

ISSN 0233-6723



ИТОГИ НАУКИ И ТЕХНИКИ

СОВРЕМЕННАЯ
МАТЕМАТИКА
И ЕЕ ПРИЛОЖЕНИЯ

Тематические
обзоры

Том 151



Москва 2018

РЕДАКЦИОННАЯ КОЛЛЕГИЯ

Главный редактор:

Р. В. Гамкрелидзе (Математический институт им. В. А. Стеклова РАН)

Заместители главного редактора:

А. В. Овчинников (МГУ им. М. В. Ломоносова, ВИНТИ РАН)

В. Л. Попов (Математический институт им. В. А. Стеклова РАН)

Члены редколлегии:

А. А. Аграчёв (Математический институт им. В. А. Стеклова РАН, SISSA)

С. С. Акбаров (ВИНТИ РАН)

Е. С. Голод (МГУ им. М. В. Ломоносова)

А. Б. Жижченко (Отделение математических наук РАН)

Е. П. Кругова (ВИНТИ РАН)

А. В. Михалёв (МГУ им. М. В. Ломоносова)

Н. Х. Розов (МГУ им. М. В. Ломоносова)

С. Е. Степанов (Финуниверситет при Правительстве РФ, ВИНТИ РАН)

М. В. Шамолин (Институт механики МГУ им. М. В. Ломоносова)

Редактор-составитель:

Г. Г. Амосов (Математический институт им. В. А. Стеклова РАН)

Научный редактор:

С. С. Акбаров (ВИНТИ РАН)

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 151

КВАНТОВАЯ ВЕРОЯТНОСТЬ



Москва 2018

СОДЕРЖАНИЕ

О различных функциональных представлениях пространства операторов Шварца (<i>Г. Г. Амосов</i>)	3
След и коммутаторы измеримых операторов, присоединенных к алгебре фон Неймана (<i>А. М. Бикчентаев</i>)	10
Применение дифференциальных операторов Леви в теории калибровочных полей (<i>Б. О. Волков</i>)	21
Аналоги меры Лебега в пространствах последовательностей и классы интегрируемых по ним функций (<i>Д. В. Завадский</i>)	37
Асимметрия локально доступной и локально передаваемой информации в термальном двухкубитном состоянии (<i>Е. О. Киктенко</i>)	45
Целевая функция в задаче оптимального лазерного разделения изотопов методом селективного торможения (<i>К. А. Ляхов, А. Н. Печень</i>)	62
Некоторые методы построения управлений для квантовых систем (<i>А. Н. Печень</i>)	67
Полугруппы преобразований пространства функций, квадратично интегрируемых по трансляционно инвариантной мере на банаховом пространстве (<i>В. Ж. Сакбаев</i>)	73
Квантовые поточные шифры: невозможность безусловной стойкости (<i>П. А. Трегубов, А. С. Трушечкин</i>)	91
Применение и исследование квантовых блужданий (<i>Л. Е. Федичкин, Ф. П. Мещанинов</i>)	105
Тензорные произведения квантовых отображений (<i>С. Н. Филиппов</i>)	117



О РАЗЛИЧНЫХ ФУНКЦИОНАЛЬНЫХ ПРЕДСТАВЛЕНИЯХ ПРОСТРАНСТВА ОПЕРАТОРОВ ШВАРЦА

© 2018 г. Г. Г. АМОСОВ

Аннотация. В работе рассматриваются различные представления, в которых пространство операторов Шварца $\mathcal{S}$ превращается в пространство основных функций, а дуальное к нему $\mathcal{S}'$ — в пространство обобщенных функций.

Ключевые слова: квантовая томография, функциональное представление, пространство операторов Шварца.

AMS Subject Classification: 81P16, 46F99

1. Введение. Как известно, идеал ядерных операторов $\mathfrak{S}_1(H)$ является сопряженным пространством для алгебры всех ограниченных операторов $B(H)$ в гильбертовом пространстве H . Если отождествить $B(H)$ с алгеброй квантовых наблюдаемых, соотношение двойственности позволяет считать наблюдаемые $A \in B(H)$ функционалами на множестве квантовых состояний $\mathfrak{S}(H)$, состоящем из положительных операторов $\rho \in \mathfrak{S}_1(H)$, нормированных условием $\text{Tr}(\rho) = 1$; действие функционала при этом определяется формулой

$$\langle A, \rho \rangle = \text{Tr}(\rho A); \quad (1)$$

здесь $A \in B(H)$, $\rho \in \mathfrak{S}(H)$. Такой подход вполне достаточен для конечномерных пространств, $\dim H < +\infty$. В бесконечномерном гильбертовом пространстве к наблюдаемым следует причислять все (даже неограниченные) самосопряженные операторы A . Чтобы сохранить дуальную структуру между состояниями и наблюдаемыми, необходимо выделить некоторое линейное подпространство $\mathcal{S} \subset \mathfrak{S}_1(H)$, и наделить его топологией с тем расчетом, что сопряженное пространство $\mathcal{S}'$ будет содержать неограниченные самосопряженные операторы хотя бы некоторого класса, причем соотношение двойственности должно превращаться в (1), если $A \in B(H)$. В недавно появившейся работе [9] было введено понятие пространства операторов Шварца $\mathcal{S}$. Было показано, что $\mathcal{S}$ имеет структуру пространства Фреше, а сопряженное с ним пространство $\mathcal{S}'$ содержит, в частности, неограниченные операторы, являющиеся полиномами от операторов координаты и импульса. Нашей задачей является рассмотрение представлений пространства операторов Шварца $\mathcal{S}$ в различных функциональных пространствах. Такие функциональные пространства будем рассматривать в качестве основных, так чтобы дуальное представление $\mathcal{S}'$ состояло из обобщенных функций над ними.

Построение функционального представления операторов напрямую связано с томографическим представлением квантовой механики. Под томографическим представлением квантовой механики мы понимаем некоторую процедуру, при которой удастся перейти от операторов состояний и наблюдаемых к функциям некоторого количества переменных. Разработка томографического представления привело к созданию следующего формализма (см. [5, 10]). В гильбертовом пространстве H вводятся множества операторов $\hat{U}(\mathbf{x})$ и $\hat{D}(\mathbf{x})$, зависящих от n -мерного вектора $\mathbf{x} = (x_1, x_2, \dots, x_n)$, таким образом, что оператору $\hat{A}$ на H ставится в соответствие функция

$$f_{\hat{A}}(\mathbf{x}) = \text{Tr}(\hat{U}(\mathbf{x})\hat{A}), \quad (2)$$

называемая его *символом*, так что оператор может быть восстановлен по своему символу по формуле

$$\hat{A} = \int \hat{D}(\mathbf{x}) f_{\hat{A}}(\mathbf{x}) d\mathbf{x}. \quad (3)$$

Семейства $\hat{U}(\mathbf{x})$ и $\hat{D}(\mathbf{x})$ получили название *деквантизатора* и *квантизатора* соответственно.

В конечномерном пространстве H (спиновая томография) такой подход может быть реализован математически безупречно (см. [6]). Этого нельзя сказать про бесконечномерный случай, когда семейства $\hat{U}(\mathbf{x})$ и $\hat{D}(\mathbf{x})$ фактически состоят не из операторов, а лишь определяют линейные формы

$$\hat{A} \rightarrow \text{Tr}(\hat{U}(\mathbf{x})\hat{A}), \quad \hat{A} \rightarrow \text{Tr}(\hat{D}(\mathbf{x})\hat{A}),$$

смысл которых необходимо математически точно объяснять. Опираясь на конструкцию из [9], мы постараемся придать различным видам томографического представления квантовой механики в бесконечномерном пространстве H точный математический смысл. Для полноты описания мы также коснемся конечномерного случая.

2. Основные обозначения. Как и выше, будем обозначать через $B(H)$ алгебру всех ограниченных операторов в гильбертовом пространстве H . Будем использовать дираковское обозначение $|\psi\rangle\langle\psi|$ для ортогонального проектора на подпространство, натянутое на единичный вектор $\psi \in H$. Будем обозначать через $S(\mathbb{R}^n)$ *пространство Шварца*, состоящее из бесконечно дифференцируемых функций, убывающих быстрее любой степени на бесконечности, с обычной для такого пространства топологией. Пусть $H = L^2(\mathbb{R})$. Пространство $S(\mathbb{R})$ плотно в области определения всех степеней операторов *координаты* $(q\psi)(x) = x\psi(x)$ и *импульса* $(p\psi)(x) = -i\frac{d\psi}{dx}(x)$.

Нам также потребуются операторы рождения $a^\dagger = \frac{q - ip}{\sqrt{2}}$ и уничтожения $a = \frac{q + ip}{\sqrt{2}}$.

Оператор $T \in B(H)$ называется *оператором Шварца* (см. [9]), если он ограничен относительно семейства полунорм

$$\|T\|_{n,m,\psi} = \|q^n p^m T\psi\|, \quad (4)$$

$n, m = 0, 1, 2, \dots$, $\psi \in S(\mathbb{R})$. Обозначим $\mathcal{S}$ *множество всех операторов Шварца*. В [9] было показано, что для того, чтобы $T \in \mathcal{S}$, необходимо и достаточно, чтобы он имел вид

$$(T\psi)(x) = \int \rho(x, y)\psi(y)dy, \quad (5)$$

где $\rho(\cdot, \cdot) \in S(\mathbb{R}^2)$. Множество $\mathcal{S}$ является пространством Фреше относительно семейства полунорм (4).

Унитарные операторы

$$W(x, y) = \exp(i(xq + yp)) \quad (6)$$

в пространстве H называются *операторами Вейля*.

Семейство функций

$$\psi_n(x) = \frac{1}{\pi^{1/4} \sqrt{2^n n!}} H_n(x) e^{-x^2/2}, \quad (7)$$

где $H_n(x)$ — полиномы Эрмита, образует ортонормированный базис в пространстве $L^2(\mathbb{R})$. Данные функции представляют из себя основное и возбужденные состояния квантового осциллятора. Отметим, что $\psi_n \in S(\mathbb{R})$. Для любого фиксированного $\alpha \in \mathbb{C}$ когерентное состояние определяется формулой

$$\psi_\alpha = e^{-|\alpha|^2/2} \sum_{n=0}^{+\infty} \frac{\psi_n}{\sqrt{n!}}. \quad (8)$$

3. Конечномерный случай. В случае $\dim H < +\infty$ деквантизатор (2) и квантизатор (3) представляют собой семейства ограниченных операторов в H . Из соотношений (2) и (3) следует, что если

$$f_\rho(\mathbf{x}) = \text{Tr}(U(\mathbf{x})\rho), \quad g_A(\mathbf{x}) = \text{Tr}(D(\mathbf{x})A) \quad (9)$$

для двух операторов $\rho, A \in B(H)$, то

$$\text{Tr}(\rho A) = \int g_A(\mathbf{x}) f_\rho(\mathbf{x}) d\mathbf{x}. \quad (10)$$

Таким образом, формулу (10) можно воспринимать как действие функционала A на элемент ρ , так что она отражает тот факт, что в конечномерном случае $B(H)^* = B(H)$.

Различные примеры деквантизаторов и квантизаторов для конечномерного случая приведены в [6, 7]. Мы не будем воспроизводить их все, ограничившись простейшим случаем $\dim H = 2$. Положим $\mathbf{x} := (m, \alpha, \beta)$, где $m = \pm 1/2$ — два возможных результата измерения величины спина по направлению, задаваемому углами Эйлера $\alpha \in [0, 2\pi]$, $\beta \in [0, \pi]$. Тогда деквантизатор и квантизатор определяются формулами

$$\begin{aligned} \hat{U}(\mathbf{x}) &= \frac{1}{2} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + m \begin{pmatrix} \cos \beta & -e^{i\alpha} \sin \beta \\ -e^{-i\alpha} \sin \beta & -\cos \beta \end{pmatrix}, \\ \hat{D}(\mathbf{x}) &= 3\hat{U}(\mathbf{x}) - \hat{I}; \end{aligned}$$

здесь нужно положить

$$\int d\mathbf{x} := \sum_{m=-1/2}^{1/2} \frac{1}{2\pi} \int_0^{2\pi} d\alpha \int_0^\pi \sin \beta d\beta.$$

4. Представление характеристическими функциями. Пусть $H = L^2(\mathbb{R})$. Положим $\mathbf{x} = (x, y)$ и определим деквантизатор с помощью оператора Вейля $U(x, y) = W(x, y)$. Тогда можно ввести символ оператора $\rho \in \mathfrak{S}_1(H)$ по формуле

$$f_\rho^W(x, y) = \text{Tr}(W(x, y)\rho). \quad (11)$$

В случае $\rho \in \mathfrak{S}(H)$ символ (11) называется *характеристической функцией* состояния ρ (см. [8]). Соответствующий квантизатор дается формулой

$$D(x, y) = \frac{1}{2\pi} W(-x, -y)$$

(см. [8]). Будем называть (11) *вейлевской характеристической функцией* оператора $\rho \in \mathfrak{S}_1(H)$.

Предложение 1. Пусть $\rho \in \mathcal{S}$. Тогда вейлевская характеристическая функция f_ρ^W принадлежит пространству Шварца $S(\mathbb{R}^2)$. Более того, если функция f принадлежит $S(\mathbb{R}^2)$, то полученный из нее с помощью квантизатора оператор T принадлежит $\mathcal{S}$.

Доказательство. Заметим, что

$$W(x, y) = e^{-\frac{i}{2}xy} V_x U_y,$$

где

$$(V_x \psi)(z) = e^{ixz} \psi(z), \quad (U_y \psi)(z) = \psi(z + y),$$

$\psi \in H$. Поскольку $\rho \in \mathcal{S}$, в силу (5) получаем

$$f_\rho^W(x, y) = \text{Tr}(W(x, y)\rho) = \int_{\mathbb{R}} e^{-\frac{i}{2}xy} e^{ix(t+y)} \rho(t+y, t) dt = \int_{\mathbb{R}} e^{ixt} \rho\left(t + \frac{y}{2}, t - \frac{y}{2}\right) dt.$$

Функция $\tilde{\rho}(t, y) = \rho(t + \frac{y}{2}, t - \frac{y}{2})$ принадлежит пространству Шварца $S(\mathbb{R}^2)$. Следовательно, её преобразование Фурье по переменной t также принадлежит $S(\mathbb{R}^2)$.

Пусть теперь $f \in S(\mathbb{R}^2)$. Положим

$$T = \frac{1}{2\pi} \int f(x, y) W(-x, -y) dx dy.$$

Определим действие T на функцию $\psi \in H$:

$$\begin{aligned} (T\psi)(t) &= \frac{1}{2\pi} \int_{\mathbb{R}^2} f(x, y) e^{-\frac{i}{2}xy} e^{-ix(t-y)} \psi(t-y) dx dy = \\ &= -\frac{1}{2\pi} \int_{\mathbb{R}^2} f(x, t-s) e^{-\frac{i}{2}x(t-s)} e^{-ixs} \psi(s) dx ds = \int_{\mathbb{R}} \rho(t, s) \psi(s) ds, \end{aligned}$$

где ядро оператора $\rho(t, s)$ определяется формулой

$$\rho(t, s) = -\frac{1}{2\pi} \int_{\mathbb{R}} e^{-\frac{i}{2}tx} f(x, t-s) dx. \quad (12)$$

Получаем, что отображение $f \rightarrow \rho$ представляет из себя композицию сдвига и преобразования Фурье по одной из переменных. Таким образом, $\rho \in S(\mathbb{R}^2)$, так что T является оператором Шварца. $\square$

Используя операторы рождения и уничтожения, формулу (11) можно переписать в виде

$$f_\rho^W(x, y) = f_\rho^W(z) = \text{Tr} \left(\exp(za^\dagger - \bar{z}a) \rho \right), \quad (13)$$

где

$$z = \frac{y + ix}{\sqrt{2}}. \quad (14)$$

В квантовой физике используются также характеристические функции (см. [4])

$$f_\rho^P(x, y) = f_\rho^P(z) = \text{Tr} \left(\exp(za^\dagger) \exp(-\bar{z}a) \rho \right) \quad (15)$$

и

$$f_\rho^Q(x, y) = f_\rho^Q(z) = \text{Tr} \left(\exp(-\bar{z}a) \exp(za^\dagger) \rho \right), \quad (16)$$

называемые соответственно *характеристической функцией Глаубера—Сударшана* и *характеристической функцией Хусими*. Функции (11), (15) и (16) связаны простым соотношением:

$$f_\rho^W(z) = f_\rho^P(z) e^{-|z|^2/2} = f_\rho^Q(x) e^{|z|^2/2}. \quad (17)$$

Характеристические функции Глаубера—Сударшана и Хусими также можно считать символами оператора ρ . Обратное преобразование (квантизатор) представляет из себя композицию (17) и квантизатора для вейлевской характеристической функции. Введем множества $S_\pm(\mathbb{R}^2)$, состоящие из функций $\psi_\pm$, представимых в виде

$$\psi_\pm(x, y) = \exp \left(\pm \frac{x^2 + y^2}{4} \right) \psi(x, y),$$

где $\psi \in S(\mathbb{R}^2)$. Предложение 1 и соотношение (17) влекут справедливость следующего утверждения.

Следствие. Пусть $\rho \in \mathcal{S}$. Тогда $f_\rho^P \in S_+(\mathbb{R}^2)$ и $f_\rho^Q \in S_-(\mathbb{R}^2)$. Более того, если функция f принадлежит соответствующему классу, то полученный из нее с помощью квантизатора оператор T принадлежит классу $\mathcal{S}$.

5. Представление квазираспределениями. Для вейлевских характеристических функций справедливо равенство (см. [8])

$$\frac{1}{(2\pi)^2} \int_{\mathbb{R}^2} f_\rho^W(x, y) f_\sigma^W(x, y) dx dy = \text{Tr}(\rho\sigma), \quad (18)$$

где $\rho, \sigma \in \mathcal{S}$. С помощью соотношения (18) можно расширить отображение $\rho \rightarrow f_\rho^W$ с $\mathcal{S}$ до $\mathcal{S}'$. В этом случае символами полиномов от операторов координаты и импульса q и p станут линейные комбинации сингулярных обобщенных функций $\delta^{(n)}(x)$ и $\delta^{(m)}(y)$ (см. [1]). По-видимому, поэтому

(см. [11, 12]) исторически был выбран другой символ, представляющий из себя преобразование Фурье от характеристической функции f^W .

Рассмотрим преобразование Фурье F функции $f \in S(\mathbb{R}^2)$:

$$F(f)(q, p) \equiv \hat{f}(q, p) = \frac{1}{(2\pi)^2} \int_{\mathbb{R}^2} e^{-iqx - ipy} f(x, y) dx dy. \quad (19)$$

Функция

$$W(q, p) = \hat{f}_\rho^W(q, p) \quad (20)$$

называется *функцией Вигнера*. Поскольку преобразование Фурье переводит $S(\mathbb{R}^2)$ в себя, справедливо следующее утверждение.

Предложение 2. *Функция Вигнера W_ρ принадлежит пространству $S(\mathbb{R}^2)$ тогда и только тогда, когда оператор ρ , по которому она построена, является оператором Шварца.*

Введем обозначение

$$\hat{S}_-(\mathbb{R}^2) = F(S_-(\mathbb{R}^2)). \quad (21)$$

Лемма. *Элементами пространства $\hat{S}_-(\mathbb{R}^2)$ являются функции ψ , представимые в виде свертки*

$$\psi = \xi_0 \star \xi, \quad (22)$$

где $\xi_0(q, p) = \exp(-q^2 - p^2)$ и $\xi \in S(\mathbb{R}^2)$.

Доказательство. При преобразовании Фурье умножение на функцию переходит в свертку. Итак, достаточно заметить, что для $f_0(x, y) = \exp\left(-\frac{x^2 + y^2}{4}\right)$ имеем $F(f_0)(q, p) = \frac{1}{2\pi} e^{-q^2 - p^2}$. $\square$

Положим

$$\alpha = \frac{q + ip}{\sqrt{2}}. \quad (23)$$

Функция

$$Q_\rho(\alpha) = \hat{f}_\rho^Q(q, p) \quad (24)$$

называется *функцией Хусими*. Известно, что

$$Q_\rho(\alpha) = \frac{1}{\pi} (\psi_\alpha, \rho \psi_\alpha). \quad (25)$$

Из определения функции Хусими получаем справедливость следующего утверждения.

Предложение 3. *Функция Хусими Q_ρ принадлежит классу $\hat{S}(\mathbb{R}^2)$ тогда и только тогда, когда оператор ρ , по которому она построена, является оператором Шварца.*

Заметим, что преобразование Фурье (19) можно расширить не только на обобщенные функции медленного роста класса $S'(\mathbb{R}^2)$ но и на функции класса $S_+(\mathbb{R}^2)$. Преобразование Фурье функции $\psi_+ \in S_+(\mathbb{R}^2)$ является обобщенной функцией $F(\psi_+) \in \hat{S}'_-(\mathbb{R}^2)$, так что

$$\left\langle F(\psi_+), \overline{F(\psi_-)} \right\rangle := \langle \psi_+, \overline{\psi_-} \rangle = \int_{\mathbb{R}^2} \psi_+(x, y) \overline{\psi_-(x, y)} dx dy, \quad (26)$$

где $\psi_\pm \in S_\pm(\mathbb{R}^2)$. Делая замену переменной (23), можно определить функцию

$$P_\rho(\alpha) = \hat{f}_\rho^P(q, p), \quad (27)$$

называемую *P-функцией Глаубера—Сударшана*. Из равенства Парсеваля следует, что

$$\int_{\mathbb{C}} P_\rho(\alpha) Q_\sigma(\alpha) d^2 \alpha = \text{Tr}(\rho \sigma) \quad (28)$$

для $\rho, \sigma \in \mathcal{S}$. Отсюда немедленно вытекает известная формула

$$\rho = \int_{\mathbb{C}} P_\rho(\alpha) |\psi_\alpha\rangle \langle \psi_\alpha| d^2 \alpha. \quad (29)$$

6. Представление оптическими томограммами и дуальное к нему. Оптическая томограмма (см. [3]) также может быть использована для определения символов операторов Шварца. Используя ядро интегрального оператора (5) можно выразить оптическую томограмму в виде (см. [2])

$$\omega_\rho(x, \varphi) = \frac{1}{2\pi} \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} e^{is(t \cos \varphi - x)} \rho \left(t - \frac{s \sin \varphi}{2}, t + \frac{s \sin \varphi}{2} \right) dt ds. \quad (30)$$

Если определить отображение

$$\Omega_\rho(x, \varphi) = \int_0^{+\infty} \int_{-\infty}^{+\infty} t e^{i(x+t \sin \varphi)s} \rho \left(t - \frac{s \sin \varphi}{2}, t + \frac{s \sin \varphi}{2} \right) dt ds, \quad (31)$$

получим (см. [2])

$$\int_0^{2\pi} \int_0^{+\infty} \Omega_\rho(x, \varphi) \omega_\sigma(x, \varphi) dx d\varphi = \text{Tr}(\rho\sigma), \quad (32)$$

где $\rho, \sigma \in \mathcal{S}$. Оптический томографический символ обладает свойством $\omega_\rho(-x, \varphi) := \omega_\rho(x, \varphi + \pi)$. Обозначим через S_{opt} образ $S(\mathbb{R}^2)$ при отображении (30). Справедливо следующее утверждение (см. [2]).

Предложение 4. *Элементы пространства S_{opt} обладают следующими двумя свойствами:*

- (i) $\omega_\rho(\cdot, \varphi) \in S(\mathbb{R})$ для фиксированного $\varphi \in [0, 2\pi]$;
- (ii) $\omega_\rho(x, \cdot)$ — бесконечно дифференцируемая 2π -периодическая функция для фиксированного $x \in \mathbb{R}$.

7. Представления пространства операторов Шварца и дуального к нему. Сведем приведенные в предыдущих разделах результаты в единое утверждение.

Теорема. *Отображения (11) и (20) задают представления пространства операторов Шварца $\rho \in \mathcal{S}$ элементами пространства $S(\mathbb{R}^2)$:*

$$\rho \rightarrow f_\rho^W, \quad \rho \rightarrow W_\rho. \quad (33)$$

Если сузить дуальное отображение, заданное на $\mathcal{S}'$, на пространство $\mathcal{S}$, получим, что отображение самодуально, т.е. задается теми же формулами (33). Отображения (29) и (30) задают представления пространства $\mathcal{S}$ элементами пространства $\mathcal{S}_-(\mathbb{R}^2)$ (см. (21)) и пространства S_{opt} из предложения 4 соответственно:

$$\rho \rightarrow Q_\rho, \quad \rho \rightarrow \omega_\rho. \quad (34)$$

Дуальные отображения, заданные на $\mathcal{S}'$ и суженные на элементы из $\mathcal{S}$, задаются отображениями (27) и (31),

$$\rho \rightarrow P_\rho, \quad \rho \rightarrow \Omega_\rho. \quad (35)$$

Таким образом, отображения (34) не являются самодуальными.

СПИСОК ЛИТЕРАТУРЫ

1. Амосов Г. Г., Коренной Я. А., Манько В. И. О вычислении средних значений квантовых наблюдаемых в представлении оптической томографии // Теор. мат. физ. — 2012. — 171. — С. 475–482.
2. Amosov G. G. On tomographic representation on the plane of the space of Schwartz operators and its dual // Lobachevskii J. Math. — 2017. — 38. — С. 595–599.
3. Bertrand J., Bertrand P. A tomographic approach to Wigner's function // Found. Phys. — 1987. — 17. — С. 397–405.
4. Cahill K. E., Glauber R. J. Density operators and quasiprobability distributions // Phys. Rev. — 1969. — 177. — С. 1882–1902.
5. D'Ariano G. M., Maccone L., Paris M. G. A. Quorum of observables for universal quantum estimation // J. Phys. A: Math. Gen. — 2001. — 34, № 1. — С. 93–104.

6. *Filippov S. N., Man'ko V. I.* Spin tomography and star-product kernel for qubits and qutrits// J. Russ. Laser Res. — 2009. — 30. — С. 129–145.
7. *Filippov S. N., Man'ko V. I.* Symmetric informationally complete positive operator valued measure and probability representation of quantum mechanics// J. Russ. Laser Res. — 2010. — 31. — С. 211–231.
8. *Holevo A. S.* Quantum systems, channels, information/ De Gruyter Stud. Math. Phys. — 16. — De Gruyter, 2012.
9. *Keyl M., Kiukas J., Werner R. F.* Schwartz operators//Rev. Math. Phys. — 2016. — 28, № 3. — С. 1630001.
10. *Manko O. V., Manko V. I., Marmo G.* Alternative commutation relations, star products and tomography//J. Phys. A: Math. Gen. — 2002. — 35, № 3. — С. 699–720.
11. *Moyal J. E.* Quantum mechanics as a statistical theory// Math. Proc. Cambridge Phil. Soc. — 1949. — 45, № 01. — С. 99–124.
12. *Wigner E.* On the quantum correction for thermodynamic equilibrium// Phys. Rev. — 1932. — 40, № 5. — С. 749–759.

Г. Г. Амосов

Математический институт им. В. А. Стеклова Российской академии наук;
Санкт-Петербургский государственный университет;
Московский физико-технический институт (государственный университет)
E-mail: gramos@mi.ras.ru



СЛЕД И КОММУТАТОРЫ ИЗМЕРИМЫХ ОПЕРАТОРОВ, ПРИСОЕДИНЕННЫХ К АЛГЕБРЕ ФОН НЕЙМАНА

© 2018 г. А. М. БИКЧЕНТАЕВ

Аннотация. Установлены новые свойства пространства $L_1(\mathcal{M}, \tau)$ интегрируемых (относительно следа τ) операторов, присоединенных к полуконечной алгебре фон Неймана $\mathcal{M}$. Для самосопряженных τ -измеримых операторов A, B найдены достаточные условия τ -интегрируемости оператора $\lambda I - AB$ и вещественности следа $\tau(\lambda I - AB)$, где $\lambda \in \mathbb{R}$. При этих условиях $[A, B] = AB - BA \in L_1(\mathcal{M}, \tau)$ и $\tau([A, B]) = 0$. Для τ -измеримых операторов $A, B = B^2$ найдены условия, достаточные для выполнения равенства $\tau([A, B]) = 0$. Для изометрии $U \in \mathcal{M}$ и неотрицательного τ -измеримого оператора A доказано, что $U - A \in L_1(\mathcal{M}, \tau)$ тогда и только тогда, когда $I - A, I - U \in L_1(\mathcal{M}, \tau)$. Для τ -измеримого оператора A найдены оценки следа самокоммутиатора $[A^*, A]$. Пусть самосопряженные τ -измеримые операторы $X \geq 0$ и Y таковы, что $[X^{1/2}, YX^{1/2}] \in L_1(\mathcal{M}, \tau)$. Тогда $\tau([X^{1/2}, YX^{1/2}]) = it$, где $t \in \mathbb{R}$ и $t = 0$ при $XY \in L_1(\mathcal{M}, \tau)$.

Ключевые слова: гильбертово пространство, линейный оператор, алгебра фон Неймана, нормальный полуконечный след, измеримый оператор, интегрируемый оператор, коммутатор, самокоммутиатор.

AMS Subject Classification: 47C15, 46L51

СОДЕРЖАНИЕ

1. Введение	10
2. Обозначения и определения	11
3. Леммы и примеры	12
4. Основные результаты	13
Список литературы	19

1. ВВЕДЕНИЕ

Пусть алгебра фон Неймана $\mathcal{M}$ операторов действует в гильбертовом пространстве $\mathcal{H}$, τ — точный нормальный полуконечный след на $\mathcal{M}$. В работе установлены новые свойства пространства $L_1(\mathcal{M}, \tau)$ интегрируемых операторов, присоединенных к алгебре $\mathcal{M}$. Для оператора $X \in L_1(\mathcal{M}, \tau)$ исследованы условия, когда $\tau(X) \in \mathbb{R}$ или $\tau(X) = 0$. Для самосопряженных τ -измеримых операторов A, B найдены достаточные условия интегрируемости оператора $\lambda I - AB$ и вещественности следа $\tau(\lambda I - AB)$, где $\lambda \in \mathbb{R}$. При этих условиях коммутатор $[A, B] = AB - BA \in L_1(\mathcal{M}, \tau)$ и $\tau([A, B]) = 0$ (теоремы 4.1 и 4.2 и предложения 4.1–4.4). Для τ -измеримых операторов $A, B = B^2$ найдены условия, достаточные для выполнения равенства $\tau([A, B]) = 0$ (теорема 4.3). Пункт (ii) теоремы 4.3 обобщает теорему 2.26 из [4].

Для изометрии $U \in \mathcal{M}$ и неотрицательного τ -измеримого оператора A доказано, что $U - A \in L_1(\mathcal{M}, \tau)$ тогда и только тогда, когда $I - A, I - U \in L_1(\mathcal{M}, \tau)$ (теорема 4.5). Для τ -измеримого оператора A найдены оценки следа самокоммутиатора $[A^*, A]$ (следствие 4.4, теорема 4.7).

Работа выполнена при поддержке Российского фонда фундаментальных исследований и правительства Республики Татарстан (проект № 15-41-02433) и субсидий, выделенными Казанскому федеральному университету для выполнения государственного задания в сфере научной деятельности (проекты № 1.1515.2017/4.6 и 1.9773.2017/8.9).

Пусть самосопряженные τ -измеримые операторы $X \geq 0$ и Y таковы, что $[X^{1/2}, YX^{1/2}] \in L_1(\mathcal{M}, \tau)$. Тогда

$$\tau([X^{1/2}, YX^{1/2}]) = it,$$

где $t \in \mathbb{R}$ и $t = 0$ при $XY \in L_1(\mathcal{M}, \tau)$ (теорема 4.8). Результаты являются новыми и для $*$ -алгебры $\mathcal{M} = \mathcal{B}(\mathcal{H})$ всех ограниченных линейных операторов в $\mathcal{H}$, снабженной каноническим следом $\tau = \text{tr}$.

2. ОБОЗНАЧЕНИЯ И ОПРЕДЕЛЕНИЯ

Пусть $\mathcal{M}$ — алгебра фон Неймана операторов в гильбертовом пространстве $\mathcal{H}$, $\mathcal{M}^{\text{pr}}$ — решетка проекторов в $\mathcal{M}$, I — единица $\mathcal{M}$, $P^\perp = I - P$ для $P \in \mathcal{M}^{\text{pr}}$, $\mathcal{M}^+$ — конус положительных элементов из $\mathcal{M}$.

Отображение $\varphi : \mathcal{M}^+ \rightarrow [0, +\infty]$ называется *следом*, если

$$\varphi(X + Y) = \varphi(X) + \varphi(Y), \quad \varphi(\lambda X) = \lambda \varphi(X)$$

для всех $X, Y \in \mathcal{M}^+$, $\lambda \geq 0$ (при этом $0 \cdot (+\infty) \equiv 0$) и $\varphi(Z^*Z) = \varphi(ZZ^*)$ для всех $Z \in \mathcal{M}$. След φ называется

- (i) *точным*, если $\varphi(X) > 0$ для всех $X \in \mathcal{M}^+$, $X \neq 0$;
- (ii) *полуконачным*, если $\varphi(X) = \sup \{ \varphi(Y) : Y \in \mathcal{M}^+, Y \leq X, \varphi(Y) < +\infty \}$ для всех $X \in \mathcal{M}^+$;
- (iii) *нормальным*, если для $X_i \nearrow X$ ($X_i, X \in \mathcal{M}^+$) имеем $\varphi(X) = \sup \varphi(X_i)$.

Для следа φ определим

$$\mathfrak{M}_\varphi^+ = \{ X \in \mathcal{M}^+ : \varphi(X) < +\infty \}, \quad \mathfrak{M}_\varphi = \text{lin}_{\mathbb{C}} \mathfrak{M}_\varphi^+.$$

Ограничение $\varphi|_{\mathfrak{M}_\varphi^+}$ корректно продолжается по линейности до функционала на $\mathfrak{M}_\varphi$, который будем обозначать той же буквой φ .

Оператор в $\mathcal{H}$ (не обязательно ограниченный или плотно определенный) называется *присоединенным к алгебре фон Неймана $\mathcal{M}$* , если он перестановочен с любым унитарным оператором из коммутанта $\mathcal{M}'$ алгебры $\mathcal{M}$. Далее всюду τ — точный нормальный полуконачный след на $\mathcal{M}$. Замкнутый оператор X , присоединенный к $\mathcal{M}$, имеющий всюду плотную в $\mathcal{H}$ область определения $\mathcal{D}(X)$, называется *τ -измеримым*, если для любого $\varepsilon > 0$ существует такой $P \in \mathcal{M}^{\text{pr}}$, что $P\mathcal{H} \subset \mathcal{D}(X)$ и $\tau(P^\perp) < \varepsilon$. Множество $\widetilde{\mathcal{M}}$ всех τ -измеримых операторов является $*$ -алгеброй относительно перехода к сопряженному оператору, умножению на скаляр и операций сильного сложения и умножения, получаемых замыканием обычных операций (см. [23, 24]). Для семейства $\mathcal{L} \subset \widetilde{\mathcal{M}}$ обозначим через $\mathcal{L}^+$ и $\mathcal{L}^{\text{sa}}$ его положительную и эрмитову части, соответственно. Частичный порядок в $\widetilde{\mathcal{M}}^{\text{sa}}$, порожденный собственным конусом $\widetilde{\mathcal{M}}^+$, будем обозначать через $\leq$. Пусть $i \in \mathbb{C}$, $i^2 = -1$, и $X \in \widetilde{\mathcal{M}}$. Для $\text{Re } X = (X + X^*)/2$ и $\text{Im } X = (X - X^*)/(2i)$ имеем $X = \text{Re } X + i \text{Im } X$ и $\text{Re } X, \text{Im } X \in \widetilde{\mathcal{M}}^{\text{sa}}$.

Если X — замкнутый плотно заданный линейный оператор, присоединенный к $\mathcal{M}$ и $|X| = (X^*X)^{1/2}$, то спектральное разложение $P^{|X|}(\cdot)$ содержится в $\mathcal{M}$ и $X \in \widetilde{\mathcal{M}}$ тогда и только тогда, когда существует такое $\lambda \in \mathbb{R}$, что

$$\tau(P^{|X|}((\lambda, +\infty))) < +\infty.$$

Если $X \in \widetilde{\mathcal{M}}$ и $X = U|X|$ — полярное разложение X , то $U \in \mathcal{M}$ и $|X| \in \widetilde{\mathcal{M}}^+$. При этом, если

$$|X| = \int_0^\infty \lambda P^{|X|}(d\lambda)$$

— спектральное разложение, то

$$\tau(P^{|X|}((\lambda, +\infty))) \rightarrow 0 \quad \text{при } \lambda \rightarrow +\infty.$$

Через $\mu_t(X)$ обозначим *перестановку* оператора $X \in \widetilde{\mathcal{M}}$ (см. [19, 27]), т.е. невозрастающую непрерывную справа функцию $\mu(X) : (0, \infty) \rightarrow [0, \infty)$, заданную формулой

$$\mu_t(X) = \inf \left\{ \|XP\| : P \in \mathcal{M}^{\text{pr}}, \tau(P^\perp) \leq t \right\}, \quad t > 0.$$

Пусть m — линейная мера Лебега на $\mathbb{R}$. Ассоциированное с $(\mathcal{M}, \tau)$ некоммутативное L_p -пространство Лебега ($0 < p < \infty$) может быть определено как

$$L_p(\mathcal{M}, \tau) = \left\{ X \in \widetilde{\mathcal{M}} : \mu(X) \in L_p(\mathbb{R}^+, m) \right\}$$

с F -нормой (нормой для $1 \leq p < \infty$) $\|X\|_p = \|\mu(X)\|_p$, $X \in L_p(\mathcal{M}, \tau)$. Ограничение $\tau|_{\mathfrak{M}_\tau^+}$ продолжается до линейного ограниченного функционала на $L_1(\mathcal{M}, \tau)$, который будем обозначать той же буквой τ . Имеем

$$\mathfrak{M}_\tau = \mathcal{M} \cap L_1(\mathcal{M}, \tau), \quad \|X\|_p = \tau(|X|^p)^{1/p}, \quad 0 < p < \infty.$$

Если $\mathcal{M} = \mathcal{B}(\mathcal{H})$ — $*$ -алгебра всех ограниченных линейных операторов в $\mathcal{H}$ и $\tau = \text{tr}$ — канонический след, то $\widetilde{\mathcal{M}}$ совпадает с $\mathcal{B}(\mathcal{H})$. Имеем

$$\mu_t(X) = \sum_{n=1}^{\infty} s_n(X) \chi_{[n-1, n)}(t), \quad t > 0,$$

где $\{s_n(X)\}_{n=1}^{\infty}$ — последовательность s -чисел оператора X , χ_A — индикатор множества $A \subset \mathbb{R}$ (см. [10, с. 46]). Тогда пространство $L_p(\mathcal{M}, \tau)$ является идеалом Шаттена—фон Неймана $\mathfrak{S}_p$, $0 < p < \infty$.

3. ЛЕММЫ И ПРИМЕРЫ

Пусть τ — точный нормальный полуконечный след на алгебре фон Неймана $\mathcal{M}$.

Лемма 3.1 (см. [16, теорема 17]). *Если $X, Y \in \widetilde{\mathcal{M}}$ и $XY, YX \in L_1(\mathcal{M}, \tau)$, то $\tau(XY) = \tau(YX)$.*

Лемма 3.2 (см. [1, теорема 3] и [14, теорема 1]). *Если $X, Y \in \widetilde{\mathcal{M}}^+$ и $XY \in L_1(\mathcal{M}, \tau)$, то $X^{1/2}YX^{1/2} \in L_1(\mathcal{M}, \tau)$ и $\tau(XY) = \tau(X^{1/2}YX^{1/2})$.*

Лемма 3.3 (см. [2, теорема 3.1]). *Если $X, Y \in \widetilde{\mathcal{M}}^{\text{sa}}$ и $XY \in L_1(\mathcal{M}, \tau)$, то $YX \in L_1(\mathcal{M}, \tau)$ и $\tau(XY) = \tau(YX) \in \mathbb{R}$.*

Лемма 3.4 (см. [2, теорема 2.3]). *Если $X \in L_1(\mathcal{M}, \tau)$, то $\tau(X^*) = \overline{\tau(X)}$.*

Здесь и ниже черта сверху означает комплексное сопряжение.

Лемма 3.5 (см. [3, теорема 4.8]). *Если $\tau(I) = 1$, то для $X \in L_1(\mathcal{M}, \tau)$ следующие условия эквивалентны:*

- (i) $\tau(X) = 0$;
- (ii) $\|I + zX\|_1 \geq 1$ для всех $z \in \mathbb{C}$.

В частности, если $\tau(I) = 1$ и $A, B \in \mathcal{M}$, то $\|I + z[A, B]\|_1 \geq 1$ для всех $z \in \mathbb{C}$. Для фактора типа II_1 алгебры $\mathcal{M}$ коммутаторы τ -измеримых операторов были исследованы в [17]; в [18] был изучен вопрос представимости произвольного τ -измеримого оператора X , обладающего свойством $\tau(X) = 0$, в виде коммутатора $X = [A, B]$.

Лемма 3.6. *Пусть операторы $A, B, D \in \widetilde{\mathcal{M}}^{\text{sa}}$ таковы, что $T = D - AB \in L_1(\mathcal{M}, \tau)$. Тогда $[A, B] \in L_1(\mathcal{M}, \tau)$ и если $\tau(T) \in \mathbb{R}$, то $\tau([A, B]) = 0$.*

Доказательство. Поскольку

$$[A, B] = T^* - T \in L_1(\mathcal{M}, \tau), \tag{1}$$

в силу леммы 3.4 при $\tau(T) \in \mathbb{R}$ имеем

$$\tau([A, B]) = \tau(T^* - T) = \tau(T^*) - \tau(T) = \overline{\tau(T)} - \tau(T) = 0. \tag{2}$$

Лемма доказана. $\square$

Лемма 3.7. Для $X \in L_1(\mathcal{M}, \tau)$ следующие условия эквивалентны:

- (i) $\tau(X) \in \mathbb{R}$;
- (ii) $\tau(\operatorname{Im} X) = 0$.

