реальном» гильбертовом пространстве окружения, которое соответствует описанному измерению в $\mathscr{H}_E$ и, следовательно, не влияет на динамику системы.

Также можно упомянуть, что близко к теории квантовых стохастических траекторий, предполагающих частые измерения окружения, находится теория квантового управления на основе неселективных измерений (см. [26, 30, 28, 4]), в которой также можно говорить о стохастических траекториях системы. Однако там измеряется сама система и смысл измерения, напротив, как раз и состоит в том, чтобы повлиять на ее динамику.

Представления о квантовых стохастических траекториях позволяет доказать теорему 2 о неотрицательности энтропии, как и следующую далее теорему 3 о неотрицательности адиабатического и неадиабатического вкладов в производство энтропии, на основе техник флуктуационных теорем (см. [16]), что сделано в [18, 19]. В следующем разделе мы приведем другое доказательство, не использующие представления о квантовых стохастических траекториях, а также докажем это утверждение для других случаев.

7. Адиабатический и неадиабатический вклады в производство энтропии

В классической и квантовой термодинамики возникает производство энтропии разделяют на адиабатическую и неадиабатическую части (см. [18, 19, 12, 34]):

$$\begin{aligned}\sigma(\rho_t,\lambda_t) &= \frac{d}{dt}S(\rho_t) + J(\rho_t,\lambda_t) = \sigma_{\mathrm{a}}(t) + \sigma_{\mathrm{na}}(\rho_t,\lambda_t),\\ \sigma_{\mathrm{na}}(\rho_t,\lambda_t) &= -S\big(\dot\rho_t\|\rho^{\mathrm{st}}(\lambda_t)\big)\\ &= \frac{d}{dt}S(\rho_t) + J_{\mathrm{ex}}(\rho_t,\lambda_t), \quad J_{\mathrm{ex}}(\rho_t,\lambda_t) = \operatorname{Tr}\dot\rho_t \ln\rho^{\mathrm{st}}(\lambda_t),\\ \sigma_{\mathrm{a}}(\rho_t,\lambda_t) &= J(\rho_t,\lambda_t) - J_{\mathrm{ex}}(\rho_t,\lambda_t) \equiv J_{\mathrm{hk}}(\rho_t,\lambda_t).\end{aligned} \tag{24}$$

Здесь $\sigma_{\mathrm{a}}(\rho_t,\lambda_t)$ и $\sigma_{\mathrm{na}}(\rho_t,\lambda_t)$ — соответственно адиабатический и неадиабатический вклады в производство энтропии, $\rho^{\mathrm{st}}(\lambda)$ — некоторое стационарное состояние при фиксированном значений λ, т.е. $\mathcal{L}(\lambda)\rho^{\mathrm{st}}(\lambda) = 0$. Как видно из формул (24), если λ_t изменяется много медленнее, чем происходит релаксация ρ_t к стационарному состоянию, т.е. можно считать, что в каждый момент времени $\rho_t = \rho^{\mathrm{st}}(\lambda_t)$ (адиабатический предел), то $\sigma_{\mathrm{na}}(\rho_t,\lambda_t) = 0$. Поэтому σ_{na} называется неадиабатическим вкладом в производство энтропии, или просто неадиабатическим производством энтропии: эта величина может быть отлична от нуля только за счет неадиабатических эффектов.

Адиабатическая часть представляет собой минимальное производство энтропии, необходимое для поддержания системы в неравновесном стационарном состоянии. В англоязычной литературе она также называется «housekeeping heat» (см. [12, 24, 17]), с чем связан нижний индекс «hk» в последней формуле в (24). Разность между полным потоком энтропии J и частью потока J_{hk}, необходимым для поддержания неравновесного стационарного состояния, называется избыточным потоком энтропии и обозначается J_{ex} (от «excess» — «избыточный»).

Разделение производства энтропии на адиабатическую и неадиабатическую части важно при изучении перевода системы из одного неравновесного стационарного состояния в другое: поскольку для поддержания неравновесного стационарного состояния системы требуется определенный постоянный поток энтропии из системы в окружение, то выделение неадиабатического вклада в производство энтропии более точно характеризует термодинамическую цену внешнего управления системой.

В классической термодинамике доказывается, что не только полное производство энтропии, но и по отдельности адиабатический и неадиабатический вклады в него неотрицательны (см. [12]). Обобщение этих теорем на квантовый случай дано в [18, 19], однако предполагаются дополнительные условия (25)–(26), которые выполнены не для всех физически интересных систем. В частности, они не выполнены для второй модели, рассмотренной в разделе 5: уравнение (1) с диссипаторами (18) имеет единственное стационарное решение, которое не коммутирует с H_S. Представляет интерес доказательство неотрицательности адиабатического и неадиабатического производства энтропии при как можно более общих условиях.

Неотрицательность неадиабатического производства энтропии гаранируется свойством монотонности относительной энтропии и уже доказана в теореме 1 (формально теорема сформулирована для случая, когда стационарное состояние — гиббсовское, однако это не было использовано в доказательстве). Поэтому стоит вопрос о неотрицательности только адиабатического производства энтропии.

В данном разделе мы сначала дадим альтернативное доказательство утверждения, доказанного в [18, 19] о неотрицательности адиабатического производства энтропии при введенных там ограничениях. Затем мы докажем неотрицательность адиабатического производства энтропии, если в стационарном состоянии адиабатическое производство энтропии равно нулю, а также в общем случае термодинамически состоятельного уравнения Линдблада, но в малой окрестности стационарного состояния.

Пусть

$$\rho^{\mathrm{st}}(\lambda)\,|\psi\rangle = 0 \Leftrightarrow |\psi\rangle = 0 \tag{25}$$

для всех λ и существует такое спектральное разложение

$$\rho^{\mathrm{st}}(\lambda) = \sum_{n=1}^{d} p_n(\lambda)|e_n(\lambda)\rangle\langle e_n(\lambda)|,$$

что выполнены следующие равенства:

$$\begin{aligned} &\rho^{\mathrm{st}} L_k(\lambda) = \varpi_k(\lambda) L_k(\lambda)\rho^{\mathrm{st}}(\lambda), \\ &[H(\lambda), \rho^{\mathrm{st}}(\lambda)] = \sum_k [L_k(\lambda)^\dagger L_k(\lambda), \rho^{\mathrm{st}}(\lambda)] = 0. \end{aligned} \tag{26}$$

Здесь $\varpi_k = p_n/p_m$ для всех $|e_n\rangle$ и $|e_m\rangle$, соединяемых оператором L_k (т.е. $\langle e_n|L_k|e_m\rangle \neq 0$). В частности, это означает, что каждый оператор L_k соединяет только те пары собственных векторов ρ^{st}, которые отвечают собственным значениям с одним и тем же отношением ϖ_k. Также второе условие в (26) означает, что стационарное состояние ρ^{st} диагонально в одном из собственных базисов гамильтониана H. Из условия (25) следует, что все $p_n > 0$, $n = 1, \ldots, d = \dim \mathscr{H}_S$.

Математически условия (25)–(26) обеспечивают то, что полугруппа, 0-двойственная к полугруппе, порождаемой генератором $\mathcal{L}$, также является квантовой марковской полугруппой (см. [14]). Это позволяет определить адиабатический и неадиабатический вклады в производство энтропии на языке квантовых стохастических траекторий и воспользоваться флуктуационными теоремами для доказательства их неотрицательности (см. [18, 19]). Дадим альтернативное доказательство.

Теорема 3. *Пусть уравнение Линдблада* (1) *термодинамически состоятельно и выполнены условия* (25)–(26). *Тогда* $\sigma_{\mathrm{a}}(\rho, \lambda) \geqslant 0$.

Доказательство. Если выполнены условия (26), то $J_{\mathrm{ex}}(t)$ может быть выражено как (см. [19])

$$J_{\mathrm{ex}}(\rho) = \sum_k \mathrm{Tr}(L_k^\dagger L_k \rho) \ln \varpi_k.$$

Тогда

$$\sigma_{\mathrm{a}}(\rho) = \sum_k \mathrm{Tr}(L_k^\dagger L_k \rho) \ln \frac{e^{\Delta s_k}}{\varpi_k}. \tag{27}$$

Поскольку ρ^{st} — стационарное состояние, то

$$-i[H, \rho^{\mathrm{st}}] + \sum_k \left(L_k \rho^{\mathrm{st}} L_k^\dagger - \frac{1}{2}\{\rho^{\mathrm{st}}, L_k^\dagger L_k\} \right) = 0.$$

Пользуясь (26), можно переписать это равенство как

$$\sum_k (\varpi_k^{-1} L_k L_k^\dagger - L_k^\dagger L_k)\rho^{\mathrm{st}} = 0,$$

или

$$\sum_k (\varpi_k^{-1} L_k L_k^\dagger - L_k^\dagger L_k) \sum_n p_n \, |e_n\rangle \, \langle e_n| = 0.$$

Умножая обе части этого равенства справа на $|e_n\rangle$ при фиксированном n и пользуясь тем, что $p_n \neq 0$, получаем

$$\sum_k (\varpi_k^{-1} L_k L_k^\dagger - L_k^\dagger L_k) \, |e_n\rangle = 0$$

при всех n, что означает

$$\sum_k \varpi_k^{-1} L_k L_k^\dagger = \sum_k L_k^\dagger L_k.$$

Следовательно,

$$\sum_k \varpi_k^{-1} \, \mathrm{Tr}(L_k L_k^\dagger \rho) = \sum_k \mathrm{Tr}(L_k^\dagger L_k \rho).$$

Воспользуемся теперь условиями термодинамической состоятельности уравнения Линдблада:

$$\sum_k \varpi_k^{-1} \operatorname{Tr}(L_k L_k^\dagger \rho) = \sum_k \varpi_{\tilde{k}}^{-1} \operatorname{Tr}(L_{\tilde{k}} L_{\tilde{k}}^\dagger \rho) = \sum_k \varpi_k e^{-\Delta s_k} \operatorname{Tr}(L_k^\dagger L_k \rho).$$

Поэтому

$$\sum_k \varpi_k e^{-\Delta s_k} \operatorname{Tr}(L_k^\dagger L_k \rho) = \sum_k \operatorname{Tr}(L_k^\dagger L_k \rho).$$

Вводя обозначение

$$\alpha_k = \operatorname{Tr}(L_k^\dagger L_k \rho) / \sum_j \operatorname{Tr}(L_j^\dagger L_j \rho),$$

получаем равенство

$$\sum_k \alpha_k \varpi_k e^{-\Delta s_k} = 1,$$

тогда как условие неотрицательности адиабатической энтропии ввиду (27) принимает вид

$$\sum_k \alpha_k \ln[\varpi_k e^{-\Delta s_k}] \leqslant 0,$$

Так как $\sum\limits_k \alpha_k = 1$, то вследствие вогнутости логарифма (применяя неравенство Иенсена) получаем, что в самом деле

$$\sum_k \alpha_k \ln[\varpi_k e^{-\Delta s_k}] \leqslant \ln \left[\sum_k \alpha_k \varpi_k e^{-\Delta s_k} \right] = 0. \qquad \square$$

Докажем теперь неотрицательность адиабатического производства энтропии, если в стационарном состоянии адиабатическое производство энтропии равно нулю, а также общем случае термодинамически состоятельного уравнения Линдблада, но в малой окрестности стационарного состояния.

Теорема 4. *Пусть уравнение Линдблада термодинамически состоятельно, $\rho^{\mathrm{st}}(\lambda)$ — некоторое стационарное состояние, зависящее от λ, и $\sigma_{\mathrm{a}}(\rho^{\mathrm{st}}(\lambda)) = 0$. Тогда $\sigma_{\mathrm{a}}(\rho, \lambda) \geqslant 0$ при всех ρ.*

Доказательство. Докажем утверждение от противного. Пусть $\sigma_{\mathrm{a}}(\bar{\rho}) < 0$ для некоторого $\bar{\rho}$. Введем тогда семейство состояний (снова для простоты опускаем λ)

$$\rho_\varepsilon = (1-\varepsilon)\rho^{\mathrm{st}} + \varepsilon\bar{\rho}, \quad 0 \leqslant \varepsilon \leqslant 1.$$

Тогда

$$\sigma_{\mathrm{na}}(\rho_\varepsilon) = \operatorname{Tr}\Big\{(\mathcal{L}\rho_\varepsilon)\big(\ln\rho_\varepsilon - \ln\rho^{\mathrm{st}}\big)\Big\} = \varepsilon \operatorname{Tr}\Big\{(\mathcal{L}\bar{\rho})\Big[\ln\big(\rho^{\mathrm{st}} + \varepsilon(\bar{\rho} - \rho^{\mathrm{st}})\big) - \ln\rho^{\mathrm{st}}\Big]\Big\} = O(\varepsilon^2)$$

при $\varepsilon \to 0$. В то же время, пользуясь линейностью $\sigma_{\mathrm{a}}(\rho)$ по ρ, имеем $\sigma_{\mathrm{a}}(\rho_\varepsilon) = \varepsilon\sigma_{\mathrm{a}}(\bar{\rho})$. Поэтому при достаточно малых $\varepsilon > 0$ имеем

$$\sigma(\rho_\varepsilon) = \varepsilon\sigma_{\mathrm{a}}(\bar{\rho}) + O(\varepsilon^2) < 0,$$

что противоречит теореме 2 о неотрицательности полного производства энтропии для термодинамически состоятельного уравнения Линдблада. $\square$

Следствие. *Пусть уравнение Линдблада термодинамически состоятельно. Существует такая окрестность стационарного состояния $\rho^{\mathrm{st}}(\lambda)$ (метрика задается, например, следовой нормой $\|\rho\|_1 = \operatorname{Tr}\sqrt{\rho\rho^\dagger}$), что $\sigma_{\mathrm{a}}(\rho, \lambda) \geqslant 0$, если ρ принадлежит этой окрестности.*

Доказательство. Если $\sigma_{\mathrm{a}}(\rho^{\mathrm{st}}(\lambda)) > 0$, то утверждение следует из непрерывной зависимости $\sigma_{\mathrm{a}}(\rho)$ от ρ. Если $\sigma_{\mathrm{a}}(\rho^{\mathrm{st}}(\lambda)) = 0$, то утверждение следует из теоремы 4. $\square$

8. Случай нескольких тепловых резервуаров

В данном разделе мы обсудим условия, при которых определение (12) сводится к определению (7), а также получим соотношение между выражениями (5) и (7).

Пусть окружение состоит из некоторого количества тепловых резервуаров, операторы L_k в (11)–(12) соответствуют определенным приращениям энтропии окружения вида $\Delta s_k(\lambda) = \beta_k\omega_k(\lambda)$, где $\omega_k(\lambda)$ — приращения энергии окружения, β_k — обратная энтропия резервуара, взаимодействию с которым отвечает оператор $L_k(\lambda)$. Также предполагаем, что уравнение Линдблада термодинамически состоятельно и $\beta_{\tilde{k}} = \beta_k$, $\omega_{\tilde{k}}(\lambda) = -\omega_{\tilde{k}}(\lambda)$.

Среди β_k могут быть и другие повторяющиеся значения, помимо пар β_k, $\beta_{\tilde{k}} = \beta_k$, если среди пар $(L_k, L_{\tilde{k}})$ есть операторы, отвечающие взаимодействию с одним и тем же резервуаром. Так, в диссипаторе (17) участвуют две пары операторов: $(F_{Ar}, F_{Ar}^\dagger)$ и $(F_{Br}, F_{Br}^\dagger)$.

Наконец, предполагаем, что для всех k выполнено следующее коммутационное соотношение:

$$[L_k(\lambda), H_S(\lambda)] = \omega_k(\lambda)L_k(\lambda). \tag{28}$$

Тогда производство энтропии (12) принимает вид

$$\sigma(\rho,\lambda) = -\frac{d}{d\tau}\sum_k S\big(e^{\mathcal{D}_k(\lambda)\tau}\rho\|\rho^{\beta_k}(\lambda)\big)\bigg|_{\tau=0}, \tag{29}$$

где $\rho^{\beta_k}(\lambda_t)$ — гиббсовское состояние (4),

$$\mathcal{D}_k(\lambda) = L_k(\lambda)\rho L_k(\lambda) - \frac{1}{2}\{L_k(\lambda)L_k(\lambda)^\dagger, \rho\}.$$

В самом деле, поток энтропии из системы в окружение имеет вид

$$J(\rho,\lambda) = \sum_k \beta_k\omega_k(\lambda)\operatorname{Tr}\Big[L_k(\lambda)^\dagger L_k(\lambda)\rho\Big].$$

При выполнении условия (28) легко показать, что

$$\omega_k \operatorname{Tr}[L_k^\dagger L_k\rho] = -\mathcal{D}_k\rho.$$

Выражая $-\mathcal{D}_k\rho$ через $\ln\rho^{\beta_k}$, как в (6), получаем (29). Пользуясь условиями (28) и (13), легко увидеть, что $\mathcal{D}_k\rho^{\beta_k} = 0$.

Если, кроме того, существует стационарное состояние $\rho^{\mathrm{st}}(\lambda)$, удовлетворяющее (25)–(26), то соотношение между полным, адиабатическим и неадиабатическим производствами энтропии принимает вид

$$\frac{d}{d\tau}S\big(e^{\mathcal{L}(\lambda)\tau}\rho\|\rho^{\mathrm{st}}(\lambda)\big)\bigg|_{\tau=0} = \frac{d}{d\tau}\sum_k S\big(e^{\mathcal{D}_k(\lambda)\tau}\rho\,\|\,\rho^{\beta_k}(\lambda)\big)\bigg|_{\tau=0} - \sum_k \operatorname{Tr}\Big[L_k(\lambda)^\dagger L_k(\lambda_t)\rho\Big]\ln\frac{e^{\Delta s_k(\lambda)}}{\varpi_k(\lambda)}. \tag{30}$$

Для адиабатического производства энтропии здесь использована формула (27).

Соотношение (30) связывает между собой определения (5), которое дано в [31] для уравнения Линдблада общего вида, и (7), полученное в [32] для случая нескольких тепловых резервуаров, взаимодействующих с системой в режиме слабой связи.

На это соотношение можно посмотреть и следующим образом. В левой части соотношения — относительная энтропия между действием оператора эволюции с полным генератором Линдблада $\mathcal{L}$ на ρ и стационарным состоянием, соответствующим данному генератору. Первая сумма в правой части — это сумма относительных энтропий между действиями операторов эволюции с частичными генераторами $\mathcal{D}_k$, которые являются слагаемыми $\mathcal{L}$, и стационарными состояниями, соответствующими этим частичным генераторам. Таким образом, вторая сумма в правой части (30) связывает друг с другом эти величины.

Отметим, что если уравнение Линдблада получено в результате микроскопического вывода (см. [2, 32, 10, 8]) и если в гамильтониане H_S отсутствуют вырожденные уровни энергии и вырожденные боровские частоты (т.е. боровские частоты, отвечающие переходам между различными уровнями энергии), то стационарное состояние, удовлетворяющее условиям (25)–(26) всегда

существует. Структура стационарных состояния в вырожденных системах до конца не изучена. Эффекты, возникающие в вырожденных открытых квантовых системах могут использоваться для целей управления квантовыми системами (см. [7, 1, 3]).

9. Заключение

Мы дали общее определение производства энтропии в марковских открытых квантовых системах, основанное на концепции комплементарного квантового канала. Для того чтобы определить производство энтропии, необходимо выбрать операторы в уравнении Линдблада таким образом, чтобы они соответствовали определенным приращениям энтропии окружения, и определить величины этих приращений. В согласии со вторым законом термодинамики производство энтропии при определенных условиях оказывается неотрицательным.

Также доказаны теоремы о неотрицательности адиабатического и неадиабатического вкладов в производство энтропии при определенных условиях, в том числе в общем случае (при условии термодинамической состоятельности уравнения Линдблада) в малой окрестности стационарного состояния.

Общее определение производства энтропии, адиабатического и неадиабатического вкладов в него важно для открытых квантовых систем, связанных с неравновесными резервуарами, а также для режимов, отличных от режима слабой связи. Поэтому предметом дальнейших исследований может быть использование данного определения для вычисления производства энтропии в таких системах.

Благодарности. Автор признателен Г. Г. Амосову, И. В. Воловичу, С. В. Козыреву, А. Н. Печеню и А. С. Холево за ценные замечания и предложения.

СПИСОК ЛИТЕРАТУРЫ

1. *Арефьева И. Я., Волович И. В., Козырев С. В.* Метод стохастического предела и интерференция в квантовых многочастичных системах// Теор. мат. физ. — 2015. — *183*, № 3. — С. 388–408.
2. *Бройер Х.-П., Петруччионе Ф.* Теория открытых квантовых систем. — М.–Ижевск: РХД, 2010.
3. *Волович И. В., Козырев С. В.* Манипуляция состояниями вырожденной квантовой системы// Тр. Мат. ин-та им. В. А. Стеклова РАН. — 2016. — *294*. — С. 256–267.
4. *Печень А. Н., Ильин Н. Б.* О задаче максимизации вероятности перехода в n-уровневой квантовой системе с помощью неселективных измерений// Тр. Мат. ин-та им. В. А. Стеклова РАН. — 2016. — *294*. — С. 248–255.
5. *Холево А. С.* Комплементарные каналы и проблема аддитивности// Теор. вер. примен. — 2006. — *51*, № 1. — С. 133–143.
6. *Холево А. С.* Квантовые системы, каналы, информация. — М: МЦНМО, 2010.
7. *Accardi L., Kozyrev S. V.* Coherent population trapping in the stochastic limit// Int. J. Theor. Phys. — 2006. — *45*, № 4. — С. 661–668.
8. *Accardi L., Lu Y. G., Volovich I.* Quantum theory and its stochastic limit. — Berlin: Springer, 2002.
9. *Barra F.* The thermodynamic cost of driving quantum systems by their boundaries// Sci. Rep. — 2015. — *5*. — С. 14873.
10. *Davies E.* Markovian master equations// Commun. Math. Phys. — 1974. — *39*. — С. 91–110.
11. *Devetak I., Shor P.* The capacity of a quantum channel for simultaneous transmission of classical and quantum information// Commun. Math. Phys. — 2005. — *256*, № 2. — С. 287–303.
12. *Esposito M., Van den Broeck C.* Three faces of the second law. I. Master equation formulation// Phys. Rev. E. — 2010. — *82*, № 1. — С. 011143.
13. *Esposito M., Lindenberg K., Van den Broek C.* Entropy production as correlation between system and reservoir// New J. Phys. — 2010. — *12*. — С. 013013.
14. *Fagnola F., Umanità V.* Generators of detailed balance quantum Markov semigroups// Inf. Dim. Anal. Quantum Prob. Rel. Top. — 2007. — *10*. — С. 335–363.
15. *Gorini V., Kossakowski A., Sudarshan E. C. G.* Completely positive dynamical semigroups of N-level systems// J. Math. Phys. — 1976. — *17*. — С. 821–825.
16. *Harris R. J., Schütz G. M.* Fluctuation theorems for stochastic dynamics// J. Stat. Mech. — 2007. — *2007*. — С. P07020.

17. *Hatano T., Sasa S.* Steady-state thermodynamics of Langevin systems// Phys. Rev. Lett. — 2001. — *86*, № 16. — С. 3463–3466.
18. *Horowitz J. M., Parrondo M. R.* Entropy production along nonequilibrium quantum jump trajectories// New J. Phys. — 2013. — *15*. — С. 085028.
19. *Horowitz J. M., Sagawa T.* Equivalent definitions of the quantum nonadiabatic entropy production// J. Stat. Phys. — 2014. — *156*, № 1. — С. 55–65.
20. *Levy A., Kosloff R.* The local approach to quantum transport may violate the second law of thermodynamics// EPL. — 2014. — *107*, № 2. — С. 20004.
21. *Lindblad G.* On the generators of quantum dynamical semigroups// Commun. Math. Phys. — 1976. — *48*. — С. 119–130.
22. *Luchnikov I. A., Filippov S. N.* Stroboscopic limit of sequential measurements/ `arxiv.org/abs/1609.05501`
23. *Ohya M., Volovich I.* Mathematical foundations of quantum information and computation and its applications to nano- and bio-systems. — Dordrecht: Springer, 2011.
24. *Oono Y., Paniconi M.* Steady state thermodynamics// Progr. Theor. Phys. Suppl. — 1997. — *130*. — С. 29–44.
25. *Pechen A.* Engineering arbitrary pure and mixed quantum states// Phys. Rev. A. — 2011. — *84*, № 6. — С. 042106.
26. *Pechen A., Il'in N., Shuang F., Rabitz H.* Quantum control by von Neumann measurements// Phys. Rev. A. — 2006. — *74*, № 5. — С. 052102.
27. *Pechen A., Rabitz H.* Teaching the environment to control quantum systems// Phys. Rev. A. — 2006. — *73*, № 4. — С. 062102.
28. *Pechen A., Trushechkin A.* Measurement-assisted Landau–Zener transitions// Phys. Rev. A. — 2015. — *91*, № 5. — С. 052316.
29. *Sakurai J.* Modern Quantum Mechanics. — New York: Addison-Wesley, 2004.
30. *Shuang F., Pechen A., Ho T.-S., Rabitz H.* Observation-assisted optimal control of quantum dynamics// J. Chem. Phys. — 2007. — *126*, № 13. — С. 134303.
31. *Spohn H.* Entropy production for quantum dynamical semigroups// J. Math. Phys. — 1978. — *19*, № 5. — С. 1227–1230.
32. *Spohn H., Lebowitz J. L.* Irreversible thermodynamics for quantum systems weakly coupled to thermal reservoirs// Adv. Chem. Phys. — 1978. — *38*. — С. 109–142.
33. *Trushechkin A. S., Volovich I. V.* Perturbative treatment of inter-site couplings in the local description of open quantum networks// EPL. — 2016. — *113*, № 3. — С. 30005.
34. *Yukawa S.* The second law of steady state thermodynamics for nonequilibrium quantum dynamics/ `arxiv.org/abs/cond-mat/0108421`

А. С. Трушечкин
Математический институт им. В. А. Стеклова РАН, Москва;
Национальный исследовательский ядерный университет «МИФИ», Москва;
Национальный исследовательский технологический университет «МИСиС», Москва
E-mail: `trushechkin@mi.ras.ru`

ИТОГИ НАУКИ И ТЕХНИКИ.
Современная математика и ее приложения.
Тематические обзоры.
Том 138 (2017). С. 99–124

УДК 530.145, 519.72

КВАНТОВЫЕ ОТОБРАЖЕНИЯ И ХАРАКТЕРИЗАЦИЯ ПЕРЕПУТАННЫХ КВАНТОВЫХ СОСТОЯНИЙ

© 2017 г. **С. Н. ФИЛИППОВ**

Аннотация. Представлен обзор квантовых отображений, используемых в задачах характеризации перепутанности двусоставных и многочастичных систем. Помимо положительных и n-тензорно постоянных положительных отображений рассмотрены физические динамические процессы, приводящие к квантовым каналам, разрушающим перепутанность, аннигилирующим перепутанность, диссоциирующим перепутанность многочастичных состояний, запрещающих дистилляцию выходного состояния. Введён новый класс абсолютно распутывающих каналов, дающих на выходе абсолютно сепарабельные состояния, а также представлена характеризация нового класса каналов, навязывающих перепутанность, все выходные состояния которого перепутаны. Представлены состояния, наиболее стойкие к потере перепутанности, и показано, что они могут отличаться от максимально перепутанных состояний.

***Ключевые слова*:** квантовый канал, положительное отображение, квантовая перепутанность, многочастичная перепутанность.

***AMS Subject Classification*:** 81P40, 47N50

СОДЕРЖАНИЕ

1. Введение

Квантовая перепутанность (запутанность, сцепленность, зацепленность; от англ. entanglement) — корреляционное свойство квантовых состояний, обсуждение которого началось в работах Эйнштейна с коллегами [50] и Шрёдингера [124, 125]. Корреляционные свойства вновь приобрели интерес уже во второй половине 20-го в. в связи с ограничениями, накладываемыми неравенствами Белла [20] и их обобщениями [36, 37], а также экспериментальными работами по их проверке [13–15, 58]. В конце 1980-х гг. были сделаны предложения по анализу свойств многочастичной перепутанности [64, 65] и прояснено понятие перепутанности для смешанных двухчастичных состояний [151]. Именно, под перепутанным состоянием двусоставной системы понимается оператор плотности

$$\varrho_{AB} \in \mathcal{B}(\mathcal{H}_A) \otimes \mathcal{B}(\mathcal{H}_B), \quad \varrho_{AB}^\dagger = \varrho_{AB} \geqslant 0, \quad \mathrm{tr}[\varrho_{AB}] = 1,$$

Работа выполнена при поддержке Российского научного фонда (проект № 16-11-00084).

не допускащий представления в виде выпуклой суммы тензорных произведений локальных операторов плотности

$$\varrho_{AB} = \sum_k p_k \varrho_A^{(k)} \otimes \varrho_B^{(k)} \tag{1}$$

или замыкания этого выражения. Состояния (1) называются сепарабельными (распутанными, расцепленными) и могут быть приготовлены с помощью локальных операций и классической коммуникации в лабораториях A и B.

В 1990-х гг. в физическом сообществе сформировалось и новое отношение к квантовой перепутанности как к физическому ресурсу, появились работы по сверхплотному кодированию [23], квантовой телепортации [24], квантовым алгоритмам [40,67,128]. В 1996 г. были получены необходимые и достаточные условия перепутанности произвольных состояний двух двухуровневых систем [81,118] с помощью частичного транспонирования, что стимулировало разработку подходов к количественному описанию степени перепутанности [120,145,152,156] и очищению перепутанности [119,146]. При количественном описании используются различные меры перепутанности, которые обладают теми или иными достоинствами и недостатками (среди недостатков можно указать, что некоторые меры перепутанности могут обращаться в нуль для перепутанных состояний, могут не быть монотонными при действии на состояния вполне положительных отображений, но чаще всего мера перепутанности является трудно вычислимымой величиной — детектирование запутанности является NP-сложной задачей [72]). Поскольку локальные неунитарные операции, реализуемые экспериментально с помощью селективных измерений, могут приводить к росту непрерывных мер перепутанности, некоторые авторы отказываются от непрерывности меры перепутанности и предлагают использовать в качестве универсальной меры ранг Шмидта [3,137]. Заинтересованный читатель может ознакомиться с обзором количественных мер перепутанности для бесконечномерных систем в [4].

Состояния, которые сохраняют положительную определённость при частичном транспонировании, не являются дистиллируемыми [82,84], т.е. даже обладая большим числом копий такого состояния, с помощью локальных операций и классической коммуникации невозможно получить максимально перепутанное двухкубитное состояние. Однако все перепутанные двухкубитные состояния могут быть дистиллированы. Полная характеризация состояний со связанной перепутанностью, не допускающих дистилляции, по-прежнему является открытой проблемой.

Состояние ϱ_{AB} называется *абсолютно сепарабельным*, если $U\varrho_{AB}U^\dagger$ является сепарабельным для любого унитарного преобразования U (см. [99,101]). Абсолютно сепарабельные состояния полностью характеризуются собственными значениями оператора плотности, которые должны удовлетворять определённому условию (см. [77,93,147]). Абсолютно сепарабельные состояния не могут быть переведены в перепутанные с помощью каких-либо унитарных вентилей (вида CNOT или $\sqrt{\mathrm{SWAP}}$, обычно используемых в квантовых цепях). Единственный способ перевести абсолютно сепарабельное состояние в перепутанное состоит в применении неунитарной динамики. Примером такой динамики может служить марковский процесс $\Phi_t = e^{t\mathcal{L}}$ с единственной фиксированной точкой ϱ_∞ в виде перепутанного состояния.

Многочастичная перепутанность обладает рядом особенностей по сравнению с двухчастичной, поскольку может обладать сложной структурой, связанной с различными разбиенями на части. Например, трехкубитное состояние ABC в [22,43] является сепарабельным по отношению к прозвольному разбиению на две части ($A|BC$, $B|AC$, $C|AB$), но является перепутанным по отношению к разбиению на три части ($A|B|C$). Другим примером может служить четырехкубитное состояние Смолина $ABCD$ (см. [135]), которое является сепарабельным по отношению к разбиениям $AB|CD$, $AC|BD$, $AD|BC$, но запутанным по отношению ко всем другим разбиениям (двухчастичным $A|BCD$, $B|ACD$, $C|ABD$, $D|ABC$, трехчастичным $A|B|CD$, $A|C|BD$, $A|BC|D$, $AB|C|D$, $AC|B|D$, $AD|B|C$ и разбиению на 4 части $A|B|C|D$). Как отдельный класс выделяют так называемые истинно перепутанные состояния, которые невозможно представить в виде выпуклой суммы состояний, сепарабельных по отношению к каким-либо разбиениям. Примером истинно перепутанных состояний являются обобщённые GHZ состояния (см. [64,65]).

Важно подчеркнуть, что изначально перепутанность рассматривалась как свойство состояний частиц, т.е. границы разбиения определялись различием частиц. Однако совершенно понятно, что разбиения могут определяться теми степенями свободы, которые доступны измерению в данной физической задаче. Например, в нерелятивистском атоме водорода пространство $\mathcal{H}$ функций $\psi(\mathbf{r}_p, \mathbf{r}_e)$ допускает следующие разбиения $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$:

1) $\mathcal{H}_A$ состоит из функций вида $\psi(\mathbf{r}_p)$, а $\mathcal{H}_B$ — из функций вида $\psi(\mathbf{r}_e)$, т.е. производится разбиение по частицам (протон и электрон);
2) $\mathcal{H}_A$ состоит из функций вида $\psi(m_p\mathbf{r}_p + m_e\mathbf{r}_p)$, а $\mathcal{H}_B$ — из функций вида $\psi(\mathbf{r}_e - \mathbf{r}_p)$, т.е. производится разбиение на движение центра масс и относительного движения (m_p и m_e — массы протона и электрона соответственно).

Основное состояние атома водорода тогда будет перепутанным по отношению к первому разбиению, но сепарабельным по отношению ко второму. Данный пример показывает, что перепутанность является не абсолютным, а относительным свойством состояния (см. [92, 142, 153]). На математическом языке можно сказать, что перепутанность определяется алгеброй наблюдаемых (см. [6]). На практике перепутанность должна определяться по отношению к конкретным степеням свободы, которые доступны экспериментальному наблюдению. В частности, данными степенями свободы для квантов электромагнитного излучения могут быть пространственно-временные моды, что позволяет получать перепутанные состояния с одним фотоном (см. [140]). Для систем с переменным числом частиц также логично вводить понятие перепутанности по отношению к модам. Для двухмодовых гауссовских состояний в 2000 г. были получены необходимые и достаточные условия перепутанности (см. [44,130]), а затем для двухмодовых (не обязательно гауссовских) бозонных состояний были получены критерии перепутанности в терминах моментов операторов рождения и уничтожения бозонов (см. [111,127]). Для фермионных систем также вводится понятие перепутанности мод [21], которое естественным образом работает и для систем с переменным числом фермионов (см. [7]).

На протяжении двух последних десятилетий теория квантовой перепутанности активно развивается в контексте квантовой теории информации (см. [80,114]); данной тематике посвящен общирный обзор [86]. Активную роль в характеризации перепутанности играют различные квантовые отображения. В [81] показано, что двусоставное квантовое состояние, задаваемое оператором плотности ϱ_{AB}, сепарабельно тогда и только тогда, когда

$$(\mathrm{Id}_A \otimes \Lambda_{B\to A})\varrho_{AB} \geqslant 0$$

для всех положительных линейных отображений

$$\Lambda_{B\to A} : \mathcal{B}(\mathcal{H}_B) \to \mathcal{B}(\mathcal{H}_A).$$

Следовательно, для каждого перепутанного состояния ϱ_{AB} существует такой оператор $W \in \mathcal{B}(\mathcal{H}_A) \otimes \mathcal{B}(\mathcal{H}_B)$, называемый *свидетелем перепутанности*, что

$$\mathrm{tr}[\varrho_{AB}W] < 0,$$

в то время как

$$\langle\varphi_A| \otimes \langle\chi_B|W|\varphi_A\rangle \otimes |\chi_B\rangle \geqslant 0 \quad \forall|\varphi_A\rangle \in \mathcal{H}_A, \quad \forall|\chi_A\rangle \in \mathcal{H}_A$$

(здесь и далее мы пользуемся обозначениями Дирака). Для фиксированного свидетеля перепутанности W равенство

$$\mathrm{tr}[\varrho_{AB}W] = 0$$

задает гиперплоскость в пространстве состояний, и выпуклое множество всех сепарабельных состояний лежит по одну сторону от этой гиперплоскости. Однако существуют также нелинейные свидетели перепутанности (см. [68]), позволяющие детектировать более широкий класс перепутанных состояний. Положительные отображения применяются и в анализе многочастичной перепутанности. В настоящей работе мы приводим характеризацию глубины перепутанности с помощью недавно исследованных n-тензорно постоянных положительных отображений.

С другой стороны, квантовые отображения выступают не только в роли вспомогательного объекта для характеризации перепутанности. Квантовые отображения естественным образом возникают в задачах квантовой динамики (см. [28]). Физическая эволюция квантовых состояний

во времени $\varrho(t)$ при отсутствии начальных корреляций между рассматриваемой системой и её окружением описывается динамическим отображением $\varrho(t) = \Phi_t[\varrho(0)]$, где Φ_t — вполне положительное, сохраняющее след отображение, называемое *квантовым каналом* (см., например, [80]). Таким образом, задача характеризации перепутанности состояния $\varrho(t)$ при заданном $\varrho(0)$ сводится к выявлению свойств отображения Φ_t. Обзор динамических свойств квантовой перепутанности предствлен в [12]. Среди частных результатов можно упомянуть так называемую внезапную потерю перепутанности при конечном t, внезапное возобновление перепутанности, неравенство для меры запутанности в случае локального канала, действующего на одну из подсистем.

Отображение Φ_t может обладать и некоторым общим свойством, если все состояния $\Phi_t[\varrho(0)]$ принадлежат одному и тому же классу перепутанности для произвольных начальных состояний $\varrho(0)$. Например, если односторонний канал $\Phi_t^{AB} = \Psi_A \otimes \mathrm{Id}_B$ даёт на выходе лишь сепарабельные состояния, то говорят, что канал Ψ разрушает перепутанность (см. [85]). Если выходное состояние канала Φ_t^{AB} всегда сепарабельно, то канал Φ_t^{AB} называют *аннигилирующим перепутанность* (см. [112]). Аналогично определяются каналы, все выходные состояния которых не могут быть дистиллированы. Для многосоставных систем вводится понятие *диссоциации перепутанности* [54], которое отражает свойства порядка сепарабельности и глубины перепутанности (см. [71, 136]). В настоящей работе даётся обзор известных общих свойств канала Φ_t, а также вводятся новые классы каналов, навязывающих перепутанность, и каналов, дающих на выходе абсолютно сепарабельные состояния.

В случае деградации перепутанности состояния $\varrho(t) = \Phi_t[\varrho(0)]$ с течением времени, параметр t_*, отвечающий переходу из перепутанного в сепарабельное состояние, может рассматриваться как мера стойкости перепутанного состояния $\varrho(0)$ к квантовому шуму Φ_t. В данной работе развивается подход к поиску перепутанных двухкубитных состояний наиболее стойких к локальным шумам, описывающим затухание амплитуды при ненулевой температуре окружения.

Таким образом, настоящая работа преследует следующие цели:

1) представить обзор квантовых каналов, обладающих общими свойствами разрушения перепутанности, аннигиляции перепутанноси, диссоциации перепутанности, недистиллируемости выходного состояния;
2) произвести характеризацию многочастичной r-перепутанности с помощью n-тензорно постоянных положительных отображений [113];
3) представить новый класс каналов, дающих на выходе абсолютно сепарабельные состояния;
4) представить алгоритм построения двухкубитных состояний, наиболее стойких к локальным шумам.

2. Квантовые состояния и линейные отображения

Рассмотрим конечномерное гильбертово пространство (унитарное пространство) $\mathcal{H}_d$, $\dim \mathcal{H}_d = d$, и множество операторов $\mathcal{B}(\mathcal{H}_d)$, действующих на $\mathcal{H}_d$. Оператор $R \in \mathcal{B}(\mathcal{H}_d)$ называется *положительно полуопределённым*, если

$$\langle\psi|R|\psi\rangle \geqslant 0 \quad \forall|\psi\rangle \in \mathcal{H}_d;$$

факт положительной полуопределённости оператора R обозначается $R \geqslant 0$. Обозначим множество всех положительно полуопределённых операторов $\mathcal{B}(\mathcal{H}_d)^+$. Квантовые состояния описываются операторами плотности $\varrho \in \mathcal{B}(\mathcal{H})^+$ с единичным следом, $\mathrm{tr}[\varrho] = 1$.

Линейное отображение

$$\Phi : \mathcal{B}(\mathcal{H}_d)^+ \mapsto \mathcal{B}(\mathcal{H}_d)^+$$

называется *положительным*. Тождественное преобразование на $\mathcal{B}(\mathcal{H}_k)$ обозначим Id_k. Линейное отображение Φ называется *k-положительным*, если отображение $\Phi \otimes \mathrm{Id}_k$ является положительным. Заметим, что 2-положительные отображения вида $\Phi^{\otimes n}$ проанализированы в [139] и используются для получения результатов в задаче дистиллируемых состояний [42]. Линейное отображение Φ называется *вполне положительным*, если оно является k-положительным для

всех $k \in \mathbb{N}$. Символом $\top_d$ будем обозначать транспонирование в некотором фиксированном ортонормированном базисе $\{|i\rangle\}_{i=1}^{d}$ в $\mathcal{H}_d$, т.е.

$$X^{\top} = \sum_{i,j} |i\rangle\langle j|X|i\rangle\langle j|.$$

Отображения вида $\top \circ \Phi$, где Φ является вполне положительным, называют вполне ко-положительными. Соотношения дуальности между конусами различных отображений исследуются, например, в [134]. Отображение

$$\Phi^{\dagger} : \mathcal{B}(\mathcal{H}_B) \mapsto \mathcal{B}(\mathcal{H}_A)$$

называется дуальным по отношению к отображению

$$\Phi : \mathcal{B}(\mathcal{H}_A) \mapsto \mathcal{B}(\mathcal{H}_B),$$

если

$$\operatorname{tr}\left[X\Phi^{\dagger}[Y]\right] = \operatorname{tr}\left[\Phi[X]Y\right] \quad \forall X \in \mathcal{B}(\mathcal{H}_A), \quad \forall Y \in \mathcal{B}(\mathcal{H}_B).$$

Линейное отображение

$$\Phi : \mathcal{B}(\mathcal{H}_d) \mapsto \mathcal{B}(\mathcal{H}_d)$$

называется *n-тензорно постоянным положительным*, если отображение $\Phi^{\otimes n}$ является положительным (см. [113]). Очевидно, если $m > n$, то множество n-тензорно постоянных положительных отображений содержит в себе множество m-тензорно постоянных положительных отображений (вложенная структура). Линейное отображение

$$\Phi : \mathcal{B}(\mathcal{H}_d) \mapsto \mathcal{B}(\mathcal{H}_d)$$

называется *тензорно постоянным положительным*, если оно n-тензорно постоянно положительно для всех $n \in \mathbb{N}$ (см. [75,113]). Вполне положительные и вполне ко-положительные отображения Φ являются тривиальными тензорно постоянными положительными отображениями. Все кубитные тензорно постоянные положительные отображения являются тривиальными (см. [113]).