Из лемм 3.5 и 3.7 следует, что если $\tau(I) = 1$ и $X \in L_1(\mathcal{M}, \tau)$, то условие $\tau(X) \in \mathbb{R}$ эквивалентно выполнению неравенства $\|I + z \operatorname{Im} X\|_1 \geq 1$ для всех $z \in \mathbb{C}$.

Пример 3.1. Пусть $\mathcal{M} = \mathbb{M}_n(\mathbb{C})$ и $\tau = \operatorname{tr}$ — след на $\mathcal{M}$. Хорошо известна формула Якоби

$$\det e^X = e^{\tau(X)}, \quad X \in \mathcal{M}.$$

В частности, если $\det e^X = 1$, то $\tau(X) = 0$. Для $X \in \mathcal{M}$ следующие условия эквивалентны:

- (i) X унитарно эквивалентна матрице с нулевой диагональю;
- (ii) $\tau(X) = 0$;
- (iii) X есть коммутатор.

Доказательство (i) $\Leftrightarrow$ (ii) см. в [9, гл. II, задача 209], (ii) $\Leftrightarrow$ (iii) — в [13, задача 182]. Поэтому каждая матрица $A \in \mathbb{M}_n(\mathbb{C})$ унитарно эквивалентна матрице с «постоянной» диагональю и представляется в виде суммы $A = \lambda I + X$, где $\tau(X) = 0$ и $\lambda = \operatorname{tr}(A)/n$.

Пример 3.2 (см. [5, пример 1]). Пусть $0 < p, q < \infty$ и $a_n = 2^{n+1}n^{-q}$, $n \in \mathbb{N}$. Снабдим алгебру фон Неймана $\mathcal{M} = \bigoplus_{n=1}^{\infty} \mathbb{M}_2(\mathbb{C})$ точным нормальным конечным следом $\tau = \bigoplus_{n=1}^{\infty} 2^{-n} \operatorname{tr}_2$ и положим

$$A = \bigoplus_{n=1}^{\infty} \begin{pmatrix} 1 & a_n \\ 0 & 0 \end{pmatrix}.$$

Имеем $A = A^2$ и $A \in L_p(\mathcal{M}, \tau)$ при $pq > 1$, $A \notin L_p(\mathcal{M}, \tau)$ при $pq \leq 1$.

4. ОСНОВНЫЕ РЕЗУЛЬТАТЫ

Пусть τ — точный нормальный полуконечный след на алгебре фон Неймана $\mathcal{M}$.

Теорема 4.1. Пусть $A, B \in \widetilde{\mathcal{M}}^{\text{sa}}$, $\lambda \in \mathbb{R}$, $n \in \mathbb{N}$.

- (i) Если $T = \lambda A^n - AB \in L_1(\mathcal{M}, \tau)$, то $\tau(T) \in \mathbb{R}$.
- (ii) Если $T = \lambda I - AB \in L_1(\mathcal{M}, \tau)$ и $A = \sum_{k=1}^n a_k P_k$, где $a_k \in \mathbb{R}$ и $P_k \in \mathcal{M}^{\text{pr}}$, $P_k P_j = 0$ при $k \neq j$ для всех $k, j = 1, \dots, n$, то $\tau(T) \in \mathbb{R}$.

В обоих случаях $[A, B] \in L_1(\mathcal{M}, \tau)$ и $\tau([A, B]) = 0$.

Доказательство. (i) Поскольку

$$T = \begin{cases} A(\lambda I - B) & \text{при } n = 1, \\ A^{n-1}(\lambda A - B) & \text{при } n \geq 2, \end{cases}$$

имеем $\tau(T) \in \mathbb{R}$ в силу леммы 3.3.

- (ii) Для каждого $k \in \{1, \dots, n\}$ имеем

$$T_k = P_k T = \lambda P_k - a_k P_k B = P_k(\lambda I - a_k B) \in L_1(\mathcal{M}, \tau)$$

и $\tau(T_k) \in \mathbb{R}$ в силу леммы 3.3. Для проектора $P = (P_1 + \dots + P_n)^\perp$ имеем

$$PT = \lambda P \in L_1(\mathcal{M}, \tau)^{\text{sa}}, \quad \tau(PT) \in \mathbb{R}.$$

Следовательно,

$$\tau(T) = \tau(PT) + \sum_{k=1}^n \tau(P_k T) \in \mathbb{R}.$$

Далее в обоих случаях работает лемма 3.6. Теорема доказана. $\square$

Теорема 4.2. Пусть операторы $A, B \in \widetilde{\mathcal{M}}^{\text{sa}}$ и числа $\lambda \in \mathbb{R}$ таковы, что

$$T = \lambda I - AB \in L_1(\mathcal{M}, \tau).$$

Если A обратим в $\widetilde{\mathcal{M}}$ или $I - B \in L_1(\mathcal{M}, \tau)$, то $\tau(T) \in \mathbb{R}$. В обоих случаях

$$[A, B] \in L_1(\mathcal{M}, \tau), \quad \tau([A, B]) = 0.$$

Доказательство. Для обратимого оператора A имеем

$$T = A(\lambda A^{-1} - B), \quad \lambda A^{-1} - B \in \widetilde{\mathcal{M}}^{\text{sa}},$$

поэтому $\tau(T) \in \mathbb{R}$ в силу леммы 3.3.

Пусть теперь $I - B \in L_1(\mathcal{M}, \tau)$. Поскольку

$$T = (\lambda I - A)B + \lambda(I - B),$$

имеем

$$(\lambda I - A)B \in L_1(\mathcal{M}, \tau)$$

и в силу леммы 3.3 получаем

$$\tau((\lambda I - A)B), \quad \tau(I - B) \in \mathbb{R}.$$

Поэтому $\tau(T) \in \mathbb{R}$. Далее в обоих случаях работает лемма 3.6. Теорема доказана. $\square$

Предложение 4.1. Пусть операторы $A, B \in \widetilde{\mathcal{M}}^{\text{sa}}$ и числа $a_1, a_2, b_1, b_2 \in \mathbb{R}$ таковы, что

$$\lambda = a_1 b_2 + a_2 b_1 \neq 0, \quad T = (a_1 A + b_1 B)(a_2 A - b_2 B) \in L_1(\mathcal{M}, \tau).$$

Тогда

$$[A, B] \in L_1(\mathcal{M}, \tau), \quad \tau([A, B]) = 0.$$

Если $\tau(I) = 1$, то $\|I + z[A, B]\|_1 \geq 1$ для всех $z \in \mathbb{C}$.

Доказательство. Имеем $\tau(T) \in \mathbb{R}$ в силу леммы 3.3. Поскольку $T^* \in L_1(\mathcal{M}, \tau)$ и $T^* - T = \lambda[A, B]$, получаем $[A, B] \in L_1(\mathcal{M}, \tau)$. Теперь в силу леммы 3.4 имеем

$$\lambda \tau([A, B]) = \tau(T^* - T) = \tau(T^*) - \tau(T) = \overline{\tau(T)} - \tau(T) = 0.$$

При $\tau(I) = 1$ применяем лемму 3.5. Утверждение доказано. $\square$

Предложение 4.2. Пусть операторы $X, Y, Z \in \widetilde{\mathcal{M}}^{\text{sa}}$ и числа $n \in \mathbb{N}$, $\lambda \in \mathbb{R}$ таковы, что

$$XY + YZ, XY - \lambda Y^n \in L_1(\mathcal{M}, \tau).$$

Тогда

$$\tau(XY + YZ) \in \mathbb{R}, \quad \tau([X - Z, Y]) = 0.$$

Если $\tau(I) = 1$, то $\|I + z[X - Z, Y]\|_1 \geq 1$ для всех $z \in \mathbb{C}$.

Доказательство. Очевидно, $\lambda Y^n + YZ \in L_1(\mathcal{M}, \tau)$. В силу леммы 3.3 имеем

$$\tau(XY + YZ) = \tau((XY - \lambda Y^n) + (\lambda Y^n + YZ)) = \tau((X - \lambda Y^{n-1})Y) + \tau(Y(\lambda Y^{n-1} + Z)) \in \mathbb{R}.$$

Поэтому в силу леммы 3.4 получаем

$$\tau([X - Z, Y]) = \tau(XY + YZ - (XY + YZ)^*) = \tau(XY + YZ) - \overline{\tau((XY + YZ))} = 0.$$

При $\tau(I) = 1$ применяем лемму 3.5. Предложение доказано. $\square$

Предложение 4.3. Пусть операторы $A \in \widetilde{\mathcal{M}}$, $B \in \mathcal{M}$ и число $n \in \mathbb{N}$ таковы, что

$$A - B^n \in L_1(\mathcal{M}, \tau).$$

Тогда

$$[A, B] \in L_1(\mathcal{M}, \tau), \quad \tau([A, B]) = 0.$$

Если $\tau(I) = 1$, то $\|I + z[A, B]\|_1 \geq 1$ для всех $z \in \mathbb{C}$.

Доказательство. Положим $X = A - B^n$, $Y = B$. Тогда

$$XY, YX \in L_1(\mathcal{M}, \tau), \quad [A, B] = [X, Y].$$

Теперь в силу леммы 3.1 имеем

$$\tau([A, B]) = \tau([X, Y]) = \tau(XY) - \tau(YX) = 0.$$

При $\tau(I) = 1$ применяем лемму 3.5. Утверждение доказано. $\square$

Предложение 4.4. Пусть числа $\lambda_1, \lambda_2 \in \mathbb{C} \setminus \{0\}$ и операторы $A \in \mathcal{M}$, $B \in \widetilde{\mathcal{M}}$ таковы, что

$$\lambda_1 I - A, \lambda_2 I - B \in L_1(\mathcal{M}, \tau).$$

Тогда

$$\lambda_1 \lambda_2 I - AB, [A, B] \in L_1(\mathcal{M}, \tau), \quad \tau([A, B]) = 0.$$

Доказательство. Оператор

$$\lambda_1 \lambda_2 I - AB = \lambda_1 \lambda_2 ((I - \lambda_1^{-1} A) + \lambda_1^{-1} A (I - \lambda_2^{-1} B)) \quad (3)$$

принадлежит $L_1(\mathcal{M}, \tau)$. Операторы $(\lambda_1 I - A)(\lambda_2 I - B)$, $(\lambda_2 I - B)(\lambda_1 I - A)$ лежат в $L_1(\mathcal{M}, \tau)$, поэтому

$$[A, B] = [\lambda_1 I - A, \lambda_2 I - B] \in L_1(\mathcal{M}, \tau)$$

и $\tau([A, B]) = \tau([\lambda_1 I - A, \lambda_2 I - B]) = 0$ в силу леммы 3.1 с $X = \lambda_1 I - A, Y = \lambda_2 I - B$. $\square$

Следствие 4.1. Пусть выполнены условия предложения 4.4 и $\lambda_1, \lambda_2 \in \mathbb{R}$, $A, B \in \widetilde{\mathcal{M}}^{\text{sa}}$. Тогда $\tau(\lambda_1 \lambda_2 I - AB) \in \mathbb{R}$.

Это утверждение вытекает из (3) и леммы 3.3.

Теорема 4.3. Пусть $A, B \in \widetilde{\mathcal{M}}$, $B = B^2$ и $[AB, B] \in L_1(\mathcal{M}, \tau)$.

- (i) Имеет место равенство $\tau([AB, B]) = 0$.
- (ii) Если $[A, B] \in L_1(\mathcal{M}, \tau)$, то $\tau([A, B]) = 0$.

Доказательство. (i) Положим

$$X = [AB, B] = AB - BAB, \quad Y = B.$$

Тогда операторы $XY = X$, $YX = 0$ принадлежат $L_1(\mathcal{M}, \tau)$ и в силу леммы 3.1 имеем

$$\tau(X) = \tau(XY) = \tau(YX) = \tau(0) = 0.$$

(ii) Поскольку $BA - BAB = AB - BAB - [A, B] \in L_1(\mathcal{M}, \tau)$, для сопряженных операторов A^* , B^* выполнены условия п. (i):

$$\tau(BA - BAB) = \overline{\tau(A^* B^* - B^* A^* B^*)} = \bar{0} = 0$$

(см. лемму 3.3). Далее,

$$\tau([A, B]) = \tau(AB - BAB - (BA - BAB)) = \tau(AB - BAB) - \tau(BA - BAB) = 0 - 0 = 0.$$

Теорема доказана. $\square$

Отметим, что п. (ii) теоремы 4.3 обобщает теорему 2.26 из [4]. Из теоремы 4.3 и леммы 3.5 получаем следующее утверждение.

Следствие 4.2. Пусть в условиях теоремы 4.3 $\tau(I) = 1$. Тогда

- (i) $\|I + z[AB, B]\|_1 \geq 1$ для всех $z \in \mathbb{C}$;
- (ii) если $[A, B] \in L_1(\mathcal{M}, \tau)$, то $\|I + z[A, B]\|_1 \geq 1$ для всех $z \in \mathbb{C}$.

Предложение 4.5. Пусть $A, B \in \widetilde{\mathcal{M}}$ и $B = B^2$. Если $[B, BA] \in L_1(\mathcal{M}, \tau)$, то $\tau([B, BA]) = 0$. Если при этом $\tau(I) = 1$, то $\|I + z[B, BA]\|_1 \geq 1$ для всех $z \in \mathbb{C}$.

Доказательство. Положим $X = [B, BA]$, $Y = B$. Тогда операторы $XY (= 0)$, $YX (= X)$ принадлежат $L_1(\mathcal{M}, \tau)$ и в силу леммы 3.1 имеем

$$\tau(X) = \tau(YX) = \tau(XY) = \tau(0) = 0.$$

При $\tau(I) = 1$ применяем лемму 3.5. Утверждение доказано. $\square$

Теорема 4.4. Пусть $A \in \widetilde{\mathcal{M}}$,

$$B = \sum_{k=1}^n b_k P_k, \quad b_k \in \mathbb{C}, \quad P_k = P_k^2 \in \mathcal{M}, \quad b_k \neq b_j, \quad P_k P_j = 0 \text{ при } k \neq j \text{ для всех } k, j = 1, \dots, n.$$

Если $[A, B] \in L_1(\mathcal{M}, \tau)$, то $\tau([A, B]) = 0$.

Доказательство. Поскольку

$$[A, B] = \sum_{k=1}^n b_k (AP_k - P_k A) \in L_1(\mathcal{M}, \tau), \quad (4)$$

для всех $k, j = 1, \dots, n$, $k \neq j$, имеем

$$P_j [A, B] = P_j AB - b_j P_j A \in L_1(\mathcal{M}, \tau), \quad (5)$$

а также $P_j [A, B] P_k = (b_k - b_j) P_j A P_k \in L_1(\mathcal{M}, \tau)$; поэтому $P_j A P_k \in L_1(\mathcal{M}, \tau)$. Теперь из (5) получаем

$$P_j A P_j - P_j A \in L_1(\mathcal{M}, \tau) \quad \text{для всех } j = 1, \dots, n. \quad (6)$$

Рассматривая вместо (5) операторы $[A, B] P_j$, аналогичным образом получаем

$$P_j A P_j - A P_j \in L_1(\mathcal{M}, \tau) \quad \text{для всех } j = 1, \dots, n.$$

Отсюда и из (6) заключаем, что $[A, P_j] \in L_1(\mathcal{M}, \tau)$ для всех $j = 1, \dots, n$. В силу теоремы 2.26 из [4] имеем $\tau([A, P_j]) = 0$ для всех $j = 1, \dots, n$ и из (4) получаем $\tau([A, B]) = 0$. $\square$

Теорема 4.5. Для изометрии $U \in \mathcal{M}$ и оператора $A \in \widetilde{\mathcal{M}}^+$ следующие условия эквивалентны:

- (i) $U - A \in L_1(\mathcal{M}, \tau)$;
- (ii) $I - A, I - U \in L_1(\mathcal{M}, \tau)$.

Доказательство. (i) $\Rightarrow$ (ii) Пусть

$$A = \int_0^\infty \lambda P^A(d\lambda)$$

— спектральное разложение оператора $A \in \widetilde{\mathcal{M}}^+$. Представим A в виде суммы

$$A = AP^A([0; 1]) + AP^A((1; \infty)) \equiv A_1 + A_2.$$

Тогда

$$A_1 \in \mathcal{M}, \quad A_2 = (U - A_1) - (U - A) \in L_1(\mathcal{M}, \tau) + \mathcal{M}.$$

Поэтому существует такое число $k \in \mathbb{N}$, что $\tau P^{A_2}((k; \infty)) < \infty$. Заметим, что

$$P^{A_2}((n; \infty)) = P^A((n; \infty)) \quad \forall n \in \mathbb{N}.$$

Таким образом, оператор $B_2 = P^{A_2}((k; \infty))$ принадлежит $L_1(\mathcal{M}, \tau)^+$. Для $B_1 = A - B_2 \in \mathcal{M}^+$ оператор $U - B_1 \in \mathfrak{M}_\tau$ и $I + B_1$ обратим в $\mathcal{M}$. В силу [8, теорема 2] операторы $I - B_1$ и $I - U$ лежат в $\mathfrak{M}_\tau$. Следовательно,

$$I - A = I - B_1 - B_2 \in L_1(\mathcal{M}, \tau).$$

(ii) $\Rightarrow$ (i) Имеем $U - A = I - A - (I - U) \in L_1(\mathcal{M}, \tau)$. $\square$

Следствие 4.3. В условиях теоремы 4.5 имеем

- (i) $[U, A] \in L_1(\mathcal{M}, \tau)$;
- (ii) $\tau(U - A) \in \mathbb{R} \iff \tau(I - U) \in \mathbb{R}$;

(iii) если еще $U = U^*$, то $\tau([U, A]) = 0$.

Доказательство. (i) Имеем

$$[U, A] = (I - A)U - U(I - A) \in L_1(\mathcal{M}, \tau).$$

(iii) В силу леммы 3.3 получаем $\tau((I - A)U) \in \mathbb{R}$, поэтому

$$\begin{aligned} \tau([U, A]) &= \tau((I - A)U) - \tau(U(I - A)) = \tau((I - A)U) - \tau(((I - A)U)^*) = \\ &= \tau((I - A)U) - \overline{\tau((I - A)U)} = 0. \end{aligned}$$

При $\tau(I) = 1$ в силу леммы 3.5 имеем $\|I + z[U, A]\|_1 \geq 1$ для всех $z \in \mathbb{C}$. $\square$

Предложение 4.6. Если $U \in \mathcal{M}$ — унитарный оператор и $A \in \widetilde{\mathcal{M}}$, то $|[U, A]| = |A - U^*AU|$.

Доказательство. Имеем

$$|[U, A]|^2 = A^*A - A^*U^*AU - U^*A^*UA + U^*A^*AU = |A - U^*AU|^2,$$

и утверждение следует из единственности квадратного корня из неотрицательного τ -измеримого оператора. $\square$

Теорема 4.6. Пусть операторы $A, B \in \mathcal{M}$ таковы, что $I - A, I - B \in \mathfrak{M}_\tau$. Тогда $[A, B] \in \mathfrak{M}_\tau$ и

$$|\tau([A, B])| \leq (1 + \|B\|)\|I - A\|_1 + (1 + \|A\|)\|I - B\|_1.$$

Доказательство. Напомним, что

$$|\tau(XY)| \leq \|X\|\tau(|Y|) \quad \text{для всех } X \in \mathcal{M}, \quad Y \in \mathfrak{M}_\tau \quad (7)$$

(см. [26, гл. V, § 2, формула (2)]). Имеем

$$I - AB = A(I - B) + I - A \in \mathfrak{M}_\tau$$

и в силу неравенства треугольника для $\mathbb{C}$ и (7) получаем

$$\begin{aligned} |\tau([A, B])| &= |\tau(I - BA - (I - AB))| \leq |\tau(I - BA)| + |\tau(I - AB)| = \\ &= |\tau(B(I - A) + I - B)| + |\tau(A(I - B) + I - A)| \leq \\ &\leq |\tau(B(I - A))| + |\tau(I - B)| + |\tau(A(I - B))| + |\tau(I - A)| \leq \\ &\leq (1 + \|B\|)\|I - A\|_1 + (1 + \|A\|)\|I - B\|_1. \end{aligned}$$

Теорема доказана. $\square$

Следствие 4.4. Пусть оператор $A \in \mathcal{M}$ таков, что $I - A \in \mathfrak{M}_\tau$. Тогда

$$[A^*, A] \in \mathfrak{M}_\tau, \quad |\tau([A^*, A])| \leq 2(1 + \|A\|)\|I - A\|_1.$$

Теорема 4.7. Пусть $A \in \widetilde{\mathcal{M}}$ и $0 < p, q, r \leq \infty$, причем $1/p + 1/q = 1/r$. Если

$$\operatorname{Re} A \in L_p(\mathcal{M}, \tau), \quad \operatorname{Im} A \in L_q(\mathcal{M}, \tau),$$

то

$$[A^*, A] \in L_r(\mathcal{M}, \tau), \quad \|[A^*, A]\|_r \leq 2^{\max\{1+1/r, 2\}} \|\operatorname{Re} A\|_p \|\operatorname{Im} A\|_q.$$

Доказательство. Положим $\|\cdot\|_\infty = \|\cdot\|$ и $L_\infty(\mathcal{M}, \tau) = \mathcal{M}$. Заметим, что

$$2[A^*, A] = [A + A^*, A - A^*] = 4i[\operatorname{Re} A, \operatorname{Im} A]. \quad (8)$$

В [21, предложение 6] для $0 < r \leq 1$ установлено, что

$$\|X + Y\|_r \leq 2^{1/r-1}(\|X\|_r + \|Y\|_r) \quad \text{для всех } X, Y \in L_r(\mathcal{M}, \tau). \quad (9)$$

Если $X \in L_p(\mathcal{M}, \tau)$ и $Y \in L_q(\mathcal{M}, \tau)$, то $XY \in L_r(\mathcal{M}, \tau)$ и в силу [21, лемма 1] имеем

$$\|XY\|_r \leq \|X\|_p \|Y\|_q. \quad (10)$$

Используя неравенство треугольника (при $r \geq 1$) или (9) (при $0 < r \leq 1$), а затем дважды применяя неравенство (10), из (8) получаем нужную оценку. Теорема доказана. $\square$

Замечание 4.1. Если оператор $A \in \widetilde{\mathcal{M}}^+$ и $P \in \mathcal{M}^{\text{pr}}$ таковы, что $AP + PA \geq 0$, то $[A, P] = 0$ в силу [6, лемма 2]. В [15] установлены достаточные условия того, что $XY, YX \in L_1(\mathcal{M}, \tau)$ для операторов $X, Y \in \widetilde{\mathcal{M}}$. Для таких операторов имеем $\tau([X, Y]) = 0$ в силу леммы 3.1. В [7] установлены достаточные условия τ -компактности произведения τ -измеримых операторов. Иногда эти условия обеспечивают τ -компактность коммутаторов этих операторов.

Теорема 4.8. Пусть операторы $X \in \widetilde{\mathcal{M}}^+$, $Y \in \widetilde{\mathcal{M}}^{\text{sa}}$ таковы, что $[X^{1/2}, YX^{1/2}] \in L_1(\mathcal{M}, \tau)$. Тогда $\tau([X^{1/2}, YX^{1/2}]) = it$, где $t \in \mathbb{R}$ и $t = 0$ при $XY \in L_1(\mathcal{M}, \tau)$.

Доказательство. Имеем $X^{1/2}YX^{1/2} - XY = ([X^{1/2}, YX^{1/2}])^* \in L_1(\mathcal{M}, \tau)$. Положим

$$A = X^{1/2}, \quad B = [X^{1/2}, Y].$$

Тогда операторы $XY - X^{1/2}YX^{1/2} = AB$, $X^{1/2}YX^{1/2} - YX = BA = [X^{1/2}, YX^{1/2}]$ лежат в $L_1(\mathcal{M}, \tau)$ и $\tau(AB) = \tau(BA)$ в силу леммы 3.1. Поскольку $AB = -(BA)^*$, в силу леммы 3.4 имеем

$$\tau(AB) = \tau(-(BA)^*) = -\tau((BA)^*) = -\overline{\tau(BA)} = -\overline{\tau(AB)}.$$

Следовательно, $\tau(AB) = \tau([X^{1/2}, YX^{1/2}]) = it$ с некоторым $t \in \mathbb{R}$. Поэтому

$$\tau(XY + YX - 2X^{1/2}YX^{1/2}) = 0. \quad (11)$$

Пусть теперь $XY \in L_1(\mathcal{M}, \tau)$ и $Y = Y_+ - Y_-$ — разложение Жордана, где $Y_+, Y_- \in \widetilde{\mathcal{M}}^+$, $Y_+Y_- = 0$, и пусть $P_+, P_- \in \mathcal{M}^{\text{pr}}$ — носители операторов Y_+ и Y_- соответственно. Если $A \in \mathcal{M}$ и $B \in \widetilde{\mathcal{M}}$, то $\mu_t(AB) \leq \|A\|\mu_t(B)$ для всех $t > 0$ (см. [19, 27]). Поэтому операторы $XY_+ = XYP_+$ и $XY_- = XYP_-$ лежат в $L_1(\mathcal{M}, \tau)$. Теперь в силу леммы 3.2 имеем $X^{1/2}Y_+X^{1/2}, X^{1/2}Y_-X^{1/2} \in L_1(\mathcal{M}, \tau)$ (тем самым и $X^{1/2}YX^{1/2} \in L_1(\mathcal{M}, \tau)$) и

$$\tau(XY) = \tau(XY_+) - \tau(XY_-) = \tau(X^{1/2}Y_+X^{1/2}) - \tau(X^{1/2}Y_-X^{1/2}) = \tau(X^{1/2}YX^{1/2}) \geq 0.$$

Поэтому

$$\tau(YX) = \tau((XY)^*) = \overline{\tau(XY)} = \overline{\tau(X^{1/2}YX^{1/2})} = \tau(X^{1/2}YX^{1/2})$$

в силу леммы 3.4. Теорема доказана. $\square$

Следствие 4.5. Пусть $\tau(I) = 1$ и операторы $X \in \widetilde{\mathcal{M}}^+$, $Y \in \widetilde{\mathcal{M}}^{\text{sa}}$ таковы, что $[X^{1/2}, YX^{1/2}] \in L_1(\mathcal{M}, \tau)$. Тогда $\|I + z(XY + YX - 2X^{1/2}YX^{1/2})\|_1 \geq 1$ для всех $z \in \mathbb{C}$.

Доказательство. Утверждение вытекает из (11) и леммы 3.5. $\square$

Линеал $\mathcal{E}$ в $\widetilde{\mathcal{M}}$ называется *идеальным пространством* на $(\mathcal{M}, \tau)$, если

- (1) из $X \in \mathcal{E}$ следует, что $X^* \in \mathcal{E}$;
- (2) из $X \in \mathcal{E}$, $Y \in \widetilde{\mathcal{M}}$ и $|Y| \leq |X|$ следует, что $Y \in \mathcal{E}$.

Таковы, например, $\mathcal{M}$, совокупность элементарных операторов $\mathcal{F}(\mathcal{M})$, $\widetilde{\mathcal{M}}_0$, $(L_1 + L_\infty)(\mathcal{M}, \tau)$ и $L_p(\mathcal{M}, \tau)$ при $0 < p < +\infty$. Если $\mathcal{E}$ — идеальное пространство на $(\mathcal{M}, \tau)$, $X \in \mathcal{E}$ и $Y, Z \in \mathcal{M}$, то $YXZ \in \mathcal{E}$.

Следующая гипотеза усиливает теорему 3 из [1] и теорему 1 из [14] (см. лемму 3.2).

Гипотеза. Пусть τ — точный нормальный полукопечный след на алгебре фон Неймана $\mathcal{M}$ и $\mathcal{E}$ — идеальное пространство на $(\mathcal{M}, \tau)$. Если $X, Y \in \widetilde{\mathcal{M}}^+$ и $XY + YX \in \mathcal{E}$, то $X^{1/2}YX^{1/2}, Y^{1/2}XY^{1/2} \in \mathcal{E}$.

Покажем, что в частном случае, когда

$$Y = \sum_{k=1}^n \lambda_k P_k, \quad \lambda_k > 0, \quad P_k \in \mathcal{M}^{\text{pr}}, \quad P_k P_j = 0 \quad \text{при } k \neq j, \quad k, j = 1, \dots, n,$$

наша гипотеза верна. Имеем

$$P = \sum_{k=1}^n P_k \in \mathcal{M}^{\text{pr}}.$$

Оператор

$$Z = P(XY + YX)P = 2 \sum_{k=1}^n \lambda_k P_k X P_k + \sum_{\substack{k=1, \\ j < k}}^n (\lambda_k + \lambda_j) (P_k X P_j + P_j X P_k)$$

лежит в $\mathcal{E}$. Тогда $P_k X P_j = (\lambda_k + \lambda_j)^{-1} P_k Z P_j \in \mathcal{E}$, $k, j = 1, \dots, n$. Теперь

$$Y^{1/2} X Y^{1/2} = \sum_{k=1}^n \lambda_k^{1/2} P_k \cdot X \cdot \sum_{k=1}^n \lambda_k^{1/2} P_k = \sum_{k=1}^n \lambda_k P_k X P_k + \sum_{\substack{k=1, \\ j < k}}^n (\lambda_k \lambda_j)^{1/2} (P_k X P_j + P_j X P_k) \in \mathcal{E}.$$

Пусть $X^{1/2} Y^{1/2} = U |X^{1/2} Y^{1/2}|$ — полярное разложение оператора $X^{1/2} Y^{1/2}$. Тогда

$$X^{1/2} Y X^{1/2} = (Y^{1/2} X^{1/2})^* (Y^{1/2} X^{1/2}) = U Y^{1/2} X^{1/2} (Y^{1/2} X^{1/2})^* U^* = U Y^{1/2} X Y^{1/2} U^* \in \mathcal{E}.$$

Замечание 4.2. Гипотеза верна для $X \in \mathcal{E} \cap \mathcal{M}^+$ и $Y \in \mathcal{M}^+$ (см. [22, предложение 14]; для $\mathcal{M} = \mathcal{B}(\mathcal{H})$ и $\tau = \text{tr}$ см. [20]). В [11] установлены коммутаторные неравенства, связанные с полярными разложениями τ -измеримых операторов. В [12, 25] были усилены [1, теорема 3] и [14, теорема 1].

СПИСОК ЛИТЕРАТУРЫ

1. Бикчентаев А. М. Об одном свойстве L_p -пространств на полуконечных алгебрах фон Неймана // Мат. заметки. — 1998. — 64, № 2. — С. 185–190.
2. Бикчентаев А. М. К теории τ -измеримых операторов, присоединенных к полуконечной алгебре фон Неймана // Мат. заметки. — 2015. — 98, № 3. — С. 337–348.
3. Бикчентаев А. М. О сходимости интегрируемых операторов, присоединенных к конечной алгебре фон Неймана // Тр. Мат. ин-та РАН им. В. А. Стеклова. — 2016. — 293. — С. 73–82.
4. Бикчентаев А. М. Об идемпотентных τ -измеримых операторах, присоединенных к алгебре фон Неймана // Мат. заметки. — 2016. — 100, № 4. — С. 492–503.
5. Бикчентаев А. М. След и интегрируемые операторы, присоединенные к полуконечной алгебре фон Неймана // Докл. РАН. — 2016. — 466, № 2. — С. 137–140.
6. Бикчентаев А. М. Об операторно монотонных и операторно выпуклых функциях // Изв. вузов. Мат. — 2016. — 5. — С. 70–74.
7. Бикчентаев А. М. О τ -компактности произведения τ -измеримых операторов, присоединенных к полуконечной алгебре фон Неймана // Итоги науки и техн. Совр. мат. прилож. Тематич. обзоры. — 2017. — 140. — С. 78–87.
8. Бикчентаев А. М. Разности идемпотентов в C^* -алгебрах и квантовый эффект Холла // Теор. мат. физ. — 2018. — 195, № 1. — С. 75–80.
9. Глазман И. М., Любич Ю. И. Конечномерный линейный анализ. — М.: Наука, 1969.
10. Гохберг И. Ц., Крейн М. Г. Введение в теорию линейных несамосопряженных операторов. — М.: Наука, 1965.
11. Дауитбек Д., Токмагамбетов Н. Е., Туленов К. С. Коммутаторные неравенства, связанные с полярными разложениями τ -измеримых операторов // Изв. вузов. Мат. — 2014. — 7. — С. 56–62.
12. Сукочев Ф. А. О гипотезе А. М. Бикчентаева // Изв. вузов. Мат. — 2012. — 6. — С. 67–70.
13. Халмош П. Гильбертово пространство в задачах. — М.: Мир, 1970.
14. Bikchentaev A. M. Majorization for products of measurable operators // Int. J. Theor. Phys. — 1998. — 37, № 1. — С. 571–576.
15. Bikchentaev A. M. Integrable products of measurable operators // Lobachevskii J. Math. 2016. — 37, № 4. — С. 397–403.
16. Brown L. G., Kosaki H. Jensen's inequality in semifinite von Neumann algebras // J. Operator Theory. — 1990. — 23, № 1. — С. 3–19.
17. Dykema K. J., Kalton N. J. Sums of commutators in ideals and modules of type II factors // Ann. Inst. Fourier (Grenoble). — 2005. — 55, № 3. — С. 931–971.
18. Dykema K., Skripka A. On single commutators in II_1 -factors // Proc. Am. Math. Soc. — 2012. — 140, № 3. — С. 931–940.
19. Fack T., Kosaki H. Generalized s -numbers of τ -measurable operators // Pac. J. Math. — 1986. — 123, № 2. — С. 269–300.

20. *Hiai F., Kosaki H.* Means of Hilbert space operators/ Lect. Notes Math. — Berlin: Springer-Verlag, 2003. — 1820.
21. *Kosaki H.* On the continuity of the map $\varphi \mapsto |\varphi|$ from the predual of a W^* -algebra// J. Funct. Anal. — 1984. — 59, № 1. — С. 123–131.
22. *Larotonda G.* Norm inequalities in operator ideals// J. Funct. Anal. — 2008. — 255, № 11. — С. 3208–3228.
23. *Nelson E.* Notes on non-commutative integration// J. Funct. Anal. — 1974. — 15, № 2. — С. 103–116.
24. *Segal I. E.* A noncommutative extension of abstract integration// *Ann. Math.* — 1953. — 57, № 3. — С. 401–457. Рус. пер: Математика (сб. переводов). — 1962. — 6, № 1. — С. 65–132.
25. *Sukochev F. A.* On a conjecture of A. Bikchentaev// в сб.: «Spectral Analysis, Differential Equations and Mathematical Physics: A Festschrift in Honor of Fritz Gesztesy's 60th Bbirthday»/ Proc. Symp. Pure Math. — Providence, Rhode Island: Am. Math. Soc., 2013. — 87. — С. 327–339.
26. *Takesaki M.* Theory of operator algebras. Vol. I. — Berlin: Springer-Verlag, 1979.
27. *Yeadon F. J.* Noncommutative L^p -spaces// Math. Proc. Cambridge Phil. Soc. — 1975. — 77, № 1. — С. 91–102.

А. М. Бикчентаев

Казанский (Приволжский) федеральный университет

E-mail: Airat.Bikchentaev@kpfu.ru



ПРИМЕНЕНИЕ ДИФФЕРЕНЦИАЛЬНЫХ ОПЕРАТОРОВ ЛЕВИ В ТЕОРИИ КАЛИБРОВОЧНЫХ ПОЛЕЙ

© 2018 г. Б. О. ВОЛКОВ

Аннотация. Статья содержит обзор некоторых результатов о связи калибровочных полей и бесконечномерных уравнений на параллельный перенос, содержащих лапласиан Леви или ассоциированную с этим лапласианом дивергенцию. Параллельно рассматривается детерминистский случай, в котором параллельный перенос — это операторнозначный функционал на пространстве кривых, и случай так называемого исчисления Маллявэна, в котором (стохастический) параллельный перенос — это операторнозначный винеровский функционал.

Ключевые слова: лапласиан Леви, дивергенция Леви, калибровочные поля, уравнения Янга—Миллса, инстантоны, исчисление Маллявэна.

AMS Subject Classification: 60H40, 81T13

СОДЕРЖАНИЕ

1. Введение	21
2. След Леви и дифференциальные операторы Леви	23
3. Дифференциальные операторы Леви и уравнения Янга—Миллса	25
4. Дифференциальные операторы Леви и инстантоны	29
5. Дифференциальные операторы Леви в исчислении Маллявэна	30
6. Дифференциальные операторы Леви в исчислении Маллявэна и инстантоны	34
Список литературы	35

1. ВВЕДЕНИЕ

В 20-е годы прошлого века П. Леви ввел следующий бесконечномерный лапласиан, впоследствии названный его именем. Лапласиан Леви действует на функцию f , определенную на $L_2([0, 1], \mathbb{R})$, по формуле

$$\Delta_L f(x) = \lim_{n \rightarrow \infty} \frac{1}{n} \sum_{k=1}^n \langle f''(x) e_k, e_k \rangle,$$

где $\{e_n\}$ — ортонормированный базис в $L_2([0, 1], \mathbb{R})$. Такое определение существенно зависит от выбора ортонормированного базиса $\{e_n\}$. Иначе П. Леви определял бесконечномерный лапласиан как интегральный функционал, порожденный специальным видом второй производной. Дифференциальными операторами Леви (лапласианом Леви, даламбертианом Леви, дивергенцией Леви) называют дифференциальные операторы, действующие на функции различных функциональных пространств, определенные по аналогии с двумя оригинальными определениями лапласиана Леви на функциях из $L_2([0, 1], \mathbb{R})$. Задача о том, как связаны определения дифференциального оператора Леви с помощью чезаровского усреднения и с помощью интегрального функционала на одном пространстве функций, может оказаться нетривиальной.

Работа посвящена связи дифференциальных операторов Леви и калибровочных полей. Уравнения Янга—Миллса — это нелинейные дифференциальные уравнения второго порядка на связность в векторном расслоении. Эти уравнения инвариантны относительно калибровочных преобразований. Одна из основных причин интереса к дифференциальным операторам Леви заключается в том, что уравнения Янга—Миллса допускают переформулировки с помощью таких дифференциальных операторов. С одной стороны, параллельный перенос, порожденный связностью, будет удовлетворять уравнению, содержащему дивергенцию Леви и являющемуся бесконечномерным аналогом уравнения движения кирального поля, тогда и только тогда, когда соответствующая связность является решением уравнений Янга—Миллса; этот факт впервые был замечен И. Я. Арефьевой и И. В. Воловичем (см. [4]). С другой стороны, параллельный перенос является решением уравнения Лапласа для лапласиана Леви тогда и только тогда, когда соответствующая связность является решением уравнений Янга—Миллса. Таким образом, система конечномерных нелинейных уравнений является эквивалентной бесконечномерному линейному дифференциальному уравнению. Теорема об эквивалентности уравнения Лапласа для лапласиана Леви и параллельного переноса и уравнений Янга—Миллса была доказана Л. Аккарди, П. Гибилиско и И. В. Воловичем (см. [13]) для связности в тривиальном векторном расслоении над $\mathbb{R}^d$ и Р. Леандром и И. В. Воловичем (см. [26]) для связности в векторном расслоении над римановым многообразием.

В [4, 12, 13, 26] дифференциальные операторы Леви определялись с помощью интегрального функционала, порожденного специальным видом второй производной. Тот факт, что лапласиан Леви, связанный с уравнениями Янга—Миллса, можно определить с помощью чезаровского усреднения, было показано в работах автора (см. [7, 9]).

В стохастическом анализе дифференциальные операторы Леви можно определить с помощью исчисления Маллявэна — теории пространств Соболева над мерами на бесконечномерных пространствах. Р. Леандр и И. В. Волович с помощью интегрального функционала перенесли определение лапласиана Леви на пространство Соболева над мерой Винера (см. [26]). В работе [31] автора были введены лапласиан и дивергенция Леви на пространстве Соболева над мерой Винера, определенные с помощью чезаровского усреднения. В [26, 31] были получены условия в терминах дифференциальных операторов Леви и стохастического параллельного переноса, эквивалентные тому, что ассоциированная связность является решением уравнения Янга—Миллса. В отличие от детерминистского случая значения лапласианов Леви, введенных в [26, 31], на стохастическом параллельном переносе не совпадают. Критерии в терминах стохастического параллельного переноса, не использующие дифференциальные операторы Леви, что ассоциированная связность является решением уравнений Янга—Миллса, были получены в [15, 17, 18, 27].

Если связность в векторном расслоении над $\mathbb{R}^4$ является решением уравнений автодуальности, то она также будет и решением уравнений Янга—Миллса. В 2014 г. автору на семинаре отдела математической физики МИАН им. В. А. Стеклова была поставлена задача: можно ли с помощью лапласианов Леви переформулировать уравнения автодуальности? Фактически эта задача была поставлена и в обзоре Л. Аккарди [11]. В работе автора [9] было показано, что уравнения автодуальности действительно можно сформулировать в терминах параллельного переноса и лапласианов Леви. В этой работе рассматривался только детерминистский случай. Как результаты работы [9] переносятся на случай исчисления Маллявэна, показано в конце настоящей статьи.

Настоящая работа содержит обзор теорем о связи дифференциальных операторов Леви и уравнений Янга—Миллса для связности в тривиальном векторном расслоении над $\mathbb{R}^d$ и уравнений автодуальности для связности в тривиальном векторном расслоении над $\mathbb{R}^4$ в детерминистском случае и в случае исчисления Маллявэна. Теоремы будут сформулированы в единообразной форме; при этом дифференциальные операторы Леви будут определены с помощью чезаровского усреднения.

Статья устроена следующим образом. В разделе 2 приводятся различные определения лапласиана и дивергенции Леви в терминах следов Леви. Во разделах 3 и 4 приводятся формулировки теорем о связи дифференциальных операторов Леви соответственно с уравнениями Янга—Миллса и уравнениями автодуальности в детерминистском случае. В разделах 5 и 6 рассматривается связь дифференциальных операторов Леви соответственно с уравнениями Янга—Миллса и уравнениями автодуальности в случае исчисления Маллявэна.

2. След Леви и дифференциальные операторы Леви

В этом разделе мы приведем различные определения лапласиана и дивергенции Леви. Определения будут даны в единообразной форме, несколько отличной от той, в которой эти определения были даны изначально. В этом разделе мы частично следуем изложению работы [30].