Квантовая эволюция описывается в формализме входного и выходного состояний квантового канала: $\varrho_{\text{out}} = \Phi[\varrho_{\in}]$, где $\Phi : \mathcal{B}(\mathcal{H}_{\text{in}}) \mapsto \mathcal{B}(\mathcal{H}_{\text{out}})$ — вполне положительное сохраняющее след линейное отображение (CPT). Физический смысл эволюции посредством CPT-отображения Φ виден через представление Стайнспринга (см. [138]):

$$\Phi[\varrho_{\in}] \equiv \operatorname{tr}_{\text{env}}\left[U(\varrho_{\text{in}} \otimes \xi_{\text{env}})U^{\dagger}\right]$$

для некоторого состояния окружения ξ_{env} и некоторого унитарного оператора $U \in \mathcal{B}(\mathcal{H}_{\text{in}} \otimes \mathcal{H}_{\text{env}})$. Вполне положительность (CP) отображения Φ, действующего на систему S, гарантирует, что

$$(\Phi^S \otimes \mathrm{Id}^{\text{anc}})[\varrho^{S+\text{anc}}] \geqslant 0$$

для всех состояний $\varrho^{S+\text{anc}}$ системы S и произвольной вспомогательной системы «anc». Равносильно, отображение Φ является вполне положительным, если оно допускает представление

$$\Phi[X] = \sum_k A_k X A_k^{\dagger}.$$

Если операторы Крауса $A_k : \mathcal{H}_{\text{in}} \mapsto \mathcal{H}_{\text{out}}$ удовлетворяют условию

$$\sum_k A_k^{\dagger} A_k = I_{\text{in}}$$

(единичный оператор), то Φ является CPT-отображением.

Для описания линейного отображения Φ, действующего на систему S, будем использовать изоморфизм Чоя—Ямиолковского (см. [33, 39, 91]):

$$\Omega_{\Phi}^{SS'} := (\Phi^S \otimes \mathrm{Id}^{S'})\left[|\Psi_+^{SS'}\rangle\langle\Psi_+^{SS'}|\right], \tag{2}$$

$$\Phi[X] = d^S \operatorname{tr}_{S'}\left[\Omega_{\Phi}^{SS'}(I_{\text{out}}^S \otimes X^{\mathrm{T}})\right], \tag{3}$$

где $d^S = \dim \mathcal{H}$,

$$|\Psi_+^{SS'}\rangle = (d^S)^{-1/2} \sum_{i=1}^{d^S} |i \otimes i'\rangle$$

— максимально перепутанное состояние системы S и её копии S',

$$X^{\mathrm{T}} = \sum_{i,j} \langle j|X|i\rangle |i'\rangle\langle j'| \in \mathcal{T}(\mathcal{H}_{\mathrm{in}}^{S'})$$

— транспонирование в ортонормированном базисе, $\mathrm{tr}_{S'}$ — частичный след по S'. Линейное отображение Φ^S является вполне положительным тогда и только тогда, когда $\Omega_\Phi^{SS'} \geqslant 0$.

3. Отображения, действующие на двусоставные системы

Рассмотрим двусоставную систему $S = AB$, претерпевающую эволюцию под действием канала Φ^S. Начнем с тождества

$$|\Psi_+^{SS'}\rangle = (d^A d^B)^{-1/2} \sum_{i=1}^{d^A} \sum_{j=1}^{d^B} |ij\rangle \otimes |i'j'\rangle = |\Psi_+^{AA'}\rangle \otimes |\Psi_+^{BB'}\rangle,$$

которое показывает сепарабельность максимально перепутанного состояния по отношению к разбиению $AA'|BB'$. При конструировании оператора Чоя (2) отображение Φ^{AB} может, в общем случае, запутать эти подсистемы.

Рассмотрим локальный канал вида $\Phi_1^A \otimes \Phi_2^B$, который является адекватной моделью таких ситуаций, где каждая частица поступает к адресату через индивидуальный квантовый канал. В этом случае

$$\Omega_{\Phi_1\otimes\Phi_2}^{ABA'B'} = \Omega_{\Phi_1}^{AA'} \otimes \Omega_{\Phi_2}^{BB'}.$$

Очевидно, $\Phi_1^A \otimes \Phi_2^B$ является вполне положительным тогда и только тогда, когда все отображения Φ_1^A, Φ_2^B являются вполне положительными.

3.1. Квантовые каналы, навязывающие перепутанность. Будем называть квантовый канал

$$\Phi : \mathcal{B}(\mathcal{H}_{AB}) \to \mathcal{B}(\mathcal{H}_{AB})$$

навязывающим перепутанность, если состояние $\Phi[\varrho_{AB}]$ является перепутанным для всех входных операторов плотности ϱ_{AB}.

Для навязывания перепутанности недостаточно требования, чтобы чистые сепарабельные состояния преобразовывались в перепутанные. В самом деле, пусть $\Phi[\varrho] = U\varrho U^\dagger$, где U — универсальный унитарный перепутыватель, т.е. чистые состояния $U|\varphi\rangle \otimes |\chi\rangle$ являются перепутанными для любых $|\varphi\rangle \in \mathcal{H}_A$ и $|\chi\rangle \in \mathcal{H}_B$. Существование универсального перепутывателя в пространствах размерности 4×4 и больше показано в [32]. Тогда канал Φ будет переводить чистые состояния $U^\dagger|\varphi\rangle \otimes |\chi\rangle$ в сепарабельные, т.е. Φ не будет навязывать перепутанность, хотя он запутывает все чистые сепарабельные состояния.

Получим критерий для введённого класса каналов.

Предложение 1. *Квантовый канал $\Phi : \mathcal{B}(\mathcal{H}_{AB}) \to \mathcal{B}(\mathcal{H}_{AB})$ навязывает перепутанность тогда и только тогда, когда существует такой свидетель перепутанности $W \in \mathcal{B}(\mathcal{H}_A) \otimes \mathcal{B}(\mathcal{H}_B)$, что $\Phi^\dagger[W]$ является отрицательным.*

Доказательство. В силу линейности отображения Φ множество всех выходных состояний $\Phi[\varrho]$ является выпуклым и замкнутым. Φ навязывает перепутанность тогда и только тогда, когда данное множество не имеет пересечений с множеством сепарабельных состояний. Следуя логике доказательства теоремы о свидетеле перепутанности (см. [81]), основанной на теореме Хана—Банаха, можем заключить, что существует свидетель перепутанноси W такой, что

$$\mathrm{tr}\left[W\Phi[\varrho]\right] < 0 \leqslant \mathrm{tr}\left[W|\varphi_A\rangle\langle\varphi_A| \otimes |\chi_B\rangle\langle\chi_B|\right] \quad \forall|\varphi_A\rangle \in \mathcal{H}_A, \quad \forall|\varphi_B\rangle \in \mathcal{H}_B.$$

Другими словами, существует гиперплоскость, разграничивающая выпуклые множества выходных состояний и сепарабельных состояний. Поскольку

$$\operatorname{tr}\left[W\Phi[\varrho]\right] = \operatorname{tr}\left[\Phi^{\dagger}[W]\varrho\right] < 0$$

для всех операторов плотности ϱ, то $\Phi^{\dagger}[W]$ содержит лишь отрицательные собственные значения. □

Пример 1. Рассмотрим квантовый канал

$$\Phi_q : \mathcal{B}(\mathcal{H}_d) \otimes \mathcal{B}(\mathcal{H}_d) \mapsto \mathcal{B}(\mathcal{H}_d) \otimes \mathcal{B}(\mathcal{H}_d),$$

задаваемый формулой

$$\Phi_q[X] = qX + (1-q)\operatorname{tr}[X]|\psi_-\rangle\langle\psi_-|,$$

где $0 \leqslant q \leqslant 1$ и

$$|\psi_-\rangle = \sqrt{\frac{2}{d(d-1)}} \sum_{i<j} \Big(|i\rangle \otimes |j\rangle - |j\rangle \otimes |i\rangle\Big); \tag{4}$$

дуальный канал —

$$\Phi_q^{\dagger}[Y] = qY + (1-q)\langle\psi_-|Y|\psi_-\rangle I.$$

Выберем свидетель перепутанности

$$W = \mathrm{SWAP} = \sum_{i,j=1}^{d} |i\rangle\langle j| \otimes |j\rangle\langle i|;$$

тогда

$$\Phi_q^{\dagger}[W] = qW - (1-q)I.$$

Отсюда видно, что Φ_q навязывает перепутанность при $0 \leqslant q < \frac{1}{2}$.

3.2. Квантовые каналы, разрушающие перепутанность. В квантовой теории информации часто рассматривается ситуация, когда квантовый канал Φ действует только на одну из подсистем составной системы, в то время как вторая подсистема эволюционирует тривиально (Id). В таком случае говорят, что привносимый квантовый шум является *односторонним*. Для одностороннего шума получены «уравнения» эволюции перепутанности (см. [63, 100, 143, 154]), которые гласят, что изменение перепутанности вследствие одностороннего шума количественно ограничено действием канала на максимально перепутанное состояние. Все шумы Φ, разрушающие перепутанность максимально перепутанного состояния, будут также расцеплять рассматриваемую подсистему (на которую действует канал) от любых других подсистем вне зависимости от начального состояния большой системы, тем самым образуя класс каналов, разрушающих перепутанность (см. [1, 2, 85, 97, 122, 129]).

Рассмотрим подсистему A, на которую действует квантовый канал Φ^A с представлением Крауса в виде операторов ранга 1, т.е.

$$A_k \propto |\varphi_k\rangle\langle\psi_k|, \quad |\psi_k\rangle \in \mathcal{H}_{\mathrm{in}}^A, \quad |\varphi_k\rangle \in \mathcal{H}_{\mathrm{out}}^A.$$

В таком случае мы имеем дело с процедурой измерения-приготовления, т.е. канал имеет вид *qcq*-канала Холево

$$\Phi[X] = \sum_k \operatorname{tr}[F_k X]\omega_k,$$

где $\{F_k\}$ — положительная операторнозначная мера и $\omega_k \in \mathcal{S}(\mathcal{H}_{\mathrm{out}})$ — оператор плотности, т.е. Φ фактически является процедурой измерения и приготовления состояний. Такой канал Φ^A разрушает перепутанность и расцепляет A ото всех остальных подсистем $B, C, \ldots$, поскольку содержит стадию классической передачи информации. Удивительно, но обратное утверждение также справедливо, т.е. {Φ разрушает перепутанность} $\Leftrightarrow$ {существует представление Крауса канала Φ в виде операторов ранга 1}. Альтернативное описание каналов, разрушающих перепутанность, использует свойство оператора Чоя: {Φ^A разрушает перепутанность} $\Leftrightarrow$ {$\Omega_{\Phi}^{AA'}$ сепарабельно по отношению к разбиению $A|A'$} (см. [2, 85, 122]).

Что касается разрушающих перепутанность каналов Φ_{EB}^{AB}, действующих на составную систему AB, то оператор Чоя $\Omega_{\Phi}^{ABA'B'}$ является сепарабельным по отношению к разбиению $AB|A'B'$, но всё ещё может быть перепутанным по отношению к разбиениям $A|BA'B'$ и $B|AA'B'$ (например, если $\Omega_{\Phi}^{ABA'B'}$ является четырёхкубитным состоянием Смолина (см. [135])). В таком случае канал расцепляет AB от всех других подсистем, но перепутанность между A и B может сохраняться. Однако, если канал Φ^{AB} имеет локальную форму

$$\Phi_{\mathrm{local}}^{AB} = \Phi_1^A \otimes \Phi_2^B,$$

то $\Phi_{\mathrm{local}}^{AB}$ разрушает перепутанность тогда и только тогда, когда и Φ_1^A, и Φ_2^B разрушают перепутанность. Этот факт непосредственно следует из свойства максимально перепутанного состояния

$$|\Psi_+^{AB|A'B'}\rangle := |\Psi_+^{AA'}\rangle \otimes |\Psi_+^{BB'}\rangle.$$

В [2] найдено общее условие разрушения перепутанности гауссовским каналом. В качестве примера укажем, что нечувствительный к фазе одномодовый усилитель или аттенюатор Φ с коэффициентом усиления $\varkappa$ и привносимым шумом μ является разрушающим перепутанность при $\mu \geqslant \frac{1}{2}(1+\varkappa)$.

3.3. Квантовые каналы, аннигилирующие перепутанность. В физическом эксперименте шум обычно не бывает односторонним. По этой причине в 2010 г. было введено понятие каналов, аннигилирующих перепутанность [112]. Канал $\Phi : \mathcal{B}(\mathcal{H}_{AB}) \to \mathcal{B}(\mathcal{H}_{AB})$, действующий на составную систему, называется *аннигилирующим перепутанность*, если $\Phi[\varrho_{AB}]$ сепарабельно для любого оператора плотности ϱ_{AB}. В отличие от каналов, разрушающих перепутанность, аннигилирующие перепутанность каналы не обязательно расцепляют систему AB от окружения, они лишь уничтожают перепутанность между A и B. Например, широко распространена ситуация, когда совместное действие локальных шумов на отдельные подсистемы является аннигилирующим перепутанность каналом, хотя ни один из локальных шумов не является разрушающим перепутанность (см. [55, 112]).

Необходимое и достаточное условие аннигиляции перепутанности может быть получено с помощью критерия Городецких (см. [81]).

Предложение 2 (см. [56]). *Квантовый канал*

$$\Phi^{AB} : \mathcal{B}(\mathcal{H}_{\mathrm{in}}^{AB}) \to \mathcal{B}(\mathcal{H}_{\mathrm{out}}^{AB})$$

аннигилирует перепутанность тогда и только тогда, когда отображение $(\mathrm{Id}^A \otimes \Lambda^B) \circ \Phi^{AB}$ *положительно для произвольного положительного отображения*

$$\Lambda^B : \mathcal{B}(\mathcal{H}_{\mathrm{out}}^{B}) \to \mathcal{B}(\mathcal{H}_{\mathrm{out}}^{A}).$$

К сожалению, данный критерий трудно применить к конкретному каналу. Однако в случае двух кубитов ($d_{\mathrm{out}}^{A,B} = 2$) полученный результат можно упростить, заменив положительное отображение Λ^B на транспонирование (см. [118]) или редуцирующее отображение (см. [87]). Это обстоятельство использовалось для характеризации локальных двухкубитных аннигилирующих перепутанность каналов в [55].

Особый интерес представляет ситуация, когда двусоставная система состоит из подсистем одинаковой размерности $d^A = d^B$, а квантовый канал имеет вид $\Phi \otimes \Phi$. В таком случае обе подсистемы испытывают действие одного и того же шума.

В [56] предложено характеризовать каналы, аннигилирующие перепутанность, как пересечение множества положительных отображений, аннигилирующих перепутанность, и множества квантовых каналов.

Предложение 3 (см. [56]). *Отображение* Φ^{AB} *является положительным и аннигилирующим перепутанность тогда и только тогда, когда*

$$\mathrm{tr}\left[(\xi_{\mathrm{BP}}^{A|B} \otimes \varrho^{A'B'})\Omega_{\Phi}^{ABA'B'}\right] \geqslant 0 \tag{5}$$

для всех блочно-положительных операторов $\xi_{\mathrm{BP}}^{A|B}$, *т.е.*

$$\langle\varphi_A| \otimes \langle\chi_B|\xi_{\mathrm{BP}}^{A|B}|\varphi_A\rangle \otimes |\chi_B\rangle \geqslant 0$$

для всех $|\varphi_A\rangle \in \mathcal{H}_A$, $|\varphi_B\rangle \in \mathcal{H}_B$ *и операторов плотности* $\varrho^{A'B'}$.

В терминах операторов Чоя данное утверждение означает, что конус положительных отображений, аннигилирующих перепутанность, является дуальным по отношению к конусу отображений вида

$$\Phi_{\mathrm{d.c.}}^{AB}[X] = \sum_k \mathrm{tr}[F_k X]\xi_{\mathrm{BP}\ k}^{A|B}, \quad F_k \geqslant 0.$$

Следствие 1 (см. [56]). *Линейное отображение* Φ^{AB} *является квантовым каналом, аннигилирующим перепутанность, тогда и только тогда, когда* $\Omega_\Phi^{ABA'B'}$ *удовлетворяет условиям* (5), $\Omega_\Phi^{ABA'B'} \geqslant 0$, *и*

$$\mathrm{tr}_{AB}\,\Omega_\Phi^{ABA'B'} = (d^A d^B)^{-1} I^{A'B'}.$$

Хотя полученные условия и дают полную характеризацию отображений, анигилирующих перепутанность, их по-прежнему трудно применить к конкретному отображению. Можно, однако, найти следующее нетривиальное достаточное условие.

Предложение 4 (см. [56]). *Если* $\Omega_\Phi^{ABA'B'}$ *можно представить в виде выпуклой суммы операторов* $\zeta_{\mathrm{BP}}^{A|A'B'} \otimes \varrho^B$ *и* $\varrho^A \otimes \zeta_{\mathrm{BP}}^{B|A'B'}$, *где операторы* ζ_{BP} *блочно положительны по отношению к соответствующему разбиению и* $\varrho \geqslant 0$, *тогда отображение* Φ^{AB} *является положительным и аннигилирует перепутанность.*

Если в последнем утверждении заменить блочно-положительные операторы $\zeta_{\mathrm{BP}}^{A|A'B'}$ и $\zeta_{\mathrm{BP}}^{B|A'B'}$ на положительные полуопределённые $\varrho^{AA'B'}$ и $\varrho^{BA'B'}$ соответственно, то полученная таким образом матрица Чоя будет автоматически неотрицательна, т.е. будет отвечать вполне положительному отображению.

Следствие 2 (см. [56]). *Если*

$$\mathrm{tr}_{AB}\,\Omega_\Phi^{ABA'B'} = (d^A d^B)^{-1} I^{A'B'}$$

и $\Omega_\Phi^{ABA'B'}$ *представляет собой выпуклую сумму операторов плотности* $\varrho^{A|BA'B'}$ *и* $\varrho^{B|AA'B'}$ (*сепарабельных относительно разбиений* $A|BA'B'$ *и* $B|AA'B'$ *соответственно*), *то* Φ^{AB} *является каналом, аннигилирующим перепутанность.*

Отметим, что состояния $\Omega_\Phi^{ABA'B'}$ принадлежат к классу так называемых *бисепарабельных состояний* (выпуклая оболочка состояний, сепарабельных относительно какого-либо разбиения). Детектирование бисепарабельности обсуждается в [19, 88, 89, 94, 95], однако следствие 2 стимулирует дальнейшие исследования в данной области.

В [56] предложение 4 применяется для исследования аннигилирующих свойств деполяризующих каналов. Деполяризующий канал, действующий на d-мерную квантовую систему, определяется формулой

$$\Phi_q = q\,\mathrm{Id} + (1-q)\,\mathrm{tr},$$

где $\mathrm{tr}[X] = \mathrm{tr}[X]\frac{1}{d} I_d$ — канал, переводящий все состояния в максимально смешанное. Заметим, что Φ_q является вполне положительным при $q \in \left[-\dfrac{1}{d^2-1}, 1\right]$, и Φ_q разрушает перепутанность при $-\dfrac{1}{d^2-1} \leqslant q \leqslant \dfrac{1}{d+1}$ (см. [56]). На двусоставную систему AB может действовать как локальный деполяризующий шум $\Phi_{q_1}^A \otimes \Phi_{q_2}^B$, так и глобальный деполяризующий шум Φ_q^{AB}.

Проиллюстрируем действие каналов на системы размерности 2×2 и 3×2, для которых есть необходимое и достаточное условие сепарабельности (см. [81]): в случае $d^A = d^B = 2$ канал $\Phi_{q_1}^A \otimes \Phi_{q_2}^B$ аннигилирует перепутанность при $q_1 q_2 \leqslant 1/3$, а канал Φ_q^{AB} аннигилирует перепутанность при $q \leqslant 1/3$; в случае $d^A = 3$ и $d^B = 2$ канал $\Phi_{q_1}^A \otimes \Phi_{q_2}^B$ аннигилирует перепутанность при

$q_1(9q_2-1)\leqslant 2$, а канал Φ_q^{AB} аннигилирует перепутанность при $q\leqslant 1/4$. Разложение, указанное в предложении 4, существует для всех двухкубитных деполяризующих каналов, аннигилирующих перепутанность [56], т.е. предложение 4 воспроизводит точные результаты работы [55]. Следствие 2 может детектировать аннигиляцию перепутанности меньшего набора отображений $\Phi_{q_1}^A\otimes\Phi_{q_2}^B$ (сравнение представлено в [56]).

Рассмотрим теперь двусоставные системы AB, для которых $d^A=d^B=d$ — произвольное число. Для локального канала $\Phi_{q_1}^A\otimes\Phi_{q_2}^B$ можно найти разложение из предложения 4, если выполнено условие

$$(d^2-1)\,q_1q_2\leqslant 1+\frac{(d-2)(d+1)}{d+2}(q_1+q_2) \tag{6}$$

(см. [56]).

Следовательно, для этих значений параметров q_1 и q_2 канал $\Phi_{q_1}^A\otimes\Phi_{q_2}^B$ будет аннигилировать перепутанность. Положив $q_{1,2}=q$ в неравенстве (6), получаем

$$q\leqslant q_{\mathrm{EA}}^{\mathrm{local}}=\frac{d-2+d\sqrt{\frac{2d}{d+1}}}{(d-1)(d+2)}. \tag{7}$$

Неравенство (7) накладывает менее строгие ограничения на параметр q, чем условие разрушения перепутанности $q\leqslant 1/(d+1)$.

Глобальный деполяризующий канал Φ_q^{AB}, действующий на две d-мерные квантовые системы A и B одновременно, является qcq каналом при $q\leqslant 1/(d^2+1)$, однако аннигилирует перепутанность при

$$q\leqslant q_{\mathrm{EA}}^{\mathrm{global}}=\frac{d+2}{(d+1)(d^2-d+2)}$$

(см. [56]).

Для произвольного унитального кубитного канала

$$\Phi:\mathcal{B}(\mathcal{H}_2)\mapsto\mathcal{B}(\mathcal{H}_2),\quad \Phi[I]=I,$$

существуют такие входные и выходные базисы из операторов Паули, что $\Phi[\sigma_i^{\mathrm{in}}]=\lambda_i\sigma_i^{\mathrm{out}}$ (см. [98, 121]). Имеют место следующие свойства аннигиляции перепутанности.

Предложение 5 (см. [55]). *Пусть Φ и Φ' — однокубитные унитальные каналы, удовлетворяющие условиям*

$$\sum_{m=1}^{3}\lambda_m^2\leqslant 1,\quad \sum_{n=1}^{3}{\lambda'_n}^2\leqslant 1.$$

Тогда $\Phi\otimes\Phi'$ аннигилирует перепутанность.

Предложение 6 (см. [55]). *Пусть Φ и Φ' — однокубитные унитальные каналы с сингулярными значениями*

$$\boldsymbol{\lambda}=(\lambda_1,\lambda_2,\lambda_3),\quad \boldsymbol{\lambda}'=(\lambda'_1,\lambda'_2,\lambda'_3)$$

соответственно. Если $\boldsymbol{\lambda}\cdot\boldsymbol{\lambda}'>1$, то $\Phi\otimes\Phi'$ не аннигилирует перепутанность. Состояние, сохраняющее при этом перепутанность, суть максимально перепутанное состояние

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

Предложение 7 (см. [55]). *Двухкубитный унитальный канал $\Phi\otimes\Phi$ аннигилирует перепутанность тогда и только тогда, когда*

$$\lambda_1^2+\lambda_2^2+\lambda_3^2\leqslant 1.$$

В [52, 57] представлен обзор аннигиляционных свойств двухмодовых локальных гауссовских каналов. В частности, показано, что для нечувствительного к фазе одномодового усилителя и аттенюатора Φ с коэффицентом усиления $\varkappa$ и привносимым шумом μ канал $\Phi\otimes\Phi$ не является аннигилирующим перепутанность при $\mu<\frac{1}{2}\sqrt{1+\varkappa^2}$.

3.4. Наиболее стойкие перепутанные состояния. В задачах квантовой коммуникации часто возникает потребность иметь перепутанное состояние между удалёнными на большое расстояние адресатами. Для этого в лаборатории приготовляется некоторое перепутанное состояние ϱ_{in}^{AB}, которое посредством квантового канала Φ^{AB} доставляется адресатам. Обычно перепутанное состояние изначально разделяется на части, эволюционирующие независимо (каждая часть взаимодействует со своим окружением, между окружениями нет корреляции). В таком случае канал Φ^{AB} имеет локальную структуру, т.е. $\Phi^{AB} = \Phi_1^A \otimes \Phi_2^B$. Даже если выходное состояние $\varrho_{\text{out}}^{AB} = \Phi^{AB}[\varrho_{\text{in}}^{AB}]$ обладает малой степенью перепутанности, при наличии большого числа таких состояний к ним можно применить протоколы очищения перепутанности и дистилляции (все перепутанные двухкубитные состояния дистиллируемы). Таким образом, фундаментальным ограничением для передачи удалённым адресатам перепутанного состояния является свойство аннигиляции перепутанности каналом Φ^{AB}. Физическая реализация канала Φ^{AB} — динамическое отображение Φ_t^{AB}, т.е. однопараметрическое семейство квантовых каналов со временем t в качестве параметра. Пусть Φ_t^{AB} аннигилирует перепутанность для всех $t \geqslant \tau$ и не аннигилирует перепутанность при $t < \tau$, тогда будем называть время τ временем аннигиляции перепутанности. Состояние $\varrho_{\text{robust}}^{AB}$ будем называть *наиболее стойким к потере перепутанности*, если выходное состояние $\Phi_t^{AB}[\varrho_{\text{robust}}^{AB}]$ перепутано при $t < \tau$.

Из данного определения и предложений 6 и 7 вытекает следующее утверждение.

Предложение 8. *Для локальных унитальных двухкубитных динамических отображений* $\Phi_t \otimes \Phi_t$ *максимально перепутанное состояние*

$$|\psi_+\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle\big)$$

является наиболее стойким к потере перепутанности.

Однако для подсистем большей размерности ($d > 2$) максимально перепутанное состояние

$$|\Psi_+^{AB}\rangle = \frac{1}{\sqrt{d}} \sum_{i=1}^{d} |i \otimes i\rangle$$

не обязательно является наиболее стойким к потере перепутанности (даже в случае унитальных отображений).

В качестве примера рассмотрим деполяризующее динамическое отображение, описываемое каналом Φ_q, где $q = q(t)$ — монотонно убывающая функция от времени t, $q(0) = 1$, $q \xrightarrow[t\to\infty]{} 0$. Для локальных отображений $\Phi_{q_1(t)}^A \otimes \Phi_{q_2(t)}^B$ функции $q_1(t)$ и $q_2(t)$ могут быть различными, что отвечает разным временам когерентности в подсистемах. Для простоты рассмотрим случай $q_1(t) = q_2(t) = q(t)$. Выходное состояние

$$\big(\Phi_q^A \otimes \Phi_q^B\big)\big[|\Psi_+^{AB}\rangle\langle\Psi_+^{AB}|\big] = \big(\Phi_{q^2}^A \otimes \mathrm{Id}^B\big)\big[|\Psi_+^{AB}\rangle\langle\Psi_+^{AB}|\big]$$

становится сепарабельным тогда, когда $\Phi_{q^2}^A$ разрушает перепутанность, т.е. при

$$q \leqslant q_{\text{MES}}^{\text{local}} = \frac{1}{\sqrt{d+1}}.$$

Рассмотрим теперь состояние

$$|\gamma^{AB}\rangle = \frac{1}{\sqrt{2}}\big(|1 \otimes 1\rangle + |d \otimes d\rangle\big),$$

которое не является максимально перепутанным при $d > 2$, поскольку обладает рангом Шмидта 2. Легко проверить, что частичное транспонирование выходного состояния

$$\big(\Phi_q^A \otimes \Phi_q^B\big)\big[|\gamma^{AB}\rangle\langle\gamma^{AB}|\big]$$

не является положительно полуопределённым при

$$q > q_{\text{nEA}}^{\text{local}} = \frac{1+\sqrt{3}}{d+1+\sqrt{3}}$$

(сохранение перепутанности). Таким образом, рассмотренное состояние с рангом Шмидта 2 обладает большей стойкостью к потере перепутанности, чем маскимально перепутанное состояние.

Аналогично, для глобального деполяризующего канала выходное состояние $\Phi_q^{AB}\big[|\gamma^{AB}\rangle\langle\gamma^{AB}|\big]$ перепутано при

$$q > q_{\mathrm{nEA}}^{\mathrm{global}} = \frac{2}{d^2+2},$$

в то время как выходное состояние

$$\Phi_q^{AB}\big[|\Psi_+^{AB}\rangle\langle\Psi_+^{AB}|\big] \equiv \big(\Phi_q^A \otimes \mathrm{Id}^B\big)\big[|\Psi_+^{AB}\rangle\langle\Psi_+^{AB}|\big]$$

сепарабельно, когда Φ_q^A разрушает перепутанность, т.е. при

$$q \leqslant q_{\mathrm{MES}}^{\mathrm{global}} = \frac{1}{d+1}.$$

Очевидно, $q_{\mathrm{nEA}}^{\mathrm{global}} < q_{\mathrm{MES}}^{\mathrm{global}}$, что показывает бóльшую стойкость к потере перепутанности у состояния $|\gamma^{AB}\rangle$, чем у максимально перепутанного состояния.

В недавней работе [102] показано, что канал $\Phi_q^A \otimes \Phi_q^B$, $q \geqslant 0$, аннигилирует перепутанность при $q \leqslant q_{\mathrm{nEA}}^{\mathrm{local}}$, а канал Φ_q^{AB} аннигилирует перепутанность при $q \leqslant q_{\mathrm{nEA}}^{\mathrm{global}}$. Основываясь на приведённые выше примеры и данный результат, мы можем сформулировать предложение о наибольшей стойкости деполяризующих каналов.

Предложение 9. *В системе из двух d-мерных квантовых подсистем наибольшей стойкостью к потере перепутанности в локальных и глобальных деполяризующих процессах обладает состояние*

$$|\gamma^{AB}\rangle = \frac{1}{\sqrt{2}}\big(|1\otimes 1\rangle + |d\otimes d\rangle\big)$$

с рангом Шмидта 2.

Что касается неунитального квантового канала Φ, то в кубитном случае его можно свести к унитальному каналу Υ по формуле

$$\Phi[X] = B\big(\Upsilon[AXA^\dagger]\big)B^\dagger$$

(см. [16, 72]). Матрицы A и B найдены для определённого вида неунитальных каналов в [53]. Очевидно, что состояние $(\Phi\otimes\Phi)[\varrho]$ будет перепутанным, если состояние

$$\big(\Upsilon\otimes\Upsilon\big)\big[A\otimes A\varrho A^\dagger\otimes A^\dagger\big]$$

перепутано. Для унитальных кубитных каналов такого вида справедливо предложение 8, из которого следует, что наибольшей стойкостью к потере перепутанности будут обладать состояния $|\psi\rangle \sim A^{-1}\otimes A^{-1}|\psi_+\rangle$ (необходима нормировка).

Предложение 10. *Для локальных двухкубитных динамических отображений $\Phi_t\otimes\Phi_t$ наибольшей стойкостью к потере перепутанности обладает состояние*

$$|\psi\rangle \sim A^{-1}\otimes A^{-1}|\psi_+\rangle,$$

где матрица A задает связь канала Φ с унитальным отображением Υ по формуле

$$\Phi[X] = B\big(\Upsilon[AXA^\dagger]\big)B^\dagger.$$

Пусть Φ — одномодовый гауссовский канал, производящий не чувствительное к фазе усиление или ослабление квантового сигнала. Из результатов работ [52, 57] следует, что для шумов вида $\Phi\otimes\Phi$ бóльшей стойкостью к потере перепутанности обладают не гауссовские состояний сжатого вакуума (аналог максимально перепутанного состояния при коэффициенте сжатия, стремящемся к бесконечности), а состояния

$$|\psi\rangle \sim |\gamma\rangle|0\rangle - |0\rangle|\gamma\rangle,$$

где $|\gamma\rangle$ — когерентное состояние, $|0\rangle$ — вакуумное состояние. Если $\gamma\to 0$, то эти состояния переходят в однофотонные $\frac{1}{\sqrt{2}}\big(|1\rangle|0\rangle - |0\rangle|1\rangle\big)$, которые можно легко реализовать в квантовой оптике с помощью делителя пучка.

3.5. Квантовые каналы, запрещающие дистилляцию перепутанности. Положительное отображение Φ^{AB}, преобразующее двусоставную систему AB, будем называть *PPT-индуцирующим*, если $\Phi^{AB}[\varrho^{AB}]$ положительно при частичном транспонировании относительно разбиения $A|B$ для всех входных состояний ϱ^{AB}. Если к тому же Φ^{AB} является вполне положительным и сохраняет след, то Φ^{AB} называют *PPT-индуцирующим квантовым каналом*.

Имеется следующая характеризация PPT-индуцирующих отображений.

Предложение 11 (см. [51]). *Положительное отображение Φ^{AB} является PPT-индуцирующим тогда и только тогда, когда оператор Чоя $\Omega_\Phi^{A(B)^\top A'B'}$ блочно положителен по отношению к разбиению $AB|A'B'$.*

В формулировке последнего утверждения можно заменить $\Omega_\Phi^{A(B)^\top A'B'}$ на $\Omega_\Phi^{(A)^\top BA'B'}$. Отметим, что положительность отображения Φ^{AB} является существенной. Поскольку положительные операторы автоматически являются блочно положительными, получаем следующий результат.

Следствие 3 (см. [51]). *Пусть канал Φ^{AB} таков, что $\Omega_\Phi^{A(B)^\top A'B'} \geqslant 0$. Тогда Φ^{AB} является PPT-индуцирующим.*

Линейное отображение Φ^{AB}, переводящее операторы плотности в недистиллируемые состояния, называется запрещающим дистилляцию. Поскольку PPT-состояния не могут быть дистиллированы (см. [82]), PPT-индуцирующие отображения образуют выпуклое подмножество отображений, запрещающих дистилляцию.

Если $\Phi\otimes\mathrm{Id}[\varrho_{\mathrm{in}}^{S+\mathrm{anc}}]$ не дистиллируемо по отношению к S и вспомогательной системе («anc») для любого начального состояния $\varrho_{\mathrm{in}}^{S+\mathrm{anc}}$, то Φ называется связывающим перепутанность (см. [83]). Оператор Чоя для связывающего перепутанность отображения является недистиллируемым (см. [83]).

В [51] приводится пример запрещающего дистилляцию отображения $\Phi_1 \otimes \Phi_2$, хотя ни Φ_1, ни Φ_2 не являются связывающими перепутанность.

3.6. Квантовые каналы с абсолютно сепарабельными выходными состояниями. Напомним, что двусоставное состояние ϱ_{AB} называется *абсолютно сепарабельным*, если $U\varrho_{AB}U^\dagger$ является сепарабельным для любого унитарного преобразования U (см. [99, 101]). Будем называть линейное положительное отображение Φ^{AB} *абсолютно распутывающим*, если $\Phi^{AB}[\varrho^{AB}]$ абсолютно сепарабельно для любого входного состояния.

В [147] показано, что двухкубитный оператор плотности ϱ является абсолютно сепарабельным, если его собственные значения $\lambda_1 \geqslant \lambda_2 \geqslant \lambda_3 \geqslant \lambda_4$ удовлетворяют неравенству

$$\lambda_1 \leqslant \lambda_3 + 2\sqrt{\lambda_2\lambda_4}.$$

Используя данную характеризацию, нетрудно получить следующий результат.

Предложение 12. *Локальный двухкубитный деполяризующий канал $\Phi_{q_1} \otimes \Phi_{q_2}$ с $q_1 \geqslant q_2$ является абсолютно распутывающим при*

$$q_1(1 + |q_2|) \leqslant \sqrt{1 - q_1^2}(1 - |q_2|).$$

Характеризация других абсолютно распутывающих отображений является открытой проблемой.

4. Структура многочастичной перепутанности

Для количественного описания структуры перепутанности будем использовать следующий формализм.

Всякий раз, когда мы говорим о перепутанности, мы подразумеваем определенное разбиение составной системы. В общем случае N-частичная система $ABC\ldots$ может быть разбита на k подсистем, где k пробегает значения от 2 до N включительно. Если же система не подвергается

разбиению, то будем считать $k = 1$. N-частичная система $ABC\ldots$ разбивается на k подсистем $\left\{{N \atop k}\right\}$ различными способами, где

$$\left\{{N \atop k}\right\} = \frac{1}{k!}\sum_{m=0}^{k}(-1)^m\binom{k}{m}(k-m)^N \tag{8}$$

— число Стирлинга второго рода. Обозначим $\mathcal{P}^k$ набор возможных разбиений на k подсистем. Упорядочим разбиения таким образом, что подсистемы с меньшим числом частиц расположены вначале. Тогда для трехчастичной системы ABC получаем

$$\mathcal{P}^1(ABC) = \{ABC\},\quad \mathcal{P}^2(ABC) = \{A|BC, B|AC, C|AB\},\quad \mathcal{P}^3(ABC) = \{A|B|C\}.$$

В случае четырехчастичной системы $ABCD$ получаем следующие наборы разбиений:

$$\mathcal{P}^1(ABCD) = \{ABCD\},$$

$$\mathcal{P}^2(ABCD) = \Big\{A|BCD,\ B|ACD,\ C|ABD,\ D|ABC,\ AB|CD,\ AC|BD,\ AD|BC\Big\},$$

$$\mathcal{P}^3(ABCD) = \Big\{A|B|CD,\ A|C|BD,\ A|D|BC,\ B|C|AD,\ B|D|AC,\ C|D|AB\Big\},$$

$$\mathcal{P}^4(ABCD) = \{A|B|C|D\}.$$

Символом $\mathcal{P}^k_j$ обозначим j-е разбиение в наборе $\mathcal{P}^k$, например, $\mathcal{P}^3_5(ABCD) = B|D|AC$. Чтобы указать m-ю подсистему разбиения $\mathcal{P}^k_j$, будем использовать обозначение $[\mathcal{P}^k_j]_m$, например, $\big[\mathcal{P}^3_5(ABCD)\big]_2 = D$.

Квантовые состояния системы $ABC\ldots$ описываются операторами плотности $\varrho^{ABC\ldots}$ (положительными и обладающие единичным следом), которые действуют в гильбертовом пространстве $\mathcal{H}^{ABC\ldots} \equiv \mathcal{H}^A \otimes \mathcal{H}^B \otimes \mathcal{H}^C \otimes \ldots$ и вместе образуют выпуклое множество $\mathcal{S}(\mathcal{H}^{ABC\ldots})$. Состояние ϱ называется сепарабельным по отношению к определенному разбиению $\mathcal{P}^k_j$, если разложение

$$\varrho = \sum_i \mu_i \varrho_i^{[\mathcal{P}^k_j]_1} \otimes \cdots \otimes \varrho_i^{[\mathcal{P}^k_j]_k} \tag{9}$$

справедливо для некоторого распределения вероятностей $\{\mu_i\}$ и операторов плотности $\varrho_i^{[\mathcal{P}^k_j]_m}$, $m = 1, \ldots, k$. Для краткости будем обозначать такое сепарабельное состояние символом σ^k_j. Если $\varrho \neq \sigma^k_j$ ни для какого σ^k_j, то говорят, что ϱ перепутано по отношению к разбиению $\mathcal{P}^k_j$.

4.1. Степень сепарабельности. Понятие k-сепарабельности показывает, что квантовое состояние содержит компоненты, каждая из которых состоит из не менее чем k отдельных частей. Состояние ϱ называется k-сепарабельным и обозначается $\varrho_{k\text{-sep}}$ если оно допускает разложение

$$\sum_{j=1}^{\left\{{N \atop k}\right\}} p^k_j \sigma^k_j$$

для некоторого распределения вероятностей $\{p^k_j\}_j$ и сепарабельных операторов плотности σ^k_j. Заметим, что $\varrho_{k\text{-sep}}$ по-прежнему может быть перепутанным по отношению к разбиениям $\mathcal{P}^k_j$, если $\left\{{N \atop k}\right\} > 1$. Понятно, что k-сепарабельное состояние является также и $(k-1)$-сепарабельным, что приводит к следующему соотношению включения для выпуклых множеств k-сепарабельных состояний:

$$\mathcal{S}_{N\text{-sep}} \subset \ldots \subset \mathcal{S}_{2\text{-sep}} \subset \mathcal{S}_{1\text{-sep}}.$$

Вводим естественным образом возникающую меру сепарабельности:

$$K_{\text{sep}}[\varrho] := \max_{\varrho = \varrho_{k\text{-sep}}} k. \tag{10}$$

Если $K_{\text{sep}}[\varrho] = 1$, то состояние ϱ называется *истинно перепутанным* (genuinely entangled, GE). Если $K_{\text{sep}}[\varrho] = N$, то состояние ϱ называется *полностью сепарабельным* (fully separable, FS).