Пусть E и V — вещественные локально выпуклые пространства. Везде ниже символом $C(E, V)$ обозначается пространство непрерывных функций из E в V , символом $C^n(E, V)$ — пространство n раз дифференцируемых по Фреше функций из E в V (подробное изложение теории дифференцирования на линейных топологических пространствах см., например, в [1]), а символом $L(E, V)$ — пространство линейных непрерывных отображений из E в V . Пусть E^* — пространство, сопряженное к E . Если $f \in C^2(E, \mathbb{R})$, то $f'(x) \in E^*$ и $f''(x) \in L(E, E^*)$ для каждого $x \in E$. Если $B \in C^1(E, E^*)$, то $B'(x) \in L(E, E^*)$ для каждого $x \in E$. Пусть $\mathcal{F}(E, \mathbb{R})$ — пространство $\mathbb{R}$ -значных функций на E .

Пусть $S : \text{dom } S \rightarrow \mathbb{R}$ — линейный функционал, причем $\text{dom } S \subset L(E, E^*)$. Функционал S определяет линейный дифференциальный оператор второго порядка $D^{2,S} : \text{dom } D^{2,S} \rightarrow \mathcal{F}(E, \mathbb{R})$, действующий по формуле

$$D^{2,S} f(x) = S(f''(x)),$$

где

$$\text{dom } D^{2,S} = \left\{ f \in C^2(E, \mathbb{R}) : f''(x) \in \text{dom } S \text{ для всех } x \in E \right\}.$$

Кроме того, функционал S определяет линейный дифференциальный оператор первого порядка $D^{1,S} : \text{dom } D^{1,S} \rightarrow \mathcal{F}(E, \mathbb{R})$, действующий по формуле

$$D^{1,S} B(x) = S(B'(x)),$$

где

$$\text{dom } D^{1,S} = \left\{ B \in C^1(E, E^*) : B'(x) \in \text{dom } S \text{ для всех } x \in E \right\}$$

(подробное изложение общей схемы определений дифференциальных операторов см. в [2]). Если выбрать $E = \mathbb{R}^d$ и $S = \text{tr}$ (след), то $D^{2,\text{tr}}$ — это конечномерный лапласиан Δ и $D^{1,\text{tr}}$ — это конечномерная дивергенция div .

Пусть теперь $E \subset H \subset E^*$ — оснащенное гильбертово пространство и $\{e_n\}$ — ортонормированный базис в вещественном сепарабельном гильбертовом пространстве H , состоящий из элементов E . След Леви $\text{tr}_L^{\{e_n\}} : \text{dom } \text{tr}_L^{\{e_n\}} \rightarrow \mathbb{R}$ определяется формулой

$$\text{tr}_L^{\{e_n\}} R = \lim_{n \rightarrow \infty} \frac{1}{n} \sum_{k=1}^n (R e_k, e_k), \quad (2.1)$$

где $\text{dom } \text{tr}_L^{\{e_n\}}$ состоит из всех отображений из $L(E, E^*)$, для которых правая часть (2.1) существует. Такое определение существенно зависит от выбора ортонормированного базиса $\{e_n\}$. Операторы $D^{1,\text{tr}_L^{\{e_n\}}}$ и $D^{2,\text{tr}_L^{\{e_n\}}}$ — это соответственно лапласиан Леви $\Delta_L^{\{e_n\}}$ и дивергенция Леви $\text{div}_L^{\{e_n\}}$. Заметим, что для $f \in C^2(E, \mathbb{R})$ выполняется равенство

$$\Delta_L^{\{e_n\}} f(x) = \text{div}_L^{\{e_n\}} f'(x).$$

Если выбрать $E = H = L_2([0, 1], \mathbb{R})$, то

$$\Delta_L^{\{e_n\}} = D^{2,\text{tr}_L^{\{e_n\}}}$$

— лапласиан, введенный П. Леви в [10].

Иначе П. Леви определял бесконечномерный лапласиан как интегральный функционал, порожденный специальным видом второй производной. Пусть dom tr_L — пространство таких билинейных функционалов K на $L_2([0, 1], \mathbb{R}) \times L_2([0, 1], \mathbb{R})$, что для всех $u, v \in L_2([0, 1], \mathbb{R})$ выполняется равенство

$$K(u, v) = \int_0^1 \int_0^1 K_V(t, s) u(t) v(s) dt ds + \int_0^1 K_L(t) u(t) v(t) dt, \quad (2.2)$$

где $K_V \in L_2([0, 1] \times [0, 1], \mathbb{R})$ и $K_L \in L_\infty([0, 1], \mathbb{R})$. Пусть след Леви $\text{tr}_L : \text{dom tr}_L \rightarrow \mathbb{R}$ действует по формуле

$$\text{tr}_L K = \int_0^1 K_L(t) dt.$$

Тогда лапласиан Леви Δ_L можно определить как дифференциальный оператор D^{2, tr_L} .

Определение 2.1 (П. Леви (см. [10])). Ортонормированный базис $\{e_n\}$ в $L_2([0, 1], \mathbb{R})$ называется *слабо равномерно плотным*, если

$$\lim_{n \rightarrow \infty} \int_0^1 h(t) \left(\frac{1}{n} \sum_{k=1}^n e_k^2(t) - 1 \right) dt = 0$$

для любой функции $h \in L_\infty([0, 1], \mathbb{R})$.

Пример 2.1. Пусть $h_n(t) = \sqrt{2} \sin(\pi n t)$. Ортонормированный базис $\{h_n\}_{n=1}^\infty$ является слабо равномерно плотным.

Очевидно, что, если $\{e_n\}$ — слабо равномерно плотный базис, то $\text{tr}_L \subset \text{tr}_L^{\{e_n\}}$ и, соответственно, $D^{2, \text{tr}_L} \subset D^{2, \text{tr}_L^{\{e_n\}}}$.

И. Я. Арефьева и И. В. Волович в связи с изучением калибровочных полей на физическом уровне строгости ввели дивергенцию Леви (см. [4], где использовался термин функциональная дивергенция). Л. Аккарди, П. Гибилско и И. В. Волович по аналогии с оператором Δ_L ввели в рассмотрение оператор, который также был назван лапласианом Леви (см. [12, 13]. В терминах следов Леви определения из [4, 12, 13] можно переформулировать следующим образом.

Пусть $\{p_1, p_2, \dots, p_d\}$ — ортонормированный базис в $\mathbb{R}^d$. Пусть $\delta = (\delta_{\mu\nu})$ — евклидова метрика на $\mathbb{R}^d$, $E = C^1([0, 1], \mathbb{R}^d)$, $E_0 = \{\gamma \in E : \gamma(0) = \gamma(1) = 0\}$, T_E^2 — пространство непрерывных билинейных функционалов на $E \times E$, ограничения которых на $E_0 \times E_0$ имеют вид

$$Q(u, v) = \int_0^1 \int_0^1 Q_{\mu\nu}^V(t, s) u^\mu(t) v^\nu(s) dt ds + \\ + \int_0^1 Q_{\mu\nu}^L(t) u^\mu(t) v^\nu(t) dt + \frac{1}{2} \int_0^1 Q_{\mu\nu}^S(t) (\dot{u}^\mu(t) v^\nu(t) + \dot{v}^\mu(t) u^\nu(t)) dt, \quad (2.3)$$

где

$$Q_{\mu\nu}^V \in L_1([0, 1] \times [0, 1], \mathbb{R}), \quad Q_{\mu\nu}^L \in L_1([0, 1], \mathbb{R}), \quad Q_{\mu\nu}^S \in L_\infty([0, 1], \mathbb{R}),$$

$Q_{\mu\nu}^L$ — симметричный тензор, т.е. $Q_{\mu\nu}^L = Q_{\nu\mu}^L$, и $Q_{\mu\nu}^S$ — антисимметричный тензор, т.е. $Q_{\mu\nu}^S = -Q_{\nu\mu}^S$.

Определение 2.2. След Леви tr_L — это линейный функционал на T_E^2 , определенный по формуле

$$\text{tr}_L Q = \int_0^1 Q_{\mu\nu}^L(t) \delta^{\mu\nu} dt. \quad (2.4)$$

В [12] была поставлена задача: можно ли представить лапласиан Леви, связанный с калибровочными полями, как среднее Чезаро вторых производных по направлению? Это действительно так.

Предложение 2.1. Пусть $\{h_n\}$ — слабо равномерно плотный базис в $L_2([0, 1], \mathbb{R})$, причем $h_n \in E_0$ для всех $n \in \mathbb{N}$, и пусть $e_n(t) = p_{a_n} h_{b_n}(t)$. Тогда $\text{tr}_L \subset d\text{tr}_L^{\{e_n\}}$ и соответственно

$$D^{1, \text{tr}_L} \subset dD^{1, \text{tr}_L^{\{e_n\}}}, \quad D^{2, \text{tr}_L} \subset dD^{2, \text{tr}_L^{\{e_n\}}}.$$

Замечание 2.1. Определения лапласианов Леви без изменения переносятся на функции, определенные на $W^{1,2}([0, 1], \mathbb{R}^d)$ и $W^{1,1}([0, 1], \mathbb{R}^d)$, и на функции, принимающие значения в конечномерных векторных пространствах.

Замечание 2.2. Если в определении следа Леви (2.4) заменить евклидову метрику на метрику Минковского, то след Леви будет порождать даламбертиан Леви (см. [12, 13]). Даламбертиан Леви и соответствующую дивергенцию можно определить и с помощью чезаровского усреднения (см. [8, 30]).

3. ДИФФЕРЕНЦИАЛЬНЫЕ ОПЕРАТОРЫ ЛЕВИ И УРАВНЕНИЯ ЯНГА—МИЛЛСА

Ниже греческие индексы пробегает $\{1, \dots, d\}$, если не оговорено обратное. Мы будем использовать обозначения Эйнштейна для суммирования и осуществлять опускание и подъем индексов с помощью евклидовой метрики.

Как и в предыдущем разделе, пусть $\{p_1, p_2, \dots, p_d\}$ — ортонормированный базис в $\mathbb{R}^d$. Ниже

$$H_0^1 = W_0^{1,2}([0, 1], \mathbb{R}^d) := \left\{ \gamma \in AC([0, 1], \mathbb{R}^d) : \dot{\gamma} \in L_2([0, 1], \mathbb{R}^d), \gamma(0) = 0 \right\}.$$

Это гильбертово пространство со скалярным произведением

$$(\gamma_1, \gamma_2)_{H_0^1} = \int_0^1 (\dot{\gamma}_1(t), \dot{\gamma}_2(t))_{\mathbb{R}^d} dt.$$

Мы считаем, что на $M_N(\mathbb{C})$ задана гильбертова норма $\|M\|^2 = \text{tr}(MM^*)$. Если $B — $M_N(\mathbb{C})$ -значный тензор ранга $(0, 2)$ над $\mathbb{R}^d$, то$

$$\|B\|^2 = \sum_{\mu=1}^d \sum_{\nu=1}^d \|B_{\mu\nu}\|^2.$$

Пусть $\mathfrak{H}^0 = L_2([0, 1], M_N(\mathbb{C}))$ и $(\cdot, \cdot)_{\mathfrak{H}^0}$ — скалярное произведение на этом пространстве.

Ниже связность в тривиальном векторном расслоении с базой $\mathbb{R}^d$, слоем $\mathbb{C}^N$ и структурной группой $U(N)$ задана на $\mathbb{R}^d$ как $u(N)$ -значная C^∞ -гладкая 1-форма $A(x) = A_\mu(x) dx^\mu$, определенная на $\mathbb{R}^d$. Если $\phi \in C^1(\mathbb{R}^d, u(N))$, то ковариантная производная $\nabla\phi$, заданная связностью A , определяется формулой $\nabla_\mu \phi = \partial_\mu \phi + [A_\mu, \phi]$. Соответствующая связности кривизна — это $u(N)$ -значная C^∞ -гладкая 2-форма

$$F(x) = \sum_{\mu < \nu} F_{\mu\nu}(x) dx^\mu \wedge dx^\nu, \quad \text{где} \quad F_{\mu\nu} = \partial_\mu A_\nu - \partial_\nu A_\mu + [A_\mu, A_\nu].$$

Функционал действия Янга—Миллса определяется формулой

$$S(A) = \frac{1}{2} \int_{\mathbb{R}^d} \|F(x)\|^2 dx. \quad (3.1)$$

Уравнения Янга—Миллса — это уравнения на связность A :

$$\nabla^\mu F_{\mu\nu} = \sum_{\mu=1}^d (\partial_\mu F_{\mu\nu} + [A_\mu, F_{\mu\nu}]) = 0. \quad (3.2)$$

Эти уравнения являются уравнениями Эйлера—Лагранжа для функционала действия (3.1). Калибровочное преобразование — это отображение $g \in C^\infty(\mathbb{R}^d, U(N))$, которое действует на связность по формуле

$$A_\mu(x) \rightarrow A'_\mu(x) = g^{-1}(x)A_\mu(x)g(x) + g^{-1}(x)\partial_\mu g(x),$$

а на кривизну — по формуле

$$F_{\mu\nu}(x) \rightarrow F'_{\mu\nu}(x) = g^{-1}(x)F_{\mu\nu}(x)g(x).$$

Таким образом, функция Лагранжа в (3.1) инвариантна относительно действия калибровочных преобразований.

Параллельный перенос $U_t^A(\gamma)$ вдоль кривой $\gamma \in H_0^1$, порожденный связностью A , — это решение дифференциального уравнения, записанного в интегральной форме:

$$U_t^A(\gamma) = I_N - \int_0^t A_\mu(\gamma(s))U_s^A(\gamma)\dot{\gamma}^\mu(s)ds. \quad (3.3)$$

У этого уравнения имеется единственное решение класса $AC([0, 1], M_N(\mathbb{C}))$.

Пусть $L_{\mu\nu}(\gamma, t)$ и $J_{\lambda\mu\nu}(\gamma, t)$ для всех $\gamma \in H_0^1$ и $t \in [0, 1]$ определены следующим образом:

$$\begin{aligned} L_{\mu\nu}(\gamma, t) &= U_t^A(\gamma)^{-1}F_{\mu\nu}(\gamma(t))U_t^A(\gamma), \\ J_{\lambda\mu\nu}(\gamma, t) &= U_t^A(\gamma)^{-1}\nabla_\lambda F_{\mu\nu}(\gamma(t))U_t^A(\gamma). \end{aligned}$$

Предложение 3.1. *Функция $H_0^1 \ni \gamma \rightarrow U_1^A(\gamma)$ бесконечно дифференцируема по Фреше, причем для $u \in H_0^1$ выполняется соотношение*

$$\partial_u U_1^A(\gamma) = -U_1^A(\gamma) \int_0^1 L_{\mu\nu}(\gamma, t)u^\mu(t)\dot{\gamma}^\nu(t)dt - A_\mu(\gamma(1))u^\mu(1)U_1^A(\gamma).$$

Для доказательства см. [21] (см. также [13, 20]).

Определение 3.1. Если $f \in C^1(H_0^1, M_N(\mathbb{C}))$, то α_0 -градиент $\text{grad}_{\alpha_0} f$ отображения f — это такой элемент из $C(H_0^1, \mathfrak{H}^0)$, что

$$\left(\text{grad}_{\alpha_0} f(\gamma), M \otimes h \right)_{\mathfrak{H}^0} = \left(\partial_h f(\gamma), M \right)_{M_N(\mathbb{C})}$$

для всех $\gamma \in H_0^1$, всех таких $h \in H_0^1$, что $h(1) = 0$, и всех $M \in M_N(\mathbb{C})$.

Конечно, у отображения $f \in C^1(H_0^1, M_N(\mathbb{C}))$ может не существовать α_0 -градиент.

Замечание 3.1. В [23] векторное расслоение над гильбертовым многообразием H^1 -путей в конечномерном римановом многообразии M , слоем которого над кривой является пространство H^0 -полей над этой кривой, обозначается символом α_0 . Определение α_0 -градиента переносится на пространство функций на гильбертовом многообразии H^1 -путей, что позволяет перенести определение лапласиана Леви на случай многообразия (ср. [26]).

Прямым следствием предложения 3.1 является следующее утверждение.

Предложение 3.2. *Имеет место соотношение*

$$\left(\text{grad}_{\alpha_0} U_1^A(\gamma) \right)_\mu(t) = -U_1^A(\gamma)L_{\mu\nu}(\gamma, t)\dot{\gamma}^\nu(t). \quad (3.4)$$

Мы изменим определения дивергенции Леви и лапласиана Леви из предыдущего раздела, так как измененные определения можно будет перенести на случай риманова многообразия.

Определение 3.2. Дивергенция Леви $\operatorname{div}_L^{\{e_n\}}$, порожденная ортонормированным базисом $\{e_n\}$ в $L_2([0, 1], \mathbb{R}^d)$, состоящим из элементов H_0^1 , — это линейное отображение из $\operatorname{dom} \operatorname{div}_L^{\{e_n\}}$ в пространство всех $M_N(\mathbb{C})$ -значных функций на H_0^1 , определенное формулой

$$\operatorname{div}_L^{\{e_n\}} B(\gamma) = \lim_{n \rightarrow \infty} \frac{1}{n} \sum_{k=1}^n d_{e_k} B(\gamma)(e_k), \quad (3.5)$$

где $\operatorname{dom} \operatorname{div}_L^{\{e_n\}}$ состоит из всех $B \in C^1(H_0^1, \mathfrak{H}^0)$, для которых правая часть (3.5) существует для всех $\gamma \in H_0^1$.

Определение 3.3. Лапласиан Леви $\Delta_L^{\{e_n\}}$, порожденный ортонормированным базисом $\{e_n\}$ в $L_2([0, 1], \mathbb{R}^d)$, состоящим из элементов H_0^1 , — это линейное отображение из $\operatorname{dom} \Delta_L^{\{e_n\}}$ в пространство всех $M_N(\mathbb{C})$ -значных функций на H_0^1 , действующее по формуле

$$\Delta_L^{\{e_n\}} f(\gamma) = \operatorname{div}_L^{\{e_n\}} \operatorname{grad}_{\alpha_0} f(\gamma), \quad (3.6)$$

где $\operatorname{dom} \Delta_L^{\{e_n\}}$ состоит из всех $f \in C^2(H_0^1, M_N(\mathbb{C}))$, для которых правая часть (3.6) существует.

Пусть $B^A \in C^1(H_0^1, \mathfrak{H}^0)$ определена формулой

$$B^A(\gamma) = (U_1^A(\gamma))^{-1} \operatorname{grad}_{\alpha_0} U_1^A(\gamma). \quad (3.7)$$

Предложение 3.3. Для всех $u, v \in H_0^1$, удовлетворяющих условию $u(1) = v(1) = 0$, выполняются соотношения

$$\begin{aligned} \partial_u B^A(\gamma) v = & \int_0^1 \left[L_{\mu\lambda}(\gamma, t) u^\mu(t) \dot{\gamma}^\lambda(t), \int_0^t L_{\nu\kappa}(\gamma, s) v^\nu(s) \dot{\gamma}^\kappa(s) ds \right] dt + \\ & + \int_0^1 \left[L_{\nu\kappa}(\gamma, t) v^\nu(t) \dot{\gamma}^\kappa(t), \int_0^t L_{\mu\lambda}(\gamma, s) u^\mu(s) \dot{\gamma}^\lambda(s) ds \right] dt - \\ & - \frac{1}{2} \int_0^1 \left(J_{\nu\mu\lambda}(\gamma, t) + J_{\mu\nu\lambda}(\gamma, t) \right) u^\mu(t) v^\nu(t) \dot{\gamma}^\lambda(t) dt - \\ & - \frac{1}{2} \int_0^1 L_{\mu\nu}(\gamma, t) \left(v^\mu(t) \dot{u}^\nu(t) + u^\mu(t) \dot{v}^\nu(t) \right) dt, \quad (3.8) \end{aligned}$$

$$\begin{aligned} \partial_v \partial_u U_1^A(\gamma) = & U_1^A(\gamma) \int_0^1 L_{\mu\lambda}(\gamma, t) u^\mu(t) \dot{\gamma}^\lambda(t) \left(\int_0^t L_{\nu\kappa}(\gamma, s) v^\nu(s) \dot{\gamma}^\kappa(s) ds \right) dt + \\ & + U_1^A(\gamma) \int_0^1 L_{\nu\kappa}(\gamma, t) v^\nu(t) \dot{\gamma}^\kappa(t) \left(\int_0^t L_{\mu\lambda}(\gamma, s) u^\mu(s) \dot{\gamma}^\lambda(s) ds \right) dt - \\ & - U_1^A(\gamma) \left(\frac{1}{2} \int_0^1 \left(J_{\nu\mu\lambda}^x(\gamma, t) + J_{\mu\nu\lambda}^x(\gamma, t) \right) u^\mu(t) v^\nu(t) \dot{\gamma}^\lambda(t) dt + \right. \\ & \left. + \frac{1}{2} \int_0^1 L_{\mu\nu}^x(\gamma, t) \left(v^\mu(t) \dot{u}^\nu(t) + u^\mu(t) \dot{v}^\nu(t) \right) dt \right). \quad (3.9) \end{aligned}$$

Формула (3.9) была доказана в [13] (см. также [9]). Формула (3.8) является следствием формулы (3.9).

Теорема 3.1. Пусть в $L_2([0, 1], \mathbb{R}^d)$ выбран ортонормированный базис $e_n(t) = p_{a_n} h_{b_n}(t)$, где

$$a_n = n - d \left\lfloor \frac{n-1}{d} \right\rfloor, \quad b_n = \left\lfloor \frac{n+d-1}{d} \right\rfloor,$$

$\{h_n\}$ — слабо равномерно плотный базис в $L_2([0, 1], \mathbb{R})$, причем $h_n \in W_0^{1,2}([0, 1], \mathbb{R})$ и $h_n(1) = 0$ для всех $n \in \mathbb{N}$. Выполняются следующие равенства:

$$\begin{aligned} \operatorname{div}_L^{\{e_n\}} B^A(\gamma) &= -\frac{1}{d} \int_0^1 J^\mu_{\mu\nu}(\gamma, t) \dot{\gamma}^\nu(t) dt, \\ \Delta_L^{\{e_n\}} U_1^A(\gamma) &= -\frac{1}{d} U_1^A(\gamma) \int_0^1 J^\mu_{\mu\nu}(\gamma, t) \dot{\gamma}^\nu(t) dt. \end{aligned} \quad (3.10)$$

Теорема 3.1 является прямым следствием предложения 3.3.

Теорема 3.2. Пусть базис $\{e_n\}$ определен, как в формулировке предыдущей теоремы. Следующие условия равносильны:

- (1) связность A на $\mathbb{R}^d$ является решением уравнений Янга—Миллса (3.2);
- (2) B^A является решением уравнения

$$\operatorname{div}_L^{\{e_n\}} B^A = 0; \quad (3.11)$$

- (3) параллельный перенос U_1^A является решением уравнения Лапласа для лапласиана $\Delta_L^{\{e_n\}}$:

$$\Delta_L^{\{e_n\}} U_1^A = 0.$$

Теорема 3.2 является следствием предыдущей теоремы 3.1. Эквивалентность условий (1) и (3) — это теорема Аккарди—Гибилеско—Воловича, которая была изначально доказана для лапласиана Леви, определенного с помощью интегрального функционала (см. [12, 13]).

Замечание 3.2. Теорема 3.2 переносится без изменений для даламбертиана Леви и соответствующей дивергенции и для уравнений Янга—Миллса на пространстве Минковского (см. [13, 30]). О связи даламбертиана Леви и соответствующей дивергенции с уравнениями Янга—Миллса—Дирака (уравнениями квантовой хромодинамики) см. [8, 30]. О связи этих операторов с уравнениями Янга—Миллса—Хиггса см. [30].

Замечание 3.3. Поле $g : \mathbb{R}^d \rightarrow U(N)$ называется главным киральным полем (см., например, [5, 6]). Его интеграл Дирихле имеет вид

$$\frac{1}{2} \int_{\mathbb{R}^d} \operatorname{tr} \left(\partial_\mu g(x) \partial^\mu g^{-1}(x) \right) dx = -\frac{1}{2} \int_{\mathbb{R}^d} \operatorname{tr} (Z_\mu(x) Z^\mu(x)) dx, \quad (3.12)$$

где $Z_\mu = g^{-1}(x) \partial_\mu g(x)$. Уравнения движения кирального поля имеют вид

$$\begin{cases} \operatorname{div} Z = 0, \\ \partial_\mu Z_\nu - \partial_\nu Z_\mu + [Z_\mu, Z_\nu] = 0, \end{cases} \quad (3.13)$$

где $Z = (Z_1, \dots, Z_d)$. Параллельный перенос можно рассматривать как киральное поле на бесконечномерном пространстве H_0^1 . Уравнение (3.11) является бесконечномерным аналогом первого уравнения системы (3.13). В [4] на физическом уровне строгости рассматривались законы сохранения для теории Янга—Миллса на $\mathbb{R}^3$ (см. также [29]). Было показано, что, если связность A является решением уравнений Янга—Миллса, то можно построить семейство сохраняющихся токов, первым элементом которого является B^A . Сохранение тока понималось в смысле (3.11).

Связь между киральными полями и полями Янга—Миллса заключается в том числе в следующем. Из некоммутативной леммы Пуанкаре, доказанной в [21], следует, что, при некоторых дополнительных условиях, если $B \in C^1(H_0^1, \mathfrak{H}^0)$ удовлетворяет бесконечномерным аналогам уравнений (3.13), то существует такая связность A , что $B = B^A$ и A является решением уравнений Янга—Миллса (см. [30]).

Замечание 3.4. Определение лапласиана Леви как интегрального функционала было перенесено на случай риманова многообразия в работе [26] Р. Леандра и И. В. Воловича. В этой статье было показано, что теорема об эквивалентности уравнений Янга—Миллса и уравнения Лапласа для лапласиана Леви верна и в этом случае. Определение лапласиана Леви с помощью чезаровского усреднения вторых производных по направлению было перенесено на случай риманова многообразия в работе [3] Л. Аккарди и О. Г. Смолянова. Теорема об эквивалентности уравнений Янга—Миллса и уравнения Лапласа—Леви для такого определения была доказана напрямую (см. [7]), при этом связь определений из [3, 26] не исследовалась. В нашей следующей статье мы покажем, что второе определение лапласиана Леви на многообразии является расширением первого.

4. ДИФФЕРЕНЦИАЛЬНЫЕ ОПЕРАТОРЫ ЛЕВИ И ИНСТАНТОНЫ

В этом разделе $d = 4$. Оказывается, что если специальным образом выбрать ортонормированный базис $\{e_n\}$ в $L_2([0, 1], \mathbb{R}^4)$, то уравнения Лапласа для параллельного переноса будут эквивалентны уравнениям автодуальности Янга—Миллса.

Пусть $\epsilon_{\mu\nu\alpha\beta}$ — полностью антисимметричный единичный тензор на $\mathbb{R}^4$, а $*$ — оператор Ходжа. Тогда

$$(*F)_{\mu\nu} = \frac{1}{2}\epsilon_{\mu\nu\alpha\beta}F^{\alpha\beta}.$$

Введем обозначения $F_+ = \frac{1}{2}(F + *F)$ и $F_- = \frac{1}{2}(F - *F)$. Функционал действия Янга—Миллса имеет тогда вид

$$S(A) = \frac{1}{2} \int_{\mathbb{R}^4} \|F(x)\|^2 dx = \frac{1}{2} \int_{\mathbb{R}^4} (\|F_+(x)\|^2 + \|F_-(x)\|^2) dx. \quad (4.1)$$

Из тождеств Бьянки следует, что если связность A является решением уравнений автодуальности

$$F = *F \quad (4.2)$$

или антиавтодуальности

$$F = -*F, \quad (4.3)$$

то связность A будет решением уравнений Янга—Миллса. Если связность A — решение уравнений автодуальности (4.2) (уравнений антиавтодуальности (4.3)) и при этом интеграл (4.1) конечен, то A называется инстантоном (антиинстантоном). Если A — инстантон, то функционал действия Янга—Миллса достигает на A своего минимума среди связностей с одинаковым топологическим зарядом

$$k(A) = \frac{1}{8\pi^2} \int_{\mathbb{R}^4} (-\|F_+(x)\|^2 + \|F_-(x)\|^2) dx$$

(см., например, [5, 6]). Пространство модулей инстантонов (классов эквивалентности относительно калибровочных преобразований) было описано в знаменитой работе [16].

Пусть $B — $M_N(\mathbb{C})$ -значный антисимметричный тензор ранга $(0, 2)$ над $\mathbb{R}^4$, $\mathbf{B}$ — антисимметричная матрица 4×4 , элементами которой являются матрицы из $M_N(\mathbb{C})$, определенная по формуле$

$$\mathbf{B}_{\mu\nu} = B \langle p_\mu, p_\nu \rangle.$$

Теорема 4.1. Пусть $T \in C^1([0, 1], SO(4))$ и пусть в $L_2([0, 1], \mathbb{R}^4)$ выбран ортонормированный базис $e_n^T(t) = (T(t)p_{a_n})h_{b_n}(t)$, где

$$a_n = n - 4 \left\lfloor \frac{n-1}{4} \right\rfloor, \quad b_n = \left\lfloor \frac{n+3}{4} \right\rfloor,$$

$\{h_n\}$ — слабо равномерно плотный базис в $L_2([0, 1], \mathbb{R})$, причем $h_n \in H_0^1$ и $h_n(1) = 0$ для всех $n \in \mathbb{N}$. Выполняются следующие равенства:

$$\operatorname{div}_L^{\{e_n^T\}} B^A(\gamma) = \frac{1}{4} \left(- \int_0^1 J^\mu_{\mu\nu}(\gamma, t) \dot{\gamma}^\nu(t) dt - \int_0^1 \operatorname{tr} \left(\dot{T}(t) T^{-1}(t) \mathbf{L}(\gamma, t) \right) dt \right), \quad (4.4)$$

$$\Delta_L^{\{e_n^T\}} U_1^A(\gamma) = \frac{1}{4} U_1^A(\gamma) \left(- \int_0^1 J^\mu_{\mu\nu}(\gamma, t) \dot{\gamma}^\nu(t) dt - \int_0^1 \operatorname{tr} \left(\dot{T}(t) T^{-1}(t) \mathbf{L}(\gamma, t) \right) dt \right). \quad (4.5)$$

Формула (4.5) доказана в [9] для ортонормированного базиса $\{h_n\}$, где $h_n(t) = \sqrt{2} \sin \pi n t$. Доказательство без изменений переносится на случай теоремы 4.1. Формулу (4.4) можно получить как следствие (4.5).

Группы S_L^3 и S_R^3 — нормальные подгруппы группы $SO(4)$, состоящие из вещественных матриц, имеющих вид соответственно

$$\begin{pmatrix} a & -b & -c & -d \\ b & a & -d & c \\ c & d & a & -b \\ d & -c & b & a \end{pmatrix}, \quad \begin{pmatrix} a & -b & -c & -d \\ b & a & d & -c \\ c & -d & a & b \\ d & c & -b & a \end{pmatrix},$$

где $a^2 + b^2 + c^2 + d^2 = 1$.

Теорема 4.2. Пусть $S(A) < \infty$. Пусть $T \in C^1([0, 1], S_R^3)$ ($T \in C^1([0, 1], S_L^3)$), причем

$$\dim \operatorname{span} \{ \dot{T}(t) T^{-1}(t) \}_{t \in [0, 1]} \geq 2.$$

Пусть базис $\{e_n^T\}$ определен, как в формулировке теоремы 4.1. Тогда следующие три условия равносильны:

- (1) связность A на $\mathbb{R}^4$ является инстантоном (антиинстантоном);
- (2) параллельный перенос U_1^A является решением уравнения Лапласа для лапласиана $\Delta_L^{\{e_n^T\}}$:

$$\Delta_L^{\{e_n^T\}} U_1^A = 0;$$

- (3) B^A является решением уравнения

$$\operatorname{div}_L^{\{e_n^T\}} B^A = 0.$$

Эквивалентность условий (1) и (2) доказана в [9]. Как следствие можно получить эквивалентность условий (1) и (3).

5. ДИФФЕРЕНЦИАЛЬНЫЕ ОПЕРАТОРЫ ЛЕВИ В ИСЧИСЛЕНИИ МАЛЛЯВЭНА

В этом и следующем разделах $h_n(t) = \sqrt{2} \sin \pi n t$.

Пусть $(\Omega, \mathcal{F}, P)$ — стандартное вероятностное пространство, ассоциированное с d -мерным броуновским движением $b_t = (b_t^1, \dots, b_t^d)$ на отрезке $[0, 1]$, т.е.

$$\Omega = C_0([0, 1], \mathbb{R}^d) := \left\{ \gamma \in C([0, 1], \mathbb{R}^d) : \gamma(0) = 0 \right\},$$

$\mathcal{F}$ — σ -алгебра, порожденная b_t , и P — мера Винера. Стохастические дифференциалы Ито и Стратоновича будем обозначать символами db и $\circ db$ соответственно.

Пусть H — вещественное или комплексное пространство. Пусть $\mathcal{FC}^\infty(H)$ — пространство H -значных C^∞ -гладких цилиндрических функций с компактным носителем на $C_0([0, 1], \mathbb{R}^d)$. Пусть $\{g_n\}$ — произвольный ортонормированный базис в H_0^1 . Соболевская норма $\|\cdot\|_{r,p}$ на $\mathcal{FC}^\infty(H)$ определяется следующим образом:

$$\|f\|_{r,p} = \sum_{k=0}^r \left(E \left(\sum_{i_1 \dots i_k=1}^{\infty} \left\| \partial_{g_{i_1}} \dots \partial_{g_{i_k}} f \right\|_H^2 \right)^{p/2} \right)^{1/p}.$$

Такое определение не зависит от выбора базиса $\{g_n\}$. Пространство Соболева $W^{r,p}(P, H)$ — это замыкание $\mathcal{FC}^\infty(H)$ с помощью нормы $\|\cdot\|_{r,p}$. Символ $W^{r,\infty}(P, H)$ обозначает проективный предел $\text{proj} \lim_{p \rightarrow +\infty} W^{r,p}(P, H)$.

Пусть $p \geq 1$. Если $h \in H_0^1$, то оператор ∂_h можно продолжить по непрерывности до линейного оператора из $W^{1,p}(P, H)$ в $L_p(P, H \otimes H_0^1)$. Это продолжение мы будем обозначать тем же символом ∂_h . Если $f \in W^{1,p}(P, H)$, то существует $Df \in L_2(P, H \otimes H_0^1)$, причем $(Df, h)_{H_0^1} = \partial_h f$. Если $f \in W^{2,p}(P, H)$, то $Df \in W^{1,p}(P, H \otimes H_0^1)$ и вторые производные f можно определить по аналогии. (О различных способах определения пространств Соболева на мерой Винера см., например, [19]). 8 Для каждого $x \in \mathbb{R}^d$ стохастический параллельный перенос $U^x(b, t)$, порожденный связностью A , — это решение стохастического дифференциального уравнения в смысле Стратоновича

$$U^x(b, t) = I_N - \int_0^t A_\mu(x + b_s) U^x(b, s) \circ db_s^\mu. \quad (5.1)$$

Если связность A и все ее производные первого и второго порядка ограничены, у уравнения (5.1) существует единственное сильное решение.

Пусть стохастические процессы $L_{\mu\nu}^x(b, t)$ и $J_{\lambda\mu\nu}^x(b, t)$, принимающие значения в пространстве тензоров, определены следующим образом:

$$\begin{aligned} L_{\mu\nu}^x(b, t) &= U^x(b, t)^{-1} F_{\mu\nu}(x + b_t) U^x(b, t), \\ J_{\lambda\mu\nu}^x(b, t) &= U^x(b, t)^{-1} \nabla_\lambda F_{\mu\nu}(x + b_t) U^x(b, t). \end{aligned}$$

Предложение 5.1. Пусть связность A и все ее производные первого и второго порядка ограничены. Тогда $U^x(b, 1) \in W^{1,\infty}(P, M_N(\mathbb{C}))$. Если $u \in H_0^1$, то

$$\partial_u U^x(b, 1) = -U^x(b, 1) \int_0^1 L_{\mu\nu}^x(b, s) u^\mu(t) \circ db_t^\nu - A_\mu(x + b_1) u^\mu(1) U^x(b, 1).$$

Для случая исчисления Маллявэна понятия α_0 -градиента, дивергенции Леви и лапласиана Леви можно перенести следующим образом.

Определение 5.1. Если $f \in W^{1,2}(P, M_N(\mathbb{C}))$, то запись

$$\text{grad}_{\alpha_0} f \in L\left(L_2([0, 1], \mathbb{R}^d), L_2(P, M_N(\mathbb{C}))\right)$$

означает, что $\text{grad}_{\alpha_0} f(\gamma)h = \partial_h f$ для всех $h \in H_0^1$, удовлетворяющих условию $h(1) = 0$.

Прямым следствием предложения 5.1 является следующее утверждение.

Предложение 5.2. Для $h \in L_2([0, 1], \mathbb{R}^d)$ выполняется соотношение

$$\left(\text{grad}_{\alpha_0} U^x(b, 1)\right)h = -U^x(b, 1) \int_0^1 L_{\mu\nu}(b, t) h^\mu(t) \circ db_t^\nu.$$

Определение 5.2. Дивергенция Леви $\text{div}_L^{\{e_n\}}$, порожденная ортонормированным базисом $\{e_n\}$ в $L_2([0, 1], \mathbb{R}^d)$, состоящим из элементов H_0^1 , — это линейное отображение из $\text{dom} \text{div}_L^{\{e_n\}}$ в $L_2(P, M_N(\mathbb{C}))$, определенное следующим образом:

$$\text{div}_L^{\{e_n\}} B(b) = \lim_{n \rightarrow \infty} \frac{1}{n} \sum_{k=1}^n \sum_{\mu=1}^d \partial_{e_k} B(b)(e_k), \quad (5.2)$$

где последовательность в правой части (5.2) сходится сильно в $L_2(P, M_N(\mathbb{C}))$ и область определения $\text{dom} \text{div}_L^{\{e_n\}}$ состоит из всех $B \in L(L_2([0, 1], \mathbb{R}^d), W^{1,2}(P, M_N(\mathbb{C})))$, для которых правая часть (5.2) существует.

Определение 5.3. Лапласиан Леви $\Delta_L^{\{e_n\}}$, порожденный ортонормированным базисом $\{e_n\}$ в $L_2([0, 1], \mathbb{R}^d)$, состоящим из элементов H_0^1 , — это линейное отображение из $\text{dom } \Delta_L^{\{e_n\}}$ в пространство $L_2(P, M_N(\mathbb{C}))$, действующее по формуле

$$\Delta_L^{\{e_n\}} f = \text{div}_L^{\{e_n\}} \text{grad}_{\alpha_0} f, \quad (5.3)$$

где $\text{dom } \Delta_L^{\{e_n\}}$ состоит из всех $f \in W^{2,2}(P, M_N(\mathbb{C}))$, для которых правая часть (5.3) существует.

Замечание 5.1. Теория Соболева—Шварца над бесконечномерной гауссовской мерой — это исчисление Хиды (white noise analysis). В стохастическом анализе наиболее изучен лапласиан Леви, действующий на обобщенных функционалах Хиды (см. [24, 25]). Можно показать, что лапласиан, заданный определением 5.3, не совпадает с таким лапласианом при естественном вложении пространства Соболева в пространство обобщенных функционалов Хиды.

Пусть

$$B^{A,x} \in L\left(L_2([0, 1], \mathbb{R}^d), L_2(P, M_N(\mathbb{C}))\right)$$

определена по формуле

$$B^{A,x}(b)u = U^x(b, 1)^{-1}(\text{grad}_{\alpha_0} U^x(b, 1)u) = - \int_0^1 L_{\mu\nu}^x(b, t)u^\mu(t) \circ db_t^\nu.$$

Замечание 5.2. Пусть χ_t — индикатор отрезка $[0, t]$. Рассмотрим случайный процесс

$$R_\mu^x(b, t) := B_\mu^{A,x}(b)(p_\mu \chi_t) = - \int_0^t L_{\mu\nu}^x(b, s) \circ db_s^\nu = - \int_0^t L_{\mu\nu}^x(b, s) db_s^\nu - \frac{1}{2} \int_0^t J_{\nu\mu}^{x\nu}(b, s) ds.$$

Процесс $R^x(b, t) = (R_1^x(b, t), \dots, R_d^x(b, t))$ является мартингалом тогда и только тогда, когда связность A является решением уравнений Янга—Миллса (ср. [14, 15, 17]).

В настоящей статье лапласиан и дивергенция Леви определяются с небольшими отличиями от статьи автора [31]. Тем не менее, доказательства из [31] переносятся практически без изменений для утверждений, приведенных ниже в этом разделе.