4.2. Глубина перепутанности. Альтернативный подход к количественному описанию многочастичной перепутанности заключается в подсчете числа частиц, которые в самом деле перепутаны (см. [62,105,126,145]). Это число показывало бы ресурсоемкость создания такого состояния. Например, состояние $\varrho^{AB}\otimes\varrho^{CDE}$ пятичастичной системы $ABCDE$ является 2-сепарабельным, но содержит часть CDE, которая может быть истинно перепутанной ($K_{\text{sep}}[\varrho^{CDE}]=1$), т.е. требует перепутывания трех частиц для его создания. Для выражения этой идеи в точной форме вводим следующее определение ресурсоемкости (совместимое с понятиями глубины перепутанности (entanglement depth, см. [136]) и продуктивности (producibility, см. [71])):

$$R_{\text{ent}}[\varrho] := \min_{\varrho=\sum\limits_{k=1}^{N}\sum\limits_{j=1}^{\binom{N}{k}} p_j^k\sigma_j^k} \max_{m=1,\ldots,k} \left\{\text{число частиц в компоненте } [\mathcal{P}_j^k]_m\right\}. \tag{11}$$

Обозначим через $\mathcal{S}_{r\text{-ent}}=\{\varrho : R_{\text{ent}}[\varrho]\leqslant r\}$ выпуклое множество r-перепутанных состояний. Очевидно,

$$\mathcal{S}_{1\text{-ent}}\subset\mathcal{S}_{2\text{-ent}}\subset\ldots\subset\mathcal{S}_{N\text{-ent}}.$$

Важно заметить также, что

$$\mathcal{S}_{1\text{-ent}}=\mathcal{S}_{N\text{-sep}},\quad \mathcal{S}_{(N-1)\text{-ent}}=\mathcal{S}_{2\text{-sep}},\quad \mathcal{S}_{N\text{-ent}}=\mathcal{S}_{1\text{-sep}}=\mathcal{S}(\mathcal{H}^{ABC\ldots}).$$

В зависимости от квантового состояния R_{ent} принимает значения в диапазоне

$$\left\lceil\frac{N}{K_{\text{sep}}}, N-K_{\text{sep}}+1\right\rceil$$

для фиксированного K_{sep}, а функционал K_{sep} принимает значения

$$\left\lceil\frac{N}{R_{\text{ent}}}, N-R_{\text{ent}}+1\right\rceil$$

для фиксированного R_{ent}.

4.3. Детектирование глубины перепутанности с помощью n-тензорно постоянных положительных отображений. Положительные отображения часто используются для детектирования различных видов перепутанности (см. [27, 31, 34, 35, 38, 73, 74, 81, 90, 103, 118, 141]). В этом разделе мы применяем n-тензорно постоянно положительные отображения для нахождения глубины перепутанности.

Предложение 13. *Пусть Φ — n-тензорно постоянно положительное кубитное отображение и $\Phi^{\otimes N}[\varrho]\not\geqslant 0$ (содержит отрицательные собственные значения). Тогда глубина перепутанности удовлетворяет неравенству $R_{\text{ent}}[\varrho]\geqslant n+1$.*

Доказательство. Предположим, что $R_{\text{ent}}[\varrho]\leqslant n$; тогда существует разложение в виде выпуклой суммы

$$\varrho=\sum_j p_{jk}\varrho_j^{(1)}\otimes\cdots\otimes\varrho_j^{(k)},$$

где каждое состояние $\varrho_j^{(m)}$ содержит не более n кубитов. Следовательно,

$$\Phi^{\otimes\#\varrho_j^{(m)}}[\varrho_j^{(m)}]\geqslant 0$$

ввиду вложенной структуры k-тензорно постоянных положительных отображений. Таким образом, $\Phi^{\otimes N}[\varrho]\geqslant 0$, что противоречит формулировке предложения. Следовательно, $R_{\text{ent}}[\varrho]\geqslant n+1$. □

Проиллюстрируем применение предложения 13 для детектирования определенного вида многочастичной перепутанности.

Пример 2 (см. [53])**.** Деполяризованное GHZ состояние трёх кубитов

$$\varrho_q^{\mathrm{GHZ}} = q|\,\mathrm{GHZ}\rangle\langle\mathrm{GHZ}\,| + (1-q)\frac{1}{8}I, \quad 0 \leqslant q \leqslant 1, \tag{12}$$

не является полностью сепарабельным при $q \geqslant 0.26$, поскольку существует такое положительное унитальное кубитное отображение Υ ($|\lambda_i| \leqslant 1$), что

$$\Upsilon^{\otimes 3}[\varrho_q^{\mathrm{GHZ}}] \ngeqslant 0.$$

Также ϱ_q^{GHZ} является истинно перепутанным при $q \geqslant 0.71$, поскольку существует 2-тензорно постоянное положительное унитальное кубитное отображение Υ такое, что

$$\Upsilon^{\otimes 3}[\varrho_q^{\mathrm{GHZ}}] \ngeqslant 0.$$

Пример 3 (см. [53])**.** Рассмотрим деполяризованное W-состояние трёх кубитов

$$\varrho_q^{\mathrm{W}} = q|\,\mathrm{W}\rangle\langle\mathrm{W}\,| + (1-q)\frac{1}{8}I, \quad 0 \leqslant q \leqslant 1, \tag{13}$$

где

$$|W\rangle = \frac{1}{\sqrt{3}}(|100\rangle + |010\rangle + |001\rangle).$$

Состояние ϱ_q^{W} не является полностью сепарабельным при $q \geqslant 0.31$, поскольку существует такое положительное унитальное кубитное отображение Υ ($|\lambda_i| \leqslant 1$), что

$$\Upsilon^{\otimes 3}[\varrho_q^{\mathrm{W}}] \ngeqslant 0.$$

Аналогично, ϱ_q^{W} истинно перепутано при $q \geqslant 0.86$, поскольку существует такое 2-тензорно постоянно положительное унитальное кубитное отображение Υ, что

$$\Upsilon^{\otimes 3}[\varrho_q^{\mathrm{W}}] \ngeqslant 0.$$

5. Динамика многочастичной перепутанности

Физическое явление многочастичной перепутанности квантовых состояний естественным образом возникает между взаимодействующими частями составной системы. Простые модели столкновений показывают, что различные виды взаимодействий приводят к различной структуре многочастичной перепутанности (см. [155]). Многочастичная перепутанность находит применения в квантовых сетевых приложениях, таких как секретная коммуникация (см. [78]), тайное голосование (см. [79]), телепортация с открытым местом назначения (см. [96]) и т. д. Для подобных целей перепутанность может быть создана не только посредством взаимодействия частей системы, но также посредством надлежащим образом реализованного взаимодействия системы с окружением (см. [108, 110, 116]).

Представим перепутанное многочастичное состояние, приготовленное для использования в некотором протоколе с удаленными адресатами. При передаче квантового состояния от приготовителя к адресатам само состояние претерпит изменения вследствие неизбежных внешних воздействий (шумов). Может оказаться, что структура многочастичной перепутанности, полученная адресатами, будет существенно отличаться от первоначальной, и реализация желаемого протокола станет невозможной. Аналогично, неконтролируемые шумы в устройствах квантовой памяти могут привести к разрушению определенных корреляций, приводя к неэффективному для дальнейшего использования высвобожденного квантового состояния (см. [117, 132]). Деградация перепутанности также накладывает ограничения на выигрыш в точности в квантовой метрологии, которая основывается на использовании истинно перепутанных состояний (см. [61]). Эти примеры явно показывают необходимость изучения динамики перепутанности (ее структуры) и нахождения уровней шумов, соотвествующих определенному изменению вида перепутанности.

Развитые ранее подходы основывались на специфических мерах перепутанности. Отрицательность (negativity; см. [148]) — мера, детектирующая отрицательность матрицы плотности под действием частичного транспонирования (NPT; см. [118]) — была использована для анализа GHZ, W и кластерных состояний, подверженных локальному деполяризующему шуму (см. [45, 131]).

Затем её использовали для изучения поведения GHZ состояний и состояний на графе, подверженных локальному однородному шуму общего вида (см. [17,76]). Обобщенные состояния вида GHZ, подверженные локальному затуханию амплитуды, были рассмотрены с помощью меры отрицательности в [109]. Мера отрицательности также использовалась для изучения влияния локальной деполяризации, дефазировки и затухания амплитуды общего вида для GHZ состояний (см. [9]) и состояний на графе (см. [11]). Перечисленные выше результаты были получены для произвольного числа кубитов (за исключением некоторых состояний на графе (см. [11]) и случайных квантовых состояний (см. [10]) благодаря предельной простоте вычисления меры отрицательности. Что касается d-уровневых квантовых систем, то деполяризация и дефазировка GHZ состояний рассматривались с помощью меры отрицательности в [106]. Аналогично, вложенные GHZ состояния (где GHZ перепутанные части сами по себе являются блоками небольшого числа кубитов в GHZ состоянии) рассматривались в [59]. Главный недостаток меры отрицательности заключается в том, что она не дает значимой информации о структуре перепутанности, поскольку чувствительна к перепутанности по отношению к разбиению только на две части (напомним, что существуют перепутанные состояния с положительным частичным транспонированием (см. [82]) и бисепарабельные, но не трисепарабельные состояния (см. [22]).

Отсутствие полной сепарабельности может быть детектировано и другими мерами. Геометрическая мера перепутанности (см. [18,149]) была использована для изучения глобальных дефазирующих процессов, действующих на 4-кубитные GHZ, W, Dicke и кластерные состояния (см. [69]). Энтропийная мера использовалась для усредненной вдоль квантовых траекторий n-частичной перепутанности (см. [66]). Теория эволюции SL-инвариантрой перепутанности для локальной декогеренции была разработана в [60]. Заметим, что ненулевое значение перечисленных величин указывает на наличие некоторой перепутанности в квантовой системе, но не дает информации о ее конкретной структуре и, следовательно, о пользе данной перепутанности для приложений. Более того, нулевые значения перечисленных выше мер не гарантируют полной сепарабельности состояния, и поэтому проблема фундаментальных уровней шумов, устраняющих произвольную форму перепутанности (приводящих к полностью сепарабельному состоянию), остается нерешенной и актуальной.

Истинная многочастичная перепутанность не сводится к перепутанности, рассредоточенной внутри менее крупных подсистем. Детектирование истинной перепутанности для определенных квантовых состояний является предметом интесивных исследований (см., например, [41, 70, 88, 89, 94, 115]). Диссипативная эволюция истинной многочастичной перепутанности анализировалась с помощью некоторых мер. Среднее значение проективноподобного свидетеля перепутанности (projector-like witness; см. [26]) использовалось в [25] для изучения нескольких кубитов в эвристической модели декогеренции, основанной на временах локальной релаксации и дефазировки. В [30] использовался коллективно-спиновый свидетель перепутанности для анализа динамики истинной многочастичной перепутанности состояний Дики под действием локального затухания амплитуды, дефазировки и деполяризации. Трехчастичная мера отрицательности использовалась для анализа динамики GHZ и W трехкубитных перепутанных состояний (см. [5, 8, 29, 123, 133, 150]). Напомним, что перечисленные выше меры не являются точными, т.е. их нулевые значения еще не гарантируют в общем случае отсутствие истинной перепутанности. С другой стороны, точные меры, использующие выпуклую конструкуцию, трудновычислимы (см. [144]). Это является основным препятствием в исследованиях по динамике квантовой перепутанности, и поэтому авторы обычно ограничиваются рассмотрением определенных начальных состояний (GHZ, W, X, Dicke и др.) и относительно легковычислимых мер перепутанности.

Несмотря на существующие результаты для шумов, сохраняющих истинную перепутанность или перепутанность вообще (отсутствие полной сепарабельности), эволюция структуры перепутанности по прежнему остается неисследованной. В данном разделе даётся краткий обзор преобразований в структуре перепутанности в диссипативных процессах. Под «структурой» мы понимаем число отдельных компонент и число частиц в каждом из них (с учетом возможных выпуклых комбинаций) (см. [46,105,126]). Идея проследить за структурой перепутанности была реализована для трехкубитных GHZ состояний под действием глобальной деполяризации (см. [48]) и

для подпространства состояний с одним возбуждением в [107]. Мы же не ограничиваемся определенными входными состояниями и разрабатываем теорию квантовых отображений, которые отображают *произвольное* начальное состояние в множество состояний с заданными свойствами. Заметим, что большая часть исследований других авторов сфокусирована на противоположной задаче: показать, что состояние находится вне множества с заданными характеристиками (см. [41, 70, 88, 89, 94, 105, 115, 126]). По отношению к нашему подходу, наиболее близкая постановка задачи представлена в [95]. Наша методология основывается на аккуратном разложении физических преобразований на более простые (но не обязательно физические) процессы с операциями, разрушающими перепутанность. Полученные критерии формулируются для квантовых каналов общего вида.

Для иллюстрации метода мы рассматриваем примеры локальных и глобальных деполяризующих шумов, моделирующих окружение в виде индивидуальных резервуаров или одного общего резервуара соответственно. Локальные деполяризующие шумы возникают в задачах квантовой коммуникации (использующей, например, оптические волокна), а также в чисто физических системах, таких как ядерные спины в молекулах (см. [49]). Глобальный деполяризующий шум является адекватной моделью в экспериментах, где возникают состояния полного ранга (см. [19,104]). С точки зрения диссипации, глобальный деполяризующий шум считается наихудшем из возможных сценариев взаимодействия системы и окружения (см. [47]). Мы в нашей работе находим уровни шумов, отвечающие определенному виду диссоциации перепутанности, и выявляем различия в поведении структуры перепутанности под действием локальных и глобальных шумов.

5.1. Квантовые каналы, диссоциирующие перепутанность. Рассмотрим составную N-частичную систему $S = ABC\ldots$, претерпевающую эволюцию $\varrho_{\text{out}} = \Phi[\varrho_{\text{in}}]$, определяемую некоторым вполне положительным отображением Φ (также предполагаем $\mathcal{H}^S_{\text{in}} = \mathcal{H}^S_{\text{out}}$). Если ϱ_{out} является сепарабельным по отношению к разбиению $\mathcal{P}^k_j$ (т.е. $\varrho_{\text{out}} = \sigma^k_j$), то будем говорить, что канал Φ диссоциирует перепутанное соединение исходного ϱ_{in} на более мелкие соединения $[\mathcal{P}^k_j]_1, \ldots, [\mathcal{P}^k_j]_k$, и обозначим через $\mathcal{D}^k_j(\varrho_{\text{in}})$ множество таких каналов. Если канал Φ подобным образом диссоциирует перепутанность всех входных состояний $\varrho_{\text{in}} \in \mathcal{S}(\mathcal{H}^S)$, то будем называть Φ диссоциирующим перепутанность по отношению к разбиению $\mathcal{P}^k_j$ и писать

$$\Phi \in \mathcal{D}^k_j \equiv \bigcap_{\varrho_{\text{in}} \in \mathcal{S}(\mathcal{H}^S)} \mathcal{D}^k_j(\varrho_{\text{in}}).$$

Используя меры перепутанности (10) и (11), мы можем количественно описать процессы динамики структуры перепутанности. В самом деле, обозначим $k\,\mathrm{Sep}(\varrho_{\text{in}})$ набор таких каналов Φ, что $K_{\text{sep}}\,[\Phi[\varrho_{\text{in}}]] \geqslant k$. По построению, $k\,\mathrm{Sep}(\varrho_{\text{in}})$ — выпуклая оболочка множеств $\mathcal{D}^k_j(\varrho_{\text{in}})$. Аналогично, $r\,\mathrm{Ent}(\varrho_{\text{in}})$ — множество таких каналов Φ, что $R_{\text{ent}}\,[\Phi[\varrho_{\text{in}}]] \leqslant r$. Для описания свойств каналов, не зависящих от входных состояний, вводим

$$k\,\mathrm{Sep} := \bigcap_{\varrho_{\text{in}} \in \mathcal{S}(\mathcal{H}^S)} k\,\mathrm{Sep}(\varrho_{\text{in}}), \quad r\,\mathrm{Ent} := \bigcap_{\varrho_{\text{in}} \in \mathcal{S}(\mathcal{H}^S)} r\,\mathrm{Ent}(\varrho_{\text{in}}).$$

Разработанный в разделе 4 формализм приводит к следующей диаграмме включения:

$$\begin{array}{ccccccccc}
N\,\mathrm{Sep} & \subset & (N-1)\,\mathrm{Sep} & \subset & \cdots & \subset & 2\,\mathrm{Sep} & \subset & 1\,\mathrm{Sep} \\
\| & & & & & & \| & & \| \\
1\,\mathrm{Ent} & \subset & 2\,\mathrm{Ent} & \subset & \cdots & \subset & (N-1)\,\mathrm{Ent} & \subset & N\,\mathrm{Ent} \\
\| & & & & & & \| & & \| \\
\mathrm{EA} & & & & & & \mathrm{DGE} & & \mathrm{CPT}
\end{array}$$

Мы использовали специальные обозначения для двух отличительных классов каналов: EA — каналы, аннигилирующие перепутанность, которые отображают произвольное входное состояние в полностью сепарабельное; DGE — каналы, диссоциирующие истинную перепутанность (dissociating genuine entanglement), приводящие к потере состояниями свойства истинной перепутанности.

Оператор ξ_j^k называется блочно-положительными по отношению к разбиению $\mathcal{P}_j^k$, если он удовлетворяет условию

$$\langle \psi_1^{[\mathcal{P}_j^k]_1} \otimes \cdots \otimes \psi_k^{[\mathcal{P}_j^k]_k} | \xi_j^k | \psi_1^{[\mathcal{P}_j^k]_1} \otimes \cdots \otimes \psi_k^{[\mathcal{P}_j^k]_k} \rangle \geqslant 0 \tag{14}$$

для всех векторов $\psi_1, \ldots, \psi_k$. Блочно-положительные операторы тесно связаны со свидетелями перепутанности (см. [81, 84]) и могут быть использованы в детектировании сепарабельности: состояние $\varrho \in \mathcal{S}(\mathcal{H}^{ABC\ldots})$ является сепарабельным по отношению к разбиению $\mathcal{P}_j^k$ тогда и только тогда, когда $\operatorname{tr}[\varrho \xi_j^k] \geqslant 0$ для всех блочно-положительных операторов ξ_j^k.

Мы должны подчеркнуть, что понятия диссоциации и аннигиляции перепутанности не подразумевают никакой вспомогательной системы помимо самой системы $S = ABC\ldots$. Это позволяет ослабить условие вполне положительности физического отображения Φ и построить расширенное множество $\mathcal{E}[\Phi]$ (математических) линейных отображений Υ, обладающих теми же самыми свойствами по отношению к перепутанности, что и Φ, на соответствующей области определения (входных состояниях). К примеру, расширенное множество $\mathcal{E}[\mathcal{D}_j^k(\varrho_{\text{in}})]$ состоит из линейных отображений Υ, удовлетворяющих единственному ограничению, что $\Upsilon[\varrho_{\text{in}}]$ равняется некоторому σ_j^k. Аналогично, $\mathcal{E}[k\operatorname{Sep}(\varrho_{\text{in}})]$ и $\mathcal{E}[r\operatorname{Ent}(\varrho_{\text{in}})]$ обозначают расширения множеств $k\operatorname{Sep}(\varrho_{\text{in}})$ и $r\operatorname{Ent}(\varrho_{\text{in}})$ соответственно. Как будет показано далее, расширения оказываются полезными в силу их простой характеризации. Первоначальный набор физических отображенией может быть найден путем пересечения расширений с вполне положительными, сохраняющими след отображениями (CPT), например, $\mathcal{D}_j^k(\varrho_{\text{in}}) = \text{CPT} \cap \mathcal{E}[\mathcal{D}_j^k(\varrho_{\text{in}})]$.

Предложение 14 (см. [54]). *Пусть Υ — линейное отображение, действующее на систему $ABC\ldots$. Включение $\Upsilon \in \mathcal{E}[\mathcal{D}_j^k(\varrho_{\text{in}})]$ имеет место тогда и только тогда, когда*

$$\operatorname{tr}\left[\Omega_\Upsilon^{ABC\ldots A'B'C'\ldots}\left((\xi_j^k)^{ABC\ldots} \otimes (\varrho_{\text{in}}^{\text{T}})^{A'B'C'\ldots}\right)\right] \geqslant 0 \tag{15}$$

для всех ξ_j^k.

Как результат, конус $\mathcal{E}[\mathcal{D}_j^k(\varrho_{\text{in}})]$ дуален по отношению к конусу отображений $\Upsilon^\circ[X] = \xi_j^k \operatorname{tr}[\varrho_{\text{in}} X]$. Что касается множества $\mathcal{D}_j^k$, отображение Υ принадлежит к множеству $\mathcal{D}_j^k$, если его матрица Чоя удовлетворяет условию

$$\operatorname{tr}\left[\Omega_\Upsilon^{ABC\ldots A'B'C'\ldots}\left((\xi_j^k)^{ABC\ldots} \otimes \varrho^{A'B'C'\ldots}\right)\right] \geqslant 0$$

для всех ξ_j^k и $\varrho^{A'B'C'\ldots}$.

Критерий из предложения 14 не является операционным. Для преодоления этой трудности в [54] получены достаточные условия диссоциации перепутанности.

Предложение 15 (см. [54]). *Последовательное применение линейного эрмитова отображения Ξ и $(k-1)$-компонентной разрушающей перепутанность операции*

$$\left(\mathcal{O}_{\text{EB}}^{[\mathcal{P}_j^k]_1} \otimes \cdots \otimes \operatorname{Id}^{[\mathcal{P}_j^k]_m} \otimes \cdots \otimes \mathcal{O}_{\text{EB}}^{[\mathcal{P}_j^k]_k}\right)$$

является элементом множества $\mathcal{E}[\mathcal{D}_j^k(\varrho_{\text{in}})]$, если $\Xi[\varrho_{\text{in}}]$ становится положительным после проецирования на правые сингулярные векторы операторов Крауса ранга 1 соответствующей разрушающей перепутанность операции.

Преимущество построенного таким образом последовательного применения отображений заключается в том, что отображение Ξ не должно быть положительным, что делает множество $\mathcal{E}[\mathcal{D}_j^k(\varrho_{\text{in}})]$ еще богаче.