Предложение 5.3. Пусть связность A и все ее частные производные до третьего порядка включительно ограничены. Тогда $U^x(b, 1) \in W^{2,\infty}(P, M_N(\mathbb{C}))$ и $B^{A,x} \in L(L_2([0, 1], \mathbb{R}^d), W^{1,2}(P, M_N(\mathbb{C})))$. Если $u, v \in H_0^1$ и $u(1) = v(1) = 0$, то

$$\begin{aligned} \partial_u B^{A,x}(b)v = & \int_0^1 \left[L_{\mu\lambda}^x(b, t)u^\mu(t), \int_0^t L_{\nu\kappa}^x(b, s)v^\nu(s) \circ db_s^\kappa \right] \circ db_t^\lambda + \\ & + \int_0^1 \left[L_{\nu\kappa}^x(b, t)v^\nu(t), \int_0^t L_{\mu\lambda}^x(b, s)u^\mu(s) \circ db_s^\lambda \right] \circ db_t^\kappa - \\ & - \frac{1}{2} \int_0^1 \left(J_{\nu\mu\lambda}^x(b, t) + J_{\mu\nu\lambda}^x(b, t) \right) u^\mu(t)v^\nu(t) \circ db_t^\lambda - \\ & - \frac{1}{2} \int_0^1 L_{\mu\nu}^x(b, t) \left(v^\mu(t)\dot{u}^\nu(t) + u^\mu(t)\dot{v}^\nu(t) \right) dt, \quad (5.4) \end{aligned}$$

$$\begin{aligned}
 \partial_v \partial_u U^x(b, 1) = & U^x(b, 1) \int_0^1 L_{\mu\lambda}^x(b, t) u^\mu(t) \left(\int_0^t L_{\nu\kappa}^x(b, s) v^\nu(s) \circ db_s^\kappa \right) \circ db_t^\lambda + \\
 & + U^x(b, 1) \int_0^1 L_{\nu\kappa}^x(b, t) v^\nu(t) \left(\int_0^t L_{\mu\lambda}^x(b, s) u^\mu(s) \circ db_s^\lambda \right) \circ db_t^\kappa - \\
 & - U^x(b, 1) \left(\frac{1}{2} \int_0^1 \left(J_{\nu\mu\lambda}^x(b, t) + J_{\mu\nu\lambda}^x(b, t) \right) u^\mu(t) v^\nu(t) \circ db_t^\lambda + \right. \\
 & \left. + \frac{1}{2} \int_0^1 L_{\mu\nu}^x(b, t) \left(v^\mu(t) \dot{u}^\nu(t) + u^\mu(t) \dot{v}^\nu(t) \right) dt \right). \quad (5.5)
 \end{aligned}$$

Теорема 5.1. Пусть связность A и все ее частные производные до третьего порядка включительно ограничены. Пусть в $L_2([0, 1], \mathbb{R}^d)$ выбран ортонормированный базис $e_n(t) = p_{a_n} h_{b_n}(t)$, где

$$a_n = n - d \left\lfloor \frac{n-1}{d} \right\rfloor, \quad b_n = \left\lfloor \frac{n+d-1}{d} \right\rfloor.$$

Выполняются следующие равенства:

$$\operatorname{div}_L^{\{e_n\}} B^{A,x}(b) = -\frac{1}{d} \int_0^1 J^{x\mu}{}_{\mu\nu}(b, s) db_s^\nu, \quad (5.6)$$

$$\Delta_L^{\{e_n\}} U^x(b, 1) = \frac{1}{d} U^x(b, 1) \left(\int_0^1 L_{\mu\nu}^x(b, t) L^{x\mu\nu}(b, t) dt - \int_0^1 J^{x\mu}{}_{\mu\nu}(b, s) db_s^\nu \right). \quad (5.7)$$

Теорема 5.2. Пусть связность A и все ее частные производные до третьего порядка включительно ограничены. Пусть базис $\{e_n\}$ определен, как в формулировке предыдущей теоремы. Следующие условия равносильны:

- (1) связность A на $\mathbb{R}^d$ является решением уравнений Янга—Миллса (3.2);
- (2) для стохастического параллельного переноса $U^x(b, 1)$ выполняется соотношение

$$\Delta_L^{\{e_n\}} U^x(b, 1) = \frac{1}{d} U^x(b, 1) \int_0^1 L_{\mu\nu}^x(b, t) L^{x\mu\nu}(b, t) dt; \quad (5.8)$$

- (3) $B^{A,x}$ является решением уравнения

$$\operatorname{div}_L^{\{e_n\}} B^{A,x} = 0.$$

Замечание 5.3. В [31] рассматривался только случай связности в тривиальном расслоении над $\mathbb{R}^d$. Лапласиан Леви на пространстве Соболева над мерой Винера на компактном римановом многообразии и его связь с уравнениями Янга—Миллса в векторном расслоении над этим многообразием рассматривались в работе [26] Р. Леандра и И. В. Воловича. При этом лапласиан Леви в этой работе определялся как интегральный функционал, заданный специальным видом второй производной. В отличие от детерминистского случая в стохастическом случае лапласиан Леви, определенный как среднее Чезаро вторых производных по направлению, не является расширением лапласиана Леви, определенного как интегральный функционал, так как у значения лапласиана Леви из [26] на стохастическом параллельном переносе нет первого слагаемого из правой части (5.7). На данный момент связь между лапласианом, заданным определением 5.3, и лапласианом, введенным в [26], не исследована.

Функционал действия Янга—Миллса можно выразить как аналог интеграла Дирихле, где стохастический параллельный перенос является киральным полем, суммирование заменено на усреднение по Чезаре, а мера Лебега замена на произведение меры Лебега и меры Винера.

Теорема 5.3. Если $S(A) < \infty$ и

$$-\int_{\mathbb{R}^d} \text{tr} \left(\nabla_\mu F^\mu{}_\nu(x) \nabla_\lambda F^{\lambda\nu}(x) \right) dx < \infty,$$

то

$$\lim_{n \rightarrow \infty} \frac{1}{n} \sum_{k=1}^n \sum_{\mu=1}^d \frac{1}{2} \int_{\mathbb{R}^d} E \left(\text{tr} \left(\partial_{p_\mu h_k} U^x(b, 1)^{-1} \partial_{p_\mu h_k} U^x(b, 1) \right) \right) dx = S(A). \quad (5.9)$$

Функционал действия Янга—Миллса выражался с помощью стохастического параллельного переноса при $d = 4$ другим способом в [14, 15, 17].

6. ДИФФЕРЕНЦИАЛЬНЫЕ ОПЕРАТОРЫ ЛЕВИ В ИСЧИСЛЕНИИ МАЛЛЯВЭНА И ИНСТАНТОНЫ

В этом разделе снова $d = 4$.

Теорема 6.1. Пусть $T \in C^1([0, 1], SO(4))$ и пусть в $L_2([0, 1], \mathbb{R}^4)$ выбран ортонормированный базис $e_n^T(t) = (T(t)p_{a_n})h_{b_n}(t)$, где

$$a_n = n - 4 \left\lfloor \frac{n-1}{4} \right\rfloor, \quad b_n = \left\lfloor \frac{n+3}{4} \right\rfloor.$$

Пусть связность A и все ее частные производные до третьего порядка включительно ограничены. Для всех $x \in \mathbb{R}^d$ выполняются равенства

$$\begin{aligned} \text{div}_L^{\{e_n^T\}} B^{A,x}(b) &= \frac{1}{4} \left(- \int_0^1 J^{x\mu}{}_{\mu\nu}(b, t) db_t^\nu - \int_0^1 \text{tr} \left(\dot{T}(t) T^{-1}(t) L^x(b, t) \right) dt \right), \\ \Delta_L^{\{e_n^T\}} U^x(b, 1) &= \frac{1}{4} U^x(b, 1) \left(\int_0^1 L_{\mu\nu}^x(b, t) L^{x\mu\nu}(b, t) dt - \right. \\ &\quad \left. - \int_0^1 J^{x\mu}{}_{\mu\nu}(b, t) db_t^\nu - \int_0^1 \text{tr} \left(\dot{T}(t) T^{-1}(t) L^x(b, t) \right) dt \right). \end{aligned}$$

Теорема 6.1 является прямым следствием предложения 5.3.

Теорема 6.2. Пусть $T \in C^1([0, 1], S_R^3)$ ($T \in C^1([0, 1], S_L^3)$), причем

$$\dim \text{span} \left\{ \dot{T}(t) T^{-1}(t) \right\}_{t \in [0, 1]} \geq 2.$$

Пусть базис $\{e_n^T\}$ определен, как в формулировке теоремы 6.1. Пусть $S(A) < \infty$. Пусть связность A и все ее частные производные до третьего порядка включительно ограничены. Пусть $x \in \mathbb{R}^d$. Тогда следующие три условия равносильны:

- (1) связность A на $\mathbb{R}^4$ является инстантоном (антиинстантоном);
- (2) для стохастического параллельного переноса $U^x(b, 1)$ выполняется:

$$\Delta_L^{\{e_n^T\}} U^x(b, 1) = \frac{1}{4} U^x(b, 1) \int_0^1 L_{\mu\nu}^x(b, t) L^{x\mu\nu}(b, t) dt;$$

- (3) $B^{A,x}$ является решением уравнения

$$\text{div}_L^{\{e_n^T\}} B^{A,x} = 0.$$

Доказательство. Докажем нетривиальную часть теоремы. Пусть для простоты $x = 0$. Будем обозначать $L^0(b, t)$ и $J^0(b, t)$ символами $L(b, t)$ и $J(b, t)$. Если выполняется условие (2) или (3) теоремы 6.2, то

$$\int_0^1 J^\mu{}_{\nu}(b, t) db_t^\nu + \int_0^1 \operatorname{tr} \left(\dot{T}(t) T^{-1}(t) \mathbf{L}(b, t) \right) dt = 0.$$

Из теоремы Струка—Варадана о носителе диффузионного процесса (см. [22, 28]) следует, что

$$\int_0^1 J^\mu{}_{\nu}(\gamma, t) \dot{\gamma}^\nu(t) dt + \int_0^1 \operatorname{tr} \left(\dot{T}(t) T^{-1}(t) \mathbf{L}(\gamma, t) \right) dt = 0$$

для всех $\gamma \in H_0^1$. Таким образом, теорема 6.2 является следствием теоремы 4.2. $\square$

Автор благодарит О. Г. Смолянова и И. В. Воловича за полезные обсуждения.

СПИСОК ЛИТЕРАТУРЫ

1. Авербух В. И., Смолянов О. Г. Теория дифференцирования в линейных топологических пространствах // Усп. мат. наук. — 1967. — 22, № 6 (138). — С. 201–260.
2. Авербух В. И., Смолянов О. Г., Фомин С. В. Обобщенные функции и дифференциальные уравнения в линейных пространствах. II. Дифференциальные операторы и их преобразования Фурье // Тр. Моск. мат. о-ва. — М.: Изд-во Моск. ун-та, 1972. — 27. — С. 249–262.
3. Аккарди Л., Смолянов О. Г. Формулы Фейнмана для эволюционных уравнений с лапласианом Леви на бесконечномерных многообразиях // Докл. РАН. — 2006. — 407, № 5. — С. 1–6.
4. Арефьева И. Я., Волович И. В. Функциональные высшие законы сохранения в калибровочных теориях, Обобщенные функции и их применения в математической физике // Тр. Междунар. конф. — М.: ВЦ АН СССР, 1981. — С. 43–49.
5. Дубровин Б. А., Новиков С. П., Фоменко А. Т. Современная геометрия: Методы и приложения. — М.: Наука, 1986.
6. Сергеев А. Г. Гармонические отображения / Лекц. курсы НОЦ. — М.: Мат. ин-т им. В. А. Стеклова, 2008. — 10.
7. Волков Б. О. Лапласианы Леви и связанные с ними конструкции / Дисс. на соиск. уч. степени канд. физ.-мат. наук. — М., 2014.
8. Волков Б. О. Даламбертианы Леви и их применение в квантовой теории // Вестн. Самарск. гос. техн. ун-та. Сер. физ.-мат. науки. — 2015. — 19, № 2. — С. 241–258.
9. Волков Б. О. Лапласианы Леви и инстантоны // в сб.: Современные проблемы математики, механики и математической физики / Тр. Мат. ин-та им. В. А. Стеклова. — М.: 2015. — 290. — С. 226–238.
10. Леви П. Конкретные проблемы функционального анализа. — М.: Наука, 1967.
11. Accardi L. Yang–Mills equations and Lévy–Laplacians // в кн.: Dirichlet Forms and Stochastic Processes (Beijing, 1993). — Berlin: de Gruyter, 1995. — С. 1–24.
12. Accardi L., Gibilisco P., Volovich I. V. The Lévy Laplacian and the Yang–Mills equations // Rend. Lincei. — 1993. — 4. — С. 201–206.
13. Accardi L., Gibilisco P., Volovich I. V. Yang–Mills gauge fields as harmonic functions for the Levy Laplacians // Russ. J. Math. Phys. — 1994. — 2, № 2. — С. 235–250.
14. Arnaudon M., Bauer R. O., Thalmaier A. A probabilistic approach to the Yang–Mills heat equation // J. Math. Pures Appl. — 2002. — 81. — С. 143–166.
15. Arnaudon M., Thalmaier A. Yang–Mills fields and random holonomy along Brownian bridges // Ann. Probab. — 2003. — 31, № 2. — С. 769–790.
16. Atiyah M. F., Drinfeld V. G., Hitchin N. J., Manin Yu. I. Construction of instantons // Phys. Lett. A. — 1978. — 65. — С. 185–187.
17. Bauer R. O. Characterizing Yang–Mills fields by stochastic parallel transport // J. Funct. Anal. — 1998. — 155, № 1. — С. 536–549.
18. Bauer R. O. Yang–Mills fields and stochastic parallel transport in small geodesic balls // Stochastic Process. Appl. — 2000. — 89, № 2. — С. 213–226.
19. Bogachev V. I. Gaussian measures. — Providence, Rhode Island: Am. Math. Soc., 1998.
20. Driver B. Classifications of bundle connection pairs by parallel translation and lassos // J. Funct. Anal. — 1989. — 83. — С. 185–231.

21. *Gross L.* A Poincarè lemma for connection forms// J. Funct. Anal. — 1985. — 63. — С. 1–46.
22. *Ikeda N., Watanabe S.* Stochastic differential equations and diffusions processes. — Amsterdam: North-Holland, 1981.
23. *Klingenberg W.* Riemannian geometry. Vol. 1. — Berlin: de Gruyter, 1982.
24. *Kuo H.-H., Obata N., Saitô K.* Lévy Laplacian of generalized functions on a nuclear space// J. Funct. Anal. — 1990. — 94, № 1. — С. 74–92.
25. *Kuo H.-H.* Recent progress on the white noise approach to the Levy Laplacian// в сб.: Quantum Information and Complexity/ Proc. Meijo Winter School 2003, Nagoya, Japan, January 6–10, 2003. — River Edge, New Jersey: World Scientific, 2004. — С. 267–295.
26. *Leandre R., Volovich I. V.* The stochastic Lévy Laplacian and Yang–Mills equation on manifolds// Infin. Dimens. Anal. Quantum Probab. Relat. Top. — 2001. — 4, № 2. — С. 151–172.
27. *Stafford S.* A stochastic criterion for Yang–Mills connections// в кн.: Diffusion Processes and Related Problems in Analysis, Vol. I. — Boston, MA: Birkhäuser, 1990. — С. 313–322.
28. *Stroock D. W., Varadhan S. R. S.* On the support of diffusion processes with applications to the strong maximum principle// Proc. 6 Berkeley Symp. on Math. Stat. and Probability. Vol. 3. Probability Theory. — Berkeley, California: University of California Press, 1972. — С. 333–359.
29. *Polyakov A. M.* Gauge fields as rings of glue// Nucl. Phys. B. — 1980. — 164. — С. 171–188.
30. *Volkov B. O.* Levy differential operators and gauge invariant equations for Dirac and Higgs fields/ e-print [arXiv: 1612.00310](https://arxiv.org/abs/1612.00310) (2016).
31. *Volkov B. O.* Stochastic Lévy differential operators and Yang–Mills equations// Infin. Dimens. Anal. Quant. Probab. Relat. Top. — 2017. — 20, № 2. — 1750008.

Б. О. Волков

Математический институт им. В. А. Стеклова Российской академии наук;
 Московский государственный технический университет им. Н. Э. Баумана
 E-mail: borisvolkov1986@gmail.com



АНАЛОГИ МЕРЫ ЛЕБЕГА В ПРОСТРАНСТВАХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ И КЛАССЫ ИНТЕГРИРУЕМЫХ ПО НИМ ФУНКЦИЙ

© 2018 г. Д. В. ЗАВАДСКИЙ

Аннотация. Изучаются трансляционно-инвариантные меры на банаховых пространствах l_p , где $p \in [1, \infty]$. Построены аналоги меры Лебега на борелевских σ -алгебрах, порожденных топологией поточечной сходимости (σ -аддитивные, инвариантные относительно сдвигов на произвольные векторы, регулярные меры). Показано, что данные меры не являются σ -конечными. Исследованы пространства интегрируемых по построенным мерам функции и показано, что такие пространства не являются сепарабельными. Изучены различные плотные подпространства в пространствах функций, интегрируемых по трансляционно инвариантной мере. Указано пространство непрерывных функций, которое является плотным в рассматриваемых функциональных пространствах. Рассматриваются борелевские σ -алгебры, отвечающие различным топологиям в пространствах l_p , где $p \in [1, \infty]$. При $p \in [1, \infty)$ установлено равенство борелевских σ -алгебр, отвечающих некоторым естественным топологиям в данных пространствах последовательностей, борелевской σ -алгебре, отвечающей топологии поточечной сходимости. Показано, что в случае пространства l_∞ аналогичные свойства не выполняются.

Ключевые слова: трансляционно инвариантная мера, топология поточечной сходимости, борелевская σ -алгебра, пространства интегрируемых функций, аппроксимация интегрируемых функций непрерывными.

AMS Subject Classification: 28C20, 81Q05, 47D08

1. Введение. Инвариантные относительно сдвигов меры применяются для исследования решений дифференциальных уравнений при помощи математических ожиданий функционалов от случайных блужданий. Применение трансляционно инвариантных мер для получения представлений решений дифференциальных уравнений можно найти в [1, 5]. В указанных работах сильно непрерывные однопараметрические полугруппы операторов, которые разрешают задачу Коши для уравнения диффузии, уравнения дробной диффузии и уравнения Шредингера с разнообразными гамильтонианами, были получены как результат усреднения случайных однопараметрических семейств операторов сдвига на векторы координатного пространства по мерам, заданным на множестве операторов сдвига. Такой подход к изучению свойств решения дифференциальных уравнений для функций на бесконечномерных пространствах требует изучения мер на бесконечномерных пространствах, инвариантных относительно сдвигов на векторы этого пространства, или относительно других групп преобразований (см. [7]).

Трансляционно инвариантные меры также оказываются эффективной конструкцией для изучения интегралов Фейнмана по траекториям (см. [4, 8]).

В [2] доказано, что не существует меры Лебега на бесконечномерном топологическом векторном пространстве, т.е. не существует ненулевой σ -аддитивной σ -конечной меры на σ -алгебре борелевских подмножеств бесконечномерного топологического векторного пространства, инвариантной относительно сдвигов на векторы этого пространства. В связи с этим изучались вопросы о существовании мер на бесконечномерных топологических векторных пространствах, которые удовлетворяют лишь некоторым свойствам меры Лебега (см. [3, 6, 7, 9]).

В данной статье изучаются меры на банаховых пространствах l_p , $p \in [1, \infty]$. В первой части статьи построены аналоги меры Лебега на борелевских σ -алгебрах относительно топологии поточечной сходимости. В случае пространства l_∞ такая мера будет получена путем сужения на l_∞ меры, построенной в [9] на пространстве $\mathbb{R}^\infty$. Однако при $p \in [1, \infty)$ таким образом удастся получить лишь нулевую меру. В статье указан способ, при помощи которого можно обойти эту сложность и получить ненулевые меры, которые являются регулярными и трансляционно инвариантными. В отличие от трансляционно инвариантных мер, построенных в [6, 7], предложенные меры являются σ -аддитивными. Заметим также, что в [6, 7] определены иные трансляционно инвариантные меры на пространствах l_p , принимающие нулевые значения на множествах, значения на которых мер, построенных в настоящей работе, конечно. Введенные в [6, 7] меры, не являются σ -конечными, но кроме того, они не являются и σ -аддитивными. В [7] исследованы трансляционно инвариантные меры на гильбертовом пространстве l_2 , инвариантные также относительно произвольного ортогонального преобразования.

Во второй части статьи изучаются пространства интегрируемых по трансляционно инвариантной мере числовых функций на пространстве l_p . Доказано, что такие пространства не являются сепарабельными. Найдены плотные подпространства пространств интегрируемых функций, состоящие из непрерывных функций специального вида.

В заключительной части статьи рассматриваются связи между различными топологиями в пространствах l_p , $p \in [1, \infty]$. Установлены зависимости между борелевскими σ -алгебрами, которые отвечают рассматриваемым топологиям, а также приведены некоторые следствия установленных зависимостей.

2. Трансляционно-инвариантные меры на пространствах l_p . Рассмотрим пространство $\mathbb{R}^\infty$ с топологией поточечной сходимости, которую обозначим через $\tau_{\mathbb{R}^\infty}$. Борелевскую σ -алгебру, которая отвечает топологии $\tau_{\mathbb{R}^\infty}$, обозначим через $\mathfrak{B}_{\mathbb{R}^\infty}$. В [9] построена σ -аддитивная мера, определенная на борелевской σ -алгебре $\mathfrak{B}_{\mathbb{R}^\infty}$, которая является регулярной и инвариантной относительно сдвигов на произвольные векторы из пространства $\mathbb{R}^\infty$. Используем эту меру для построения меры на пространствах l_p , $p \in [1, \infty]$, которая обладает аналогичными свойствами. Прежде всего заметим, что топология поточечной сходимости в пространстве $\mathbb{R}^\infty$ является метризуемой. Метрика, которая порождает топологию $\tau_{\mathbb{R}^\infty}$, имеет вид

$$d(x, y) = \sum_{i=1}^{\infty} \frac{1}{2^i} \frac{|x_i - y_i|}{1 + |x_i - y_i|}, \quad x = (x_1, x_2, \dots), \quad y = (y_1, y_2, \dots) \in \mathbb{R}^\infty.$$

Сначала исследуем случай пространства l_∞ . Обозначим топологию поточечной сходимости в l_∞ через τ_{l_∞} (она наследуется из $\mathbb{R}^\infty$ и задается аналогичной метрикой). Обозначим через $\mathfrak{B}_{l_\infty}$ борелевскую σ -алгебру, которая отвечает топологии τ_{l_∞} . Для того, чтобы перенести меру с пространства $\mathbb{R}^\infty$ на пространство l_∞ докажем некоторые вспомогательные утверждения.

Лемма 1. *Множества $A_n = [-n, n] \times [-n, n] \times \dots$, где $n \in \mathbb{N}$, являются замкнутыми подмножествами пространства $\mathbb{R}^\infty$ относительно топологии $\tau_{\mathbb{R}^\infty}$.*

Доказательство. Так как топология $\tau_{\mathbb{R}^\infty}$ является метризуемой, то достаточно доказать секвенциальную замкнутость множеств A_n . Пусть $x_k = (x_k^1, x_k^2, \dots) \in [-n, n] \times [-n, n] \times \dots$. Предположим, что данная последовательность сходится к вектору $x = (x^1, x^2, \dots)$. Тогда справедливо следующее утверждение:

$$\lim_{k \rightarrow \infty} x_k^i = x^i \quad \text{для всех } i \in \mathbb{N}.$$

Следовательно $x \in [-n, n] \times [-n, n] \times \dots$ (так как $x_n^i \in [-n, n]$ при $i, n \in \mathbb{N}$). Следовательно, множества A_n являются замкнутыми относительно топологии $\tau_{\mathbb{R}^\infty}$. $\square$

Лемма 2. *Пространство l_∞ является борелевским подмножеством пространства $\mathbb{R}^\infty$ относительно топологии $\tau_{\mathbb{R}^\infty}$.*

Доказательство. Пространство l_∞ можно представить следующим образом:

$$l_\infty = \bigcup_{n=1}^{\infty} [-n, n] \times [-n, n] \times \dots$$

Лемма 1 утверждает, что множества $A_n = [-n, n] \times [-n, n] \times \dots$ являются замкнутыми в топологии $\tau_{\mathbb{R}^\infty}$. Следовательно, пространство l_∞ является борелевским подмножеством пространства $\mathbb{R}^\infty$ относительно топологии $\tau_{\mathbb{R}^\infty}$. $\square$

Заметим, что подмножество пространства l_∞ является открытым в топологии τ_{l_∞} тогда и только тогда, когда оно является пересечением открытого в топологии $\tau_{\mathbb{R}^\infty}$ множества и пространства l_∞ . Следовательно, аналогичное утверждение является верным и для борелевских σ -алгебр $\mathfrak{B}_{l_\infty}$ и $\mathfrak{B}_{\mathbb{R}^\infty}$. Также заметим, что в пространстве $\mathbb{R}^\infty$ сдвиг на произвольный фиксированный вектор является непрерывным отображением относительно топологии $\tau_{\mathbb{R}^\infty}$. Следовательно, сдвиги оставляют борелевские относительно топологии $\tau_{\mathbb{R}^\infty}$ множества в классе $\mathfrak{B}_{\mathbb{R}^\infty}$. Аналогичное замечание справедливо и для пространства l_∞ .

Таким образом, путем сужения на пространство l_∞ построенной в [9] меры λ , заданной на σ -алгебре $\mathfrak{B}_{\mathbb{R}^\infty}$ борелевских подмножеств, мы получаем σ -аддитивную, инвариантную относительно сдвигов меру, определенную на борелевской σ -алгебре $\mathfrak{B}_{l_\infty}$. Обозначим полученную меру через λ_∞ .

Теорема 1. Мера λ_∞ является регулярной относительно топологии τ_{l_∞} .

Доказательство. Пусть A — борелевское множество в пространстве l_∞ относительно топологии τ_{l_∞} . Тогда $A = B \cap l_\infty$, где B — борелевское множество в пространстве $\mathbb{R}^\infty$ относительно топологии $\tau_{\mathbb{R}^\infty}$. Зафиксируем $\epsilon > 0$. Так как мера λ является регулярной относительно топологии $\tau_{\mathbb{R}^\infty}$, то существуют такие замкнутое множество K и открытое множество U , что

$$\lambda(B \setminus K) < \epsilon, \quad \lambda(U \setminus B) < \epsilon,$$

где $\epsilon > 0$. Тогда множество $U \cap l_\infty$ является открытым, а множество $K \cap l_\infty$ — замкнутым в топологии τ_{l_∞} . Но

$$\lambda((U \cap l_\infty) \setminus A) = \lambda((U \setminus B) \cap l_\infty) \leq \lambda(U \setminus B) < \epsilon.$$

Аналогичное заключение верно и в случае с K . Следовательно, мера λ_∞ является регулярной относительно топологии τ_{l_∞} . $\square$

Отметим, что мера λ_∞ не является σ -конечной, так как согласно теореме Вейля не существует полного аналога меры Лебега в бесконечномерном линейном топологическом пространстве.

Рассмотрим теперь случай пространства l_p , $p \in [1, \infty)$. В первую очередь стоит отметить, что алгоритм, при помощи которого была построена мера λ_∞ , не приносит желаемых результатов в случае пространств l_p , $p \in [1, \infty)$. Это обусловлено следующим утверждением.

Лемма 3. При $p \in [1, \infty)$ пространство l_p содержится в счетном объединении подмножеств пространства $\mathbb{R}^\infty$, значение меры λ на каждом из которых равно нулю.

Доказательство. Пространство l_p содержится в счетном объединении вида $\bigcup_{k=1}^{\infty} A_k$, где

$$A_k = \mathbb{R}^k \times \left[-\frac{1}{4}, \frac{1}{4}\right] \times \left[-\frac{1}{4}, \frac{1}{4}\right] \times \dots$$

Множества A_k можно представить в виде

$$A_k = \bigcup_{j=1}^{\infty} [-j, j]^k \times \left[-\frac{1}{4}, \frac{1}{4}\right] \times \left[-\frac{1}{4}, \frac{1}{4}\right] \times \dots$$

Заметим, что при $j, k \in \mathbb{N}$

$$\lambda \left([-j, j]^k \times \left[-\frac{1}{4}, \frac{1}{4}\right] \times \left[-\frac{1}{4}, \frac{1}{4}\right] \times \dots \right) = 0$$

по построению (см. [9]). Следовательно, пространство l_p содержится в счетном объединении подмножеств пространства $\mathbb{R}^\infty$, значение меры λ на каждом из которых равно нулю. $\square$

Исходя из результата леммы 3, приведем другой алгоритм построения меры на пространствах l_p , $p \in [1, \infty)$. Обозначим топологию поточечной сходимости в пространстве l_p через τ_{l_p} . Борелевскую σ -алгебру, которая отвечает топологии τ_{l_p} , обозначим через $\mathfrak{B}_{l_p}$. Зафиксируем вектор $x = (x_1, x_2, \dots) \in l_p$, у которого все координаты положительны. Рассмотрим отображение $f : \mathbb{R}^\infty \rightarrow \mathbb{R}^\infty$, которое действует на вектор $y = (y_1, y_2, \dots) \in \mathbb{R}^\infty$ по правилу $f(y) = (x_1 y_1, x_2 y_2, \dots)$. Отображение f является биекцией. Кроме того, отображение f является непрерывным относительно топологии τ_{l_p} . Так как обратное к f отображение также является непрерывным, то отображение f является гомеоморфизмом. Как и в случае пространства $\mathbb{R}^\infty$, будем рассматривать пространство l_p с топологией поточечной сходимости. Докажем некоторые вспомогательные утверждения.

Лемма 4. В пространстве $\mathbb{R}^\infty$ множества вида

$$M_r = \left\{ y \mid y \in l_p, \|y\|_p \leq r \right\}, \quad r > 0,$$

являются замкнутыми относительно топологии $\tau_{\mathbb{R}^\infty}$ при $p \in [1, \infty)$.

Доказательство. Так как топология поточечной сходимости метризуема, то достаточно доказать секвенциальную замкнутость множеств M_r . Зафиксируем $r > 0$. Пусть $y_k = (y_k^1, y_k^2, \dots) \in M_r$. Предположим, что последовательность y_k сходится поточечно к вектору $y = (y^1, y^2, \dots)$ и что

$$\sum_{i=1}^{\infty} |y^i|^p > r^p.$$

Тогда существует такой номер $n \in \mathbb{N}$, что

$$\sum_{i=1}^n |y^i|^p > r^p.$$

Ввиду того, что последовательность y_k сходится поточечно к вектору y , получаем следующее неравенство:

$$\sum_{i=1}^n \left| \lim_{k \rightarrow \infty} y_k^i \right|^p > r^p.$$

Следовательно для достаточно больших k выполняется неравенство

$$\sum_{i=1}^n |y_k^i|^p > r^p,$$

что невозможно ввиду построения элементов последовательности y_k . Значит, $y \in M_r$. Следовательно, множество M_r является замкнутым в топологии $\tau_{\mathbb{R}^\infty}$. $\square$

Лемма 5. При $p \in [1, \infty)$ множество $f^{-1}(l_p)$ является борелевским относительно топологии $\tau_{\mathbb{R}^\infty}$.

Доказательство. Так как отображение f является непрерывным относительно топологии $\tau_{\mathbb{R}^\infty}$, то достаточно показать, что пространство l_p является борелевским множеством относительно топологии $\tau_{\mathbb{R}^\infty}$. Представим пространство l_p в виде

$$l_p = \bigcup_{n=1}^{\infty} M_n.$$

Из леммы 4 следует, что множества M_n являются замкнутыми в топологии $\tau_{\mathbb{R}^\infty}$. Следовательно, пространство l_p является борелевским относительно топологии $\tau_{\mathbb{R}^\infty}$. Значит, множество $f^{-1}(l_p)$ также является борелевским относительно топологии $\tau_{\mathbb{R}^\infty}$. $\square$

Заметим, что, как и в случае с пространством l_∞ , подмножество пространства l_p является открытым в топологии τ_{l_p} тогда и только тогда, когда оно является пересечением открытого в топологии $\tau_{\mathbb{R}^\infty}$ множества и пространства l_p , $p \in [1, \infty)$. Следовательно, аналогичное утверждение является верным и для борелевских σ -алгебр $\mathfrak{B}_{l_p}$ и $\mathfrak{B}_{\mathbb{R}^\infty}$. Также заметим, что в пространстве l_p сдвиг на произвольный фиксированный вектор является непрерывным отображением относительно топологии τ_{l_p} . Следовательно, сдвиги оставляют борелевские относительно топологии τ_{l_p} множества в классе $\mathfrak{B}_{l_p}$.

Определим σ -аддитивную меру λ_p на борелевских относительно топологии τ_{l_p} множествах следующим образом:

$$\lambda_p(B) = \lambda(f^{-1}(B)),$$

где B является борелевским относительно топологии τ_{l_p} множеством. Лемма 5 гарантирует корректность определения меры λ_p . Опишем теперь некоторые свойства меры λ_p .

Лемма 6. Мера λ_p является инвариантной относительно сдвигов при $p \in [1, \infty)$.

Доказательство. При сдвигах на произвольный вектор элементы из борелевской σ -алгебры $\mathfrak{B}_{l_p}$ остаются в σ -алгебре $\mathfrak{B}_{l_p}$. Зафиксируем вектор $h \in l_p$ и борелевское множество $H \in \mathfrak{B}_{l_p}$. Используя инвариантность относительно сдвигов меры λ , получаем следующую цепочку равенств:

$$\lambda_p(h + H) = \lambda(f^{-1}(h + H)) = \lambda(f^{-1}(h) + f^{-1}(H)) = \lambda(f^{-1}(H)) = \lambda_p(H).$$

Следовательно, мера λ_p является инвариантной относительно сдвигов. $\square$

Теорема 2. Мера λ_p является регулярной при $p \in [1, \infty)$.

Доказательство. Зафиксируем $\epsilon > 0$ и борелевское множество $H \in \mathfrak{B}_{l_p}$. Множество $f^{-1}(H)$ является борелевским относительно топологии $\tau_{\mathbb{R}^\infty}$. Тогда найдется замкнутое относительно топологии $\tau_{\mathbb{R}^\infty}$ множество K , которое удовлетворяет условию

$$\lambda(f^{-1}(H) \setminus K) < \epsilon$$

и является подмножеством множества $f^{-1}(H)$. Тогда множество $f(K)$ является замкнутым относительно топологии τ_{l_p} . В таком случае

$$\lambda_p(H \setminus (f(K))) = \lambda(f^{-1}(H) \setminus K) < \epsilon.$$

Аналогично можно показать, что имеет место и приближение открытыми множествами. Следовательно, мера λ_p является регулярной. $\square$

Отметим, что построенная на пространстве l_p мера не является σ -конечной, так как согласно теореме Вейля не существует полного аналога меры Лебега в бесконечномерном линейном топологическом пространстве. Кроме того отметим, что мера l_p зависит от выбора вектора x .

3. Пространства интегрируемых функций. Перейдем теперь к изучению пространств функций, которые являются интегрируемыми относительно мер λ_p , $p \in [1, \infty]$. Пусть $p \in [1, \infty]$, $q \in [1, \infty)$. Ответ на вопрос о приближении интегрируемых функций непрерывными дает следующая теорема.

Теорема 3. Множество непрерывных относительно топологии τ_p функций, каждая из которых сосредоточена на множестве конечной меры, является плотным в пространстве $L_q(l_p, \mathfrak{B}_{l_p}, \lambda_p)$, где $p \in [1, \infty]$, $q \in [1, \infty)$.

Доказательство. Прежде всего заметим, что класс непрерывных относительно топологии τ_p функций, каждая из которых обращается в нуль всюду, кроме множества конечной меры, образует линейное пространство; обозначим это пространство через L . Множество простых измеримых функций, каждая из которых сосредоточена на множестве конечной меры, плотно в пространствах L_q , $q \in [1, \infty)$; обозначим это множество простых функций через Q . Для доказательства теоремы достаточно показать плотность L в Q . Для этого, ввиду непрерывности сложения и умножения на скаляр в линейных топологических пространствах, достаточно показать, что индикатор борелевского относительно топологии τ_{l_p} множества, которое имеет ограниченную меру,

можно с любой степенью точности приблизить непрерывной функцией из L . Зафиксируем $\epsilon > 0$ и борелевское множество $B \in \mathfrak{B}_{l_p}$. Так как мера λ_p является регулярной, то существует такое замкнутое в топологии τ_{l_p} множество $K \subset B$, что $\lambda_p(B \setminus K) < \epsilon$. Найдется такое открытое в топологии τ_{l_p} множество U , что $\lambda_p(U \setminus K) < \epsilon$. Определим теперь функцию $g : l_p \rightarrow \mathbb{R}$. Пусть функция g принимает значение 1 на множестве K и значение 0 на множестве $l_p \setminus U$. Тогда теорема Титце о продолжении утверждает, что можно доопределить функцию g на множестве $U \setminus K$ так, что функция g станет непрерывной относительно топологии τ_p и будет ограничена единицей. Функция g является непрерывной относительно топологии τ_p функцией, которая равна нулю вне множества конечной меры. Теперь получаем следующую оценку на расстояние между функциями I_B и g :

$$\|I_B - g\|_{L_q} = \left(\int_{l_p} |I_B(x) - g(x)|^q \lambda_p(dx) \right)^{1/q} = \left(\int_{U \setminus K} |I_B(x) - g(x)|^q \lambda_p(dx) \right)^{1/q} \leq (2\epsilon)^{\frac{1}{q}}.$$

Итак, пространство L является плотным в пространстве $L_q(l_p, \mathfrak{B}_{l_p}, \lambda_p)$. $\square$

Ответ на вопрос о сепарабельности пространств $L_q(l_p, \mathfrak{B}_p, \lambda_p)$ дает следующая лемма.

Лемма 7. *Пространства $L_q(l_p, \mathfrak{B}_{l_p}, \lambda_p)$ не являются сепарабельными при $p \in [1, \infty]$, $q \in [1, \infty)$.*

Доказательство. Докажем лемму при $p \in [1, \infty)$ (при $p = \infty$ доказательство аналогично). Зафиксируем значения p и q . Пусть $x = (x_1, x_2, \dots) \in l_p$ — вектор, при помощи которого была построена мера λ_p . Рассмотрим различные сдвиги множества $[0, x_1] \times [0, x_2] \times \dots$ на векторы вида $(2\alpha_1 x_1, 2\alpha_2 x_2, \dots)$, где $\alpha_i \in \{0, 1\}$ при всех $i \in N$. В результате получается континуальное семейство непересекающихся измеримых множеств, на каждом из которых мера λ_p принимает значение 1; обозначим данное множество через G , а через D — класс индикаторов множеств из G . Класс D имеет мощность континуума. Расстояние между двумя различными функциями из класса D равно $2^{1/q}$. Таким образом, пространства $L_q(l_p, \mathfrak{B}_{l_p}, \lambda_p)$ не могут быть сепарабельными. $\square$

4. Связи между борелевскими σ -алгебрами, порожденными различными топологиями в пространствах l_p . Теперь рассмотрим вопрос о корреляциях между различными топологиями и σ -алгебрами в пространствах l_p . Пусть $p \in [1, \infty)$. Введем следующие обозначения: τ_p — стандартная топология в пространстве l_p , $\tau_{l_p, \infty}$ — топология равномерной сходимости в пространстве l_p . Так как из сходимости в стандартной топологии пространства l_p следует сходимость в равномерной топологии, а из сходимости в равномерной топологии следует сходимость в топологии поточечной сходимости, то получаем следующую цепочку вложений:

$$\tau_{l_p} \subset \tau_{l_p, \infty} \subset \tau_p.$$

Заметим, что все включения являются строгими. Рассмотрим теперь вопрос о том, как связаны между собой борелевские σ -алгебры, относящиеся к топологиям τ_p , $\tau_{l_p, \infty}$ и τ_{l_p} . Для этого введем следующие обозначения: $\mathfrak{B}_p$ — борелевская σ -алгебра, отвечающая топологии τ_p , $\mathfrak{B}_{p, \infty}$ — отвечающая топологии $\tau_{p, \infty}$, $\mathfrak{B}_{l_p}$ — отвечающая топологии τ_{l_p} . Ответ на вопрос о том, как между собой связаны борелевские σ -алгебры $\mathfrak{B}_p$, $\mathfrak{B}_{p, \infty}$ и $\mathfrak{B}_{l_p}$, дает следующая теорема.

Теорема 4. *Борелевские σ -алгебры $\mathfrak{B}_p$, $\mathfrak{B}_{p, \infty}$ и $\mathfrak{B}_{l_p}$ совпадают при $p \in [1, \infty)$.*

Доказательство. Из того факта, что

$$\tau_{l_p} \subset \tau_{l_p, \infty} \subset \tau_p,$$

следует, что

$$\mathfrak{B}_{l_p} \subset \mathfrak{B}_{p, \infty} \subset \mathfrak{B}_p.$$

Докажем теперь обратные включения. Ранее было показано, что замкнутый в стандартной топологии пространства l_p шар с центром в точке 0 является замкнутым относительно топологии поточечной сходимости. Следовательно, открытый в стандартной топологии пространства l_p

шар с центром в точке 0 является борелевским множеством относительно топологии поточечной сходимости. Аналогичное утверждение верно и для открытых шаров с любым центром. Так как пространство l_p со стандартной топологией является сепарабельным, то любое открытое в топологии τ_p множество является борелевским относительно топологии поточечно сходимости. Следовательно, $\mathfrak{B}_p = \mathfrak{B}_{l_p}$, откуда следует равенство борелевских σ -алгебр $\mathfrak{B}_p$, $\mathfrak{B}_{p,\infty}$ и $\mathfrak{B}_{l_p}$. $\square$

Отметим, что в случае пространства l_∞ дело обстоит несколько иначе. Обозначим стандартную топологию в пространстве через τ^∞ . Пространство l_∞ не является сепарабельным относительно топологии τ^∞ . Рассмотрим открытый шар с центром в точке 0 и радиусом $r < 1/5$ в топологии τ^∞ . Рассмотрим всевозможные сдвиги данного шара на векторы, каждая координата которых принимает значение 0 или 1. Таким образом, мы получили континуальное семейство непересекающихся открытых множеств, которое обозначим через S . Рассматривая всевозможные объединения открытых множеств из класса S , получаем систему открытых множеств, мощность которой равна 2^c , где c — мощность континуума. Таким образом, найдется открытое в стандартной топологии пространства l_∞ множество, которое не является борелевским относительно топологии поточечной сходимости, так как в случае произвольного сепарабельного пространства с топологией τ борелевская σ -алгебра, которая отвечает топологии τ , будет континуальной. Значит, борелевская σ -алгебра $\mathfrak{B}_{l_\infty}$ является собственным подмножеством борелевской σ -алгебры, которая отвечает топологии τ^∞ . Так как в случае топологии поточечной сходимости пространства l_p являются сепарабельными при $p \in [1, \infty]$, то справедлива следующая лемма.

Лемма 8. При $p \in [1, \infty]$ меры λ_p не являются полными.

Доказательство. Рассмотрим множество $A = [0, 1] \times \{0\} \times \{0\} \times \dots$. По построению $\lambda_p(A) = 0$, $p \in [1, \infty]$. Множество A является континуальным. Следовательно, мощность системы его подмножеств равна 2^c , где c — мощность континуума. Из этого следует, что при $p \in [1, \infty]$ меры λ_p не являются полными, так как борелевские σ -алгебры $\mathfrak{B}_{l_p}$ имеют мощность континуума. $\square$

Теорема 5. Существует непрерывная относительно топологии τ^∞ функция, которая не является измеримой относительно борелевской σ -алгебры $\mathfrak{B}_{l_\infty}$.

Доказательство. Пусть U — открытое в топологии τ^∞ множество, которое не принадлежит борелевской σ -алгебре $\mathfrak{B}_{l_\infty}$. Пусть $K = l_\infty \setminus U$. Зададим функцию $f : l_\infty \rightarrow \mathbb{R}$ следующим образом: $f(x) = d(x, K)$ для всех $x \in l_\infty$, где $d(\cdot, K)$ — равномерное расстояние до множества K . Отображение f является непрерывным относительно топологии τ^∞ , но не является измеримым относительно борелевской σ -алгебры $\mathfrak{B}_{l_\infty}$, так как множество $f^{-1}(0) = K$ не является элементом σ -алгебры $\mathfrak{B}_{l_\infty}$. $\square$

Автор благодарит В. Ж. Сакбаева за плодотворные обсуждения затронутых в работе проблем.

СПИСОК ЛИТЕРАТУРЫ

1. Борисов Л. А., Орлов Ю. Н., Сакбаев В. Ж. Формулы Фейнмана для усреднения полугрупп, порожденных операторами типа Шредингера/ Препринт ИПМ им. М. В. Келдыша. — 2015. — № 057.
2. Вейль А. Интегрирование в топологических группах и его применение. — М.: ИЛ, 1950.
3. Вершик А. М. Существует ли мера Лебега в бесконечномерном пространстве?// Тр. Мат. ин-та РАН им. В. А. Стеклова. — 2007. — 259. — С. 256–281.
4. Гарсиа-Наранхо Л. С., Монтальди Дж., Смолянов О. Г. Преобразования интегралов Фейнмана по траекториям и обобщенные плотности псевдомер Фейнмана// Докл. РАН. — 2016. 468, № 4. — С. 367–371.
5. Орлов Ю. Н., Сакбаев В. Ж., Смолянов О. Г. Случайные неограниченные операторы и формулы Фейнмана// Изв. РАН. — 2016. — 80, № 6. — С. 141–172.
6. Сакбаев В. Ж. Меры на бесконечномерных пространствах, инвариантные относительно сдвигов// Тр. МФТИ. — 2016. — 8, № 2. — С. 134–141.

7. *Сакбаев В. Ж.* Усреднение случайных блужданий и меры на гильбертовом пространстве, инвариантные относительно сдвига // Теор. мат. физ. — 2017. — 191, № 3. — С. 473–502.
8. *Смолянов О. Г., Шавгулидзе Е. Т.* Континуальные интегралы. — М.: УРСС, 2015.
9. *Baker R.* «Lebesgue measure» on $\mathbb{R}^\infty$ // Proc. Am. Math. Soc. — 1991. — 113, № 4. — С. 1023–1029.

Д. В. Завадский

Московский физико-технический институт (государственный университет)

E-mail: fumi2003@mail.ru



АСИММЕТРИЯ ЛОКАЛЬНО ДОСТУПНОЙ И ЛОКАЛЬНО ПЕРЕДАВАЕМОЙ ИНФОРМАЦИИ В ТЕРМАЛЬНОМ ДВУХКУБИТНОМ СОСТОЯНИИ

© 2018 г. Е. О. КИКТЕНКО

Аннотация. Рассматривается термальное состояние двух частиц со спином $1/2$ (кубитов), находящихся в неоднородном поперечном магнитном поле и взаимодействующих согласно ХУ-модели Гейзенберга. Вводится понятие величины и направления энтропийной асимметрии состояния, а также величины и асимметрии потоков локально передаваемой информации. Показано, что для рассматриваемой системы энтропийная асимметрия направлена от частицы в более слабом магнитном поле к частице в более сильном магнитном поле, и данное направление совпадает с направлением избыточного потока локально передаваемой информации. Также продемонстрировано, что данное направление асимметрии согласуется с направлением избыточного потока локально доступной информации: измерение над частицей в более слабом магнитном поле обеспечивает больший уровень локально доступной информации, чем измерение частицы в более сильном магнитном поле.

Ключевые слова: квантовый дискорд, ХУ-взаимодействие Гейзенберга, локально доступная информация.

AMS Subject Classification: 81V99, 81Q99

СОДЕРЖАНИЕ

1. Введение	45
2. Подходы к описанию асимметрии двусоставных квантовых состояний	46
3. Асимметричная система двух кубитов	50
4. Асимметрия основного состояния	52
5. Асимметрия термального состояния	55
6. Выводы	59
Список литературы	60

1. ВВЕДЕНИЕ

Одной из важнейших задач квантовой теории информации является количественное описание квантовых корреляций между подсистемами составных квантовых систем, являющихся ресурсом для реализации различных задач квантово-информационных технологий (см. [2, 3, 23]). Ключевую роль в этих приложениях играет квантовая запутанность — не имеющее классического аналога свойство составных квантовых систем, при котором их общую волновую функцию невозможно представить в факторизованном виде (для чистых состояний) или их матрицу плотности невозможно представить в виде суммы факторизованных матриц плотности (для смешанных состояний). Несмотря на простоту формального определения выявление наличия запутанности в общем случае смешанного двусоставного состояния сопряжено с серьезными вычислительными трудностями.

Работа выполнена при поддержке гранта Президента Российской Федерации № МК-2815.2017.1.

Для характеристики полной величины корреляций (включающей как квантовую, так и классическую составляющие) используется квантовая взаимная информация, определяющая пропускную способность квантовых каналов с использованием запутанности (см. [10]). Данная величина представляет собой обобщение классической взаимной информации на область квантовых состояний, осуществляемое путем замены классических энтропий Шеннона на энтропии фон Неймана.

Рассмотренные выше меры квантовых корреляций являются *симметричными* в том смысле, что для них выполняется равенство $\mathcal{M}(A, B) = \mathcal{M}(B, A)$, где A и B — подсистемы двусоставной системы AB и $\mathcal{M}$ — мера квантовых корреляций. Однако в работе, озаглавленной «Являются ли квантовые корреляции симметричными?» (см. [11]) дан отрицательный ответ на этот вопрос: показано, что в общем случае две стороны, обладающие частями двусоставного квантового состояния, не могут произвести операции обмена состояниями подсистем при помощи одних лишь локальных операций и классической коммуникации.

Важной асимметричной мерой квантовых корреляций, не обязательно включающих в себя запутанность, является квантовый дискорд (квантовый разлад) независимо предложенный Х. Олливером и В. Зуреком [21], а также независимо Л. Гендерсоном и В. Ведралом [9]. Данная величина представляет собой разницу между величиной квантовой взаимной информации исходного двусоставного состояния и локально доступной информацией (см. [6]), получаемой об одной из подсистем при оптимальном измерении другой подсистемы, и, таким образом, зависит от того, над какой из двух подсистем производится измерение. На основании этого возможно введение величины *асимметрии дискорда*, в свою очередь определяемой разницей между величинами локально доступной информации при измерении различных частей двусоставной системы.

Альтернативный подход к количественному описанию информационной асимметрии квантовых состояний, основанный на квантовом обобщении аппарата классического причинного анализа (см. [1]), представлен в [7, 16–18]. В рамках данного подхода вычисление степени асимметрии квантового двусоставного состояния основано на получении энтропий фон Неймана общей и редуцированных матриц плотности и, в отличие от вычисления дискорда, не требует каких-либо оптимизационных процедур. В [17, 19] показано, что введенная таким образом *энтропийная асимметрия* помогает выявить наиболее устойчивые и наиболее уязвимые квантовые подсистемы с точки зрения воздействия декогеренции. Также важным аспектом, обуславливающим актуальность данного подхода, является возможность его обобщения на томографическое описание квантовых систем, представленная в [7, 16].

В настоящей работе рассматривается вопрос о соответствии энтропийной асимметрии и асимметрии дискорда для состояния термального равновесия двух частиц со спином $1/2$ в неоднородном поле, взаимодействующих в рамках XU -модели Гейзенберга. Вопрос об асимметрии квантового дискорда и влияния на него физических параметров системы был рассмотрен ранее Э. Б. Фельдманом и А. И. Зенчуком (см. [8]). В настоящей работе также рассматривается вопрос о связи представленных выше величин с асимметрией потоков локально передаваемой информации, обусловленных взаимодействием кубитов. В отличие от дискорда и квантовой взаимной информации последняя величина описывает корреляции между состояниями кубитов в различные моменты времени.

Статья организована следующим образом. В разделе 2 вводятся понятия энтропийной асимметрии, асимметрии дискордов и асимметрии локально передаваемой информации. Основные свойства исследуемого XU -взаимодействия и соответствующего термального состояния рассматриваются в разделе 3. Асимметричные характеристики основного и термального состояний рассматриваются в разделах 4 и 5 соответственно. Основные выводы представлены в разделе 6.

2. Подходы к описанию асимметрии двусоставных квантовых состояний

2.1. Энтропийная асимметрия. Рассмотрим двусоставную систему AB , имеющую (в некоторый момент времени) матрицу плотности ρ_{AB} , удовлетворяющую стандартным требованиям:

$$\text{Tr } \rho_{AB} = 1, \quad \rho_{AB} \geq 0,$$

где Tr — оператор следа. Матрицы плотности отдельных подсистем могут быть получены из общей ρ_{AB} путем взятия частичного следа по пространству другой подсистемы:

$$\rho_A = \text{Tr}_B \rho_{AB}, \quad \rho_B = \text{Tr}_A \rho_{AB}.$$

Обобщением безусловной шенноновской энтропии в квантовой теории информации выступает энтропия фон Неймана, которая для произвольного оператора плотности ρ_Ξ записывается в виде

$$S_\Xi \equiv S[\rho_\Xi] \equiv -\text{Tr}[\rho_\Xi \log \rho_\Xi],$$

где под $\log$ мы будем подразумевать двоичный логарифм.

Используя формулу для условной энтропии на основе безусловных энтропий Шеннона для совместного распределения вероятностей, мы можем ввести следующие определения условных энтропий фон Неймана:

$$S_{A|B} \equiv S_{AB} - S_B, \quad S_{B|A} \equiv S_{AB} - S_A. \quad (1)$$

Важнейшим отличием между классической и квантовой теорией информации является то, что в квантовом случае величины (1) могут принимать отрицательные значения (см. [4, 5]), а именно, их диапазоны определяются неравенствами

$$|S_A - S_B| \leq S_{AB} \leq S_A + S_B.$$

Возможная интерпретация отрицательных значений может быть рассмотрена в рамках протокола слияния состояний («state-merging protocol»; см. [12, 13]).

Используя определение (1), получаем формулу для квантовой взаимной информации

$$I = S_A + S_B - S_{AB}, \quad (2)$$

представляющую собой прямой аналог классической взаимной информации. Введем квантовые функции независимости (см. [1]) путем замены энтропий Шеннона на энтропии фон Неймана:

$$i_{A|B} \equiv S_{B|A}/S_B, \quad i_{A|B} \equiv S_{A|B}/S_A, \quad (3)$$

Отметим, что данные величины могут приобретать значения на отрезке $[-1, 1]$, причем отрицательные значения функций независимости можно интерпретировать как наличие более глубоких по сравнению с классическими квантовых корреляций: отрицательное значение хотя бы одной из функций независимости является достаточным условием для наличия запутанности между подсистемами (см. [14]). Предельному случаю чистого запутанного состояния соответствует $i_{A|B} = i_{B|A} = -1$.

Под наличием *энтропийной асимметрии, направленной от подсистемы A к подсистеме B* в двусоставном квантовом состоянии с матрицей плотности ρ_{AB} , будем понимать выполнение неравенства

$$i_{A|B} > i_{B|A}. \quad (4)$$

В случае выполнения обратного неравенства $i_{A|B} < i_{B|A}$ будем говорить о наличии в состоянии ρ_{AB} энтропийной асимметрии, направленной от B к A. Отметим, что вследствие разложения Шмидта для произвольных чистых состояний $\rho_{AB} = |\psi\rangle_{AB}\langle\psi|$ справедливо тождество $S_A = S_B$, что влечет за собой равенство функций независимости $i_{A|B} = i_{B|A}$. Таким образом, необходимым условием наличия энтропийной асимметрии в двусоставном квантовом состоянии является его смешанность.

В качестве количественного описания степени энтропийной асимметрии квантовых состояний будем рассматривать величину

$$d \equiv i_{A|B} - i_{B|A}, \quad (5)$$

которая при подстановке определений функций независимости (3) может быть переписана в виде $d = I(S_A - S_B)/(S_A S_B)$.

Перечислим основные свойства данной величины.

- 1) Знак d определяет направление энтропийной асимметрии. Согласно неравенству (4) значения $d > 0$ соответствуют направленности энтропийной асимметрии от A к B, $d < 0$ — в обратную сторону.
- 2) Тождество $d = 0$ выполняется в двух случаях:

- (i) когда отсутствует энтропийная асимметрия ($S_A = S_B$),
 - (ii) когда корреляции между A и B отсутствуют ($I = 0$).
- 3) Чем больше модуль величины d , тем, очевидно, сильнее энтропийная асимметрия. Абсолютное значение d ограничено неравенством $|d| < 2$.

2.2. Асимметрия дискорда. Квантовый дискорд [9, 21] представляет собой разницу между взаимной информацией в двусоставном состоянии и локально доступной информацией, получаемой оптимальным измерением одной из подсистем. В случае, когда измерение производится над подсистемой A двусоставной системы с матрицей плотности ρ_{AB} и редуцированными матрицами ρ_A и ρ_B , квантовый дискорд может быть записан как

$$D^{(A)} \equiv I - J^{(A)}, \quad (6)$$

где I — квантовая взаимная информация, а $J^{(A)}$ — локально доступная информация, определяемая как

$$J^{(A)} \equiv \max_{\{\Pi_i^A\}} \left(S[\rho_B] - \sum_i p_i S[\rho_B^i] \right), \quad (7)$$

где $\{\Pi_i^A\}$ — положительная операторнозначная мера (ПОЗМ), соответствующая измерению над подсистемой A , $p_i = \text{Tr}[\rho_A \Pi_i^A]$ — вероятности исходов этого измерения, $\rho_B^i = \text{Tr}_A[\rho_{AB} \Pi_i^A]/p_i$ — матрицы плотности, в которые превращается исходная матрица ρ_B в результате измерения над подсистемой A .

Аналогичным образом можно ввести величину квантового дискорда $D^{(B)}$, определенного для измерения на подсистемой B . Важно отметить, что в общем случае дискорд несимметричен: $D^{(A)} \neq D^{(B)}$. В [8] показано, что применительно к рассматриваемой системе частиц со спином $1/2$ в неоднородном магнитном поле наличие неоднородности поля приводит к появлению асимметрии квантового дискорда. В качестве количественного описания асимметрии дискорда будем использовать безразмерную величину

$$\Delta D \equiv \frac{D^{(B)} - D^{(A)}}{I} = \frac{J^{(A)} - J^{(B)}}{I}, \quad (8)$$

сводящуюся к разности значений локально доступной информации при измерении над подсистемами B и A .

2.3. Асимметрия локально передаваемой информации. Далее рассмотрим вопрос о локальной передаче информации в стационарных состояниях квантовых систем. Пусть имеется некоторая двусоставная система, эволюция которой определяется ее гамильтонианом $\mathcal{H}$. В случае, если $\mathcal{H}$ не зависит от времени, оператор эволюции системы может быть получен как $U(t) = e^{-i\mathcal{H}t}$ (здесь и далее мы полагаем $\hbar = 1$). Рассмотрим стационарное двусоставное состояние ρ_{AB} (см. рис. 1), инвариантное к действию оператора собственной эволюции $U(t)$:

$$U(t)\rho_{AB}U^\dagger(t) = \rho_{AB}.$$

Введем локальные базисы $\{|i\rangle_A\}$ и $\{|j\rangle_B\}$ в пространствах подсистем, в которых редуцированные матрицы плотности подсистем ρ_A и ρ_B имеют диагональный вид:

$$\rho_A = \sum_i p_A^i |i\rangle_A \langle i|, \quad \rho_B = \sum_j p_B^j |j\rangle_B \langle j|. \quad (9)$$

Без ограничения общности будем рассматривать вопрос о локальной передаче информации в направлении от A к B . Для этого также введем характерное время локального взаимодействия между подсистемами t_{loc} . Для того, чтобы получить сведения о корреляциях между состоянием подсистемы A в момент времени $t = 0$ и состоянием подсистемы B в момент времени $t = t_{\text{loc}}$, введем дополнительную подсистему A' , имеющую такую же размерность и набор базисных состояний, что и A , и приготовленную изначально в состоянии $|0\rangle_{A'}$. Пусть в момент времени $t = 0$ происходит проектирующее измерение подсистемы A с записью результатов измерения на подсистему A' в соответствии с преобразованием

$$|0i\rangle_{A'A} \rightarrow |ii\rangle_{A'A}. \quad (10)$$

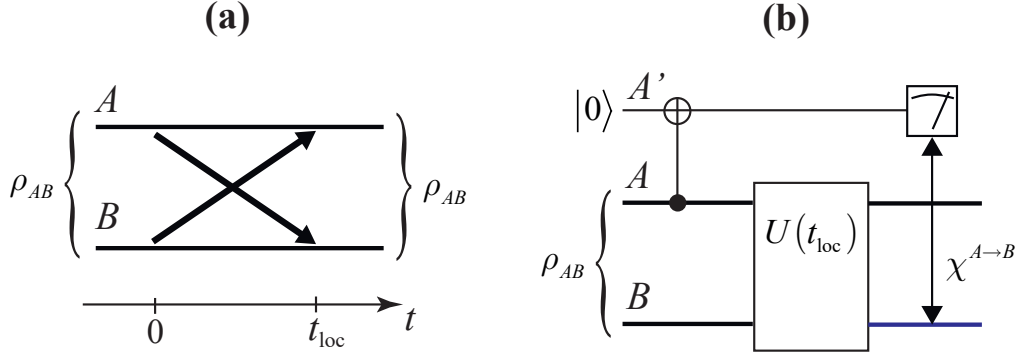


Рис. 1. (a) Схематичное изображение локальных потоков информации в стационарном двусоставном состоянии. (b) Эквивалентное представление потоков информации в квантово-информационных обозначениях для двухкубитных состояний: вертикальной линией обозначен вентиль CNOT, связывающий контролирующий (•) и контролируемый ($\oplus$) кубиты.

В случае кубитов это преобразование соответствует действию вентиль CNOT (см. рис. 1), в котором контролирующим является кубит A . Другими словами, в момент времени $t = 0$ мы производим «копирование» состояния A на A' . Данное утверждение не противоречит известной теореме о запрете квантового клонирования (см. [26]) в силу изначальной договоренности о диагональности матрицы ρ_A в рассматриваемом базисе $\{|i\rangle_A\}$ (см. (9)). С точки зрения всего ансамбля возможных результатов измерения преобразование (10) оставляет состояние подсистемы A неизменным, в то время как общее состояние всей системы ρ_{AB} деформируется. В конкретном случае получения i -го результата измерения, реализующегося с вероятностью p_A^i , матрица плотности ρ_{AB} претерпевает следующее изменение:

$$\rho_{AB} \rightarrow \frac{1}{p_A^i} |i\rangle_A \langle i| \otimes \langle i|_A \rho_{AB} |i\rangle_A.$$

Далее, если оставить систему эволюционировать в соответствии с ее оператором эволюции $U(t)$, состояние подсистемы B в зависимости от времени при условии реализации i -го результата измерения будет иметь вид

$$\tilde{\rho}_B^i(t) = \frac{1}{p_A^i} \text{Tr}_A \left[U(t) (|i\rangle_A \langle i| \otimes \langle i|_A \rho_{AB} |i\rangle_A) U^\dagger(t) \right]. \quad (11)$$

Величину взаимной информации между подсистемой A' , хранящей память о подсистеме в момент времени $t = 0$, и подсистемой B в произвольный момент времени t можно вычислить как разницу безусловной и условных энтропий:

$$\chi^{A \rightarrow B}(t) = S \left[\sum_i p_A^i \tilde{\rho}_B^i(t) \right] - \sum_i p_A^i S[\tilde{\rho}_B^i(t)]. \quad (12)$$

В некотором роде мы можем говорить о наличии однопараметрического семейства классически-квантовых каналов (см. [10]), на вход которых подается классическое вероятностное распределение $\{p_A^i\}$, а на выходе соответственно реализуются состояния $\{\tilde{\rho}_B^i(t)\}$. В такой интерпретации величина $\chi^{A \rightarrow B}(t)$ представляет собой границу Холево такого канала. Основным отличием же рассматриваемой ситуации от действия настоящих квантовых каналов является, конечно же, невозможность варьирования входного сигнала, что снимает возможность постановки вопроса о пропускных способностях.

Очевидно, все представленные выше рассуждения можно провести для случая измерения над B и получить величину $\chi^{B \rightarrow A}(t)$. Также отметим, что из общих физических соображений величины $\chi^{A \rightarrow B}(t)$ и $\chi^{B \rightarrow A}(t)$ должны достигать локальных максимумов при $t = t_{\text{loc}}$.

В настоящей работе основной интерес будет представлять величина средней локально передаваемой информации

$$\chi \equiv \frac{1}{2} (\chi^{A \rightarrow B}(t_{\text{loc}}) + \chi^{B \rightarrow A}(t_{\text{loc}})), \quad (13)$$

а также относительная асимметрия локально передаваемой информации

$$\Delta\chi \equiv \frac{\chi^{A \rightarrow B}(t_{\text{loc}}) - \chi^{B \rightarrow A}(t_{\text{loc}})}{\chi^{A \rightarrow B}(t_{\text{loc}}) + \chi^{B \rightarrow A}(t_{\text{loc}})}. \quad (14)$$

Важно отметить, что в выражении (11) мы пренебрегли возможным действием окружающей среды; таким образом, все вышеприведенные рассуждения верны в пределе

$$t_{\text{loc}} \ll t_{\text{rel}},$$

где t_{rel} — время релаксации к исходному состоянию ρ_{AB} .

3. АСИММЕТРИЧНАЯ СИСТЕМА ДВУХ КУБИТОВ

Рассмотрим систему, состоящую из двух частиц со спином $1/2$, находящихся в неоднородном магнитном поле и взаимодействующих друг с другом согласно XY -модели Гейзенберга. Гамильтониан исследуемой системы имеет вид

$$\mathcal{H} = B_1 S_z \otimes \mathbf{I}_2 + B_2 \mathbf{I}_2 \otimes S_z + g(S_x \otimes S_x + S_y \otimes S_y) \quad (15)$$

где $S_\alpha = \sigma_\alpha/2$ ($\alpha = x, y, z$) — операторы проекций спина $1/2$, σ_α — стандартные матрицы Паули

$$\sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix},$$

$\mathbf{I}_n$ — единичная матрица размерности $n \times n$, g — константа взаимодействия между частицами, B_1 и B_2 — величины магнитных полей, выраженных в энергетических единицах с учетом величины магнитных моментов. В качестве вариантов физической реализации систем, описываемых данной моделью, можно рассматривать пару зарядовых кубитов с фазовой связью за счет джозефсоновских переходов (см. [22]), электронные спины в полупроводниковых квантовых точках (см. [15, 27]), а также ядерный магнитный резонанс в жидких кристаллах (см. [29]).

Для состояний частиц со спинами, направленным вдоль и противоположно оси z , договоримся использовать квантово-информационные обозначения $|\uparrow_z\rangle \equiv |0\rangle$, $|\downarrow_z\rangle \equiv |1\rangle$.

В качестве основного объекта исследования будем рассматривать состояние термального равновесия

$$\rho_{AB} = \frac{1}{Z} \exp\left(-\frac{\mathcal{H}}{k_B T}\right), \quad Z = \text{Tr}\left[\exp\left(-\frac{\mathcal{H}}{k_B T}\right)\right], \quad (16)$$

где T и k_B — температура и константа Больцмана соответственно. Особый интерес представляет собой основное состояние гамильтониана (15), получаемое из состояния (16) в пределе $T \rightarrow 0$.

Для удобства представления результатов перейдем к безразмерным величинам, положив $\hbar = k_B = g = 1$. Таким образом, рассматриваемая система в общем случае термального состояния определяются тремя независимыми безразмерными параметрами B_1 , B_2 и T , характеризующими отношение соответствующих видов энергии к энергии взаимодействия между частицами.

В результате решения задачи на собственные векторы и собственные значения гамильтониана (15)

$$\mathcal{H}|\psi^{(i)}\rangle = E^{(i)}|\psi^{(i)}\rangle, \quad i = 1, \dots, 4,$$

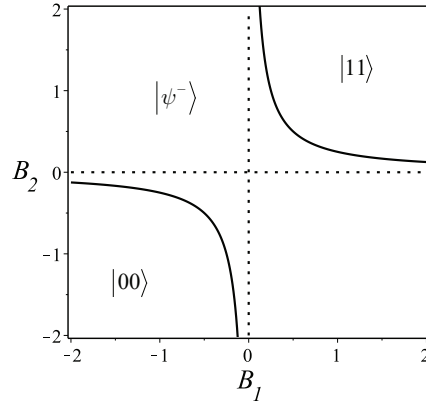


Рис. 2. Фазовая диаграмма основного состояния гамильтониана (15)

имеем

$$\begin{aligned} |\psi^{(1)}\rangle &= |00\rangle, & E^{(1)} &= \frac{B_1 + B_2}{2}, \\ |\psi^{(2)}\rangle &= |11\rangle, & E^{(2)} &= -\frac{B_1 + B_2}{2}, \\ |\psi^{(3)}\rangle &= |\psi^+\rangle, & E^{(3)} &= \frac{K}{2}, \\ |\psi^{(4)}\rangle &= |\psi^-\rangle, & E^{(4)} &= -\frac{K}{2}, \end{aligned}$$

где

$$|\psi^\pm\rangle = \frac{1}{N^\pm} [|01\rangle + (\Delta B \pm K)|10\rangle] \quad (17)$$

и приняты следующие обозначения:

$$\Delta B = B_2 - B_1, \quad K = \sqrt{\Delta B^2 + 1}, \quad N^\pm = \sqrt{1 + (\Delta B \pm \sqrt{K})^2}. \quad (18)$$

Сравнивая значения энергий $E^{(i)}$ в зависимости от наложенных полей B_1 и B_2 , легко получить фазовую диаграмму основного состояния, представленную на 2. Гипербола

$$B_2 = \frac{1}{4B_1} \quad (19)$$

разделяет пространство на три области: при $B_1 B_2 < 1/4$ основному состоянию соответствует чистое запутанное состояние $|\psi^-\rangle$, при $B_1 B_2 > 1/4$ основное состояние является чистым и сепарабельным ($|00\rangle$ при положительных B_1 и B_2 и $|11\rangle$ при отрицательных).

Для удобства дальнейших вычислений перепишем векторы $|\psi^\pm\rangle$ в виде

$$|\psi^+\rangle = \cos \frac{\theta}{2} |01\rangle + \sin \frac{\theta}{2} |10\rangle, \quad |\psi^-\rangle = -\sin \frac{\theta}{2} |01\rangle + \cos \frac{\theta}{2} |10\rangle,$$

где параметр θ определяется формулой

$$\theta = 2 \arctg(\Delta B + K) = 2 \arctg(\Delta B + \sqrt{\Delta B^2 + 1}). \quad (20)$$

Тогда матрица оператора эволюции системы

$$U(t) = e^{-i\mathcal{H}t} = \sum_{j=1}^4 e^{-iE^{(j)}t} |\psi^{(j)}\rangle \langle \psi^{(j)}|$$

будет иметь в вычислительном базисе вид

$$U(t) = \begin{bmatrix} e^{-i(B_1+B_2)t/2} & 0 & 0 & 0 \\ 0 & \cos^2 \frac{\theta}{2} e^{-iKt/2} + \sin^2 \frac{\theta}{2} e^{iKt/2} & -i \sin \theta \sin \frac{Kt}{2} & 0 \\ 0 & -i \sin \theta \sin \frac{Kt}{2} & \sin^2 \frac{\theta}{2} e^{-iKt/2} + \cos^2 \frac{\theta}{2} e^{iKt/2} & 0 \\ 0 & 0 & 0 & e^{i(B_1+B_2)t/2} \end{bmatrix}. \quad (21)$$

Исходя из вида оператора (21) для рассматриваемой системы локального обмена информацией t_{loc} можно ввести как минимальное время, максимизирующее амплитуды недиагональных элементов $|\langle 01|U(t)|10\rangle| = |\langle 10|U(t)|01\rangle|$:

$$t_{loc} = \frac{\pi}{K}. \quad (22)$$

Подставляя (22) в (21), получим

$$U(t_{loc}) = \begin{bmatrix} e^{-i(B_1+B_2)\pi/(2K)} & 0 & 0 & 0 \\ 0 & -i \cos \theta & -i \sin \theta & 0 \\ 0 & -i \sin \theta & i \cos \theta & 0 \\ 0 & 0 & 0 & e^{i(B_1+B_2)\pi/(2K)} \end{bmatrix}.$$

Как нетрудно убедиться, наиболее эффективный локальный обмен информацией осуществляется в случае резонанса $B_1 = B_2 = B_0$, при котором $K = 1$, $\theta = \pi/2$ и

$$U(t_{loc}) = \begin{bmatrix} e^{iB_0 t} & 0 & 0 & 0 \\ 0 & 0 & -i & 0 \\ 0 & -i & 0 & 0 \\ 0 & 0 & 0 & e^{-iB_0 t} \end{bmatrix},$$

что соответствует действию оператора обмена iSWAP совместно с действием локальных фазовых операторов на каждую из частиц. Появление неоднородности поля ΔB ведет к отстройке от резонанса, уменьшению значения $\sin \theta$ и ухудшению локального обмена информацией.

4. АСИММЕТРИЯ ОСНОВНОГО СОСТОЯНИЯ

Как было показано ранее, можно выделить следующие типы основных состояний исследуемого гамильтониана в зависимости от соотношения полей B_1 и B_2 (см. рис. 2): чистое сепарабельное состояние $|00\rangle$ и $|11\rangle$, чистое запутанное состояние $|\psi^-\rangle$, вырожденное основное состояние

$$\rho_{AB}^{\text{gr}} = \frac{1}{2}|11\rangle\langle 11| + \frac{1}{2}|\psi^-\rangle\langle \psi^-| = \frac{1}{2} \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & \sin^2 \frac{\theta}{2} & -\sin \frac{\theta}{2} & 0 \\ 0 & -\sin \frac{\theta}{2} & \cos^2 \frac{\theta}{2} & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad (23)$$

на ветви гиперболы (19) $B_1, B_2 > 0$, а также

$$\tilde{\rho}_{AB}^{\text{gr}} = \frac{1}{2}|00\rangle\langle 00| + \frac{1}{2}|\psi^-\rangle\langle \psi^-| \quad (24)$$

на ветви гиперболы (19) $B_1, B_2 < 0$.

В рамках изучения энтропийной асимметрии основной интерес представляет случай вырождения, при котором оно становится смешанным. Однако прежде чем переходить к смешанному основному состоянию, рассмотрим вопрос о локальных потоках информации в чистых основных состояниях.

Очевидно, в случаях состояний $|00\rangle$ (или $|11\rangle$) ситуация тривиальна: проективное измерение в вычислительном базисе какой-либо из частиц с вероятностью 1 оставляет состояние неизменным, а последующая эволюция может добавляет лишь дополнительный фазовый множитель. Таким образом, для основного состояния $B_1 B_2 > 1/4$ имеем $\chi = \Delta\chi = 0$.

Более интересная ситуация реализуется для состояний $|\psi^-\rangle$ (см. (17)). Проективное измерение этого состояния приводит к его коллапсу либо в вектор $|01\rangle$ с вероятностью $\sin^2(\theta/2)$, либо в вектор $|10\rangle$ с вероятностью $\cos^2(\theta/2)$. Последующая эволюция полного ансамбля этих состояний в соответствии с оператором (21) приводит к матрице с общим видом ненулевых элементов

$$\tilde{\rho}_{AB}(t) = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & \bullet & \bullet & 0 \\ 0 & \bullet & \bullet & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \quad (25)$$

редуцирование которой дает одинаковые матрицы плотности подсистем. Вследствие этого имеем отсутствие асимметрии локальных потоков информации $\Delta\chi = 0$.

Перейдем к изучению вырожденного основного состояния, лежащего на гиперболе $B_1 B_2 = 1/4$. Рассмотрим состояния, принадлежащие ветви, располагающейся в квадранте $B_1, B_2 > 0$ (для квадранта $B_1, B_2 < 0$ результаты будут аналогичными вследствие общей симметрии). В данной области матрица плотности основного состояния принимает вид (23), а редуцированные матрицы подсистем соответственно

$$\begin{aligned} \rho_A^{\text{gr}} &= \frac{1}{2(N^-)^2} \begin{bmatrix} 1 & 0 \\ 0 & (K - \Delta B)^2 + (N^-)^2 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} \sin^2 \frac{\theta}{2} & 0 \\ 0 & 1 + \cos^2 \frac{\theta}{2} \end{bmatrix}, \\ \rho_B^{\text{gr}} &= \frac{1}{2(N^-)^2} \begin{bmatrix} (K - \Delta B)^2 & 0 \\ 0 & 1 + (N^-)^2 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} \cos^2 \frac{\theta}{2} & 0 \\ 0 & 1 + \sin^2 \frac{\theta}{2} \end{bmatrix}. \end{aligned} \quad (26)$$

Важно отметить, что все элементы матриц (23) и (26) однозначно определяются неоднородностью поля ΔB (см. (18)).

Для вычисления величины энтропийной асимметрии d и взаимной информации I воспользуемся явным видом общей (23) и редуцированных (26) матриц плотности. Легко видеть, что

$$S[\rho_{AB}^{\text{gr}}] = 1, \quad S[\rho_A^{\text{gr}}] = h_b \left(\frac{1}{2} \sin^2 \frac{\theta}{2} \right), \quad S[\rho_B^{\text{gr}}] = h_b \left(\frac{1}{2} \cos^2 \frac{\theta}{2} \right),$$

где

$$h_b(x) \equiv -x \log x - (1-x) \log(1-x) \quad (27)$$

— бинарная энтропийная функция.

Из-за неоднородности поля ΔB от 0 до $+\infty$ мы имеем возрастание величины $\sin^2(\theta/2)/2$ от $1/4$ до $1/2$ и убывание $\cos^2(\theta/2)/2$ от $1/4$ до 0. Таким образом при $\Delta B > 0$ имеем $S[\rho_A^{\text{gr}}] > S[\rho_B^{\text{gr}}]$. Соответственно при $\Delta B < 0$ ситуация меняется на противоположную, и мы получаем $S[\rho_A^{\text{gr}}] < S[\rho_B^{\text{gr}}]$.

Важным свойством матрицы (23) является то, что она относится к семейству матриц X -типу (см. [28]), что значительно упрощает вычисление величин квантового дискорда (см. [20]). Максимумы локально доступной информации $J^{(A)}$ и $J^{(B)}$ достигаются при измерении проекций спина частиц A и B на ось x и оказываются равными

$$\begin{aligned} J^{(A)} &= 1 + h_b \left(\frac{1}{2} \cos^2 \frac{\theta}{2} \right) - h_q \left(\sin \frac{\theta}{2} \right), \\ J^{(B)} &= 1 + h_b \left(\frac{1}{2} \sin^2 \frac{\theta}{2} \right) - h_q \left(\cos \frac{\theta}{2} \right), \end{aligned} \quad (28)$$

где

$$h_q = -\frac{1}{2}(1-x) \log \frac{1-x}{4} - \frac{1}{2}(1+x) \log \frac{1+x}{4}. \quad (29)$$

Для вычисления локального потока информации $\chi^{A \rightarrow B}(t_{\text{loc}})$ необходимо получить вид матриц плотности $\tilde{\rho}_B^i(t_{\text{loc}})$ и соответствующих вероятностей p_A^i . Для исследуемого состояния они оказываются равными

$$\begin{aligned} p_A^0 &= \frac{1}{2} \sin^2 \frac{\theta}{2}, & \tilde{\rho}_B^0(t_{\text{loc}}) &= \sin^2 \theta |0\rangle\langle 0| + \cos^2(\theta) |1\rangle\langle 1|, \\ p_A^1 &= 1 - \frac{1}{2} \sin^2 \frac{\theta}{2}, & \tilde{\rho}_B^1(t_{\text{loc}}) &= (1 - \Gamma) |0\rangle\langle 0| + \Gamma |1\rangle\langle 1|, \end{aligned} \quad (30)$$

где

$$\Gamma = \frac{4 \cos\left(\frac{\theta}{2}\right)^4 \sin^2 \frac{\theta}{2} + 1}{\cos\left(\frac{\theta}{2}\right)^2 + 1}.$$

Противоположный поток информации вычисляется путем замены $\theta \rightarrow \bar{\theta} = 2 \arctg(-\Delta B + K)$, в свою очередь подразумевающую замену $\sin(\theta/2) \leftrightarrow \cos(\theta/2)$.

Также рассмотрим величину согласованности (меры запутанности двухкубитных состояний, см. [25]) в состоянии (23), которую для двухкубитного состояния ρ_{AB} можно вычислить по формуле

$$C[\rho_{AB}] = \max\left(0, \tilde{\lambda}_1 - \tilde{\lambda}_2 - \tilde{\lambda}_3 - \tilde{\lambda}_4\right), \quad (31)$$

где упорядоченное множество $\{\tilde{\lambda}_i\}$ представляет собой убывающие по абсолютным значениям собственные числа матрицы

$$\tilde{\rho}_{AB} = \sqrt{\sqrt{\rho_{AB}}(\sigma_y \otimes \sigma_y)\rho_{AB}^*(\sigma_y \otimes \sigma_y)\sqrt{\rho_{AB}}} \quad (32)$$

(* обозначает комплексное сопряжение).

Для рассматриваемого состояния (23) величина согласованности $C[\rho_{AB}^{\text{gr}}] = \frac{1}{2} \sin \theta$.

Таким образом, все исследуемые меры корреляций определяются параметром θ , который в свою очередь зависит только от неоднородности поля ΔB (см. (20)).

Поведение величин d , ΔD и $\Delta \chi$, характеризующих асимметрию состояния, как функций ΔB представлено на рис. 3(a), соответствующее поведение величин C , I и χ , характеризующих общий уровень корреляций, — на рис. 3(b). В согласии с интуитивными представлениями в случае однородности поля $\Delta B = 0$ исследуемое состояние является симметричным, и для него выполняется равенство энтропий подсистем $S[\rho_A^{\text{gr}}] = S[\rho_B^{\text{gr}}]$. Кроме того, при $\Delta B = 0$ вектор $|\psi^-\rangle$, отвечающий за наличие запутанности в смешанном состоянии (23), превращается в максимально запутанное белловское состояние, чему соответствует максимум согласованности C и взаимной информации I .

Неоднородность магнитного поля влечет за собой возникновение энтропийной асимметрии d , которая совпадает со знаком ΔB . Данное обстоятельство объясняется стабилизирующей ролью магнитного поля: чем больше напряженность поля, тем сильнее оно ограничивает неопределенность в направлении соответствующего спина в основном состоянии. Также отметим, что величина d монотонно возрастает (убывает) с возрастанием (убыванием) ΔB .

Из представленного поведения величины ΔD следует, что наибольший локальный доступ к взаимной информации достигается при измерении, проводимом над спином, находящимся в более слабом магнитном поле и обладающим большей энтропией. Таким образом, направление асимметрии дискордов совпадает с направлением энтропийной асимметрии. Кроме того, для представленной области параметров с большой степенью точности выполняется равенство $d \approx 4.1 \Delta D$, из которого после умножения на величину взаимной информации I следует соотношение на безусловную асимметрию дискордов:

$$d \cdot I \approx 4.1 \left(D^{(B)} - D^{(A)} \right) = 4.1 \left(J^{(A)} - J^{(B)} \right),$$

где, напомним, $J^{(A)}$ и $J^{(B)}$ представляют собой величины локально доступной информации при измерениях над A и B соответственно.

Перейдем к рассмотрению поведения локальных потоков информации, характеризующихся величинами χ и $\Delta \chi$. Как мы видим, в случае $\Delta B > 0$, что соответствует $B_2 > B_1$, локальный поток

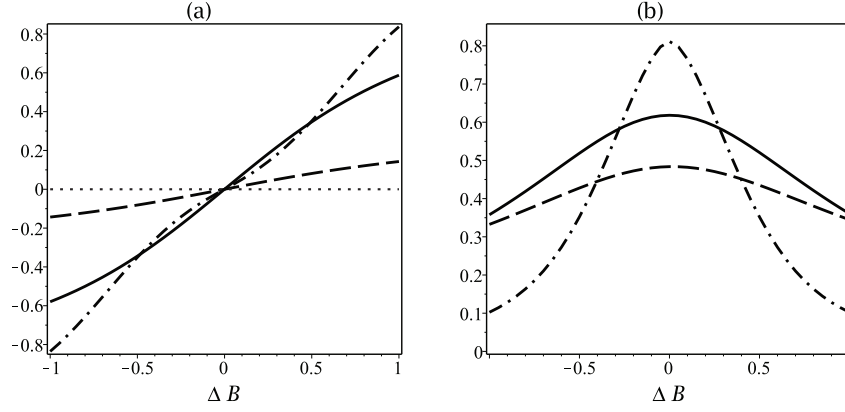


Рис. 3. (а) Поведение энтропийной асимметрии d (сплошная линия), относительной асимметрии дискорда ΔD (пунктирная линия) и относительной асимметрии локально передаваемой информации $\Delta\chi$ (штрихпунктирная линия) как функции неоднородности магнитного поля ΔB . (б) Поведение взаимной информации I (сплошная линия), согласованности C (пунктирная линия) и средней локально передаваемой информации χ как функции неоднородности магнитного поля ΔB

информации $\chi^{A \rightarrow B}(t_{\text{loc}})$ от частицы A к частице B превышает противоположный поток информации $\chi^{B \rightarrow A}(t_{\text{loc}})$. Данное поведение полностью согласуется со значениями остальных величин, характеризующими асимметрию корреляций, т.е. d и ΔD .