При рассмотрении всех возможных состояний ϱ_{in} выполнение условия (15) становится равнозначным положительности отображения

$$\left(\mathcal{O}_{\text{EB}}^{[\mathcal{P}_j^k]_1} \otimes \cdots \otimes \operatorname{Id}^{[\mathcal{P}_j^k]_m} \otimes \cdots \otimes \mathcal{O}_{\text{EB}}^{[\mathcal{P}_j^k]_k}\right) \circ \Xi.$$

Это отображение автоматически является положительным, если Ξ отображает операторы плотности в блочно-положительные операторы ξ_j^k, что, в свою очередь, эквивалентно тому, что соответствующий оператор Чоя является блочно-положительным оператором вида

$$\Omega_\Xi^{ABC\ldots A'B'C'\ldots} = \xi^{\mathcal{P}_j^k(ABC\ldots)|A'B'C'\ldots}.$$

Следствие 4 (см. [54]). *Если $\Omega_\Xi^{ABC\ldots A'B'C'\ldots}$ является блочно-положительным по отношению к разбиению $\mathcal{P}_j^k(ABC\ldots)|A'B'C'\ldots$, то*

$$\left(\mathcal{O}_{\mathrm{EB}}^{[\mathcal{P}_j^k]_1} \otimes \cdots \otimes \mathrm{Id}^{[\mathcal{P}_j^k]_m} \otimes \cdots \otimes \mathcal{O}_{\mathrm{EB}}^{[\mathcal{P}_j^k]_k}\right) \circ \Xi \in \mathcal{D}_j^k$$

для произвольной разрушающей перепутанность операции.

Множества $\mathcal{E}[k\,\mathrm{Sep}(\varrho_{\mathrm{in}})]$ и $\mathcal{E}[r\,\mathrm{Ent}(\varrho_{\mathrm{in}})]$ представляют собой не что иное, как соответствующие выпуклые оболочки множеств $\mathcal{E}[\mathcal{D}_j^k(\varrho_{\mathrm{in}})]$, которые могут быть детектированы предложением 15. Вспомним, однако, что мы заинтересованы в характеризации множеств $k\,\mathrm{Sep}(\varrho_{\mathrm{in}})$ и $r\,\mathrm{Ent}(\varrho_{\mathrm{in}})$ физических (CPT) отображений. Поскольку рассматриваемое отображение Φ с самого начала является CPT, его разложение в математические отображения не нарушает этого свойства, однако гарантирует, что оно принадлежит к желаемому множеству отображений. Таким образом, мы получаем следующее утверждение.

Предложение 16 (см. [54]). *Пусть Φ — квантовый канал, допускающий разложение*

$$\Phi = \sum_{\mathcal{P}_j^k \in \mathsf{P}} \mathcal{M}_j^k,$$

где каждое элементарное отображение $\mathcal{M}_j^k \in \mathcal{E}[\mathcal{D}_j^k(\varrho_{\mathrm{in}})]$ строится согласно предложению 15. Если P — подмножество разбиений, входящих в k-сепарабельные или r-перепутанные состояния, то Φ принадлежит $k\mathrm{Sep}(\varrho_{\mathrm{in}})$ или $r\mathrm{Ent}(\varrho_{\mathrm{in}})$ соответственно.

Аналогично, для детектирования отображений из множеств $k\,\mathrm{Sep}$ и $r\,\mathrm{Ent}$ в формулировке предложения 16 можно использовать следствие 4 вместо предложения 15.

Достаточный критерий детектирования подмножеств каналов $k\,\mathrm{Sep}(\varrho_{\mathrm{in}})$ и $r\,\mathrm{Ent}(\varrho_{\mathrm{in}})$, предложение 16, предполагает наличие разложения канала Φ. В [54] представлена методика построения этого разложения для относительно простого однопараметрического семейства деполяризующих каналов, действующих на N кубитов: локальный деполяризующий шум $\Phi_q^{\mathrm{local}} \equiv \Phi_q^{\otimes N}$, где Φ_q — однокубитное отображение ($d = 2$), и глобальный деполяризующий шум Φ_q^{global} ($d = 2^N$). Для фиксированных k и r найдены области параметра q, в которых канал Φ_q^{local} (или Φ_q^{global}) допускает разложение на элементарные блоки, составляющие $k\,\mathrm{Sep} \cap r\,\mathrm{Ent}$.

Разработанная методология была применена в [54] для локальных и глобальных N-кубитных деполяризующих каналов. Были выявлены различия в динамике квантовой перепутанности под действием локальных и глобальных шумов: частицы отделяются одна за другой от перепутанного соединения в случае локального шума и стремятся образовывать кластеры в случае глобального шума. Полученные результаты могут быть расширены к другим моделям шума и дать дополнительную информацию о динамике структуры квантовой перепутанности.

6. Заключение

В настоящей работе представлен обзор использования квантовых отображений в задачах характеризации перепутанных состояний. Квантовые отображения могут быть не связаны с физической эволюцией системы (например, положительные и n-тензорно постоянные положительные отображения), а могут быть и физическими динамическими отображениями (однопараметрическими квантовыми каналами). Представлен обзор известных свойств квантовых каналов, разрушающих перепутанность, аннигилирующих перепутанность, диссоциирующих перепутанность, запрещающих дистилляцию. Кроме этого, представлены и частично характеризованы новые классы квантовых каналов: абсолютно распутывающие квантовые каналы и каналы, навязывающие перепутанность. Для каналов, навязывающих перепутанность, получено необходимое

и достаточное условие в терминах действия дуального отображения на свидетель перепутанности. Введено определение состояний, наиболее стойких к потере перепутанности. Показано, что максимально перепутанное состояние не является наиболее стойким к деполяризующим шумам в двухкудитных системах. Для таких шумов найдено состояние ранга Шмидта 2, обладающее наибольшей стойкостью к деполяризующим шумам. Представлен алгоритм нахождения наиболее стойких состояний для тензорного произведения неунитальных кубитных отображений. Сделан обзор структуры многочастичной перепутанности с помощью степени сепарабельности и глубины перепутанности, а также динамики многочастичной перепутанности. Исследовано разложение многочастичного канала по линейным отображениям (не обязательно вполне положительным), обеспечивающим желаемую форму выходной перепутанности. Представлен метод построения таких разложений с помощью разрушающих перепутанность отображений. Найдено условие многочастичной r-перепутанности с помощью n-тензорно постоянных положительных отображений.

СПИСОК ЛИТЕРАТУРЫ

1. *Холево А. С.* Квантовые теоремы кодирования// Усп. ма. наук. — 1998. — *53*, № 6 (324). — С. 193–230.
2. *Холево А. С.* Каналы, разрушающие сцепленность, в бесконечных размерностях// Пробл. передачи информ. — 2008. — *44*, № 3. — С. 3–18.
3. *Широков М. Е.* Число Шмидта и каналы, частично разрушающие сцепленность, в бесконечномерных квантовых системах// Мат. заметки. — 2013. — *93*, № 5. — С. 775–789.
4. *Широков М. Е.* Меры корреляций в бесконечномерных квантовых системах// Мат. сб. — 2016. — *207*, № 5. — С. 93–142.
5. *Altintas F., Eryigit R.* Quantum correlations in non-Markovian environments// Phys. Lett. A. — 2010. — *374*. — С. 4283.
6. *Amosov G. G., Mancini S.* Entanglement from operators splitting// AIP Conf. Proc. — 2009. — *1101*. — С. 100.
7. *Amosov G. G., Filippov S. N.* Spectral properties of reduced fermionic density operators and parity superselection rule/ `arXiv:1512.01828[quant-ph]`
8. *An N. B., Kim J., Kim K.* Entanglement dynamics of three interacting two-level atoms within a common structured environment// Phys. Rev. A. — 2011. — *84*. — С. 022329.
9. *Aolita L., Chaves R., Cavalcanti D., Acín A., Davidovich L.* Scaling laws for the decay of multiqubit entanglement// Phys. Rev. Lett. — 2008. — *100*. — С. 080501.
10. *Aolita L., Cavalcanti D., Acín A., Salles A., Tiersch M., Buchleitner A., de Melo F.* Scalability of Greenberger—Horne—Zeilinger and random-state entanglement in the presence of decoherence// Phys. Rev. A. — 2009. — *79*. — С. 032322.
11. *Aolita L., Cavalcanti D., Chaves R., Dhara C., Davidovich L., Acín A.* Noisy evolution of graph-state entanglement// Phys. Rev. A. — 2010. — *82*. — С. 032317.
12. *Aolita L, de Melo F., Davidovich L.* Open-system dynamics of entanglement: A key issues review// Rep. Progr. Phys. — 2015. — *78*. — С. 042001.
13. *Aspect A., Dalibard J., Roger G.* Experimental test of Bell's inequalities using time-varying analyzers// Phys. Rev. Lett. — 1982. — *49*. — С. 1804–1807.
14. *Aspect A., Grangier P., Roger G.* Experimental tests of realistic local theories via Bell's theorem// Phys. Rev. Lett. — 1981. — *47*. — С. 460–463.
15. *Aspect A., Grangier P., Roger G.* Experimental realization of Einstein—Podolsky—Rosen—Bohm Gedankenexperiment: A new violation of Bell's inequalities// Phys. Rev. Lett. — 1982. — *49*. — С. 91–94.
16. *Aubrun G., Szarek S. J.* Two proofs of Størmer's theorem/ `arXiv:1512.03293[math.FA]`
17. *Bandyopadhyay S., Lidar D. A.* Robustness of multiqubit entanglement in the independent decoherence model// Phys. Rev. A. — 2005. — *72*. — С. 042339.
18. *Barnum H., Linden N.* Monotones and invariants for multi-particle quantumstates// J. Phys. A: Math. Gen. — 2001. — *34*. — С. 6787.
19. *Barreiro J. T., Schindler P., Gühne O., Monz T., Chwalla M., Roos C. F., Hennrich M., Blatt R.* Experimental multiparticle entanglement dynamics induced by decoherence// Nature Phys. — 2010. — *6*. — С. 943.
20. *Bell J. S.* On the Einstein—Podolsky—Rosen paradox// Physics. — 1964. — *1*. — С. 195–200.
21. *Benatti F., Floreanini R., Marzolino U.* Entanglement in fermion systems and quantum metrology// Phys. Rev. A. — 2014. — *89*. — С. 032326.

22. *Bennett C. H., DiVincenzo D. P., Mor T., Shor P. W., Smolin J. A., Terhal B. M.* Unextendible product bases and bound entanglement// Phys. Rev. Lett. — 1999. — *82*. — С. 5385.
23. *Bennett C., Wiesner S.* Communication via one- and two-particle operators on Einstein—Podolsky—Rosen states// Phys. Rev. Lett. — 1992. — *69*. — С. 2881.
24. *Bennett C., Brassard G., Crépeau C., Jozsa R., Peres A., Wootters W. K.* Teleporting an unknown quantum state via dual classical and Einstein—Podolsky—Rosen channels// Phys. Rev. Lett. — 1993. — *70*. — С. 1895.
25. *Bodoky F., Gühne O., Blaauboer M.* Modeling the decay of entanglement for electron spin qubits in quantum dots// J. Phys. Condensed Matter. — 2009, — *21*. — С. 395602.
26. *Bourennane M., Eibl M., Kurtsiefer C., Gaertner S., Weinfurter H., Gühne O., Hyllus P., Bruß D., Lewenstein M., Sanpera A.* Experimental detection of multipartite entanglement using witness operators// Phys. Rev. Lett. — 2004. — *92*. — С. 087902.
27. *Breuer H.-P.* Optimal entanglement criterion for mixed quantum states// Phys. Rev. Lett. — 2006. — *97*. — С. 080501.
28. *Breuer H.-P., Petruccione F.* The theory of open quantum systems. — New York: Oxford Univ. Press, 2002.
29. *Buscemi F., Bordone P.* Time evolution of tripartite quantum discord and entanglement under local and nonlocal random telegraph noise// Phys. Rev. A. — 2013. — *87*. — С. 042310.
30. *Campbell S., Tame M. S., Paternostro M.* Characterizing multipartite symmetric Dicke states under the effects of noise// New J. Phys. — 2009. — *11*. — С. 073039.
31. *Chen K., Wu L.-A.* Test for entanglement using physically observable witness operators and positive maps// Phys. Rev. A. — 2004. — *69*. — С. 022312.
32. *Chen J., Duan R., Ji Z., Ying M., Yu J.* Existence of universal entangler// J. Math. Phys. — 2008. — *49* — С. 012103.
33. *Choi M.-D.* Completely positive linear maps on complex matrices// Linear Algebra Appl. — 1975. — *10* — С. 285.
34. *Chruściński D., Kossakowski A.* On the structure of entanglement witnesses and new class of positive indecomposable maps// Open Syst. Inform. Dynam. — 2007. — *14*. — С. 275.
35. *Chruściński D., Sarbicki G.* Entanglement witnesses: construction, analysis and classification// J. Phys. A: Math. Theor. — 2014. — *47*. — С. 483001.
36. *Clauser J., Horne M., Shimony A., Holt R.* Proposed experiment to test local hidden-variable theories// Phys. Rev. Lett. — 1969. — *23*. — С. 880–884.
37. *Clauser J. F., Horne M. A.* Experimental consequences of objective local theories// Phys. Rev. D. — 1974. — *10*. — С. 526–535.
38. *Collins B., Hayden P., Nechita I.* Random and free positive maps with applications to entanglement detection// Int. Math. Res. Not. — 2016. — *2016*. — С. 1.
39. *De Pillis J.* Linear transformations which preserve Hermitian and positive semidefinite operators// Pac. J. Math. — 1967. — *23*. — С. 129.
40. *Deutsch D., Jozsa R.* Rapid solutions of problems by quantum computation// Proc. Roy. Soc. Lond. A. — 1992. — *439*. — С. 553.
41. *De Vicente J. I., Huber M.* Multipartite entanglement detection from correlation tensors// Phys. Rev. A. — 2011. — *84*. — С. 062306.
42. *DiVincenzo D. P., Shor P. W., Smolin J. A., Terhal B. M., Thapliyal A. V.* Evidence for bound entangled states with negative partial transpose// Phys. Rev. A. — 2000. — *61*. — С. 062312.
43. *DiVincenzo D. P., Mor T., Shor P. W., Smolin J. A., Terhal B. M.* Unextendible product bases, uncompletable product bases and bound entanglement// Commun. Math. Phys. — 2003. — *238*. — С. 379.
44. *Duan L.-M., Giedke G., Cirac J. I., Zoller P.* Inseparability criterion for continuous variable systems// Phys. Rev. Lett. — 2000. — *84*. — С. 2722.
45. *Dür W., Briegel H.-J.* Stability of macroscopic entanglement under decoherence// Phys. Rev. Lett. — 2004. — *92*. — С. 180403.
46. *Dür W., Cirac J. I., Tarrach R.* Separability and distillability of multiparticle quantum systems// Phys. Rev. Lett. — 1999. — *83*. — С. 3562–3565.
47. *Dür W., Hein M., Cirac J. I., Briegel H.-J.* Standard forms of noisy quantum operations via depolarization// Phys. Rev. A. — 2005. — *72*. — С. 052326.
48. *Eltschka C., Siewert J.* Entanglement of three-qubit Greenberger—Horne—Zeilinger–symmetric states// Phys. Rev. Lett. — 2012. — *108*. — С. 020502.

49. *Emerson J., Silva M., Moussa O., Ryan C., Laforest M., Baugh J., Cory D. G., Laflamme R.* Symmetrized characterization of noisy quantum processes// Science. — 2007. — *317*. — С. 1893.
50. *Einstein A., Podolsky B., Rosen N.* Can quantum-mechanical description of physical reality be considered complete?// Phys. Rev. — 1935. — *47*. — С. 777–780.
51. *Filippov S. N.* PPT-inducing, distillation-prohibiting, and entanglement-binding quantum channels// J. Russ. Laser Res. — 2014. — *35*. — С. 484–491.
52. *Filippov S. N.* Influence of deterministic attenuation and amplification of optical signals on entanglement and distillation of Gaussian and non-Gaussian quantum states// EPJ Web Conf. — 2015. — *103*. — С. 03003.
53. *Filippov S. N., Magadov K. Yu.* Positive tensor products of qubit maps and 2-tensor-stable positive qubit maps/ `arXiv:1604.01716[quant-ph]`.
54. *Filippov S. N., Melnikov A. A., Ziman M.* Dissociation and annihilation of multipartite entanglement structure in dissipative quantum dynamics// Phys. Rev. A. — 2013. — *88*. — С. 062328.
55. *Filippov S. N., Rybár T., Ziman M.* Local two-qubit entanglement-annihilating channels// Phys. Rev. A. — 2012. — *85*. — С. 012303.
56. *Filippov S. N., Ziman M.* Bipartite entanglement-annihilating maps: Necessary and sufficient conditions// Phys. Rev. A. — 2013. — *88*. — С. 032316.
57. *Filippov S. N., Ziman M.* Entanglement sensitivity to signal attenuation and amplification// Phys. Rev. A. — 2014. — *90*. — С. 010301(R).
58. *Freedman S. J., Clauser J. F.* Experimental test of local hidden-variable theories// Phys. Rev. Lett. — 1972. — *28*. — С. 938–941.
59. *Fröwis F., Dür W.* Stable macroscopic quantum superpositions// Phys. Rev. Lett. — 2011. — *106*. — С. 110402.
60. *Gheorghiu V., Gour G.* Multipartite entanglement evolution under separable operations// Phys. Rev. A. — 2012. — *86*. — С. 050302.
61. *Giovannetti V., Lloyd S., Maccone L.* Advances in quantum etrology// Nature Photonics. — 2011. — *5*. — С. 222.
62. *Gisin N., Bechmann-Pasquinucci H.* Bell inequality, Bell states and maximally entangled states for n qubits// Phys. Lett. A. — 1998. — *246*. — С. 1.
63. *Gour G.* Evolution and symmetry of multipartite entanglement// Phys. Rev. Lett. — 2010. — *105*. — С. 190504.
64. *Greenberger D. M., Horne M. A., Shimony A., Zeilinger A.* Bell's theorem without inequalities// Am. J. Phys. — 1990. — *58*. — С. 1131.
65. *Greenberger D. M., Horne M. A., Zeilinger A.* Going beyond Bell's theorem// in: Bell's Theorem, Quantum Theory, and Conceptions of the Universe/ Kafatos M., ed. — Dordrecht: Kluwer Academic, 1989.
66. *Grimsmo A. L., Parkins S., Skagerstam B.-S. K.* Dynamics of genuine multipartite correlations in open quantum systems// Phys. Rev. A. — 2012. — *86*. — С. 022310.
67. *Grover L. K.* Quantum mechanics helps in searching for a needle in a haystack// Phys. Rev. Lett. — 1997. — *79*. — С. 325.
68. *Gühne O., Lütkenhaus N.* Nonlinear entanglement witnesses// Phys. Rev. Lett. — 2006. — *96*. — С. 170502.
69. *Gühne O., Bodoky F., Blaauboer M.* Multiparticle entanglement under the influence of decoherence// Phys. Rev. A. — 2008. — *78*. — С. 060301.
70. *Gühne O., Seevinck M.* Separability criteria for genuine multiparticle entanglement// New J. Phys. — 2010. — *12*. — С. 053002.
71. *Gühne O., Tóth G., Briegel H. J.* Multipartite entanglement in spin chains// New J. Phys. — 2005. — *7*. — С. 229.
72. *Gurvits L.* Classical complexity and quantum entanglement// J. Comput. Syst. Sci. — 2004. — *69*. — С. 448–484.
73. *Ha K.-C., Kye S.-H.* Entanglement witnesses arising from exposed positive linear maps// Open Syst. Inform. Dynam. — 2011. — *18*. — С. 323.
74. *Hall W.* A new criterion for indecomposability of positive maps// J. Phys. A. Math. Gen. — 2006. — *39*. — С. 14119.
75. *Hayashi M.* Quantum Information. An Introduction. — Berlin–Heidelberg: Springer-Verlag, 2006.
76. *Hein M., Dür W., Briegel H.-J.* Entanglement properties of multipartite entangled states under the influence of decoherence// Phys. Rev. A. — 2005. — *71*. — С. 032350.
77. *Hildebrand R.* Positive partial transpose from spectra// Phys. Rev. A. — 2007. — *76*. — С. 052325.