5. АСИММЕТРИЯ ТЕРМАЛЬНОГО СОСТОЯНИЯ

Перейдем к рассмотрению состояния термального равновесия (16) при ненулевых температурах. Его матрица плотности в явном виде может быть записана как

$$\rho_{AB} = \frac{1}{Z} \begin{bmatrix} \exp \frac{-B_1 - B_2}{2T} & 0 & 0 & 0 \\ 0 & m - n & -s & 0 \\ 0 & -s & m + n & 0 \\ 0 & 0 & 0 & \exp \frac{B_1 + B_2}{2T} \end{bmatrix}, \quad (33)$$

где приняты обозначения

$$m = \text{ch} \frac{K}{2T}, \quad n = -\cos \theta \text{sh} \frac{K}{2T}, \quad s = \sin \theta \text{sh} \frac{K}{2T},$$

$$Z = 2m + \exp \frac{B_1 + B_2}{2T} + \exp \frac{-B_1 - B_2}{2T}.$$

Матрицы подсистем соответственно принимают вид

$$\rho_A = \frac{1}{Z} \begin{bmatrix} \exp \frac{-B_1 - B_2}{2T} + m - n & 0 \\ 0 & \exp \frac{B_1 + B_2}{2T} + m + n \end{bmatrix},$$

$$\rho_B = \frac{1}{Z} \begin{bmatrix} \exp \frac{-B_1 - B_2}{2T} + m + n & 0 \\ 0 & \exp \frac{B_1 + B_2}{2T} + m - n \end{bmatrix}. \quad (34)$$

Энтропии всей системы и подсистем могут быть получены следующим образом:

$$S[\rho_{AB}] = \log Z + \frac{E}{T},$$

$$S[\rho_A] = h_b \left(\frac{1}{Z} \exp \frac{-B_1 - B_2}{2T} + m - n \right), \quad S[\rho_B] = h_b \left(\frac{1}{Z} \exp \frac{-B_1 - B_2}{2T} + m + n \right).$$

В случае однородности магнитного поля $B_1 = B_2 = B_0$ получаем, очевидно, равенство редуцированных матриц плотности:

$$\rho_A = \rho_B = \frac{1}{Z} \begin{bmatrix} \exp \frac{-B_0}{T} + \operatorname{ch} \frac{1}{2T} & 0 \\ 0 & \exp \frac{B_0}{T} + \operatorname{ch} \frac{1}{2T} \end{bmatrix},$$

а также их энтропий фон Неймана.

С другой стороны, в случае равных по модулю антипараллельных полей, $B_1 = -B_2 = B_0$, матрицы плотности подсистем принимают вид

$$\rho_A = \begin{bmatrix} 1 + m_0 + n_0 & 0 \\ 0 & 1 + m_0 - n_0 \end{bmatrix}, \quad \rho_B = \begin{bmatrix} 1 + m_0 - n_0 & 0 \\ 0 & 1 + m_0 + n_0 \end{bmatrix},$$

где m_0 и n_0 — соответствующие данным полям значения величин m и n , и мы вновь получаем равенство их энтропий фон Неймана. Таким образом, мы можем заключить, что при $|B_1| = |B_2|$ энтропийная асимметрия в состоянии (33) отсутствует.

Рассмотрим соотношения между энтропиями фон Неймана редуцированных матриц плотности в случае $|B_1| \neq |B_2|$. Для этой цели рассмотрим разность мер смешанности $1 - \operatorname{Tr} \rho_A^2$ и $1 - \operatorname{Tr} \rho_B^2$. Подставляя явный вид матриц (34), получаем

$$\operatorname{Tr} \rho_B^2 - \operatorname{Tr} \rho_A^2 = \frac{4}{Z^2} n \exp \left(-\frac{B_1 + B_2}{T} \right) \left(1 - \exp \left(\frac{B_1 + B_2}{T} \right) \right). \quad (35)$$

Знак выражения (35) определяется, с одной стороны, знаком суммы полей $B_1 + B_2$, а с другой стороны знаком величины n , определяющимся, в свою очередь, знаком ΔB ($\operatorname{sign} n = \Delta B$). В результате имеем $\operatorname{Tr} \rho_B^2 > \operatorname{Tr} \rho_A^2$ при $|B_1| < |B_2|$ и $\operatorname{Tr} \rho_B^2 < \operatorname{Tr} \rho_A^2$ при $|B_1| > |B_2|$. Однако знак $\operatorname{sign}(\operatorname{Tr} \rho_B^2 - \operatorname{Tr} \rho_A^2)$ очевидно совпадает со знаком $\operatorname{sign}(S[\rho_A] - S[\rho_B])$, таким образом энтропийная асимметрии направлена от частицы в более слабом магнитном поле к частице в более сильном магнитном поле.

Величина согласованности для состояния (33) будет иметь вид

$$C[\rho_{AB}] = \max\{0, 2(s - 1)/Z\}.$$

Рассмотрим три конфигурации магнитных полей:

- (i) $B_1 = B_1^c, B_2 = B_2^c$;
- (ii) $B_1 = B_1^c, B_2 = B_2^c + 0,4$;
- (iii) $B_1 = B_1^c, B_2 = B_2^c - 0,4$;

в которых значения $B_1^c \approx 0,309$ и $B_2^c \approx 0,809$ определяются соотношением $B_1^c B_2^c = 1/4$, соответствующим гиперболе вырожденных основных состояний, и величине неоднородности поля $B_2^c - B_1^c = 0,5$. На рис. 4 представлены все основные характеристики, описывающие асимметрию и величины корреляций в исследуемых состояниях как функции температуры.

Как было показано ранее, в случае нулевой температуры асимметрия корреляций присутствует лишь в вырожденных основных состояниях. Из зависимостей, представленных на рис. 4(a)–(c) следует, что с ростом температуры невырожденные основные состояния также приобретают асимметрию с позиции всех трех исследуемых величин: d , ΔD и $\Delta \chi$; причем поведение всех величин имеет качественно схожий характер. Отметим, что для пары полей $(B_1^c, B_2^c + 0,4)$, которой соответствует сепарабельное состояние $|11\rangle$, имеет место более резкое возникновение асимметрии по сравнению с конфигурацией $B_1^c, B_2^c - 0,4$, которой соответствует чистое запутанное основное состояние $|\psi^-\rangle$. Меры асимметрии для вырожденного основного состояния сохраняют свои значения при $T \lesssim 0,2$, после чего происходит их убывание с дальнейшим ростом температуры. Таким образом, при $T \rightarrow \infty$ термальное состояние теряет асимметрию при фиксированных значениях магнитных полей.

Перейдем к рассмотрению поведения величин, характеризующих объем корреляций, представленных на рис. 4(d)–(f). Для конфигурации полей $(B_1^c, B_2^c + 0,4)$ имеет место возникновение и рост величин I и C с возрастанием температуры при $T \lesssim 0,2$, объясняющийся появлением компоненты $|\psi^-\rangle\langle\psi^-|$, ответственной за корреляции, в общей термальной смеси. Дальнейший рост

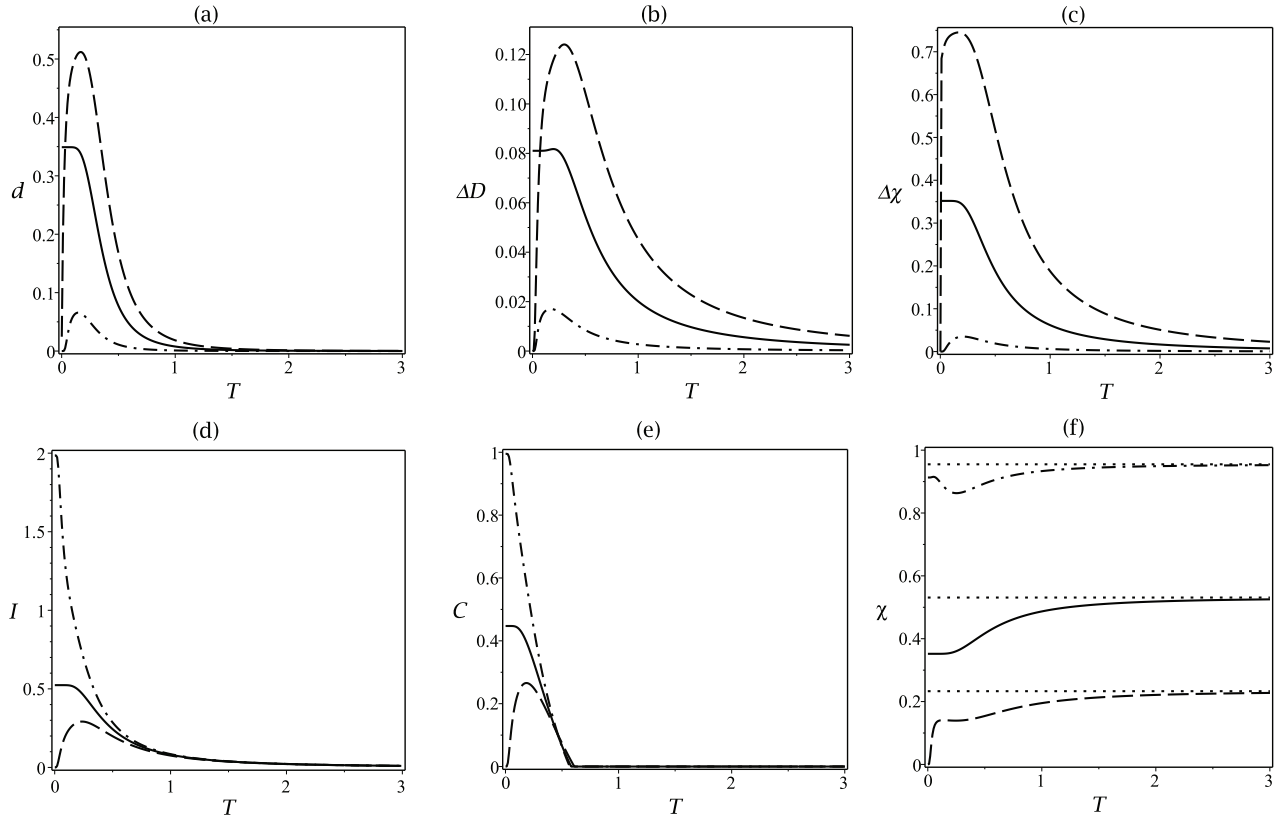


Рис. 4. Зависимость (а) энтропийной асимметрии d , (б) относительной асимметрии дискорда ΔD , (с) относительной асимметрии локально передаваемой информации $\Delta\chi$, (д) взаимной информации I , (е) согласованности C и (ф) средней локально передаваемой информации χ от температуры T в состоянии (33) при соответствующих значениях магнитных полей B_1^c, B_2^c (сплошная линия), $B_1^c, B_2^c + 0,4$ (пунктирная линия), $B_1^c, B_2^c - 0,4$ (штрихпунктирная линия). На рисунке (ф) дополнительно представлены асимптотические значения, вычисленные по формуле (41)

температуры ведет к увеличению смешанности состояния, и в пределе $T \rightarrow \infty$ мы получаем максимально смешанное двухкубитное состояние

$$\rho_{AB}^{\text{asympt}} = \frac{1}{4}\mathbf{I}_4, \quad (36)$$

в котором мгновенные корреляции отсутствуют.

Качественно иное поведение демонстрирует величина χ , соответствующая потокам локальной информации и отвечающая за запаздывающие корреляции между подсистемами. Зависимости, представленные на рис. 4(ф), демонстрируют наличие горизонтальных асимптот, на которые выходят зависимости χ в пределе $T \rightarrow \infty$. Получим аналитические выражения для данных асимптот, исходя из вида матрицы плотности (36) и оператора эволюции (21).

Измерение частицы A приведет к коллапсу состояния (36) в состояния $|0\rangle\langle 0| \otimes \mathbf{I}_2/2$ или $|1\rangle\langle 1| \otimes \mathbf{I}_2/2$ с одинаковыми вероятностями $p_A^1 = p_A^2 = 1/2$. Их последующая эволюция в течение промежутка времени $t = t_{\text{loc}}$ приведет к соответствующим состояниям частицы B :

$$\tilde{\rho}_B^1(t_{\text{loc}}) = \begin{bmatrix} 1 - \cos^2 \frac{\theta}{2} & 0 \\ 0 & \cos^2 \frac{\theta}{2} \end{bmatrix}, \quad \tilde{\rho}_B^2(t_{\text{loc}}) = \begin{bmatrix} \cos^2 \frac{\theta}{2} & 0 \\ 0 & 1 - \cos^2 \frac{\theta}{2} \end{bmatrix}, \quad (37)$$

удовлетворяющим соотношению

$$\frac{1}{2}\tilde{\rho}_B^1(t_{\text{loc}}) + \frac{1}{2}\tilde{\rho}_B^2(t_{\text{loc}}) = \frac{1}{2}\mathbf{I}_2. \quad (38)$$

Подставляя полученные результаты в выражение (12), получаем локальный поток информации от A к B :

$$\chi^{A \rightarrow B}(t_{\text{loc}}) = 1 - h_b \left(\frac{1}{2} \cos^2 \frac{\theta}{2} \right), \quad (39)$$

записанный через бинарную энтропийную функцию (27).

Чтобы получить противоположный поток информации от B к A , воспользуемся заменой $\theta \rightarrow \bar{\theta}$, в которой новый параметр

$$\bar{\theta} = 2 \arctg(-\Delta B + K) \quad (40)$$

получается изменением знака у неоднородности поля ΔB . Используя тригонометрические преобразования, легко показать выполнение равенства $\cos^2 \theta = \cos^2 \bar{\theta}$, из которого при подстановке в (39) автоматически следует тождество

$$\chi^{\text{asympt}} = \chi^{A \rightarrow B}(t_{\text{loc}}) = \chi^{B \rightarrow A}(t_{\text{loc}}) = 1 - h_b \left(\frac{1}{2} \cos^2 \frac{\theta}{2} \right), \quad (41)$$

а также отсутствие асимметрии локальных потоков информации $\Delta\chi = 0$ в полном соответствии с результатами, представленными на рис. 4(е). Полученные значения χ^{asympt} для исследуемых конфигураций полей также показаны на рис. 4(ф).

Таким образом, мы можем заключить, что с ростом температуры, соответствующим переходу квантовой системы в классическую, роль мгновенных корреляций ослабляется, в то время как роль корреляций, обусловленных локальным переносом информации, увеличивается. Кроме того, повышение температуры способствуют сглаживанию асимметрии всех видов корреляций.

Далее рассмотрим зависимость различных характеристик мгновенных и запаздывающих корреляций от силы магнитного поля B_2 при фиксированном значении поля $B_1 = 1$ и наборе температур $T = 0,75, 1, 1,25$. Полученные результаты представлены на рис. 5. Зависимость для согласованности C опущена по причине отсутствия запутанности при рассматриваемых температурах.

В первую очередь проанализируем поведение энтропийной асимметрии d . Как было показано ранее, при равенстве модулей полей $|B_1| = |B_2|$ энтропии фон Неймана обеих частиц равны друг другу, и мы имеем $d = 0$. Как показывают результаты вычислений, в случае наличия неоднородности поля знак величины d совпадает со знаком разности $|B_2| - |B_1|$; таким образом, энтропийная асимметрия направлена от частицы в более слабом магнитном поле к частице в более сильном магнитном поле. Данный результат, в свою очередь, полностью соответствует выводам, полученным при изучении вырожденного основного состояния.

Две другие меры асимметрии корреляций ΔD и $\Delta\chi$ демонстрируют полностью аналогичное поведение: в случае неоднородности поля их знаки совпадают со знаком разности $|B_2| - |B_1|$, и в случае равенства модулей полей $|B_1| = |B_2|$ обе меры асимметрии корреляций обращаются в нуль. Таким образом, измерение состояния частицы, находящейся в более слабом магнитном поле, дает больше информации о частице в более сильном магнитном поле, чем наоборот. В тоже время, за счет локального взаимодействия от частицы в более слабом магнитном поле к частице в более сильном магнитном поле передается больше информации, чем в противоположном направлении. Следует отметить, однако, что величина $\Delta\chi$ в случае параллельных и антипараллельных полей демонстрирует гораздо более выраженное отличие в своем поведении по сравнению с соответствующим поведением величин d и ΔD .

Яркое отличие между мгновенными и запаздывающими корреляциями также показывают величины I и χ , представленные на рис. 5(d), (e). Максимум взаимной информации I смещен в сторону антипараллельных полей, что соответствует результатам работы [24], посвященной сохранению запутанности за счет применения антипараллельных полей, в то время как максимум средней локально передаваемой информации приходится на резонанс $B_1 = B_2$, что соответствует общей закономерности классических взаимодействий.

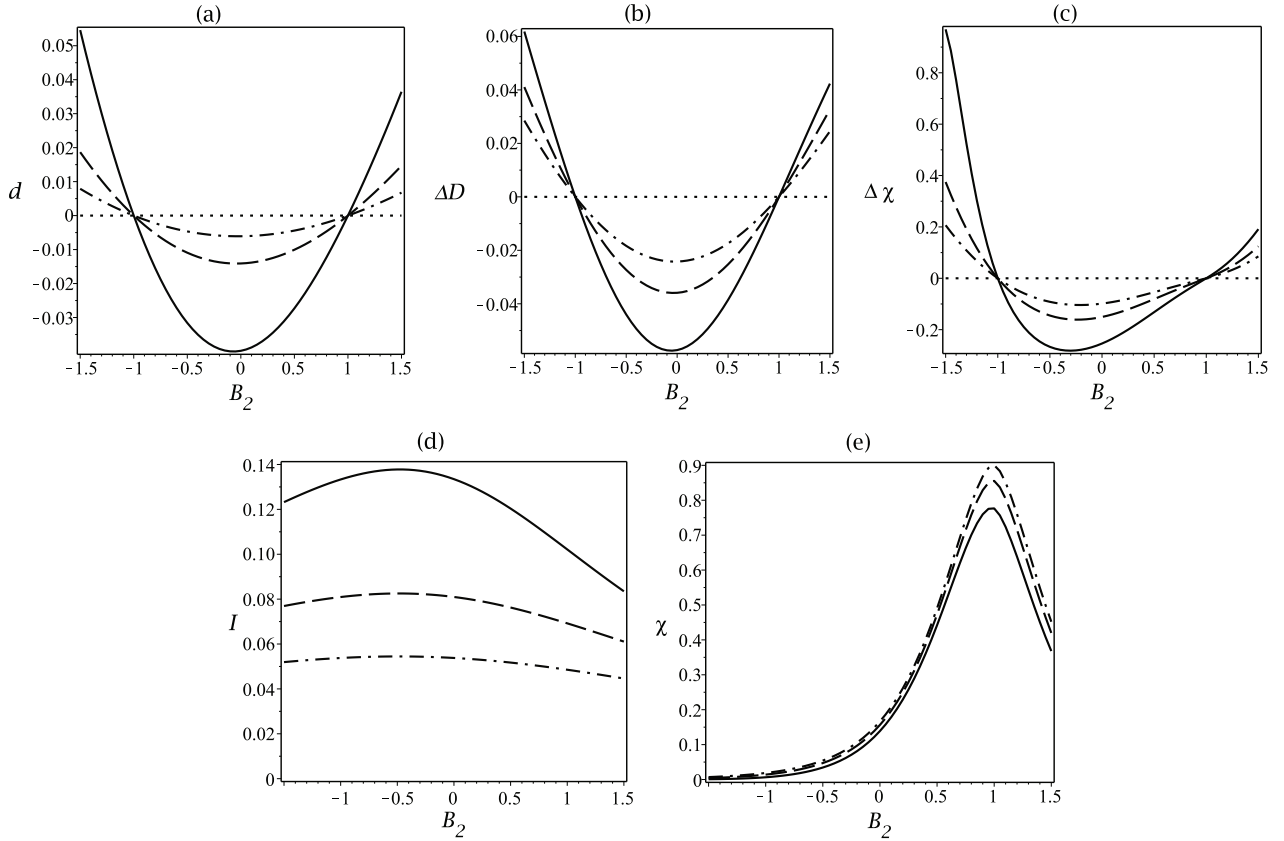


Рис. 5. Зависимость (а) энтропийной асимметрии d , (б) относительной асимметрии дискорда ΔD , (с) относительной асимметрии локально передаваемой информации $\Delta\chi$, (д) взаимной информации I и (е) средней локально передаваемой информации χ от поля B_2 в состоянии (33) при фиксированном значении $B_1 = 1$ и температуры $T = 0,75$ (сплошная линия), $T = 1$ (пунктирная линия) и $T = 1,25$ (штрихпунктирная линия)

6. ВЫВОДЫ

В работе был рассмотрен вопрос об асимметрии корреляций в термальном состоянии двух частиц со спином $1/2$, находящихся в неоднородном магнитном поле и взаимодействующих согласно XY -модели Гейзенберга. В качестве основных характеристик описывающих мгновенные корреляции рассматривались величины энтропийной асимметрии d , относительной асимметрии дискорда ΔD , квантовой взаимной информации I и согласованности C . В качестве характеристик, описывающих запаздывающие корреляции, обусловленные локальным взаимодействием между частицами, была введена величина относительной асимметрии локально передаваемой информации $\Delta\chi$, а также величина средней локально передаваемой информации χ .

В результате проведенных исследований были получены следующие результаты.

1. Обнаружено, что в основном состоянии рассматриваемого гамильтониана асимметрия корреляций (с точки зрения всех рассматриваемых мер асимметрии) может иметь место только в случае его вырождения.

2. Получено, что в случае равенства модулей магнитных полей, действующих на частицы, термальное состояние симметрично с позиции всех рассматриваемых мер асимметрии.

3. В случае наличия неоднородности поля энтропийная асимметрия направлена от частицы в более слабом магнитном поле к частице в более сильном магнитном поле. Данное поведение сопровождается тем фактом, что измерение над частицей в более слабом магнитном поле дает

доступ к большей величине локально доступной информации, чем измерение над в более сильном магнитном поле. Кроме того, частица в более слабом магнитном поле передает посредством локального взаимодействия больше информации частице в более сильном локальном поле, чем наоборот. Данные результаты соответствуют одинаковым знакам у величин d , ΔD и $\Delta \chi$.

4. Рост температуры способствует ослаблению мгновенных корреляций, характеризующихся величинами квантовой взаимной информации I и согласованности C , и увеличению величины средней локально передаваемой информации χ . В пределе бесконечных температур мгновенные корреляции между частицами исчезают, в то время как запаздывающие корреляции, обусловленные локальным взаимодействием между частицами, выходят на положительный асимптотический уровень, определяемый величиной магнитных полей. Возможная исходная асимметрия состояния с точки зрения всех рассматриваемых мер асимметрий корреляций исчезает с ростом температуры.

5. Наибольшая интенсивность потоков локально передаваемой информации имеет место в случае однородности магнитного поля, в то время как сохранению мгновенных корреляций способствует помещение частиц в антипараллельные поля.

Ожидается, что полученные результаты могут способствовать более глубокому пониманию вопроса о переходе границы между классическим и квантовым описанием систем системы, а также более эффективному управлению асимметричными двухкубитными системами. К одному из наиболее перспективных направлений дальнейшего развития данных исследований можно отнести рассмотрение взаимосвязи между поведением энтропийной асимметрии и асимметрии локально передаваемой информации в более крупных и сложных физических системах.

СПИСОК ЛИТЕРАТУРЫ

1. Коротаев С. М. О возможности причинного анализа геофизических процессов// Геомагнетизм и аэрономия. — 1992. — 32. — С. 27–33.
2. Bennett C. H., Brassard G., Crepeau 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.
3. Bennet H., Wiesner S. J. Communication via one- and two-particle operators on Einstein–Podolsky–Rosen states// Phys. Rev. Lett. — 1992. — 69. — С. 2881.
4. Cerf N. J., Adami C. Negative entropy and information in quantum mechanics// Phys. Rev. Lett. — 1997. — 79. — С. 5194–5197.
5. Cerf N. J., Adami C. Quantum extension of conditional probability// Phys. Rev. A. — 1999. — 60. — С. 893–897.
6. Fanchini F. F., Castelano L. K., Cornelio M. F., de Oliveira M. C. Locally inaccessible information as a fundamental ingredient to quantum information// New J. Phys. — 2012. — 14. — 013027.
7. Fedorov A. K., Kiktenko E. O., Man'ko O. V., Man'ko V. I. Tomographic discord for a system of two coupled nanoelectric circuits// Phys. Scr. — 2015. — 90. — 055101.
8. Fel'dman E. B., Zenchuk A. I. Asymmetry of bipartite quantum discord// JETP Lett. — 2011. — 93. — С. 459–462.
9. Henderson L., Vedral V. Classical, quantum and total correlations// J. Phys. A. — 2001. — 34. — С. 6899.
10. Holevo A. S. Quantum Systems, Channels, Information: A Mathematical Introduction. — Walter de Gruyter, 2012.
11. Horodecki K., Horodecki M., Horodecki P. Are quantum correlations symmetric?// Quantum Inf. Comput. — 2010. — 10. — С. 901–910.
12. Horodecki M., Oppenheim J., Winter A. Partial quantum information// Nature. — 2005. — 436. — С. 673–676.
13. Horodecki M., Oppenheim J., Winter A. Quantum state merging and negative information// Commun. Math. Phys. — 2007. — 269. — С. 107–136.
14. Horodecki R., Horodecki P. Quantum redundancies and local realism// Phys. Lett. A. — 1994. — 194. — С. 147–152.
15. Imamoglu A., Awschalom D. D., Burkard G., DiVincenzo D. P., Loss D., Sherwin M., Small A. Quantum information processing using quantum dot spins and cavity QED// Phys. Rev. Lett. — 1999. — 83. — С. 4204–4207.

16. *Kiktenko E. O., Fedorov A. K.* Tomographic causal analysis of two-qubit states and tomographic discord// Phys. Lett. A. — 2014. — 378. — С. 1704.
17. *Kiktenko E. O., Korotaev S. M.* Causal analysis of asymmetric entangled states under decoherence// Phys. Lett. A. — 2012. — 376. — С. 820.
18. *Korotaev S. M., Kiktenko E. O.* Causal analysis of the quantum states// AIP Conf. Proc. — 2010. — 1316. — С. 295–331.
19. *Korotaev S. M., Kiktenko E. O.* Causality and decoherence in the asymmetric states// Phys. Scr. — 2012. — 85. — 055006.
20. *Maldonado-Trapp A., Hu A., Roa L.* Analytical solutions and criteria for the quantum discord of two-qubit X -states// Quantum Inf. Process. — 2015. — 14. — С. 1947–1958.
21. *Ollivier H., Zurek W. H.* Quantum discord: A measure of the quantumness of correlations// Phys. Rev. Lett. — 2001. — 88. — 017901.
22. *Siewert J., Fazio R., Palma G. M., Sciacca E.* Aspects of qubit dynamics in the presence of leakage// J. Low Temp. Phys. — 2000. — 118. — С. 795–804.
23. *Su X., Wang W., Wang Y., Jia X., Xie C., Peng K.* Continuous variable quantum key distribution based on optical entangled states without signal modulation// Eur. Phys. Lett. — 2009. — 87. — С. 2005.
24. *Sun Y., Chen Yu., Chen H.* Thermal entanglement in the two-qubit Heisenberg XY model under a nonuniform external magnetic field// Phys. Rev. A. — 2003. — 68. — 044301.
25. *Wotters W. K.* Entanglement of formation of an arbitrary state of two qubits// Phys. Rev. Lett. — 1998. — 80. — С. 2245.
26. *Wotters W. K., Zurek W. H.* A single quantum cannot be cloned// Nature. — 1982. — 299. — С. 802–803.
27. *Ye Y., Tongqi L., Yu-En L., Qi-Zhong Y.* Quantum teleportation via a two-qubit Heisenberg XY chain: effects of anisotropy and magnetic field// J. Phys. A. — 2005. — 38. — С. 3235.
28. *Yu T., Eberly J. H.* Evolution from entanglement to decoherence of bipartite mixed “ X ” states// Quantum Inf. Comput. — 2007. — 7. — С. 459–468.
29. *Zhang J., Long G. L., Zhang W., Deng Z., Liu W., Lu Z.* Simulation of Heisenberg XY interactions and realization of a perfect state transfer in spin chains using liquid nuclear magnetic resonance// Phys. Rev. A. — 2005. — 72. — 012331.

Е. О. Киктенко

Математический институт им. В. А. Стеклова РАН;

Международный центр квантовой оптики и квантовых технологий

(Российский квантовый центр), Москва, Сколково;

Московский государственный технический университет им. Н. Э. Баумана;

Центр геоэлектромагнитных исследований

Института физики Земли им. О. Ю. Шмидта РАН, Троицк, Москва

E-mail: e.kiktenko@rqc.ru



ЦЕЛЕВАЯ ФУНКЦИЯ В ЗАДАЧЕ ОПТИМАЛЬНОГО ЛАЗЕРНОГО РАЗДЕЛЕНИЯ ИЗОТОПОВ МЕТОДОМ СЕЛЕКТИВНОГО ТОРМОЖЕНИЯ

© 2018 г. К. А. ЛЯХОВ, А. Н. ПЕЧЕНЬ

Аннотация. На основе метода селективного торможения конденсации во внешнем лазерном поле ранее был предложен дизайн промышленной обогатительной установки. В работе представлен обзор результатов о критерии оптимизации (целевой функции), предложенном для нахождения оптимальных параметров данной схемы, связанных с геометрией и операционными характеристиками. В качестве ограничений в задаче оптимизации рассматривалось влияние скорости конденсации, резонансное и нерезонансное поглощение в разделительной ячейке на ее геометрию. Разделительная ячейка играет роль поглотителя в лазерном резонаторе.

Ключевые слова: оптимальное управление, изотопы бора, динамика переохлажденного и разреженного газового потока.

AMS Subject Classification: 49K99

1. Введение. В ядерной энергетике довольно остро стоит проблема получения изотопов бора-10 в тонновых количествах. Это связано с тем, что данный изотоп имеет ряд привлекательных свойств, связанных с его большим сечением поглощения тепловых и быстрых нейтронов. Остальные претенденты, такие как, например, гадолиний и кадмий, хоть и имеют гораздо большие сечения, но имеют резонансный спектр поглощения и более жесткое гамма-излучение при их трансмутации. Сравнительно меньшие потребности в изотопически чистом боре существуют в полупроводниковой промышленности и ядерной медицине, однако его высокая стоимость сдерживает развитие указанных направлений.

Целью данной работы является осветить полученные авторами за последние годы результаты в области формулировки математической задачи оптимального разделения изотопов бора с помощью метода селективного торможения конденсации в переохлажденных газовых струях при помощи лазерного излучения (см. [1,2]). Привлекательность этого метода состоит в том, что наряду с достаточно низкими энергозатратами по сравнению с остальными в настоящее время активно используемыми методами (центрифугирование и химический обмен) он достаточно производительен в связи с более высокой селективностью, универсален (подходит для разделения как легких, так и тяжелых изотопов при условии, что давление насыщенного пара используемого соединения достаточно велико при комнатной температуре) и компактен, а поэтому менее капиталоемок.

2. Операционные принципы. На начальном этапе извлечения целевых изотопов из природной смеси, BCl_3 разбавляется газом-носителем, имеющим хорошие аэродинамические свойства (например аргон), до мольной доли, которая с одной стороны должна быть достаточно велика, чтобы обеспечить приемлемую скорость извлечения, а с другой стороны — достаточно мала, чтобы минимизировать резонансную потерю возбуждения при столкновении различных изотопологов) в смесительном баке. В нем газ при комнатной температуре поддерживается при давлении на предварительно заданном уровне.

Из него газ расширяется через целевое сопло в разделительную ячейку, где он облучается многократно отраженным лазерным лучом, так, что при достаточно малом угле отклонения от

Работа выполнена при поддержке Российского научного фонда (проект № 17-11-01388) в Математическом институте им. В. А. Стеклова Российской академии наук.

перпендикулярного направления, почти весь газовый поток может быть засвечен (лазерный луч падает с торца газового потока). На противоположном от сопла конце ячейки скиммер разделяет газовый поток на две фракции. Часть потока, прошедшая через скиммер, соответствует обогащенной ^{10}B , а отраженная от его внешних стенок — ^{11}B . Так происходит потому, что спектральная линия излучения CO_2 лазера $\nu = 958 \text{ см}^{-1}$, используемого для селективного возбуждения, имеет резонансное перекрытие только с областью фотопоглощения $^{11}\text{BCl}_3$ и, таким образом, образование кластеров с селективно возбужденным $^{11}\text{BCl}_3$ в переохлажденном потоке задерживается, а это — на основании эффекта разделения по массам частиц вокруг оси сверхзвукового потока — приводит к тому, что тяжелые частицы (кластеры) остаются в центре потока, а легкие (возбужденные) распределяются по его периферии.

Однородный профиль скорости, соответствующий наибольшему объему газа, имеющего оптимальное температурное поле, может быть получен с помощью специально спроектированной стенки целевого сопла. В случае коаксиального сопла протяженность оптимального температурного поля меньше и, следовательно, потенциальное количество селективно возбужденных молекул тоже меньше. Сопло спроектировано так, что истекающая из него струя являлась изобарической. В этом случае селективная передача энергии от лазерного пучка к газовому потоку является наиболее более полной в силу их максимального перекрытия.

Расстояния между продольными стенками разделительной ячейки подобраны таким образом, чтобы минимизировать их возмущающее воздействие на газовый поток. Наклон внешней стенки входного отверстия скиммер выбрано таким образом, чтобы поток обтекающего его газа был безотрывным. В этом случае нарушения оптимального поля температуры, вызываемое косыми скачками уплотнения, можно избежать.

Скорости откачки центральной и периферической фракций газового потока выбраны так, чтобы предотвратить нарастание давления на выходе и их смешивание.

В силу того, что доля извлечения целевого изотопа за время пролета разделительной ячейки довольно мала, необходимо многократно рециркулировать как обогащенную, так и обедненную компоненты газового потока. Транспортная модель, положенная в основу вычисления фактора обогащения β_j и доли извлечения θ_j на каждой итерации, была построена в [3]. Рассмотрен случай, когда мольная доля BCl_3 на каждой итерации остается неизменной. Это может быть достигнуто при помощи непрерывного смешивания рециркулированного газа с компенсирующим притоком природной смеси. Предполагая, что весь BCl_3 захватывается в криоловушке, компенсирующий его приток газа $\Delta Q_{\text{in}}^{(j)}$ должен удовлетворять на каждой итерации j следующей системе уравнений:

$$\begin{cases} \Delta Q_{\text{in}}^{(j)} = \Delta Q_{\text{out}}^{(j)}, & j = \overline{1, N_i}; \\ \Delta Q_{\text{out}}^{(j)} = \mu_j \theta_j Q_f t_{\text{tr}}; \\ \Delta Q_{\text{in}}^{(j)} = \mu \Delta Q_{\text{out}}^{(j)} + (1 - \mu) \Delta Q_{\text{out}}^{(j)} \end{cases} \quad (1)$$

Таким образом, можно показать, что мольные фракции на текущем и предыдущем циклах взаимосвязаны следующим образом:

$$\mu_j = \mu_{j-1} (1 - \theta_{j-1} + \mu_1 \theta_{j-1}), \quad j = \overline{2, N_i}. \quad (2)$$

Применяя уравнение (2) и систему уравнений (1), получим следующее рекуррентное соотношение между относительными концентрациями изотопов на смежных циклах:

$$x_j = \frac{x_{j-1} (1 - \beta_{j-1} \theta_{j-1}) + x_i \mu_1 \theta_{j-1}}{1 - \theta_{j-1} + \mu_1 \theta_{j-1}}, \quad j = \overline{2, N_i}.$$

В случае, если только BCl_3 добавляется на каждом цикле в камеру смешивания $\mu_1 = 1$ и при этом $\mu_j = \mu = \text{const}$, данное выражение упростится:

$$x_j = x_{j-1} (1 - \beta_{j-1} \theta_{j-1}) + x_i \theta_{j-1}.$$

3. Целевая функция в задаче оптимизации. Так как эффективность разделения изотопов обусловлена скоростью потребления энергии и скоростью их выделения, целевая функция в задаче оптимизации может быть введена исходя из требования выделять наибольшее количество изотопов в течение кратчайшего времени при наименьших затратах энергии:

$$\left\langle \frac{dE}{dt} \right\rangle = \left\langle \varepsilon \frac{dN}{dt} \right\rangle, \quad (3)$$

где dE/dt — потребляемая мощность, а dN/dt — скорость разделения. Предполагая, что усреднение выполняется по формуле

$$\langle O \rangle = \frac{1}{T_{\text{tot}}} \int_0^{T_{\text{tot}}} O dt,$$

правая часть уравнения (3) может быть преобразована следующим образом:

$$\left\langle \varepsilon \frac{dN}{dt} \right\rangle = \frac{\Psi}{T_{\text{tot}}} \sum_{j=1}^{N_{\text{it}}} \frac{\Delta N_j}{t_{\text{tr}}} t_{\text{tr}},$$

где Ψ — электроэнергия, приходящаяся на выделение одного изотопа из природной смеси, ΔN_j — общее количество изотопов, выделенных за один быстрый цикл, $T_{\text{tot}} = N_{\text{it}} t_{\text{tr}}$ — полное время работы разделительной установки. Общее число итераций задается как

$$N = N_c N_i,$$

где N_i — число итераций (быстрых циклов), необходимое для обогащения до окончательного уровня x_{fin} , соответствующего изотопическому равновесию, и

$$N_c = \frac{\mathcal{M}}{Q_i x_{\text{fin}} m_i}$$

— число циклов для извлечения заданной массы изотопологов

$$\mathcal{M} = N x_i m_i, \quad \text{где} \quad m_i = \frac{10 + M_{\text{3Cl}}}{N_A}.$$

Очевидно, общее число BCl_3 молекул N равно

$$M = N m_Q, \quad \text{где} \quad m_Q = \frac{10 x_i + 11(1 - x_i) + M_{\text{3Cl}}}{N_A}.$$

Таким образом, целевая функция Ψ может быть задана следующим выражением:

$$\Psi(T_{\text{flow}}, p_{\text{flow}}, \mu, W_t, H_t, I_0) = \frac{T_{\text{tot}} \left\langle \frac{dE}{dt} \right\rangle}{\frac{M}{m_Q} \left(1 - \frac{x_i}{x_{\text{fin}}} \right)};$$

наша задача найти глобальный минимум $\min_{\Omega} \Psi$ этой функции.

4. Условия облучения. Наиболее важным параметром эффективности разделения изотопов является сечение фотопоглощения σ_A . При комнатной температуре колебательные спектры возбуждаемых изотопологов являются достаточно широкими и, следовательно, обладают низкой чувствительностью к лазерному излучению. Однако при снижении температуры (в нашем случае — переохлаждением газового потока) они становятся узкими.

Также важным параметром эффективности разделения является скорость возбуждения

$$k_A = \sigma_A \frac{I}{\pi R_L^2},$$

поскольку чем она выше, тем больше вероятность селективного возбуждения. С другой стороны, существуют ограничения (сверху и снизу) на мощность лазерного излучения, вызванные как принципиальной применимостью рассматриваемого в настоящей статье метода, так и прочностных характеристик используемых оптических материалов.

Было показано, что использование разделительной ячейки в качестве поглотителя в оптическом резонаторе CO_2 лазера, позволяет сократить потребление электроэнергии для его накачки в 3,5–4,5 раза. Для этого было произведено вычисление распределения интенсивности на каждом проходе через газовый поток, отраженного от зеркальных стенок камеры облучения (разделительной ячейки) лазерного пучка. На j -м пересечении оно имеет вид

$$I^{(j)}(x) = Q_{\text{las}}^{(j)}(x) I_{\text{CW}},$$

где I_{CW} — начальная интенсивность лазера при входе в разделительную ячейку, $Q_{\text{las}}^{(j)}$ — модулирующий фактор, накладываемый резонансными условиями на геометрию разделительной ячейки:

$$Q_{\text{las}}^{(j)}(x) = \frac{T_1}{(1 - \tilde{\rho}_1 \tilde{\rho}^{2N_{\text{tr}}-1})^2} \left[\tilde{\rho}^{2j} \exp(-2Im\alpha_j) + \tilde{\rho}^{2(2N_{\text{tr}}-1-j)} e^{-\gamma W_{\text{IC}}} \exp(2Im\alpha_j) + 2\tilde{\rho}^{2N_{\text{tr}}-1} e^{-\gamma W_{\text{IC}}/2} \cos(2Re\phi_j) \right],$$

где

$$\alpha_j(x) = \pi q_0 j + \phi_j(x), \quad \phi_j(x) = \frac{\omega n x}{c \cos \alpha}, \quad q_0 \in \mathbb{Z},$$

n — показатель преломления, α — угол между нормалью, совпадающей с большей стороной газового потока W_{IC} , и направлением лазерного луча, T_1 — пропускная способность окна из ZnSe между кюветой, заполненной инверсно заселенной средой и разделительной ячейкой, которая в то же время является продолжением резонатора CO_2 лазера, N_{tr} — число проходов лазерным лучом всей длины газового потока. Поглощение напряженности электрического поля лазера за один проход дается формулой

$$\tilde{\rho} = \rho \exp \left\{ -\frac{\omega n'' W_{\text{IC}}}{c \cos \alpha} \right\},$$

где ρ — индекс отражения от поверхности зеркала внутри разделительной ячейки. Мнимая часть показателя преломления, как хорошо известно, связана с локальной плотностью газа, частотой излучения и сечением фотопоглощения формулой

$$\frac{2\omega n''}{c} = \sigma_A n_i = \gamma \cos \alpha.$$

5. Результаты. В данной работе обсуждается задача оптимизации в предложенной ранее многомодульной конструкции промышленной установки по разделению изотопов на основе метода селективного торможения конденсации в переохлажденных газовых струях. Каждый разделительный модуль состоит из камеры облучения, в которую газ поступает из специально спроектированного сопла и механически разделяется при помощи скиммера, установленного на его противоположном конце. Геометрия установки, а также интенсивность лазерного излучения, давление и температура газового потока, находятся на основе предложенного критерия оптимизации с соответствующими физическими и физико-химическими ограничениями. Данный критерий можно интерпретировать как средние энергетические затраты на выделение одного изотопа из изначальной природной смеси в течение полного времени, необходимого для выделения заданного количества изотопов. Было обнаружено (см. [2]), что он требует примерно в три раза меньше энергии, затрачиваемой на отдельный изотоп в сравнении с другим, в настоящее время активно развиваемым методом MOLIS (см. [4]).