78. *Hillery M., Bužek V., Berthiaume A.* Quantum secret sharing// Phys. Rev. A. — 1999. — *59*. — C. 1829.
79. *Hillery M., Ziman M., Bužek V., Bieliková M.* Towards quantum-based privacy and voting// Phys. Lett. A. — 2006. — *349*. — C. 75.
80. *Holevo A. S.* Quantum systems, channels, information. — Berlin: Walter de Gruyter, 2012.
81. *Horodecki M., Horodecki P., Horodecki R.* Separability of mixed states: necessary and sufficient conditions// Phys. Lett. A. — 1996. — *223*. — C. 1.
82. *Horodecki M., Horodecki P., Horodecki R.* Mixed-state entanglement and distillation: Is there a "bound" entanglement in nature?// Phys. Rev. Lett. — 1998. — *80*. — C. 5239.
83. *Horodecki P., Horodecki M., Horodecki R.* Binding entanglement channels// J. Mod. Opt. — 2000. — *47*. — C. 347.
84. *Horodecki M., Horodecki P., Horodecki R.* Separability of mixed states: necessary and sufficient conditions// Phys. Lett. A. — 2001. — *283*. — C. 1.
85. *Horodecki M., Shor P. W., Ruskai M. B.* Entanglement breaking channels// Rev. Math. Phys. — 2003. — *15*. — C. 629.
86. *Horodecki R., Horodecki P., Horodecki M., Horodecki K.* Quantum entanglement// Rev. Mod. Phys. — 2009. — *81*. — C. 865.
87. *Horodecki M., Horodecki P.* Reduction criterion of separability and limits for a class of distillation protocols// Phys. Rev. A. — 1999. — *59*. — C. 4206.
88. *Huber M., Mintert F., Gabriel A., Hiesmayr B. C.* Detection of high-dimensional genuine multipartite entanglement of mixed states// Phys. Rev. Lett. — 2010. — *104*. — C. 210501.
89. *Huber M., Perarnau-Llobet M., de Vicente J. I.* Entropy vector formalism and the structure of multidimensional entanglement in multipartite systems// Phys. Rev. A. — 2013. — *88*. — C. 042328.
90. *Huber M., Sengupta R.* Witnessing genuine multipartite entanglement with positive maps// Phys. Rev. Lett. — 2014. — *113*. — C. 100501.
91. *Jamiołkowski A.* Linear transformations which preserve trace and positive semidefiniteness of operators// Rep. Math. Phys. — 1972. — *3*. — C. 275.
92. *Jeknic-Dugić J., Dugić M., Francom A., Arsenijević M.* Quantum structures of the hydrogen atom// Open Access Lib. J. — 2014. — *1*. — C. e501.
93. *Johnston N.* Separability from spectrum for qubit–qudit states// Phys. Rev. A. — 2013. — *88*. — C. 062330.
94. *Jungnitsch B., Moroder T., Gühne O.* Taming multiparticle entanglement// Phys. Rev. Lett. — 2011. — *106*. — C. 190502.
95. *Kampermann H., Gühne O., Wilmott C., Bruß D.* Algorithm for characterizing stochastic local operations and classical communication classes of multiparticle entanglement// Phys. Rev. A. — 2012. — *86*. — C. 032307.
96. *Karlsson A., Bourennane M.* Quantum teleportation using three-particle entanglement// Phys. Rev. A. — 1998. — *58*. — C. 4394.
97. *King C.* Maximization of capacity and l_p norms for some product channels// J. Math. Phys. — 2002. — *43*. — C. 1247.
98. *King C., Ruskai M. B.* Minimal entropy of states emerging from noisy quantum channels// IEEE Trans. Inform. Theory. — 2001. — *47*. — C. 192.
99. *Knill E.* Separability from spectrum/ `http://qig.itp.uni-hannover.de/qiproblems/15` (2003).
100. *Konrad T., de Melo F., Tiersch M., Kasztelan C., Aragão A., Buchleitner A.* Evolution equation for quantum entanglement// Nature Phys. — 2008. — *4*. — C. 99.
101. *Kuś M., Życzkowski K.* Geometry of entangled states// Phys. Rev. A. — 2001. — *63*. — C. 032307.
102. *Lami L., Huber M.* Bipartite depolarizing maps// J. Math. Phys. — 2016. — *57*. — C. 092201.
103. *Lancien C., Gühne O., Sengupta R., Huber M.* Relaxations of separability in multipartite systems: Semidefinite programs, witnesses and volumes// J. Phys. A. Math. Theor. — 2015. — *48*. — C. 505302.
104. *Lavoie J., Kaltenbaek R., Piani M., Resch K. J.* Experimental bound entanglement in a four-photon state// Phys. Rev. Lett. — 2010. — *105*. — C. 130501.
105. *Levi F., Mintert F.* Hierarchies of multipartite entanglement// Phys. Rev. Lett. — 2013. — *110*. — C. 150402.
106. *Liu Z., Fan H.* Decay of multiqudit entanglement// Phys. Rev. A. — 2009. — *79*. — C. 064305.
107. *Lougovski P., Enk S. J. V., Choi K. S., Papp S. B., Deng H., Kimble H. J.* Verifying multipartite mode entanglement of W states// New J. Phys. — 2009. — *11*. — C. 063029.
108. *Lucas F., Mintert F., Buchleitner A.* Tailoring many-body entanglement through local control// Phys. Rev. A. — 2013. — *88*. — C. 032306.

109. *Man Z.-X., Xia Y.-J., and An N. B.* Robustness of multiqubit entanglement against local decoherence// Phys. Rev. A. — 2008. — *78*. — C. 064301.
110. *Marr C., Beige A., Rempe G.* Entangled-state preparation via dissipation-assisted adiabatic passages// Phys. Rev. A. — 2003. — *68*. — C. 033817.
111. *Miranowicz A., Piani M., Horodecki P., Horodecki R.* Inseparability criteria based on matrices of moments// Phys. Rev. A. — 2009. — *80*. — C. 052303.
112. *Moravčíková L., Ziman M.* Entanglement-annihilating and entanglement-breaking channels// J. Phys. A. Math. Theor. — 2010. — *43*. — C. 275306.
113. *Müller-Hermes A., Reeb D., Wolf M. M.* Positivity of linear maps under tensor powers// J. Math. Phys. — 2016. — *57*. — C. 015202.
114. *Nielsen M. A., Chuang I. L.* Quantum Computation and Quantum Information. — Cambridge: Cambridge Univ. Press, 2000.
115. *Novo L., Moroder T., Gühne O.* Genuine multiparticle entanglement of permutationally invariant states// Phys. Rev. A. — 2013. — *88*. — C. 012305.
116. *Palma G. M., Knight P. L.* Phase-sensitive population decay: The two-atom Dicke model in a broadband squeezed vacuum// Phys. Rev. A. — 1989. — *39*. — C. 1962.
117. *Pastawski F., Kay A., Schuch N., Cirac I.* How long can a quantum memory withstand depolarizing noise?// Phys. Rev. Lett. — 2009. — *103*. — C. 080501.
118. *Peres A.* Separability criterion for density matrices// Phys. Rev. Lett. — 1996. — *77*. — C. 1413.
119. *Plenio M. B., Virmani S.* An introduction to entanglement measures// Quantum Inform. Comput. — 2007. — *7*. — C. 1–51.
120. *Popescu S., Rohrlich D.* Thermodynamics and the measure of entanglement// Phys. Rev. A. — 1997. — *56*. — C. R3319.
121. *Ruskai M. B., Szarek S., Werner E.* An analysis of completely-positive trace-preserving maps on M_2// Linear Algebra Appl. — 2002. — *347*. — C. 159.
122. *Ruskai M. B.* Qubit entanglement breaking channels// Rev. Math. Phys. — 2003. — *15*. — C. 643.
123. *Ryu S., Lee S.-S. B., Sim H.-S.* Minimax optimization of entanglement witness operator for the quantification of three-qubit mixed-state entanglement// Phys. Rev. A. — 2012. — *86*. — C. 042324.
124. *Schrödinger E.* Discussion of probability relations between separated systems// Math. Proc. Cambridge Phil. Soc. — 1935. — *31*. — C. 555–563.
125. *Schrödinger E.* Probability relations between separated systems// Math. Proc. Cambridge Phil. Soc. — 1936. — *32*. — C. 446–452.
126. *Seevinck M., Uffink J.* Partial separability and entanglement criteria for multiqubit quantum states// Phys. Rev. A. — 2008. — *78*. — C. 032101.
127. *Shchukin E., Vogel W.* Inseparability criteria for continuous bipartite quantum states// Phys. Rev. Lett. — 2005. — *95*. — C. 230502.
128. *Shor P. W.* Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer// SIAM J. Comput. — 1997. — *26*. — C. 1484–1509.
129. *Shor P. W.* Additivity of the classical capacity of entanglement-breaking quantum channels// J. Math. Phys. — 2002. — *43*. — C. 4334.
130. *Simon R.* Peres—Horodecki separability criterion for continuous variable systems// Phys. Rev. Lett. — 2000. — *84*. — C. 2726.
131. *Simon C., Kempe J.* Robustness of multiparty entanglement// Phys. Rev. A. — 2002. — *65*. — C. 052327.
132. *Simon C. et al.* Quantum memories// Eur. Phys. J. D. — 2010. — *58*. — C. 1.
133. *Siomau M.* Entanglement dynamics of three-qubit states in local many-sided noisy channels// J. Phys. B. Atom. Molecul. Opt. Phys. — 2012. — *45*. — C. 035501.
134. *Skowronek Ł., Størmer E., Życzkowski K.* Cones of positive maps and their duality relations// J. Math. Phys. — 2009. — *50*. — C. 062106.
135. *Smolin J. A.* Four-party unlockable bound entangled state// Phys. Rev. A. — 2001. — *63*. — C. 032306.
136. *Sørensen A. S., Mølmer K.* Entanglement and extreme spin squeezing// Phys. Rev. Lett. — 2001. — *86*. — C. 4431.
137. *Sperling J., Vogel W.* The Schmidt number as a universal entanglement measure// Physica Scripta. — 2011. — *83*. — C. 045002.
138. *Stinespring W. F.* Positive functions on C^*-algebras// Proc. Am. Math. Soc. — 1955. — *6*. — C. 211.
139. *Størmer E.* Tensor powers of 2-positive maps// J. Math. Phys. — 2010. — *51*. — C. 102203.
140. *Tan S. M., Walls D. F., Collett M. J.* Nonlocality of a single photon// Phys. Rev. Lett. — 1991. — *66*. — C. 252.

141. *Terhal B. M.* A family of indecomposable positive linear maps based on entangled quantum states// Linear Algebra Appl. — 2001. — *323*. — С. 61.
142. *Terra Cunha M. O., Dunningham J. A., Vedral V.* Entanglement in single particle systems// Proc. Roy. Soc. A. — 2007. — *463*. — С. 2277.
143. *Tiersch M., de Melo F., Buchleitner A.* Entanglement evolution in finite dimensions// Phys. Rev. Lett. — 2008. — *101*. — С. 170502.
144. *Tóth G., Moroder T., Gühne O.* Evaluating convex roof entanglement measures// Phys. Rev. Lett. — 2015. — *114*. — С. 160501.
145. *Vedral V., Plenio M. B., Rippin M. A., Knight P. L.* Quantifying entanglement// Phys. Rev. Lett. — 1997. — *78*. — С. 2275.
146. *Vedral V., Plenio M. B.* Entanglement measures and purification procedures// Phys. Rev. A. — 1998. — *57*. — С. 1619–1633.
147. *Verstraete F., Audenaert K., Moor B. D.* Maximally entangled mixed states of two qubits// Phys. Rev. A. — 2001. — *64*. — С. 012316.
148. *Vidal G., Werner R. F.* Computable measure of entanglement// Phys. Rev. A. — 2002. — *65*. — С. 032314.
149. *Wei T.-C., Goldbart P. M.* Geometric measure of entanglement and applications to bipartite and multipartite quantum states// Phys. Rev. A. — 2003. — *68*. — С. 042307.
150. *Weinstein Y. S.* Tripartite entanglement witnesses and entanglement sudden death// Phys. Rev. A. — 2009. — *79*. — С. 012318.
151. *Werner R. F.* Quantum states with Einstein—Podolsky—Rosen correlations admitting a hidden-variable model// Phys. Rev. A. — 1989. — *40*. — С. 4277.
152. *Wootters W. K.* Entanglement of formation of an arbitrary state of two qubits// Phys. Rev. Lett. — 1998. — *80*. — С. 2245.
153. *Zanardi P., Lidar D. A., Lloyd S.* Quantum tensor product structures are observable induced// Phys. Rev. Lett. — 2004. — *92*. — С. 060402.
154. *Zhang H., Luo J., Ren T.-T., Sun X.-P.* Testing evolution equation for entanglement of two-qubit systems in noisy channels on ensemble quantum computers// Chinese Phys. Lett. — 2010.— *27*. — С. 090303.
155. *Ziman M., Bužek V.* Open system dynamics of simple collision models// in: Quantum Dynamics and Information/ Olkiewicz R. et al., eds. — Singapore: World Scientific, 2011. — С. 199–227.
156. *Życzkowski K., Horodecki P., Sanpera A., Lewenstein M.* Volume of the set of separable states// Phys. Rev. A. — 1998. — *58*. — С. 883.

С. Н. Филиппов
Московский физико-технический институт
E-mail: sergey.filippov@phystech.edu

ИТОГИ НАУКИ И ТЕХНИКИ.
Современная математика и ее приложения.
Тематические обзоры.
Том 138 (2017). С. 125–131

УДК 519.248.3

ОЦЕНКИ СНИЗУ РАССТОЯНИЙ ОТ ЗАДАННОГО КВАНТОВОГО КАНАЛА ДО НЕКОТОРЫХ КЛАССОВ КВАНТОВЫХ КАНАЛОВ

© 2017 г. **М. Е. ШИРОКОВ, А. В. БУЛИНСКИЙ**

Аннотация. Получены ε-точные оценки снизу расстояний от заданного квантового канала до множеств деградируемых, антидеградируемых и разрушающих сцепленность каналов с помощью оценок вариации квантовой взаимной информации и относительной энтропии сцепленности. В качестве вспомогательного результата получены ε-точные оценки снизу расстояния от заданного двухчастичного состояния до множества всех сепарабельных состояний.

***Ключевые слова*:** квантовое состояние, квантовый канал, когерентная информация, сепарабельные состояния, относительная энтропия сцепленности.

***AMS Subject Classification*:** 81P45, 94A40

1. Введение и основные понятия. Оценки вариации энтропийных характеристик квантовых состояний и каналов обычно используются при исследовании вопросов, в которых важна равномерная непрерывность этих характеристик. Достаточно заметить, что хорошо известные оценки Фаннеса для вариации энтропии фон Неймана и Алиски—Фаннеса для вариации квантовой условной энтропии играют существенную роль в доказательствах многих результатов квантовой теории информации (см. [1, 4, 6, 7, 13]).

В данной статье показано, что оценки вариации можно также использовать для получения оценок снизу расстояния от заданного квантового состояния (канала) до определенного класса состояний (каналов). Иначе говоря, оценки вариации позволяют оценить размер окрестности заданного состояния (канала), не содержащей состояний (каналов) определенного типа. Именно в этом «нестандартном» применении оценок вариации точность этих оценок играет центральную роль.

Пусть $\mathcal{H}$ — конечномерное гильбертово пространство, $\mathfrak{B}(\mathcal{H})$ и $\mathfrak{T}(\mathcal{H})$ — пространства всех линейных операторов в $\mathcal{H}$ с операторной нормой $\|\cdot\|$ и со следовой нормой $\|\cdot\|_1 = \operatorname{Tr}|\cdot|$ соответственно. Обозначим через $\mathfrak{T}_+(\mathcal{H})$ конус положительных операторов в $\mathfrak{T}(\mathcal{H})$, а через $\mathfrak{S}(\mathcal{H})$ — выпуклое множество операторов плотности, т.е. операторов из $\mathfrak{T}_+(\mathcal{H})$ с единичным следом, описывающих *квантовые состояния* (см. [6, 13]).

Пусть $I_{\mathcal{H}}$ — единичный оператор в гильбертовом пространстве $\mathcal{H}$, а $\mathrm{Id}_{\mathcal{H}}$ — тождественное преобразование банахова пространства $\mathfrak{T}(\mathcal{H})$.

Энтропия *фон Неймана* квантового состояния $\rho \in \mathfrak{S}(\mathcal{H})$, определяемая формулой $H(\rho) = \operatorname{Tr}\eta(\rho)$, в которой $\eta(x) = -x\log x$ при $x > 0$ и $\eta(0) = 0$, является неотрицательной вогнутой непрерывной функцией на множестве $\mathfrak{S}(\mathcal{H})$ (см. [9, 6, 13]). В статье будем также использовать бинарную энтропию $h_2(x) = \eta(x) + \eta(1-x)$.

Квантовая относительная энтропия состояний ρ и σ из $\mathfrak{T}_+(\mathcal{H})$ определяется выражением (см. [9])

$$H(\rho\|\sigma) = \sum_{i=1}^{+\infty}\langle i|\rho\log\rho - \rho\log\sigma|i\rangle,$$

Работа М. Е. Широкова выполнена при поддержке Российского научного фонда (проект № 14-21-00162) в Математическом институте им. В. А. Стеклова РАН..

в котором $\{|i\rangle\}_{i=1}^{+\infty}$ — ортонормированный базис из собственных векторов состояния ρ, если $\operatorname{supp}\rho \subseteq \operatorname{supp}\sigma$ и $H(\rho\|\sigma) = +\infty$ в противном случае.[1]

Если квантовые системы A и B описываются гильбертовыми пространствами $\mathcal{H}_A$ и $\mathcal{H}_B$, то составная система AB описывается тензорным произведением пространств $\mathcal{H}_{AB} \doteq \mathcal{H}_A \otimes \mathcal{H}_B$. Если ω_{AB} — состояние из $\mathfrak{S}(\mathcal{H}_{AB})$, то его частичные состояния суть $\omega_A = \operatorname{Tr}_B \omega_{AB}$ и $\omega_B = \operatorname{Tr}_A \omega_{AB}$, где Tr_B — частичный след по $\mathcal{H}_B$ (и аналогично для A).

Квантовая взаимная информация составной квантовой системы в состоянии ω_{AB} определяется выражениями (см. [8])

$$I(A{:}B)_\omega = H(\omega_{AB}\|\omega_A \otimes \omega_B) = H(\omega_A) + H(\omega_B) - H(\omega_{AB}).$$

С помощью метода Алиски—Фаннеса (оптимизированного Винтером в [14]) в [11] показано, что

$$|I(A{:}B)_\rho - I(A{:}B)_\sigma| \leqslant 2\varepsilon \log d + 2g(\varepsilon) \tag{1}$$

для любых состояний ρ и σ из $\mathfrak{S}(\mathcal{H}_{AB})$, где

$$\varepsilon = \frac{1}{2}\|\rho - \sigma\|_1, \quad d \doteq \min\{\dim \mathcal{H}_A, \dim \mathcal{H}_B\}, \quad g(\varepsilon) \doteq (1+\varepsilon) h_2\left(\frac{\varepsilon}{1+\varepsilon}\right).$$

Оценка (1) является ε-точной (при больших d).

2. Об «обратном» использовании оценок вариации. Следующая лемма показывает, как оценки вариации различных характеристик квантовых состояний (каналов) могут быть использованы для получения оценок снизу расстояния между квантовыми состояниями (каналами), а также расстояния от заданного состояния (канала) до определенного класса состояний (каналов).

Лемма 1.

(A) *Пусть X — множество с метрикой*[2] *D и F — такая функция на X, такая что*

$$|F(x_1) - F(x_2)| \leqslant A\varepsilon + r(\varepsilon), \quad \varepsilon = D(x_1, x_2)$$

для всех $x_1, x_2 \in X$, где $A > 0$ и r — такая неубывающая функция на $\mathbb{R}_+$, что $r(0) = 0$. Тогда

$$D(x_1, x_2) \geqslant A^{-1}\left(\Delta - r(A^{-1}\Delta)\right), \quad \Delta = |F(x_1) - F(x_2)|.$$

(B) *Если $F(x) \leqslant 0$ для всех $x \in X_0 \subset X$ и $F(x_*) > 0$ для некоторого $x_* \in X$, то*

$$\inf_{x \in X_0} D(x_*, x) \geqslant A^{-1}\left(G - r(A^{-1}G)\right)$$

для всех положительных $G \leqslant F(x_*)$.

Доказательство. (A) Поскольку $h(\varepsilon) \doteq \varepsilon + A^{-1}r(\varepsilon)$ — такая возрастающая неотрицательная функция, что $h(0) = 0$, имеем

$$\varepsilon \geqslant h^{-1}(A^{-1}\Delta) \geqslant A^{-1}\Delta - A^{-1}r(A^{-1}\Delta),$$

где h^{-1} — обратная функция к функции h, а последнее неравенство следует из монотонности r:

$$h^{-1}(t) \geqslant t - A^{-1}r(t) \quad \Leftrightarrow \quad t \geqslant h(t - A^{-1}r(t)) = t - A^{-1}r(t) + A^{-1}r(t - A^{-1}r(t)),$$

где $t = A^{-1}\Delta$ (мы можем считать, что $r(x) = 0$, если $x < 0$).

(B) Это утверждение следует из приведенного выше рассуждения, поскольку для любого $x \in X_0$ имеем

$$G \leqslant F(x_*) \leqslant A\varepsilon + r(\varepsilon), \quad \varepsilon = D(x_*, x).$$

□

[1] Здесь и далее в статье используются дираковские обозначения, см., например, [6], в которых ортонормированный набор векторов традиционно обозначается $\{|i\rangle\}_{i\in I}$, где $I = \{1, 2, \ldots, n\}$ или $I = \mathbb{N}$.

[2] Утверждения леммы имеют место для любой неотрицательной функции D на $X \times X$.

3. Оценки снизу расстояния от заданного двухчастичного состояния до множества всех сепарабельных состояний. Пусть ρ_{AB} — произвольное состояние из $\mathfrak{S}(\mathcal{H}_{AB})$. В силу второй части леммы 1 оценку снизу расстояния от состояния ρ_{AB} до множества $\mathfrak{S}_{\mathrm{s}}(\mathcal{H}_{AB})$ всех сепарабельных состояний из $\mathfrak{S}(\mathcal{H}_{AB})$, т.е. величины

$$D_{\mathrm{s}}(\rho_{AB}) = \inf_{\sigma\in\mathfrak{S}_{\mathrm{s}}(\mathcal{H}_{AB})} \|\rho-\sigma\|_1,$$

можно получить, используя оценки вариации любого индикатора сцепленности на $\mathfrak{S}(\mathcal{H}_{AB})$, т.е. такой неотрицательной функции E на $\mathfrak{S}(\mathcal{H}_{AB})$, что $E^{-1}(0) = \mathfrak{S}_{\mathrm{s}}(\mathcal{H}_{AB})$ (при условии, что эта оценка имеет вид, рассмотренный в лемме 1). В частности, можно использовать любую асимптотически непрерывную меру сцепленности E на $\mathfrak{S}(\mathcal{H}_{AB})$ (см. [10]).