Для более эффективного использования лазерных фотонов было предложено выполнить каждую камеру облучения как резонатор. Было показано, что в этом случае расход электроэнергии, затрачиваемый на поддержание инверсной населенности в CO_2 лазере, может быть сокращен в 3,5–4,5 раза (см. [1]).

Была предложена новая схема для итеративного извлечения изотопов; обнаружено, что в ней равновесная относительная концентрация изотопов крайне мала. Изотопическое равновесие достигается за число итераций, которое варьируется в зависимости от расчетной температуры газового потока на выходе из сопла, плотности энергии лазерного излучения и общей протяженности

газового потока. Например, равновесная изотопическая относительная концентрация 0,1991 достигается за 39 быстрых итераций при температуре 33 К, соответствующей расстоянию от выхода сопла до входа в скиммер, на котором еще не успели сформироваться критические кластеры, 67 см. При этом начальная интенсивность лазерного излучения равна 100 Вт. В то время как равновесная изотопическая концентрация $x_{\text{fin}} = 0,2015$ достигается за 112 быстрых итераций при той же лазерной интенсивности, но при меньшей расчетной температуре газового потока на выходе из сопла 26 К. Различие во временах достижения изотопического равновесия объясняется пикообразной формой зависимости фактора обогащения от температуры.

СПИСОК ЛИТЕРАТУРЫ

1. *Lyakhov K. A., Pechen A. N., Lee H. J.* Some features of boron isotopes separation by the laser-assisted retardation of condensation method in multipass irradiation cell implemented as a resonator// IEEE J. Quantum Electr. — 2016. — 52. — С. 1400208-1-8.
2. *Lyakhov K. A., Pechen A. N., Lee H. J.* Some issues of industrial scale boron isotopes separation by the laser assisted retarded condensation (SILARC) method// Separation and Purification Technology. — 2017. — 176. — С. 402–411.
3. *Eerkens J. W.* Laser-induced migration and isotope separation of epi-thermal monomers and dimers in supercooled free jets// Laser and Particle Beams. — 2005. — 25. — С. 225–253.
4. *Mathi P., Parthasarathy V., Nayak A. K., Mittal J. P., Sarkar S. K.* Laser isotope separation: Science and technology// Proc. Natl. Acad. Sci. India, Sec. A: Phys. Sci. — 2015. — С. 1–16.

К. А. Ляхов

Математический институт им. В. А. Стеклова РАН;
Национальный университет г. Чеджу (Южная Корея)
E-mail: lyakhov2000@yahoo.com

А. Н. Печень

Национальный исследовательский технологический университет «МИСиС»;
Математический институт им. В. А. Стеклова РАН
E-mail: apechen@gmail.com



НЕКОТОРЫЕ МЕТОДЫ ПОСТРОЕНИЯ УПРАВЛЕНИЙ ДЛЯ КВАНТОВЫХ СИСТЕМ

© 2018 г. А. Н. ПЕЧЕНЬ

Аннотация. В настоящее время активно исследуются задачи управления квантовыми системами, такими, как отдельные атомы, молекулы, состояния электронов в квантовых точках и т. д. В работе кратко рассмотрены методы построения управлений для квантовых систем с помощью градиентных алгоритмов, генетических алгоритмов и скоростного градиента. Доказано нарушение условия асимптотической стабилизируемости для задачи генерации унитарных операций методом скоростного градиента в двухуровневых квантовых системах.

Ключевые слова: управление квантовыми системами, квантовые эффекты.

AMS Subject Classification: 81Q93

1. Введение. В задачах квантовых технологий, т.е. технологий, основанных на использовании квантовых эффектов и отдельных квантовых систем, требуется разрабатывать методы управления квантовыми системами (см. [6, 11, 12, 20, 27, 29]). Управление может осуществляться с использованием лазерного импульса модулируемой формы, некогерентного воздействия резервуаром, с помощью измерений и т. п. Целью управления может являться создание заданного состояния системы при дополнительном условии минимальности энергии либо длительности управления, генерация заданной унитарной операции, стабилизация среднего значения некоторой наблюдаемой величины квантовой системы. Для построения управлений используются различные алгоритмы, такие как gradient ascent pulse engineering (GRAPE, см. [19]), метод Кротова (см. [2, 30]), алгоритм Broyden–Fletcher–Goldfarb–Shanno (BFGS) и его модификации (см. [10, 15, 16, 28]), машинное обучение (см. [17]), метод скоростного градиента (см. [1, 7, 22]), генетические алгоритмы (см. [18, 24]), смешанные подходы (см. [21]). Далее рассматриваются такие методы построения управлений для квантовых систем, как градиентные методы, генетические алгоритмы, метод скоростного градиента.

2. Задачи управления квантовыми системами. Рассмотрим квантовую систему с гильбертовым пространством $\mathcal{H}$. Наиболее общее состояние системы описывается матрицей плотности, т.е. неотрицательным оператором $\rho : \mathcal{H} \rightarrow \mathcal{H}$, $\rho \geq 0$, имеющим единичный след, $\text{Tr } \rho = 1$. Чистым состояниям соответствуют матрицы плотности, которые являются проекторами, т.е. такие, что $\rho^2 = \rho$. Остальные матрицы плотности соответствуют смешанным состояниям.

Динамика изолированной от влияния окружения квантовой системы под воздействием когерентного управления $u(t)$, например лазерного импульса, описывается уравнением Шрёдингера:

$$\frac{dU_t}{dt} = -i(H_0 + V u(t))U_t, \quad U_{t=0} = \mathbb{I}; \quad (1)$$

здесь U_t — унитарный оператор эволюции, H_0 и V — самосопряженные операторы в $\mathcal{H}$, являющиеся свободным гамильтонианом и гамильтонианом взаимодействия системы с когерентным управлением. Матрица плотности системы в этом случае преобразуется по формуле

$$\rho_t = U_t \rho_0 U_t^\dagger;$$

здесь ρ_0 — состояние системы в начальный момент времени $t = 0$.

Работа выполнена при поддержке Министерства образования и науки Российской Федерации (проект № 1.669.2016/1.4).

Если квантовая система является открытой, т.е. взаимодействует с резервуаром, то ее эволюция описывается мастер-уравнением для матрицы плотности

$$\frac{d\rho_t}{dt} = -i[H_0 + Vu(t), \rho_t] + \mathcal{L}(\rho_t).$$

Если резервуар марковский, то диссипативный генератор имеет форму Горини—Коссаковского—Сударшана—Линдблада:

$$\mathcal{L}(\rho_t) = \sum_i \left(2L_i \rho_t L_i^\dagger - L_i^\dagger L_i \rho_t - \rho_t L_i^\dagger L_i \right);$$

здесь L_i — операторы в $\mathcal{H}$. Существуют различные методы вывода мастер-уравнений (см. [9, 13, 31]). Преобразование матрицы плотности открытой квантовой системы является неунитарным и описывается вполне положительным сохраняющим след отображением (см. [8]).

Широкий класс задач управления квантовыми системами можно сформулировать как задачу максимизации некоторого целевого функционала $\mathcal{F}(u)$. Мы рассмотрим два класса целевых функционалов.

Первый класс описывает задачу максимизации среднего значения некоторой наблюдаемой O квантовой системы (самосопряженного оператора в гильбертовом пространстве $\mathcal{H}$) в финальный момент времени $T > 0$. Соответствующий целевой функционал имеет вид

$$\mathcal{F}_O(u) = \text{Tr} [U_T \rho_0 U_T^\dagger O]$$

Второй класс описывает задачу генерации в n -уровневой квантовой системе некоторой заданной унитарной операции $W \in SU(n)$. Соответствующий целевой функционал имеет вид

$$\mathcal{F}_W(u) = \frac{1}{n^2} |\text{Tr}(W^\dagger U_T)|^2.$$

Как правило, для достаточно сложных систем не удается явно найти управление, на котором целевой функционал достигает максимума. Более того, не всегда известны с хорошей точностью параметры системы, например, гамильтониан ее взаимодействия с управлением. В таких случаях применяются различные алгоритмы поиска оптимальных (либо близких к оптимальным) управлений. Если параметры системы известны с хорошей точностью, то производится численный поиск оптимальных управлений. Если не все параметры системы известны, то алгоритмы применяются для поиска оптимальных управлений в лабораторных условиях.

3. Градиентные методы. Основная идея градиентных методов заключается в том, чтобы производить поиск оптимального управления, двигаясь в направлении наискорейшего подъема, которое задаётся градиентом $\nabla \mathcal{F}$. Препятствием для поиска глобальных максимумов целевого функционала с помощью градиентных методов могут являться локальные, но не глобальные максимумы целевого функционала, которые называются ловушками. При отсутствии ловушек градиентные методы могли бы иметь высокую эффективность поиска глобальных максимумов целевого функционала. В этой связи в [26] была высказана гипотеза об отсутствии ловушек у широкого класса задач управления квантовыми системами.

Гипотеза об отсутствии ловушек была доказана для $n = 2$ при достаточно больших целевых временах T (см. [4, 23]). Рассмотрим такую двухуровневую квантовую систему с эволюцией (1), что $[H_0, V] \neq 0$. Положим

$$u_0 = \frac{-\text{Tr} H_0 \text{Tr} V + 2 \text{Tr}(H_0 V)}{(\text{Tr} V)^2 - 2 \text{Tr} V^2}, \quad (2)$$

$$T_0 = \frac{\pi}{\|H_0 - \text{Tr} H_0/2 + f_0(V - \text{Tr} V/2)\|}. \quad (3)$$

Тогда при $T \geq T_0$ все максимумы целевых функционалов $\mathcal{F}_O(u)$ и $\mathcal{F}_W(u)$ — глобальные (см. [4]).

Также доказано отсутствие ловушек у целевых функционалов $\mathcal{F}_W$ для систем с эволюцией вида (1) с $n = 2$ и $[H_0, V] \neq 0$ при почти всех W и малых T . Именно, пусть

$$d = \left\| H_0 + u_0 V - \mathbb{I} \frac{\text{Tr} H_0}{2} - u_0 \mathbb{I} \frac{\text{Tr} V}{2} \right\|.$$

Произвольная матрица W , удовлетворяющая соотношению $[H_0 + u_0 V, W] = 0$, имеет вид

$$W = e^{i\alpha_W(H_0 + u_0 V) + i\beta_W}, \quad \text{где } \alpha_W \in \left(0, \frac{\pi}{d}\right], \quad \beta_W \in [0, 2\pi). \quad (4)$$

Пусть $[H_0 + u_0 V, W] \neq 0$. Тогда для любого $T > 0$ все максимумы целевого функционала $\mathcal{F}_W$ — глобальные. Пусть $[H_0 + u_0 V, W] = 0$. Если $\alpha_W \in (0, \pi/(2d))$, то все максимумы целевого функционала $\mathcal{F}_W$ — глобальные для любого $T > 0$; если же $\alpha_W \in [\pi/(2d), \pi/d]$, то все максимумы целевого функционала $\mathcal{F}_W$ — глобальные для любого $T > \pi/d - \alpha_W$ (см. [5]).

Ловушками второго порядка называются критические точки целевого функционала, в которых гессиан целевого функционала отрицательно полуопределен, причем $\mathcal{F}(u) < \mathcal{F}_{\max}$. Для n -уровневых систем с $n \geq 3$ под воздействием когерентного управления в [25] показано, что 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 $\mathcal{F}_O$ имеет по крайней мере одну ловушку второго порядка. В [14] построены примеры ловушек для систем с $n = 4$.

Таким образом, в некоторых случаях можно доказать отсутствие ловушек у задач управления квантовыми системами. В этих случаях градиентные методы могут быть эффективны для поиска глобально оптимальных управлений. В других случаях доказано наличие ловушек либо ловушек второго порядка. В этих случаях предпочтительным может оказаться использование методов глобального поиска.

4. Генетические алгоритмы. В случае, если целевой функционал имеет ловушки, градиентные методы могут оказаться неэффективными для поиска глобально оптимальных управлений. В таких случаях более эффективными могут быть эволюционные алгоритмы, в основе которых лежит моделирование процессов естественного отбора.

В задачах управления квантовыми системами часто применяются генетические эволюционные алгоритмы. В этом случае управление кодируется вектором X в некотором пространстве. На первой итерации формируется некоторое множество из N управлений $P_1 = \{X_1^1, \dots, X_N^1\}$, называемое *начальной популяцией*. Начальная популяция может формироваться либо полностью случайным образом, либо на основе предварительной «грубой» информации о точке глобального максимума.

На $(k + 1)$ -й итерации из k -й популяции с использованием операций отбора, скрещивания и мутаций создается $(k + 1)$ -я популяция P_{k+1} . При этом для каждого вектора из популяции $P_k = \{X_1^k, \dots, X_N^k\}$ вычисляется (в случае численной оптимизации) или измеряется (в случае лабораторных экспериментов) значение фитнес-функции (целевого функционала) $f_i^k = \mathcal{F}(X_i^k)$. Операция отбора в простейшем случае заключается в копировании в $(k + 1)$ -ю популяцию некоторой (как правило, относительно небольшой) доли векторов с наибольшими значениями фитнес-функции. Могут использоваться и более сложные механизмы отбора. Операция скрещивания заключается в формировании новых векторов путем смешения двух или более родительских векторов. В простейшем случае для двух родительских векторов $X = (x_1, \dots, x_n)$ и $Y = (y_1, \dots, y_n)$ потомки определяются как векторы $x = (x_1, \dots, x_k, y_{k+1}, \dots, y_n)$ и $y = (y_1, \dots, y_k, x_{k+1}, \dots, x_n)$ для некоторого $1 \leq k < n$. Операция мутации заключается в изменении значений некоторого небольшого числа элементов родительского вектора случайно либо в соответствии с некоторым алгоритмом. Алгоритм завершает работу при выполнении критерия остановки, которым, как правило, является достижение заданного достаточно большого значения целевого функционала либо достижение некоторого предельного числа итераций.

Генетические алгоритмы были предложено использовать для изолированных от влияния окружения квантовых систем в [18]. Для открытых квантовых систем, находящихся под воздействием когерентного и некогерентного управлений, генетические алгоритмы применялись в [24]. Генетические алгоритмы получили широкое применение в связи с относительной простотой их реализации в лабораторных условиях и эффективностью при поиске глобальных экстремумов у целевых функций со сложным ландшафтом.

5. Метод скоростного градиента. Метод скоростного градиента использует градиент скорости изменения целевой функции вдоль траекторий системы (см. [7]). Данный метод применялся для стабилизации средних значений наблюдаемых в конечноуровневых квантовых системах (см. [1]) управления энергией квантово-механического осциллятора (см. [22]), генерации унитарных операций (см. [3]).

Пусть состояние системы описывается вектором $x(t)$ и эволюция состояния под воздействием управления u описывается уравнением

$$\dot{x} = F(x, u, t).$$

Пусть задача состоит в минимизации целевой функции $\mathcal{F}_t$. Скорость изменения целевой функции вдоль траектории системы имеет вид

$$\omega(u) = \frac{\partial \mathcal{F}_t}{\partial x} \dot{x} = \frac{\partial \mathcal{F}_t}{\partial x} F(x, u, t).$$

Общая форма метода скоростного градиента имеет вид

$$\frac{d}{dt}[u + \psi(u)] = -\Gamma \nabla_u \omega(u); \quad (5)$$

здесь $\Gamma \geq 0$ и вектор ψ удовлетворяет условию псевдоградиентности $\langle \psi, \nabla_u \omega \rangle \geq 0$. Дифференциальная форма получается, если положить $\psi = 0$, конечная форма — если положить $u + \psi(u) = 0$ и выбрать $\psi(u) = \Gamma \nabla_u \omega(u)$ так, что $u = -\Gamma \nabla_u \omega(u)$.

Рассмотрим, например, метод скоростного градиента для задачи генерации унитарного процесса W (см. [3]). Целевую функцию удобно представить в виде

$$\mathcal{F}_t^W = 1 - \frac{1}{n^2} |\text{Tr}(U_t^u W^\dagger)|^2. \quad (6)$$

Целевая функция неотрицательна, $\mathcal{F}_t^W \geq 0$, и $\mathcal{F}_t^W \rightarrow 0$ если и только если $U_t^u \rightarrow e^{i\phi(t)} W$, где $\phi(t) \in [0, 2\pi)$ — произвольная физически несущественная фаза.

Скорость изменения $\mathcal{F}_t^W$ вдоль траекторий имеет вид

$$\omega_W(U, u) = -\frac{2}{n^2} \text{Im} \left[\text{Tr}(W U^\dagger) \text{Tr}(W^\dagger (H_0 + V u) U) \right]. \quad (7)$$

Градиент $\omega_W(U, u)$ по управлению есть

$$\nabla_u \omega_W(U, u) = -\frac{2}{n^2} \text{Im} \left[\text{Tr}(W U^\dagger) \text{Tr}(W^\dagger V U) \right].$$

В итоге получаем общую форму метода скоростного градиента для задачи генерации унитарного процесса W :

$$\frac{d}{dt}[u + \psi(U, u)] = -\Gamma \nabla_u \omega_W(U, u) = \frac{2\Gamma}{n^2} \text{Im} \left[\text{Tr}(W U^\dagger) \text{Tr}(W^\dagger V U) \right];$$

здесь $\Gamma \geq 0$ и вектор ψ удовлетворяет условию псевдоградиентности $\langle \psi, \nabla_u \omega_W \rangle \geq 0$.

Дифференциальная форма получается, если положить $\psi = 0$:

$$\frac{du}{dt} = -\Gamma \nabla_u \omega_W(U, u) = \frac{2\Gamma}{n^2} \text{Im} \left[\text{Tr}(W U^\dagger) \text{Tr}(W^\dagger V U) \right];$$

конечная форма имеет вид

$$u = -\Gamma \nabla_u \omega_W(U, u) = \frac{2\Gamma}{n^2} \text{Im} \left[\text{Tr}(W U^\dagger) \text{Tr}(W^\dagger V U) \right].$$

Важным критерием для анализа метода скоростного градиента в дифференциальной форме является условие стабилизируемости [см. [7, (2.7)]]. Это условие для задачи генерации унитарной операции имеет вид

$$\text{существует такое } u_* \in \mathbb{R}, \text{ что } \omega_W(U, u_*) \leq 0 \text{ для всех } U \in SU(n). \quad (8)$$

В [3] было доказано, что для дифференциальной формы метода скоростного градиента в задаче генерации унитарной операции условие асимптотической стабилизируемости не выполняется.

Однако приведенное доказательство работает только для $n > 2$. Ниже мы восполняем пробел и доказываем нарушение условия стабилизируемости для $n = 2$.

Теорема. *Условие стабилизируемости (8) не выполняется ни для какого $W \in SU(2)$.*

Доказательство. Предположим, что существует такое u_* , что $\omega_W(U, u_*) \leq 0$ для всех $U \in SU(2)$. Используя выражение (7) для ω_W , получим

$$\operatorname{Im} \left[\operatorname{Tr}(WU^\dagger) \operatorname{Tr}(W^\dagger(H_0 + Vu_*)U) \right] \geq 0. \quad (9)$$

Введем обозначение $\tilde{U} = UW^\dagger \in SU(2)$. Тогда (9) означает, что для всех $\tilde{U} \in SU(2)$ выполняется неравенство

$$u_* \operatorname{Im} \left[\operatorname{Tr}(\tilde{U}^\dagger) \operatorname{Tr}(V\tilde{U}) \right] \leq \operatorname{Im} \left[\operatorname{Tr}(\tilde{U}^\dagger) \operatorname{Tr}(H_0\tilde{U}) \right]. \quad (10)$$

Без потери общности можно положить $H_0 = \operatorname{diag}(-1, 1)$. Рассмотрим произвольную специальную унитарную (2×2) -матрицу

$$\tilde{U} = \begin{pmatrix} a & b \\ -b^* & a^* \end{pmatrix}, \quad |a|^2 + |b|^2 = 1.$$

Введем обозначение $v = V_{12}$. Несложные вычисления с учетом того, что $\operatorname{Tr}(\tilde{U}^\dagger) = 2\Re(a)$ показывают, что условие (10) принимает вид

$$u_* \operatorname{Im}(b^*v) \geq \operatorname{Im} a \text{ для всех таких } a, b \in \mathbb{C}, \text{ таких, что } |a|^2 + |b|^2 = 1, \Re(a) \neq 0. \quad (11)$$

Если $v = 0$ или $u_* = 0$, то условие (11) нарушается, например, для $b = 0$ и $a = e^{i\phi}$, $\phi \in (0, \pi/2)$. Если $v \neq 0$ и $u_* \neq 0$, то положим $a = 1/\sqrt{2}$, $b = iv/(\sqrt{2}|v|)$ при $u_* > 0$ и $a = 1/\sqrt{2}$, $b = -iv/(\sqrt{2}|v|)$ при $u_* < 0$. В обоих случаях имеем $|a|^2 + |b|^2 = 1$. При $u_* > 0$ имеем

$$u_* \operatorname{Im}(b^*v) = \frac{u_* \operatorname{Im}(-i|v|)}{\sqrt{2}} = -\frac{u_*|v|}{\sqrt{2}} < \operatorname{Im} a = 0.$$

Аналогично, при $u_* < 0$ имеем

$$u_* \operatorname{Im}(b^*v) = \frac{u_* \operatorname{Im}(i|v|)}{\sqrt{2}} = \frac{u_*|v|}{\sqrt{2}} < \operatorname{Im} a = 0.$$

В каждом случае по найденным a и b можно построить матрицу $\tilde{U}$ и затем матрицу $U = \tilde{U}W \in SU(2)$. Таким образом, для любых $u_* \in \mathbb{R}$ и V (с $V_{ii} = 0$) существует матрица $U \in SU(2)$, для которой $\omega_W(U, u_*) > 0$. Теорема доказана. $\square$

СПИСОК ЛИТЕРАТУРЫ

1. Ананьевский М. С., Фрадков А. Л. Управление наблюдаемыми в конечноуровневых квантовых системах// Автомат. телемех. — 2005. — 5. — С. 63–75.
2. Кротов В. Ф. Управление квантовыми системами и некоторые идеи теории оптимального управления// Автомат. телемех. — 2009. — 3. — С. 15–23.
3. Печень А. Н. О методе скоростного градиента для генерации унитарных квантовых операций в замкнутых квантовых системах// Усп. мат. наук. — 2016. — 71, № 3. — С. 205–206.
4. 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.
5. 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.
6. Управление молекулярными и квантовыми системами/ Сб. статей. Пер. с англ. И. А. Макарова, под ред. А. Л. Фрадкова и О. А. Якубовского. — М.: Ижевск: Институт компьютерных исследований, 2003.
7. Фрадков А. Л. Схема скоростного градиента и ее применение в задачах адаптивного управления// Автомат. телемех. — 1979. — 9. — С. 90–101.
8. Холево А. С. Квантовые системы, каналы, информация. — М.: МЦНМО, 2010.
9. Accardi L., Lu Y. G., Volovich I. V. Quantum Theory and Its Stochastic Limit. — Springer-Verlag, 2002.
10. Broyden C. G. The convergence of a class of double-rank minimization algorithms. 1. General consideration// J. Inst. Math. Appl. — 1970. — 6. — С. 76–90.

11. *Brumer P. W., Shapiro M.* Principles of the Quantum Control of Molecular Processes. — Wiley-Interscience, 2003.
12. *D'Alessandro D.* Introduction to Quantum Control and Dynamics. — Boca Raton: Chapman&Hall, 2007.
13. *Davis E. B.* Quantum theory of open systems. — Academic Press, 1976.
14. *de Fouquières P., Schirmer S. G.* Quantum control landscapes: a closer look// *Infin. Dimens. Anal. Quantum. Probab. Relat. Top.* — 2013. — 16, № 3. — С. 1350021.
15. *Fletcher R. A.* A new pproach to variable metric algorithms// *Comput. J.* — 1970. — 13. — С. 317–322.
16. *Goldfarb D. A.* A family of variable-metric methods derived by variational means// *Math. Comput.* — 1970. — 24. — С. 23–26.
17. *Hentschel A., Sanders B. C.* Efficient algorithm for optimizing adaptive quantum metrology processes// *Phys. Rev. Lett.* — 2011. — 107. — С. 233601.
18. *Judson R. S., Rabitz H.* Teaching lasers to control molecules// *Phys. Rev. Lett.* — 1992. — 68. — С. 1500–1503.
19. *Khaneja N., Reiss T., Kehlet C., Schulte-Herbrüggen T., Glaser S. J.* Optimal control of coupled spin dynamics: design of nmr pulse sequences by gradient ascent algorithms// *J. Magn. Reson.* — 2005. — 172, № 2. — С. 296–305.
20. *Letokhov V. S.* Laser Control of Atoms and Molecules. — Oxford Univ. Press, 2007.
21. *Machnes S., Sander U., Glaser S. J., de Fouquières P., Grushys A., Schirmer S., Schulte-Herbrüggen T.* Comparing, optimizing, and benchmarking quantum-control algorithms in a unifying programming framework// *Phys. Rev. A.* — 2011. — 84. — С. 022305.
22. *Pechen A., Borisenok S.* Energy transfer in two-level quantum systems via speed gradient-based algorithm// *IFAC-PapersOnLine.* — 2015. — 48, № 11. — С. 446–450.
23. *Pechen A., Il'in N.* Trap-free manipulation in the Landau-Zener system// *Phys. Rev. A.* — 2012. — 86. — С. 052117.
24. *Pechen A., Rabitz H.* Teaching the environment to control quantum systems// *Phys. Rev. A.* — 2006. — 73. — С. 062102.
25. *Pechen A., Tannor D.* Are there traps in quantum control landscapes?// *Phys. Rev. Lett.* — 2011. — 106. — С. 120402.
26. *Rabitz H., Hsieh M., Rosenthal C.* Quantum optimally controlled transition landscapes// *Science.* — 2004. — 303. — С. 1998.
27. *Rice S. A., Zhao M.* Optical Control of Molecular Dynamics. — New York: Wiley, 2000.
28. *Shanno D. F.* Conditioning of quasi-Newton methods for function minimization// *Math. Comput.* — 1970. — 24. — С. 647–656.
29. *Tannor D. J.* Introduction to Quantum Mechanics: A Time Dependent Perspective. — Sausalito: Univ. Sci. Press, 2007.
30. *Tannor D. J., Kazakov V., Orlov V.* Control of photochemical branching: Novel procedures for finding optimal pulses and global upper bounds// в сб.: *Time Dependent Quantum Molecular Dynamics*/ J. Broeckhove, L. Lathouwers, eds. — Plenum, 1992. — С. 347–360.
31. *Trushechkin A. S., Volovich I. V.* Perturbative treatment of inter-site couplings in the local description of open quantum networks// *Europhys. Lett.* — 2016. — 113. — С. 30005.

А. Н. Печень

Национальный исследовательский технологический университет «МИСиС», Москва;

Математический институт им. В. А. Стеклова РАН

E-mail: apechen@gmail.com



ПОЛУГРУППЫ ПРЕОБРАЗОВАНИЙ ПРОСТРАНСТВА ФУНКЦИЙ, КВАДРАТИЧНО ИНТЕГРИРУЕМЫХ ПО ТРАНСЛЯЦИОННО ИНВАРИАНТНОЙ МЕРЕ НА БАНАХОВОМ ПРОСТРАНСТВЕ

© 2018 г. В. Ж. САКБАЕВ

Аннотация. Изучаются меры на банаховом пространстве E , инвариантные относительно сдвигов на произвольные векторы пространства и являющиеся аддитивным продолжением функции множества, заданной на совокупности брусков со сходящимся произведением длин ребер, однако не удовлетворяющие условию σ -конечности и, быть может, счетной аддитивности. Определено гильбертово пространство $\mathcal{H}$ комплекснозначных функций на пространстве E , квадратично интегрируемых по инвариантной относительно сдвигов мере. Исследованы свойства полугрупп операторов сдвига в пространстве $\mathcal{H}$ и соответствующих им генераторов и резольвент. Получен критерий сильной непрерывности таких полугрупп. Определены и исследованы математические ожидания операторов сдвига вдоль случайных векторов по однопараметрическому семейству гауссовских мер, образующих полугруппу относительно свертки. Установлено, что рассмотренное семейство математических ожиданий образует однопараметрическую полугруппу линейных самосопряженных сжатий пространства $\mathcal{H}$, найдены инвариантные подпространства операторов этой полугруппы и получены условия ее сильной непрерывности.

Ключевые слова: конечно-аддитивная мера, инвариантная мера на группе, случайное блуждание, непрерывная однопараметрическая полугруппа, генератор, резольвента.

AMS Subject Classification: 28C20, 81Q05, 47D08

СОДЕРЖАНИЕ

1. Введение	73
2. Трансляционно инвариантные меры на банаховых пространствах	74
3. Пространство квадратично интегрируемых по инвариантной мере функций	78
4. Полугруппы операторов сдвига и их свойства	78
5. Меры на гильбертовом пространстве, инвариантные относительно сдвигов и поворотов	82
6. Случайные сдвиги и их математические ожидания	84
Список литературы	90

1. ВВЕДЕНИЕ

Развитие теории трансляционно инвариантных мер на бесконечномерных линейных пространствах осложняется тем, что в силу теоремы Вейля (см. [5]), не существует меры Лебега на бесконечномерном топологическом векторном пространстве, то есть не существует ненулевой счетно-аддитивной σ -конечной меры на σ -кольце борелевских подмножеств бесконечномерного топологического векторного пространства, инвариантной относительно сдвигов на векторы этого пространства. В связи с этим изучались вопросы о существовании мер на бесконечномерных топологических векторных пространствах, инвариантных относительно сдвига на векторы из некоторого максимального допустимого подпространства (см. [6]), о существовании инвариантных мер, не являющихся σ -конечными (см. [15]), о существовании мер, не являющихся счетно-аддитивными (см. [10]). Для сепарабельных гильбертовых пространств в работе [10] установлено существование

неотрицательной конечно-аддитивной меры, заданной на некотором кольце подмножеств вещественного гильбертова пространства H (содержащем все единичные брусы этого пространства), инвариантной относительно сдвига на любой вектор пространства H и относительно любого ортогонального преобразования.

В предлагаемом в настоящей работе подходе исследуются неотрицательные конечно-аддитивные меры λ_p , заданные на некоторых кольцах $\mathcal{R}(l_p)$ подмножеств банаховых пространств l_p , $p \in [1, +\infty]$, содержащих все брусы с ребрами единичной длины и обладающие свойством инвариантности относительно сдвигов на произвольные векторы банахова пространства. В разделе 2 будут исследованы меры на банаховых пространствах, изометрически изоморфные пространствам l_p , $1 \leq p \leq \infty$, вещественных числовых последовательностей. Для гильбертовых пространств в разделе 5 будет, как и в [10], исследован класс мер, инвариантных не только относительно сдвига на произвольный вектор, но и относительно произвольного ортогонального преобразования. Показано, что введенные трансляционно инвариантные меры на пространствах l_p , $p \in [1, +\infty]$, не являются σ -конечными, а их значения на любом компакте пространства l_p равно нулю. Установлено, что в шкале пространств l_p , $p \in [1, +\infty]$, пространство l_∞ выделяется тем, что мера λ_p на кольце $\Lambda(l_p)$ является счетно-аддитивной тогда и только тогда, когда $p = +\infty$.

Отказ от условия счетной аддитивности меры приводит к ряду трудностей, но в некоторых задачах использование таких мер необходимо. Так, в [1, 2] показано, что конечно-аддитивные меры дают полное описание множества квантовых состояний, и именно меры, не удовлетворяющие условию счетной аддитивности, задают квантовые состояния, возникающие при измерении наблюдаемых с непрерывным спектром. Кроме того, усреднение по конечно-аддитивным мерам возникает при описании квантовых систем со случайными гамильтонианами (см. [9, 11]) и динамики квантовых систем с сингулярными гамильтонианами (см. [8, 12, 16]).

В разделе 3 исследовано гильбертово пространство $\mathcal{H}(l_p)$ классов эквивалентности комплекснозначных функций на пространстве l_p (называемых далее функциями), квадратично интегрируемых по трансляционно инвариантной конечно-аддитивной мере λ_p . В разделе 4 исследованы однопараметрические семейства $\mathbf{S}_{th}$, $t \in \mathbb{R}$, операторов сдвига вдоль вектора h пространства l_p , представляющие собой унитарную группу в пространстве $\mathcal{H}(l_p)$. Получен критерий сильной непрерывности такой унитарной группы и исследованы свойства ее генератора и резольвенты. В шкале пространств l_p , $p \in [1, +\infty]$, пространство l_1 играет особую роль, поскольку только при $p = 1$ имеет место сильная непрерывность унитарной группы $\mathbf{S}_{th}$, $t \in \mathbb{R}$, в пространстве $\mathcal{H}(l_p)$ при произвольном векторе $h \in l_p$. Гильбертово пространство l_2 выделено тем, что только при $p = 2$ на пространствах l_p в разделе 5 определены и исследованы меры, инвариантные относительно произвольных биективных изометрий, и в разделе 6 изучены средние значения оператора сдвига на случайный вектор, распределение которого задается гауссовской мерой на пространстве l_p .

В разделе 6 изучается однопараметрическое семейство $\mathcal{U}(t)$, $t \geq 0$, математических ожиданий операторов сдвига $\mathbf{S}_h$ на случайные векторы гильбертова пространства H , распределения которых задаются однопараметрическим семейством гауссовских мер ν_t , $t \geq 0$, на пространстве H , образующим полугруппу относительно операции свертки:

$$\nu_{t+s} = \nu_t * \nu_s, \quad t, s \geq 0.$$

Установлены условия, при которых семейство $\mathcal{U}(t)$, $t \geq 0$, представляет собой полугруппу сжимающих операторов в пространстве $\mathcal{H}(H)$ функций, квадратично интегрируемых по мере на пространстве H , инвариантной относительно сдвигов и ортогональных преобразований. Установлено отсутствие сильной непрерывности полугруппы $\mathcal{U}$ на пространстве $\mathcal{H}$, определены ее инвариантные подпространства, среди которых выделены подпространства, на которых полугруппа $\mathcal{U}$ проявляет свойство сильной непрерывности и обладает самосопряженным генератором.

2. ТРАНСЛЯЦИОННО ИНВАРИАНТНЫЕ МЕРЫ НА БАНАХОВЫХ ПРОСТРАНСТВАХ

В этом разделе исследуем множество конечно-аддитивных мер на банаховых пространствах l_p , $1 \leq p \leq \infty$, инвариантных относительно сдвига на произвольных вектор из этого банахова

пространства и заданных на минимальном кольце $\mathcal{R}(l_p)$, содержащем совокупность $\mathcal{P}(l_p)$ измеримых параллелепипедов с ребрами, параллельными координатным осям (т.е. таких, что бесконечное произведение длин их ребер сходится; см. ниже и [10, 15]). Показано, что на кольце $\mathcal{R}(l_\infty)$ мера, удовлетворяющая перечисленным условиям, определена однозначно с точностью до числового множителя, но при каждом $p \in [1, +\infty)$ на кольце $\mathcal{R}(l_p)$ существуют различные меры, инвариантные относительно сдвига на произвольный вектор из пространства l_p .

Как и в [13, 15], при каждом значении $p \in [1, +\infty]$ определим на банаховом пространстве l_p семейство множеств $\mathcal{Q}(l_p)$ вида

$$\Pi_{a,b}^p = \left\{ \{x_j\} \in l_p : \forall j \in \mathbb{N} : x_j \in \langle a_j, b_j \rangle \right\}, \quad a, b \in l_\infty,$$

где $-\infty < a_j \leq b_j < +\infty$ при всех $j \in \mathbb{N}$; символ $\langle a_j, b_j \rangle$ означает ограниченный промежуток с концами a_j и b_j при условии $a_j \leq b_j$ (если $a_j = b_j$, то представляющий собой либо одноточечное, либо пустое множество).

Множества вида $\Pi_{a,b}^p$ при произвольных $a, b \in l_\infty$, удовлетворяющих условиям $a_j \leq b_j$ для всех $j \in \mathbb{N}$, будем называть *брусами* в пространстве l_p ; брус $\Pi_{a,b}^\infty \in \mathcal{Q}(l_\infty)$ является пустым множеством, если и только если существует такое $j \in \mathbb{N}$, что $\langle a_j, b_j \rangle = \emptyset$. Заметим (см. [13]), что при $p \in [1, +\infty)$ множества $\Pi_{a,b}^p \in \mathcal{Q}(l_p)$ непусты тогда и только тогда, когда $c = c(a, b) \in l_p$, где числовая последовательность $c = \{c_j\}$ определяется из условия $c_j = \inf_{x \in \langle a_j, b_j \rangle} |x|$, $j \in \mathbb{N}$.

Определение 2.1 (см. [10, 13]). Будем называть брус $\Pi_{a,b}^p \in \mathcal{Q}(l_p)$ *абсолютно измеримым*, если либо он является пустым множеством, либо сходится ряд

$$\sum_{j=1}^{\infty} \max \{0, \ln(b_j - a_j)\}. \quad (1)$$

Символом $\mathcal{P}(l_p)$ обозначим совокупность абсолютно измеримых брусов. Заметим, что в [15] исследуется мера, являющаяся продолжением функции множества, изначально заданной на совокупности измеримых брусов, для которых вместо ряда (1) сходится другой ряд (возможно, условно). Поэтому такая функция множества и продолженная с нее мера не обладают инвариантностью относительно перенумерации координат. Чтобы задать меру, инвариантную относительно изменения нумерации координат, зададим на классе $\mathcal{P}(l_p)$ абсолютно измеримых брусов аддитивную функцию множества $\lambda_p : \mathcal{P}(l_p) \rightarrow [0, +\infty)$.

Из условия аддитивности и локальной конечности функции λ_p следует, что $\lambda_p(\emptyset) = 0$. Значение функции λ_p на любом непустом измеримом брусе $\Pi_{a,b}^p \in \mathcal{P}(l_p)$ определим равенством

$$\lambda_p(\Pi_{a,b}^p) = \exp \left(\sum_{j \in \mathbb{N}} \ln(b_j - a_j) \right), \quad (2)$$

доопределив на пустых измеримых брусах из класса $\mathcal{P}(l_p)$ функцию λ_p нулем. В силу определения измеримости для любого бруса $\Pi_{a,b}^p \in \mathcal{P}(l_p)$ выполняется условие

$$\lambda_p(\Pi_{a,b}^p) \in [0, +\infty),$$

причем если $a, b \in l_\infty$ удовлетворяют условию

$$\exists j \in \mathbb{N} : a_j = b_j,$$

то сумма ряда в (1) равна $-\infty$ и в таком случае $\lambda_p(\Pi_{a,b}^p) = 0$.

Напомним, что функция μ , заданная на классе множеств $\mathcal{S}$, называется *аддитивной*, если из условий

$$A, A_1, \dots, A_m \in \mathcal{S}, \quad A = \bigcup_{j=1}^m A_j, \quad A_j \cap A_k = \emptyset, \quad j, k \in \overline{1, m}, \quad j \neq k,$$

следует, что

$$\mu(A) = \sum_{j=1}^m \mu(A_j).$$

Лемма 2.1 (см. [13, лемма 3.1]). *При любом $p \in [1, +\infty]$ функция множества $\lambda_p : \mathcal{P}(l_p) \rightarrow [0, +\infty)$, заданная равенством (2), является инвариантной относительно сдвига на произвольный вектор из пространства l_p и аддитивной на классе множеств $\mathcal{P}(l_p)$.*

Заметим, что класс $\mathcal{P}(l_p)$ является замкнутым относительно пересечений. Пусть $\mathcal{R}(l_p)$ — минимальное кольцо подмножеств пространства l_p , содержащее класс множеств $\mathcal{P}(l_p)$.

Теорема 2.1 (см. [13, теоремы 3.2, 3.4]). *Пусть $p \in [1, +\infty]$ и пусть на множестве измеримых брусков $\mathcal{P}(l_p)$ задана функция $\nu : \mathcal{P}(l_p) \rightarrow [0, +\infty]$, аддитивная и инвариантная относительно сдвига на произвольный вектор из l_p . Тогда функция ν однозначно продолжается до аддитивной функции на кольце $\mathcal{R}(l_p)$. При этом продолжение является мерой, инвариантной относительно сдвига на произвольный вектор из l_p .*

Обозначим аддитивное продолжение на кольцо $\mathcal{R}(l_p)$ функции (2) тем же символом λ_p . Множество $A \subset l_p$ назовем λ_p -измеримым, если для каждого $\varepsilon > 0$ найдутся такие множества $A_1, A_2 \in \mathcal{R}(l_p)$, что $A_1 \subset A \subset A_2$ и $\lambda_p(A_2 \setminus A_1) < \varepsilon$. Через $\Lambda(l_p)$ обозначим совокупность λ_p -измеримых множеств.

Лемма 2.2 (см. [10, лемма 2]). *Совокупность $\Lambda(l_p)$ всех λ_p -измеримых множеств является кольцом.*

Мера λ_p допускает однозначное продолжение с кольца $\mathcal{R}(l_p)$ на кольцо $\Lambda(l_p)$, также обозначаемое через λ_p . Мера λ_p на кольце $\Lambda(l_p)$ является полной.

Замечание 2.1. Мера λ_∞ , заданная на кольце $\Lambda(l_\infty)$, является счетно-аддитивной (см. [15]).