Выбор конкретной функции E для данной задачи определяется следующими требованиями:

(i) существование достаточно точной оценки вариации функции E;
(ii) возможность вычисления $E(\rho_{AB})$ для произвольного состояния ρ_{AB} или наличие вычислимой оценки снизу для $E(\rho_{AB})$.

Первое требование обусловлено стремлением получить достаточно точную оценку снизу для $D_{\mathrm{s}}(\rho_{AB})$, второе — необходимостью иметь вычислимую оценку.

Среди общеизвестных мер сцепленности на $\mathfrak{S}(\mathcal{H}_{AB})$ оптимальным представляется выбор в качестве функции E *относительной энтропии сцепленности* E_R, которая определяется для любого состояния ρ из $\mathfrak{S}(\mathcal{H}_{AB})$ следующим выражением (см. [12, 10]):

$$E_R(\rho) = \inf_{\sigma\in\mathfrak{S}_{\mathrm{s}}(\mathcal{H}_{AB})} H(\rho\|\sigma). \tag{2}$$

Недавно Винтер получил в [14] следующую ε-точную оценку вариации величины E_R:

$$|E_R(\rho) - E_R(\sigma)| \leqslant \varepsilon\log d + g(\varepsilon) \tag{3}$$

для любых состояний ρ и σ из $\mathfrak{S}(\mathcal{H}_{AB})$, где

$$d = \min\{\dim\mathcal{H}_A, \dim\mathcal{H}_B\}, \quad \varepsilon = \frac{1}{2}\|\rho-\sigma\|_1, \quad g(\varepsilon) = (1+\varepsilon)h_2\left(\frac{\varepsilon}{1+\varepsilon}\right).$$

Эта оценка существенно уточняет оценку вариации величины E_R, полученную в [3].

Подобно всем мерам сцепленности относительная энтропии сцепленности трудновычислима для произвольного состояния $\rho\in\mathfrak{S}(\mathcal{H}_{AB})$, однако, она имеет легко вычислимую оценку снизу (см. [10]):

$$E_R(\rho) \geqslant I_c(\rho) \doteq \max\left\{I(A\rangle B)_\rho,\ I(B\rangle A)_\rho\right\} = \max_{X=A,B} H(\rho_X) - H(\rho), \tag{4}$$

где $I(X\rangle Y)_\rho \doteq -H(X|Y)_\rho$ — когерентная информация состояния ρ.

Применяя лемму 1 к функции $F = E_R$ и используя (3) и (4), получаем следующее предложение.

Предложение 1 (А. В. Булинский)**.** *Пусть ρ — любое состояние из $\mathfrak{S}(\mathcal{H}_{AB})$. Тогда*

$$D_{\mathrm{s}}(\rho) \geqslant 2\frac{E_R(\rho)}{\log d} - \frac{2}{\log d}g\left(\frac{E_R(\rho)}{\log d}\right), \tag{5}$$

где

$$d = \min\left\{\dim\mathcal{H}_A, \dim\mathcal{H}_B\right\}, \quad g(\varepsilon) = (1+\varepsilon)h_2\left(\frac{\varepsilon}{1+\varepsilon}\right).$$

Если $I_c(\rho) > 0$, где $I_c(\rho)$ определено формулой (4)*, то*

$$D_{\mathrm{s}}(\rho) \geqslant 2\frac{I_c(\rho)}{\log d} - \frac{2}{\log d}g\left(\frac{I_c(\rho)}{\log d}\right). \tag{6}$$

Если $\mathcal{H}_A = \mathcal{H}_B$ и ρ — максимально сцепленное чистое состояние из $\mathfrak{S}(\mathcal{H}_{AB})$, то $E_R(\rho) = I_c(\rho) = \log d$ и, следовательно, (5) и (6) дают одну и ту же оценку

$$D_{\mathrm{s}}(\rho) \geqslant 2 - \frac{2g(1)}{\log d} = 2 - \frac{4\log 2}{\log d}, \tag{7}$$

которая дает альтернативное доказательство известного факта, что $D_{\mathrm{s}}(\rho)$ близко 2 при больших d (см. [15]). Заметим также, что неравенство (7) показывает, что обе оценки (5) и (6) асимптотически точны.

Применяя лемму 1 к оценке вариации (1) и к ее обобщению на квантовую условную взаимную информацию (см. [11, следствие 1]) можно получить оценки снизу для

(i) $\|\cdot\|_1$-расстояния от заданного двухчастичного состояния ρ_{AB} до множества всех состояний-произведений (т.е. состояний вида $\sigma_A \otimes \sigma_B$);

(ii) $\|\cdot\|_1$-расстояния от заданного трехчастичного состояния ρ_{ABC} до множества всех коротких марковских цепей (т.е. таких состояний σ_{ABC}, что $\sigma_{ABC} = \mathrm{Id}_A \otimes \Phi(\sigma_{AB})$ для некоторого канала $\Phi : B \to BC$; см. [5]).

4. Оценки снизу расстояний от заданного канала до множеств деградируемых, антидеградируемых и разрушающих сцепленность каналов. *Квантовый канал* Φ из системы A в систему B — это вполне положительное сохраняющее след линейное отображение $\mathfrak{T}(\mathcal{H}_A) \to \mathfrak{T}(\mathcal{H}_B)$, где $\mathcal{H}_A$ и $\mathcal{H}_B$ — гильбертовы пространства, ассоциированные с системами A и B (см. [6, 13]). Для краткости будем писать $\Phi : A \to B$.

Множество $\mathfrak{F}(A, B)$ всех квантовых каналов из системы A в систему B обычно снабжается метрикой, порожденной нормой полной ограниченности

$$\|\Phi\|_\diamond \doteq \sup_{\rho \in \mathfrak{T}(\mathcal{H}_{AR}), \|\rho\|_1 = 1} \|\Phi \otimes \mathrm{Id}_R(\rho)\|_1 \tag{8}$$

на множестве всех вполне ограниченных отображений из $\mathfrak{T}(\mathcal{H}_A)$ в $\mathfrak{T}(\mathcal{H}_B)$.[1]

Для любого квантового канала $\Phi : A \to B$ теорема Стайнспринга гарантирует существование таких гильбертова пространства $\mathcal{H}_E$ (окружения) и изометрии $V : \mathcal{H}_A \to \mathcal{H}_B \otimes \mathcal{H}_E$, что

$$\Phi(\rho) = \mathrm{Tr}_E\, V \rho V^*, \quad \rho \in \mathfrak{T}(\mathcal{H}_A). \tag{9}$$

Квантовый канал $\widehat{\Phi} : A \to E$, определяемый выражением

$$\widehat{\Phi}(\rho) = \mathrm{Tr}_B\, V \rho V^*, \tag{10}$$

называется *комплементарным* к каналу Φ (см. [6, гл. 6].

Канал $\Phi : A \to B$ называется *деградируемым*, если $\widehat{\Phi} = \Theta \circ \Phi$ для некоторого канала $\Theta : B \to E$. Канал $\Phi : A \to B$ называется *антидеградируемым*, если $\widehat{\Phi}$ — деградируемый канал (см. [2]). Обозначим через $\mathfrak{F}_d(A, B)$ и $\mathfrak{F}_a(A, B)$ множества всех деградируемых и антидеградируемых каналов между системами A и B соответственно. Эти множества имеют непустое пересечение: например, стирающий канал

$$\Phi_p(\rho) = \begin{bmatrix} (1-p)\rho & 0 \\ 0 & p\,\mathrm{Tr}\,\rho \end{bmatrix}, \quad p \in [0, 1], \tag{11}$$

из d-мерной системы A в $(d+1)$-мерную систему B является одновременно деградируемым и антидеградируемым при $p = 1/2$.

Множество $\mathfrak{F}_a(A, B)$ содержит важное подмножество $\mathfrak{F}_{eb}(A, B)$ каналов, *разрушающих сцепленность*, т.е. таких каналов $\Phi : A \to B$, что $\Phi \otimes \mathrm{Id}_R(\omega_{AR})$ — сепарабельное состояние из $\mathfrak{S}(\mathcal{H}_{BR})$ для любого состояния ω_{AR}, где R — произвольная квантовая система (см. [2]).

Важное свойство любого деградируемого (соответственно, антидеградируемого) канала Φ состоит в неотрицательности (соответственно, неположительности) когерентной информации

$$I_{\mathrm{c}}(\Phi, \rho) = H(\Phi(\rho)) - H(\widehat{\Phi}(\rho))$$

для любого входного состояния ρ (см. [6, 13]). Замечая, что

$$I_{\mathrm{c}}(\Phi, \rho) = I(B\!:\!R)_{\Phi \otimes \mathrm{Id}_R(\hat{\rho})} - H(\rho),$$

[1] Строго говоря, норма (8) совпадает с нормой полной ограниченности дуального отображения $\Phi^* : \mathfrak{B}(\mathcal{H}_B) \to \mathfrak{B}(\mathcal{H}_A)$ к отображению Φ (см. [6, 7, 13]).

где $\mathcal{H}_R \cong \mathcal{H}_A$, а $\hat{\rho}$ — такое чистое состояние из $\mathfrak{S}(\mathcal{H}_{AR})$, что $\hat{\rho}_A = \rho$, нетрудно получить из (1) следующую оценку вариации когерентной информации как функции канала:

$$|I_{\mathrm{c}}(\Phi,\rho) - I_{\mathrm{c}}(\Psi,\rho)| \leqslant 2\varepsilon \log d + 2g(\varepsilon), \tag{12}$$

где Φ и Ψ — любые квантовые каналы из A в B,

$$\varepsilon = \frac{1}{2}\|\Phi - \Psi\|_\diamond, \quad d = \min\{\dim \mathcal{H}_A, \dim \mathcal{H}_B\}, \quad g(\varepsilon) = (1+\varepsilon)h_2\left(\frac{\varepsilon}{1+\varepsilon}\right).$$

Следующее предложение содержит оценки снизу для величин

$$D_d(\Phi) \doteq \inf_{\Psi\in\mathfrak{F}_d(A,B)} \|\Phi - \Psi\|_\diamond, \quad D_a(\Phi) \doteq \inf_{\Psi\in\mathfrak{F}_a(A,B)} \|\Phi - \Psi\|_\diamond, \quad D_{eb}(\Phi) \doteq \inf_{\Psi\in\mathfrak{F}_{eb}(A,B)} \|\Phi - \Psi\|_\diamond,$$

которые определяют радиусы наибольших открытых окрестностей канала Φ, не содержащих, соответственно, деградируемых, антидеградируемых и разрушающих сцепленность каналов.

Предложение 2 (М. Е. Широков)**.** *Пусть $\Phi : A \to B$ — квантовый канал,*

$$d = \min\{\dim \mathcal{H}_A, \dim \mathcal{H}_B\}, \quad g(\varepsilon) = (1+\varepsilon)h_2\left(\frac{\varepsilon}{1+\varepsilon}\right).$$

(A) *Если существует такое входное состояние ρ, что*

$$I_{\mathrm{c}}(\Phi,\rho) > 0,$$

то

$$D_a(\Phi) \geqslant \frac{I_{\mathrm{c}}(\Phi,\rho)}{\log d} - \frac{2}{\log d} g\left(\frac{I_{\mathrm{c}}(\Phi,\rho)}{2\log d}\right), \tag{13}$$

$$D_{eb}(\Phi) \geqslant 2\frac{I_{\mathrm{c}}(\Phi,\rho)}{\log d} - \frac{2}{\log d} g\left(\frac{I_{\mathrm{c}}(\Phi,\rho)}{\log d}\right). \tag{14}$$

(B) *Если существует такое входное состояние ρ, что*

$$L(\Phi,\rho) \doteq H(\rho) - H(\widehat{\Phi}(\rho)) > 0,$$

то

$$D_{eb}(\Phi) \geqslant 2\frac{L(\Phi,\rho)}{\log d} - \frac{2}{\log d} g\left(\frac{L(\Phi,\rho)}{\log d}\right). \tag{15}$$

(C) *Если $R \cong A$ и ω — любое состояние из $\mathfrak{S}(\mathcal{H}_{AR})$, то*

$$D_{eb}(\Phi) \geqslant 2\frac{E_R(\Phi\otimes \mathrm{Id}_R(\omega))}{\log d} - \frac{2}{\log d} g\left(\frac{E_R(\Phi\otimes \mathrm{Id}_R(\omega))}{\log d}\right), \tag{16}$$

где E_R — относительная энтропия сцепленности в $\mathfrak{S}(\mathcal{H}_{BR})$.

(D) *Если существует такое входное состояние ρ, что*

$$I_{\mathrm{c}}(\Phi,\rho) < 0,$$

то

$$D_d(\Phi) \geqslant \frac{-I_{\mathrm{c}}(\Phi,\rho)}{\log d} - \frac{2}{\log d} g\left(\frac{-I_{\mathrm{c}}(\Phi,\rho)}{2\log d}\right). \tag{17}$$

Неравенства (13)–(17) *являются ε-точными оценками в том смысле, что для каждого из этих неравенств и любого $\varepsilon > 0$ существуют канал Φ и состояние ρ, такие что разность между правой и левой частями неравенства меньше ε.*

Замечание 1. Оценки (14) и (15) являются вычислимыми, их можно считать ослабленными вариантами оценки (16), трудновычислимой в общем случае (см. приведенный ниже пример 2, в котором все эти оценки явно вычисляются).

Доказательство. Неравенства (13) и (17) получаются применением второй части леммы 1 к оценке вариации (12).

Для доказательства неравенств (14)–(16) заметим, что

$$D_{eb}(\Phi) \geqslant \sup_{\omega_{AR}} D_{\mathrm{s}}(\Phi \otimes \mathrm{Id}_R(\omega_{AR})),$$

где супремум берется по всем состояниям из $\mathfrak{S}(\mathcal{H}_{AR})$, а $D_{\mathrm{s}}(\rho_{BR})$ — расстояние от состояния ρ_{BR} до множества всех сепарабельных состояний в $\mathfrak{S}(\mathcal{H}_{BR})$ (см. п. 2). В силу стандартных аргументов, основанных на свойстве выпуклости, данный супремум можно брать только по чистым состояниям ω_{AR}. Таким образом, оценки (14)–(16) следуют из предложения 1, поскольку легко видеть, что

$$I(R\rangle B)_{\Phi\otimes\mathrm{Id}_R(\omega_{AR})} = I_{\mathrm{c}}(\Phi,\omega_A), \quad I(B\rangle R)_{\Phi\otimes\mathrm{Id}_R(\omega_{AR})} = L(\Phi,\omega_A)$$

для любого чистого состояния ω_{AR}.

ε-Точность оценок (13) и (17) можно показать, используя семейство стирающих каналов (11). Известно, что канал Φ_{p} является деградируемым, если $p \leqslant 1/2$, и антидеградируемым, если $p \geqslant 1/2$, и что $I_{\mathrm{c}}(\Phi,\rho) = (1-2p)H(\rho)$ для всех $p \in [0,1]$ (см. [6, гл. 10]). Поэтому, если $\Phi = \Phi_{1/2-x}$, а ρ — хаотическое состояние, то правая часть (13) равна

$$2x - \frac{2g(x)}{\log d} \quad \text{при условии, что} \quad D_a(\Phi_{1/2-x}) \leqslant \|\Phi_{1/2-x} - \Phi_{1/2}\|_\diamond = 2x. \tag{18}$$

ε-Точность оценки (17) доказывается аналогично с использованием канала $\Phi_{1/2+x}$. □

Приведенный ниже пример 1 показывает ε-точность оценок (14)–(16).

Пример 1. Если $\dim\mathcal{H}_A \leqslant \dim\mathcal{H}_B$, $\Phi = \mathrm{Id}_A$ — тождественное вложение множества $\mathfrak{S}(\mathcal{H}_A)$ в $\mathfrak{S}(\mathcal{H}_B)$, а ρ — хаотическое состояние в $\mathfrak{S}(\mathcal{H}_A)$, то из неравенства (13) следует, что

$$D_a(\mathrm{Id}_A) \geqslant 1 - \frac{2g(1/2)}{\log d_A} \approx 1 - \frac{1{,}9}{\log d_A},$$

где $d_A = \dim\mathcal{H}_A$, в то время как все неравенства (14)–(16) дают одну и ту же оценку

$$D_{eb}(\mathrm{Id}_A) \geqslant 2 - \frac{2g(1)}{\log d_A} \approx 2 - \frac{2.8}{\log d_A}.$$

Таким образом, радиус открытого шара с центром в Id_A, не содержащего антидеградируемых (соответственно, разрушающих сцепленность) каналов близок к 1 (соответственно, к 2) при больших размерностях d_A. С другой стороны, из (18) при $x = 1/2$ и определения нормы полной ограниченности (8) следует, что

$$D_a(\mathrm{Id}_A) \leqslant 1, \quad D_{eb}(\mathrm{Id}_A) \leqslant 2.$$

при любой размерности d_A.

Пример 2. Если Φ_p — стирающий канал (11), то нетрудно видеть, что

$$I_{\mathrm{c}}(\Phi_p,\rho) = (1-2p)H(\rho), \quad L(\Phi_p,\rho) = (1-p)H(\rho) - h_2(p),$$

где h_2 — бинарная энтропия (см. [6, гл. 6]). Поэтому из неравенств (14) и (15) с хаотическим состоянием ρ следует, соответственно, что

$$D_{eb}(\Phi_p) \geqslant 2(1-2p) - \frac{2}{\log d_A} g(1-p),$$

$$D_{eb}(\Phi_p) \geqslant 2(1-p) - \frac{2}{\log d_A}\left(h_2(p) + g\left((1-p) - \frac{h_2(p)}{\log d_A}\right)\right),$$

где предполагается, что $g(x) = 0$ при $x < 0$.

Поскольку

$$\Phi_p \otimes \mathrm{Id}_R(\omega) = (1-p)\omega \oplus p|\varphi\rangle\langle\varphi| \otimes \mathrm{Tr}_A\,\omega,$$

где φ — единичный вектор в $\mathcal{H}_B \ominus \mathcal{H}_A$, то используя основные свойства относительной энтропия и выпуклость E_R, можно показать, что

$$E_R(\Phi_p \otimes \mathrm{Id}_R(\omega)) = (1-p)E_R(\omega).$$

Поэтому из неравенства (16) с максимально сцепленным чистым состоянием ω следует, что

$$D_{eb}(\Phi_p) \geqslant 2(1-p) - \frac{2}{\log d_A} g(1-p).$$

Поскольку

$$D_{eb}(\Phi_p) \leqslant \|\Phi_p - \Phi_1\|_\diamond = 2(1-p),$$

мы видим, что неравенства (15) и (16) дают ε-точные оценки величины $D_{eb}(\Phi_p)$ при большой размерности d_A (в отличие от неравенства (14)). Мы также видим, что неравенство (16) дает наиболее точную оценку $D_{eb}(\Phi_p)$ при всех p (как и ожидалось). К сожалению, применимость этой оценки к произвольному каналу Φ ограничена трудностью вычисления E_R.

СПИСОК ЛИТЕРАТУРЫ

1. *Alicki R., Fannes M.* Continuity of quantum conditional information// J. Phys. A: Math. Gen. — 2004. *37*, № 5. — C. L55–L57.
2. *Cubitt T. S., Ruskai M. B., Smith G.* The structure of degradable quantum channels// J. Math. Phys. — 2008. — *49*. — C. 102104.
3. *Donald M. J., Horodecki M.* Continuity of the relative entropy of entanglement// Phys. Lett. A. — 1999. — *264*. — C. 257–260.
4. *Fannes M.* A continuity property of the entropy density for spin lattice systems// Commun. Math. Phys. — 1973. — *31*. — C. 291–294.
5. *Hayden P., Jozsa R., Petz D., Winter A.* Structure of states which satisfy strong subadditivity of quantum entropy with equality// Commun. Math. Phys. — 2004. — *246*, № 2. — C. 359–374; `arXiv:quant-ph/0304007`
6. *Holevo A. S.* Quantum Systems, Channels, Information. A Mathematical Introduction. — Berlin: DeGruyter, 2012.
7. *Leung D., Smith G.* Continuity of quantum channel capacities// Commun. Math. Phys. — 2009. — *292*. — C. 201–215.
8. *Lindblad G.* Entropy, information and quantum measurements// Commun. Math. Phys. — 1973. — *33*.— C. 305–322.
9. *Lindblad G.* Expectation and entropy inequalities for finite quantum systems// Commun. Math. Phys. — 1974. — *39*, № 2. — C. 111–119.
10. *Plenio M. B., Virmani S.* An introduction to entanglement measures// Quantum Inf. Comput. — 2007. — *7*. — C. 1–51.
11. *Shirokov M. E.* Tight continuity bounds for the quantum conditional mutual information, for the Holevo quantity and for capacities of a channel/ `arXiv:1512.09047`
12. *Vedral V., Plenio M. B.* Entanglement measures and purification procedures// Phys. Rev. A. — 1998. — *57*. — C. 1619–1633.
13. *Wilde M. M.* From classical to quantum Shannon theory/ `arXiv:1106.1445`
14. *Winter A.* Tight uniform continuity bounds for quantum entropies: conditional entropy, relative entropy distance and energy constraints// Commun. Math. Phys. — 2016. — *347*, № 1. — 291–313.
15. *Winter A.* Private communication.

М. Е. Широков
Математический институт им. В. А. Стеклова РАН, Москва
E-mail: `msh@mi.ras.ru`

А. В. Булинский
Московский физико-технический институт
E-mail: `andrey.bulinski@yandex.ru`