Теорема 2.2 (см. [10, теорема 1]). *Мера λ на пространстве l_p , заданная на кольце $\Lambda(l_p)$, не является счетно-аддитивной при всех $p \in [1, +\infty)$.*

Доказательство. Рассмотрим пример из [13]. Пусть Π^p — брусок в l_p , каждое ребро которого $\langle a_j, b_j \rangle$ представляет собой полуинтервал $[0, 1)$, а множество $\Pi_n^p \in \mathcal{P}(l_p)$ при любом $n \in \mathbb{N}$ — брусок, каждое ребро которого представляет собой полуинтервал $[0, 1 - 1/n)$. Тогда

$$\Pi^p = \bigcup_{j=1}^{\infty} \Pi_j^p,$$

ибо для любой точки $x = \{x_k\} \in \Pi^p \subset l_p$ найдется такой номер $N = N(x)$, что $x \in \Pi_j^p$ при всех $j \geq N$, что исключает счетную аддитивность меры λ_p , поскольку

$$\lambda_p(\Pi^p) = 1 > 0 = \sum_{j=1}^{\infty} \lambda_p(\Pi_j^p).$$

Теорема доказана. □

Эти аргументы неприменимы к мере λ_∞ на пространстве l_∞ , ибо в этом случае равенство

$$\Pi^\infty = \bigcup_{j=1}^{\infty} \Pi_j^\infty$$

не справедливо, поскольку существуют такие элементы $x = \{x_k\} \in \Pi^\infty \subset l_\infty$, что $x \notin \Pi_n^\infty$ для любого $n \in \mathbb{N}$.

Лемма 2.3. *При $r < 1/2$ шар $B_r(l_p)$ является λ_p -измеримым множеством нулевой λ_p -меры.*

Доказательство. Заметим, что при любых $p \in [1, +\infty]$ и $r > 0$ шар $B_r(l_p)$ радиуса r в пространстве l_p может быть вписан в брус из класса $\mathcal{P}(l_p)$ с ребрами длины $2r$ (см. [10, лемма 4]).

□

Следовательно, мера λ_p является локально конечной.

Следствие 2.1. *Если K — компактное множество в пространстве l_p , то $\lambda_p(K) = 0$.*

Доказательство. Компактное множество ограничено и, следовательно, лежит в шаре некоторого радиуса $R > 0$. Кроме того, для любого $\varepsilon > 0$ существует такое натуральное N , что множество K лежит в ε -окрестности N -мерной гиперплоскости пространства H . Поэтому множество K можно покрыть конечным числом брусов нулевой λ_p -меры. □

Лемма 2.4. *При любом $p \in [1, +\infty]$ мера λ_p не является σ -конечной.*

Доказательство. При любом $p \in [1, +\infty]$ пространство l_p содержит систему брусов $Q_\alpha \in \mathcal{P}(l_p)$, где $\alpha = \{\alpha_j\}$, с ребрами $[\alpha_j, \alpha_j + 1)$, $j \in \mathbb{N}$, при условии, что все числа α_j могут принимать произвольные значения из двухэлементного множества $\{-1, 0\}$. Таким образом, каждое отображение $\alpha : \mathbb{N} \rightarrow \{-1, 0\}$ задает единичный брус Q_α , причем для различных отображений $\alpha, \beta : \mathbb{N} \rightarrow \{-1, 0\}$ брусы Q_α, Q_β не имеют общих точек. При этом, поскольку при любом $\alpha : \mathbb{N} \rightarrow \{-1, 0\}$ брус Q_α является непустым брусом с ребрами единичной длины, то $\lambda_p(Q_\alpha) = 1$. Поскольку множество отображений $\alpha : \mathbb{N} \rightarrow \{-1, 0\}$ несчетно, то пространство l_p содержит несчетную систему попарно непересекающихся подмножеств единичной меры. □

Таким образом, установлено следующее утверждение.

Теорема 2.3. *При любом $p \in [1, +\infty]$ мера λ_p , заданная на кольце $\Lambda(l_p)$, является неотрицательной локально конечной полной мерой на пространстве l_p , инвариантной относительно сдвига на произвольный вектор пространства l_p , но не являющейся σ -конечной. При $p = \infty$ мера λ_p счетно-аддитивна, а при $p \in [1, +\infty)$ не является счетно-аддитивной.*

Теорема 2.1 устанавливает единственность аддитивного продолжения аддитивной l_p -инвариантной функции множества, заданной на классе $\mathcal{P}(l_p)$ измеримых брусов в пространстве l_p , на минимальное содержащее этот класс $\mathcal{P}(l_p)$ кольцо $\mathcal{R}(l_p)$.

Тем не менее, в [13] указано на неединственность выбора таких l_p -инвариантных мер на пространстве l_p при всех $p \in [1, +\infty)$; это связано с неоднозначностью выбора аддитивной l_p -инвариантной функции множества, заданной на классе $\mathcal{P}(l_p)$.

Для множеств пространства l_p в [13] введено понятие l_p -эквивалентности: два множества из l_p называются l_p -эквивалентными, если одно является образом другого при сдвиге на вектор из пространства l_p . В пространстве l_p существуют различные непустые брусы $\Pi_{a',b'}, \Pi_{a'',b''} \in \mathcal{P}(l_p)$, обладающие тем свойством, что найдется элемент $h \in l_\infty \setminus l_p$, удовлетворяющий условию $a'' = a' + h$, $b'' = b' + h$. Такие брусы входят в непересекающиеся классы l_p -эквивалентности, но в силу свойства повышенной инвариантности функция λ_p принимает одинаковые значения на таких брусах.

Пример 2.1. Выделим в классе $\mathcal{P}(l_p)$ подкласс $\mathcal{P}_0(l_p)$ центрированных брусов — брусов из $\mathcal{P}(l_p)$, имеющих точку 0 пространства l_p своим геометрическим центром симметрии, а также брусов, входящих с ними в один класс l_p -эквивалентности. Определим функцию множества $\nu_0 : \mathcal{P}(l_p) \rightarrow [0, +\infty]$ из условия

$$\nu_0(\Pi) = \sup_{\substack{Q \in \mathcal{P}_0(l_p), \\ Q \subset \Pi}} \lambda_p(Q)$$

для любого бруса $\Pi \in \mathcal{P}(l_p)$. Тогда ν_0 — также аддитивная функция на классе $\mathcal{P}(l_p)$, инвариантная относительно сдвигов на векторы из пространства l_p , но не совпадающая с мерой λ_p : например, $\lambda_p(\Pi_{0,1}) = 1$, но $\nu_0(\Pi_{0,1}) = 0$. Поэтому в силу теоремы 2.1 функция ν_0 однозначно продолжается до аддитивной и инвариантной относительно сдвига на произвольный вектор пространства l_p меры на кольце $\mathcal{R}(l_p)$, которая отличается от меры λ_p .

3. ПРОСТРАНСТВО КВАДРАТИЧНО ИНТЕГРИРУЕМЫХ ПО ИНВАРИАНТНОЙ МЕРЕ ФУНКЦИЙ

Определим гильбертово пространство функций, квадратично интегрируемых по конечно-аддитивной мере. Пусть E — банахово пространство, изометрически изоморфное пространству последовательностей l_p . При этом через $\mathcal{E}$ обозначим такую счетную систему элементов $\{e_k, k \in \mathbb{N}\}$ пространства E , что отображение $\Phi : l_p \rightarrow E$, действующее по правилу

$$\Phi(\{x_k\}) = \sum_{k=1}^{\infty} x_k e_k, \quad (3)$$

является изометрическим изоморфизмом:

$$\|\Phi(\{x_k\})\|_E = \|\{x_k\}\|_{l_p}.$$

Обозначим через $\lambda_{\mathcal{E}}$ образ меры λ_p на пространстве l_p при изоморфизме Φ . Тогда $\mathcal{P}_{\mathcal{E}} = \Phi(\mathcal{P}(l_p))$ — класс измеримых брусков пространства E , $\mathcal{K}_{\mathcal{E}} = \Phi(\Lambda(l_p))$ — кольцо $\lambda_{\mathcal{E}}$ -измеримых множеств пространства E , на котором мера $\lambda_{\mathcal{E}}$ является неотрицательной локально конечной, конечно-аддитивной, трансляционно инвариантной и полной, но не является σ -конечной. Будем отождествлять λ_p -измеримые множества в пространстве l_p с их образами в пространстве E при изоморфизме Φ .

Рассмотрим линейное пространство $\mathcal{L}_{\mathcal{E}}(E)$ над полем $\mathcal{C}$ линейных комбинаций индикаторных функций из кольца $\mathcal{K}_{\mathcal{E}}$ и определим на пространстве $\mathcal{L}_{\mathcal{E}}(E)$ неотрицательно определенную эрмитову полуторалинейную форму по следующему правилу: для любых $A, B \in \mathcal{K}_{\mathcal{E}}$ положим

$$(\chi_A, \chi_B) = \lambda_{\mathcal{E}}(A \cap B),$$

а для произвольных функций $u, v \in \mathcal{L}_{\mathcal{E}}(E)$ вида

$$u = \sum_{j=1}^n c_j \chi_{A_j}, \quad v = \sum_{k=1}^m b_k \chi_{B_k}$$

положим

$$\beta_{\mathcal{E}}(u, v) \equiv (u, v)_{\mathcal{H}(E)} = \left(\sum_{j=1}^n c_j \chi_{A_j}, \sum_{k=1}^m b_k \chi_{B_k} \right) = \sum_{k=1}^m \sum_{j=1}^n \bar{b}_k c_j (\chi_{A_j}, \chi_{B_k}). \quad (4)$$

Две функции u и v из линейного пространства $\mathcal{L}_{\mathcal{E}}(E)$ назовем *эквивалентными*, если

$$\beta_{\mathcal{E}}(u - v, u - v) = 0.$$

Линейное пространство классов эквивалентности функций из пространства $\mathcal{L}(\mathcal{E})$ с введенной полуторалинейной формой $\beta_{\mathcal{E}}$ является предгильбертовым; по нему с помощью стандартной процедуры пополнения определяется гильбертово пространство, обозначаемое далее через $L_2(E, \mathcal{K}_{\mathcal{E}}, \lambda_{\mathcal{E}}) \equiv \mathcal{H}_{\mathcal{E}}(E)$.

Лемма 3.1 (см. [13]). *Пространство $\mathcal{H}_{\mathcal{E}}(E)$ несепарабельно.*

Это утверждение следует из существования континуальной ортонормированной системы элементов в пространстве $\mathcal{H}_{\mathcal{E}}(E)$ (см. лемму 2.4 и [13, лемма 3.10]).

4. ПОЛУГРУППЫ ОПЕРАТОРОВ СДВИГА И ИХ СВОЙСТВА

Определим на пространстве $\mathcal{H}_{\mathcal{E}}(E)$ оператор S_h сдвига на вектор $h \in E$, действующий по правилу $S_h u(x) = u(x + h)$. По определению пространства $\mathcal{H}_{\mathcal{E}}(E)$ оператор сдвига S_h при любом выборе вектора $h \in E$ определен на всем пространстве $\mathcal{H}_{\mathcal{E}}(E)$ и является унитарным оператором в $\mathcal{H}_{\mathcal{E}}(E)$.

Для каждого вектора $h \in E$ определим на пространстве $\mathcal{H}_{\mathcal{E}}(E)$ однопараметрическое семейство операторов S_{th} , $t \in \mathbb{R}$, сдвига на вектор $th \in E$, действующих по правилу

$$S_{th} u(x) = u(x + th). \quad (5)$$

Такое семейство операторов является однопараметрической группой унитарных операторов в гильбертовом пространстве $\mathcal{H}_{\mathcal{E}}(E)$.

Лемма 4.1. *Однопараметрические группы унитарных операторов $\mathbf{S}_{te_j}$, $t \in \mathbb{R}$, являются сильно непрерывными в подпространстве $\mathcal{H}_{\mathcal{E}}(E)$ при любом $j \in \mathbb{N}$. При этом для любого $u \in \mathcal{H}_{\mathcal{E}}(E)$ и любого $\varepsilon > 0$ существует такое $\delta > 0$, что при всех $t \in (-\delta, \delta)$ и всех $j \in \mathbb{N}$ выполняется неравенство*

$$\|\mathbf{S}_{te_j}u - u\|_{\mathcal{H}_{\mathcal{E}}(E)} < \varepsilon. \quad (6)$$

Доказательство. Если функция u_{Π} является индикатором измеримого бруса $\Pi \in \mathcal{K}_{\mathcal{E}}$ и $h = e_j$, то операторы $\mathbf{S}_{th}$, $t \in \mathbb{R}$, действуют как операторы сдвига вдоль j -го ребра бруса. Если мера бруса Π равна нулю, то $\|\mathbf{S}_{th}u_{\Pi} - u_{\Pi}\|_{\mathcal{H}(E)} = 0$ при всех $t > 0$, а если $\lambda(\Pi) > 0$, то длина j -го ребра бруса $b_j - a_j > 0$ положительна. Следовательно, для любого $\varepsilon > 0$ существует такое $\delta > 0$, что при всех $t \in (-\delta, \delta)$ выполняется неравенство

$$\|\mathbf{S}_{te_j}u_{\Pi} - u_{\Pi}\|_{\mathcal{H}(E)} < \varepsilon,$$

поскольку

$$\|\mathbf{S}_{te_j}u_{\Pi} - u_{\Pi}\|_{\mathcal{H}(E)}^p \leq \frac{2t}{b_j - a_j} \|u_{\Pi}\|_{\mathcal{H}(E)}^p.$$

Более того, из условия $0 < \lambda(\Pi) < +\infty$ следует, что $\ln(b_j - a_j) \rightarrow 0$ при $j \rightarrow \infty$; следовательно, существует такое $\sigma > 0$, что $b_j - a_j > \sigma$ при всех $j \in \mathbb{N}$. Поэтому для любых $j \in \mathbb{N}$ выполняется неравенство

$$\|\mathbf{S}_{te_j}u_{\Pi} - u_{\Pi}\|_{\mathcal{H}_{\mathcal{E}}(E)} < \left(\frac{2t}{\sigma}\right)^{1/p} \|u_{\Pi}\|_{\mathcal{H}(E)}. \quad (7)$$

Для произвольных элементов $u, v \in \mathcal{H}_{\mathcal{E}}(E)$ справедлива оценка

$$\|\mathbf{S}_{te_j}u - u\|_{\mathcal{H}_{\mathcal{E}}} \leq \|\mathbf{S}_{te_j}(u - v)\|_{\mathcal{H}_{\mathcal{E}}} + \|\mathbf{S}_{te_j}v - v\|_{\mathcal{H}_{\mathcal{E}}} + \|v - u\|_{\mathcal{H}_{\mathcal{E}}}.$$

Поскольку любой элемент $u \in \mathcal{H}_{\mathcal{E}}(E)$ может быть с любой точностью приближен в $\mathcal{H}_{\mathcal{E}}(E)$ -норме линейной комбинацией индикаторов измеримых брусков, то в неравенстве (7) можно заменить функцию u_{Π} на произвольную функцию $u \in \mathcal{H}(E)$. Следовательно, справедливо неравенство (6). Лемма 4.1 доказана. $\square$

Следствие 4.1. *Если банахово пространство E изометрически изоморфно пространству l_1 , то для любого вектора $h \in E$ однопараметрическая унитарная группа операторов $\mathbf{S}_{th}$, $t \in \mathbb{R}$, является сильно непрерывной, причем для любого $u \in \mathcal{H}_{\mathcal{E}}(E)$ существует такая постоянная $C > 0$, что*

$$\|\mathbf{S}_{th}u - u\|_{\mathcal{H}_{\mathcal{E}}(E)} < Ct\|h\|_E\|u\|_{\mathcal{H}_{\mathcal{E}}(E)}. \quad (8)$$

Доказательство. В силу неравенств (7) для любого измеримого бруса $\Pi \in \mathcal{K}_{\mathcal{E}}(E)$ существует такая постоянная $C > 0$, что

$$\|\mathbf{S}_{th}u_{\Pi} - u_{\Pi}\|_{\mathcal{H}_{\mathcal{E}}(E)} < C(t\|\{h_k\}\|_{l_1})\|u\|_{\mathcal{H}_{\mathcal{E}}(E)}. \quad (9)$$

При любом выборе единичного вектора $h \in E$ однопараметрическая группа унитарных операторов $\mathbf{S}_{th}$, $t \in \mathbb{R}$, является в силу (9) непрерывной на индикаторах измеримых брусков, а поскольку любой элемент $u \in \mathcal{H}(E)$ может быть с любой точностью приближен в $\mathcal{H}(E)$ -норме линейной комбинацией индикаторов измеримых брусков, то, следовательно, группа унитарных операторов $\mathbf{S}_{th}$, $t \in \mathbb{R}$, является непрерывной в сильной операторной топологии пространства $B(\mathcal{H}_{\mathcal{E}}(E))$. $\square$

Лемма 4.2. *Если $p \in (1, +\infty]$, то для произвольного $h \in E$, $\|h\|_E = 1$, унитарная группа $\mathbf{S}_{th}$, $t \in \mathbb{R}$, может не являться сильно непрерывной в $\mathcal{H}(E)$.*

Доказательство. Пусть вектор $h \in H$ имеет в базисе $\mathcal{E}$ координаты $h_k = 1/k$, $k \in \mathbb{N}$. Поскольку $p \in (1, +\infty]$, то $h \in E$ и

$$\|h\|_E = \left(\sum_{k=1}^{\infty} k^{-p} \right)^{1/p}.$$

Пусть $\Pi \in \mathcal{P}(E)$ — непустой брус, каждое ребро которого имеют длину 1 и сонаправлено с одним из векторов базиса $\mathcal{E}$, а u_Π — индикаторная функция бруса Π . Тогда

$$\|S_{th}u_\Pi - u_\Pi\|_{\mathcal{H}_\mathcal{E}}^p = 2\lambda((S_{th}\Pi) \setminus \Pi) = 2(1 - \lambda_\mathcal{E}(S_{th}\Pi \cap \Pi)) = 2 \left(1 - \exp \sum_{k=1}^{\infty} \ln \left(1 - \frac{t}{k} \right) \right).$$

Поскольку сумма ряда $\sum_{k=1}^{\infty} \ln(1 - t/k)$ равна $-\infty$ при любом $t > 0$, заключаем, что

$$\|S_{th}u_\Pi - u_\Pi\|_{\mathcal{H}_\mathcal{E}} \geq 1$$

при всех $t > 0$. Таким образом,

$$\lim_{t \rightarrow +0} \|S_{th}u_\Pi - u_\Pi\|_{\mathcal{H}_\mathcal{E}} \neq 0,$$

и группа унитарных преобразований S_{th} , $t \in \mathbb{R}$, пространства $\mathcal{H}_\mathcal{E}$ не является непрерывной в сильной операторной топологии на банаховом пространстве ограниченных линейных операторов $B(\mathcal{H}(E))$. $\square$

По выбранной в пространстве E системе элементов $\mathcal{E}$, задающей изоморфизм $\Phi : l_p \rightarrow E$ (см. (3)), определим линейное подпространство $L_1(E, \mathcal{E})$ пространства E , состоящее из таких элементов h , что $\{h_k\} \in l_1$, где $\{h_k\} = \Phi^{-1}(h)$. Пространство $L_1(E, \mathcal{E})$ изоморфно банахову пространству l_1 .

В теории однопараметрических полугрупп линейных операторов в банаховых пространствах известно, что сильная непрерывность полугруппы $U(t)$, $t \geq 0$, является следствием ее слабой измеримости и почти сепарабельнозначности (см. [14, теорема 9.3.1]). Унитарная группа S_{th} , $t \in \mathbb{R}$, преобразований пространства $\mathcal{H}_\mathcal{E}(E)$ при условии $\Phi^{-1}h \notin l_1$ не является почти сепарабельнозначной, как показывает лемма 4.2, ибо функция $S_{th}u_\Pi$, $t \in (0, \delta)$, при любом $\delta > 0$ принимает континуум значений, норма разности между любой парой из которых превосходит единицу.

Приведем критерий сильной непрерывности полугруппы S_{th} в терминах свойств вектора h .

Теорема 4.1. Пусть банахово пространство E изометрически изоморфно пространству l_p при $p \in (1, +\infty]$ и пусть $h \in E$. Однопараметрическая группа унитарных операторов S_{th} , $t \in \mathbb{R}$, является сильно непрерывной в пространстве $B(\mathcal{H}_\mathcal{E}(E))$ тогда и только тогда, когда образ $\{h_k\}$ вектора h при изоморфизме $\Phi^{-1} : E \rightarrow l_p$ принадлежит пространству l_1 .

Доказательство. Если $\Phi^{-1}(h) \in l_1$ т.е. $\sum_{k=1}^{\infty} |h_k| < \infty$, то для любого бруса $\Pi \in \mathcal{K}_\mathcal{E}$ с конечной мерой в силу соотношений (7) существует такая постоянная $C_\Pi \in [0, +\infty)$, что выполняется оценка

$$\|S_{th}u_\Pi - u_\Pi\|_{\mathcal{H}_\mathcal{E}(E)} \leq C_\Pi |t| \sum_{k=1}^{\infty} |h_k|.$$

Следовательно, подобная оценка имеет место и для любой линейной комбинации индикаторов измеримых брусов и, как было показано в доказательстве следствия 4.1, для произвольной функции $u \in \mathcal{H}_\mathcal{E}(E)$ имеет место оценка (8).

Пусть теперь $\sum_{k=1}^{\infty} |h_k| = +\infty$, где $\{h_k\} = \Phi^{-1}(h)$. Тогда так же, как и в лемме 4.2, устанавливается справедливость неравенства

$$\|S_{th}u_{\Pi_{0,1}} - u_{\Pi_{0,1}}\|_{\mathcal{H}_\mathcal{E}(E)} \geq 1 \quad \forall t > 0,$$

где $\Pi_{0,1}$ — брус, все ребра которого являются промежутками $[0, 1)$, а $u_{\Pi_{0,1}}$ — его индикаторная функция. $\square$

Таким образом, в шкале пространств l_p , $p \in [1, +\infty]$, пространство l_1 выделяется тем, что в гильбертовом пространстве $L_2(l_p, \Lambda(l_p), \lambda_p, \mathbf{C})$ унитарная группа $\mathbf{S}_{th}$, $t \in \mathbb{R}$, является сильно непрерывной при любом выборе вектора $h \in l_p$ если и только если $p = 1$.

Будем говорить, что функция $u \in \mathcal{H}_{\mathcal{E}}(E)$ обладает частной производной по направлению вектора $e_j \in \mathcal{E}$, $\|e_j\|_E = 1$, если существует такая функция $u_j \in \mathcal{H}_{\mathcal{E}}(E)$, что

$$\lim_{s \rightarrow 0} \left\| \frac{\mathbf{S}_{se_j} u - u}{s} - u_j \right\|_{\mathcal{H}_{\mathcal{E}}(E)} = 0.$$

В этом случае частная производная функции u по направлению e_j обозначается $u_j = \partial u / \partial x_j$.

Для каждого $j \in \mathbb{N}$ обозначим через $\mathcal{D}_{\mathcal{E},j}$ плотное в пространстве $\mathcal{H}_{\mathcal{E}}(E)$ линейное пространство, состоящее из таких функций пространства $\mathcal{H}_{\mathcal{E}}(E)$, для которых справедливо представление $u(x) = u_j(x_j)v(\hat{x})$, где $x = x_j \times \hat{x}$, $x_j \in \mathbb{R}$, $x \in H$ и выполняется условие $u_j \in C_0^\infty(\mathbb{R})$. Тогда на линейном пространстве $\mathcal{D}_{\mathcal{E},j}$ при каждом $j \in \mathbb{N}$ определен линейный оператор $\partial_j : \mathcal{D}_{\mathcal{E},j} \rightarrow \mathcal{D}_{\mathcal{E},j}$, ставящий в соответствие функции $u \in \mathcal{D}_{\mathcal{E},j}$ функцию $\partial u(x) / \partial x_j = u'_j(x_j)v(\hat{x}) \in \mathcal{D}_{\mathcal{E},j}$, $x \in E$, (точнее, классу функций, содержащих в качестве представителя функцию u , класс функций, содержащих в качестве представителя функцию $u'_j v$).

Лемма 4.3. *При каждом $j \in \mathbb{N}$ оператор $i\partial_j$ является симметрическим плотно определенным оператором в пространстве $\mathcal{H}_{\mathcal{E}}(E)$, замыкание которого $\overline{i\partial_j}$ является самосопряженным оператором в пространстве $\mathcal{H}_{\mathcal{E}}(E)$.*

Определим на пространстве $\mathcal{H}_{\mathcal{E}}(E)$ операторы $\mathbf{S}_h$ сдвига на вектор $h \in E$, действующие по правилу $\mathbf{S}_h u(x) = u(x + h)$. По определению пространства $\mathcal{H}_{\mathcal{E}}(E)$ оператор сдвига $\mathbf{S}_h$ при любом $h \in E$ определен на всем пространстве $\mathcal{H}_{\mathcal{E}}(E)$ и является унитарным оператором в $\mathcal{H}_{\mathcal{E}}(E)$.

Для каждого вектора $h \in E$ определим на пространстве $\mathcal{H}_{\mathcal{E}}(E)$ однопараметрическое семейство операторов $\mathbf{S}_{th}$, $t \in \mathbb{R}$, сдвига на векторы $th \in E$, действующих по правилу

$$\mathbf{S}_{th} u(x) = u(x + th). \quad (10)$$

Такое семейство операторов является однопараметрической группой унитарных операторов в гильбертовом пространстве $\mathcal{H}_{\mathcal{E}}(E)$. У каждой сильно непрерывной группы унитарных операторов в пространстве $\mathcal{H}_{\mathcal{E}}(E)$ должен быть самосопряженный в пространстве $\mathcal{H}_{\mathcal{E}}(E)$ генератор. Если $h = e_j$, то в силу леммы 4.1 группа унитарных операторов $\mathbf{S}_{th}$, $t \in \mathbb{R}$, сильно непрерывна, а ее генератором является оператор $\overline{i\partial_j}$.

Если $h \notin L_1(E, \mathcal{E})$, то унитарная группа $\mathbf{S}_{th}$, $t \in \mathbb{R}$, не является сильно непрерывной в пространстве $\mathcal{H}_{\mathcal{E}}(E)$. При этом

$$\lim_{t \rightarrow 0} \left\| \frac{1}{t} (\mathbf{S}_{th} - \mathbf{I}) u \right\|_{\mathcal{H}_{\mathcal{E}}(E)} = +\infty$$

для любого ненулевого вектора $u \in \mathcal{H}_{\mathcal{E}}(E)$, т.е. область определения генератора группы $\mathbf{S}_{th}$, $t \in \mathbb{R}$, состоит из одного нулевого вектора.

По группе $\mathbf{S}_{th}$, $t \in \mathbb{R}$, можно определить оператор-функцию $\mathbf{R}_h(\lambda)$, $\operatorname{Re}(\lambda) > 0$, со значениями в пространстве $B(\mathcal{H}_{\mathcal{E}}(E))$ ограниченных линейных операторов, называемую резольвентой полугруппы унитарных операторов (см. [14]), которая определяется из условий

$$(\mathbf{R}_h(\lambda)u, v)_{\mathcal{H}_{\mathcal{E}}} = \int_0^{+\infty} (\mathbf{S}_{th} u, v)_{\mathcal{H}_{\mathcal{E}}} e^{-\lambda t} dt, \quad \operatorname{Re}(\lambda) > 0, \quad u, v \in \mathcal{H}_{\mathcal{E}}(E). \quad (11)$$

При каждом $h \in H$ оператор-функция $\mathbf{R}_h$ определена в полуплоскости $\operatorname{Re}(\lambda) > 0$, поскольку в ней несобственный интеграл (11) сходится и задает на пространстве $\mathcal{H}_{\mathcal{E}}$ ограниченную полуторалинейную форму. Справедливо равенство

$$(\mathbf{R}_h(\lambda)u, v)_{\mathcal{H}_{\mathcal{E}}} - (u, \mathbf{R}_{-h}(\lambda)v)_{\mathcal{H}_{\mathcal{E}}} = \int_0^{+\infty} \left((\mathbf{S}_{th} u, v) - (u, \mathbf{S}_{-th} v) \right) e^{-\lambda t} dt = 0;$$

следовательно,

$$(\mathbf{R}_h(\lambda))^* = \mathbf{R}_{-h}(\bar{\lambda}).$$

Лемма 4.4. Если $h \notin L_1(E, \mathcal{E})$ и $\operatorname{Re}(\lambda) > 0$, то $(\mathbf{R}_h(\lambda)u, v) = 0$ для любых $u, v \in \mathcal{H}_{\mathcal{E}}(E)$.

Доказательство. Предположим сначала, что $u = v = \chi_{\Pi}$ — индикаторная функция измеримого бруса из класса $\mathcal{P}(\mathcal{E})$ положительной меры со сторонами $b_j - a_j = 1 + \delta_j$. Так как ряд $\sum_{j=1}^{\infty} \max\{0, \ln(1 + \delta_j)\}$ сходится, то $\{\max(0, \delta_j)\} \in l_1$. Как показано выше в лемме 4.2,

$$f_{u,u}(t) = (u, \mathbf{S}_{th}u)_{\mathcal{H}_{\mathcal{E}}} = \prod_{k=1}^{\infty} (1 + \delta_k - th_k) = 0$$

при всех $t > 0$, поскольку

$$\exp \sum_{k=1}^{\infty} \ln(1 + \delta_k - th_k) = 0.$$

Следовательно, подынтегральное выражение в (11) равно нулю.

Если предположить, что u и v — индикаторные функции различных измеримых брусков, то аналогичным образом можно показать, что функция $f_{u,v}(t) = (u, \mathbf{S}_{th}v)_{\mathcal{H}_{\mathcal{E}}}$, $t \in \mathbb{R}$, обращается в нуль всюду кроме, быть может, одной точки. Если предположить, что u и v — линейные комбинации индикаторных функций измеримых брусков, то функция $f_{u,v}$ обращается в нуль всюду, за исключением конечного множества точек прямой $\mathbb{R}$. Следовательно, в силу (11), $(\mathbf{R}u, v)_{\mathcal{H}_{\mathcal{E}}} = 0$, если u и v — линейные комбинации индикаторных функций измеримых брусков. Если $u, v \in \mathcal{H}_{\mathcal{E}}(E)$ — произвольные функции, то при любом $\varepsilon > 0$ из условия $\operatorname{Re}(\lambda) > 0$ следует, что $|(\mathbf{R}u, v)_{\mathcal{H}_{\mathcal{E}}}| < \varepsilon$ и, следовательно, $(\mathbf{R}u, v)_{\mathcal{H}_{\mathcal{E}}} = 0$ при всех $u, v \in \mathcal{H}_{\mathcal{E}}$, если только $\operatorname{Re}(\lambda) > 0$. $\square$

5. МЕРЫ НА ГИЛЬБЕРТОВОМ ПРОСТРАНСТВЕ, ИНВАРИАНТНЫЕ ОТНОСИТЕЛЬНО СДВИГОВ И ПОВОРОТОВ

Для меры на гильбертовом пространстве H , инвариантной относительно сдвига, выбор ортонормированного базиса $\mathcal{E}$ в гильбертовом пространстве H осуществляет изометрический изоморфизм $\Phi_{\mathcal{E}}$ пространства H на l_2 (см. (3)). Поэтому для каждого ортонормированного базиса $\mathcal{E}$ в пространстве H изоморфизмом $\Phi_{\mathcal{E}}$ из пространства l_2 индуцирована структура кольца $K_{\mathcal{E}}$ подмножеств пространства H с заданной на нем конечно-аддитивной неотрицательной мерой $\lambda_{\mathcal{E}}$, инвариантной относительно сдвигов на векторы пространства H .

Для каждого ортонормированного базиса $\mathcal{E}$ обозначим через $\mathcal{P}_{\mathcal{E}}$ совокупность абсолютно измеримых брусков с ребрами, сонаправленными с векторами базиса $\mathcal{E}$; через $\mathcal{R}_{\mathcal{E}}$ обозначим минимальное кольцо множеств, содержащее $\mathcal{P}_{\mathcal{E}}$; через $\mathcal{K}_{\mathcal{E}}$ обозначим кольцо $\lambda_{\mathcal{E}}$ -измеримых множеств в пространстве H , на котором мера $\lambda_{\mathcal{E}}$ является полной неотрицательной конечно-аддитивной трансляционно инвариантной мерой, связанной с мерой λ_2 на кольце $\Lambda(l_2)$ изоморфизмом $\Phi_{\mathcal{E}}$. Тогда для каждого ортонормированного базиса $\mathcal{E}$ в пространстве H имеется кольцо $\mathcal{K}_{\mathcal{E}}$ $\lambda_{\mathcal{E}}$ -измеримых множеств, на котором определена мера $\lambda_{\mathcal{E}}$, и определено гильбертово пространство $\mathcal{H}_{\mathcal{E}}$ квадратично интегрируемых $\lambda_{\mathcal{E}}$ -измеримых функций на пространстве H .

Лемма 5.1. Пусть A, B — два множества в H , которые конгруэнтны в том смысле, что существует унитарное преобразование U пространства H и, быть может, параллельный перенос P в H , композиция которых переводит одно множество в другое: $B = P \circ U(A)$ и $A \in K_{\mathcal{E}}$ для некоторого ортонормированного базиса $\mathcal{E}$. Тогда найдется такой ортонормированный базис $\mathcal{F}$, что $B \in K_{\mathcal{F}}$ и $\lambda_{\mathcal{F}}(B) = \lambda_{\mathcal{E}}(A)$.

Доказательство. Выберем ортонормированный базис (ОНБ) $\mathcal{F}$, который получается из ОНБ $\mathcal{E}$ действием унитарного преобразования U . Если $A \in \mathcal{P}_{\mathcal{E}}$, то $U(A) \in \mathcal{K}_{\mathcal{F}}$, причем $\lambda_{\mathcal{F}}(U(A)) = \lambda_{\mathcal{E}}(A)$. Поскольку меры измеримых брусков сохраняются при параллельных переносах и унитарных преобразованиях, то сохраняются и меры измеримых относительно ОНБ множеств: если $A \in K_{\mathcal{E}}$ для некоторого ОНБ $\mathcal{E}$, $\mathcal{F} = U(\mathcal{E})$ и $B = P \circ U(A)$, то $B \in K_{\mathcal{F}}$ и $\lambda_{\mathcal{F}}(B) = \lambda_{\mathcal{E}}(A)$. $\square$

Множества $A, B \subset H$ назовем *конгруэнтными*, если существуют такие ортогональное преобразование U пространства H и вектор $h \in H$, что $A = S_h \circ U(A)$ (здесь $S_h x = x + h \forall x \in H$). Лемма 5.1 связывает значения мер конгруэнтных множеств.

Пусть $\mathcal{S}$ — множество всех ортонормированных базисов в гильбертовом пространстве H . Тогда $\{K_{\mathcal{E}}, \mathcal{E} \in \mathcal{S}\}$ — семейство колец подмножеств пространства H . Обозначим через $\mathcal{M}$ множество всех подмножеств пространства H , входящих хотя бы в одно из колец этого семейства. Множество $\mathcal{M}$ не является ни кольцом, ни полукольцом. Введем функцию

$$\lambda : \mathcal{M} \rightarrow [0, +\infty], \quad \lambda(A) = \lambda_{\mathcal{E}}(A), \text{ если } A \in K_{\mathcal{E}}.$$

Функция λ определена корректно, так как если $A \in K_{\mathcal{E}} \cap K_{\mathcal{F}}$, то $\lambda_{\mathcal{E}}(A) = \lambda_{\mathcal{F}}(A)$, ибо в силу леммы 5.1 функция λ обладает тем свойством, что если множества $A, B \in \mathcal{M}$ конгруэнтны, то $\lambda(A) = \lambda(B)$. Рассмотрим теперь минимальное кольцо $\mathcal{K}$, содержащее систему множеств $\mathcal{M}$, и поставим задачу о продолжении функции λ с множества $\mathcal{M}$ на кольцо $\mathcal{K}$. Эта задача будет решена далее.

Определим *продолжение скалярного произведения на линейную оболочку пространств $\mathcal{H}_{\mathcal{E}}$* . Для каждого ортонормированного базиса $\mathcal{E} \in \mathcal{S}$ выше было определено гильбертово пространство $\mathcal{H}_{\mathcal{E}}$, скалярное произведение в котором определяется полуторалинейной формой $\beta_{\mathcal{E}}$. Элементами пространства $\mathcal{H}_{\mathcal{E}}$ являются классы эквивалентности функций $u : H \rightarrow \mathbb{C}$, измеримых относительно алгебры $\mathcal{A}_{\mathcal{E}}$ подмножеств пространства H (минимальной алгебры, содержащей кольцо $K_{\mathcal{E}}$ и состоящей из элементов этого кольца и дополнений элементов этого кольца) и квадратично интегрируемых относительно меры $\lambda_{\mathcal{E}}$. Для каждой функции $u : H \rightarrow \mathbb{C}$, являющейся представителем класса эквивалентности из пространства $\mathcal{H}_{\mathcal{E}}$, существует последовательность простых $\mathcal{A}_{\mathcal{E}}$ -измеримых функций на H , сходящихся к функции u по норме пространства $\mathcal{H}_{\mathcal{E}}$. Поэтому если $\mathcal{E}, \mathcal{F}$ — два различных базиса в пространстве H , то представители элементов $u \in \mathcal{H}_{\mathcal{E}}, v \in \mathcal{H}_{\mathcal{F}}$ можно складывать поточечно как функции $H \rightarrow \mathbb{C}$ и, следовательно, определены линейные оболочки элементов пространств $\mathcal{H}_{\mathcal{E}}, \mathcal{E} \in \mathcal{S}$.

Рассмотрим линейную оболочку $\mathcal{L} = \text{lin}(\mathcal{H}_{\mathcal{E}}, \mathcal{E} \in \mathcal{S})$ пространств $\mathcal{H}_{\mathcal{E}}, \mathcal{E} \in \mathcal{S}$ как линейное пространство, на линейных подпространствах $\mathcal{H}_{\mathcal{E}}$ которого заданы эрмитовы положительно определенные полуторалинейные формы $\beta_{\mathcal{E}}$, определяющие скалярное произведение в $\mathcal{H}_{\mathcal{E}}$. Поставим вопрос о существовании такой полуторалинейной формы β на линейном пространстве $\mathcal{L}$, сужение которой на любое линейное подпространство $\mathcal{H}_{\mathcal{E}}$ совпадает с эрмитовой полуторалинейной формой $\beta_{\mathcal{E}}$. Решение этого вопроса дают следующие две теоремы, подробное доказательство которых содержится в [10].

Теорема 5.1 (см. [10, теорема 3]). *Каждому отношению полного порядка $\prec$ на множестве ортонормированных базисов $\mathcal{S}$ соответствует эрмитова положительно определенная полуторалинейная форма $\beta_{\prec}$, заданная на линейной оболочке $\mathcal{L} = \text{lin}(\mathcal{H}_{\mathcal{E}}, \mathcal{E} \in \mathcal{S})$ пространств $\mathcal{H}_{\mathcal{E}}, \mathcal{E} \in \mathcal{S}$, сужение которой на пространство $\mathcal{H}_{\mathcal{E}}$ совпадает с полуторалинейной формой $\beta_{\mathcal{E}}$ при любом $\mathcal{E} \in \mathcal{S}$.*

Теорема 5.2 (см. [10, теорема 4]). *Полуторалинейная форма $\beta_{\prec}$ на линейном пространстве $\mathcal{L}$ не зависит от выбора отношения полного порядка $\prec$ на множестве $\mathcal{S}$.*

Обозначим через β эрмитову положительно определенную полуторалинейную форму на линейном пространстве $\mathcal{L}$, соответствующую какому-либо выбору отношения полного порядка $\prec$ на множестве $\mathcal{S}$ и, в силу теоремы 5.2, не зависящую от выбора отношения $\prec$. Определим гильбертово пространство $\mathcal{H}$ как пополнение предгильбертова пространства $(\mathcal{L}, \beta)$.

Определим *продолжение меры $\lambda_{\mathcal{E}}$ с колец $K_{\mathcal{E}}, \mathcal{E} \in \mathcal{S}$ на порожденное ими кольцо $\mathcal{K}$* . Рассмотрим минимальное кольцо $\mathcal{K}$, содержащее множества, входящие в кольца $K_{\mathcal{E}}, \mathcal{E} \in \mathcal{S}$. Поставим вопрос о существовании конечно аддитивной меры λ , заданной на кольце $\mathcal{K}$, сужение которой на любое кольцо $K_{\mathcal{E}}$ совпадает с мерой $\lambda_{\mathcal{E}}$.

Теорема 5.3 (см. [10, следствие 4]). *Продолжение β скалярного произведения с пространств $\mathcal{H}_{\mathcal{E}}, \mathcal{E} \in \mathcal{S}$, на пространство $\mathcal{H}$ однозначно определяет продолжение меры λ на минимальное кольцо $\mathcal{K}$, содержащее множества, входящие в какое-либо из колец $K_{\mathcal{E}}, \mathcal{E} \in \mathcal{S}$, удовлетворяющее*

условию $\lambda|_{\mathcal{K}_\mathcal{E}} = \lambda_\mathcal{E}$. При этом мера λ инвариантна относительно сдвигов на произвольный вектор пространства H и произвольных его ортогональных преобразований.

В [10] установлено, что для произвольных $A \in \mathcal{K}_\mathcal{E}$, $B \in \mathcal{K}_\mathcal{F}$ выполняется равенство $\lambda(A \cap B) = \beta(\chi_A, \chi_B)$. На других множества из алгебры $\mathcal{K}$ мера λ определяется из условия аддитивности.

Мера λ является конечно-аддитивным аналогом меры Лебега на бесконечномерном гильбертовом пространстве как инвариантная относительно движений мера на минимальном кольце, содержащем все измеримые брусы из пространства H . Мера λ является продолжением любой из мер $\lambda_\mathcal{E}$ с кольца $\mathcal{K}_\mathcal{E}$ на кольцо $\mathcal{K}$. Пространство $\mathcal{H}$ содержит пространство $\mathcal{H}_\mathcal{E}$ как замкнутое подпространство.

Рассмотрим теперь унитарную группу $S_h(t)$, $t \in \mathbb{R}$ преобразований пространства $\mathcal{H}$, действующих по правилу $S_h(t)u(x) = u(x + th)$, $u \in \mathcal{H}$, при произвольном $h \neq 0$, $h \in H$. Эта унитарная группа не является сильно непрерывной в пространстве $\mathcal{H}$ поскольку она в силу теоремы 4.1 не является сильно непрерывной на любом таком его подпространстве $\mathcal{H}_\mathcal{E}$, что $\{(h, e_k)\} \notin l_1$, но является сильно непрерывной на любом таком подпространстве $\mathcal{H}_\mathcal{F}$, что $\{(h, f_k)\} \in l_1$.

Из леммы 4.4 следует, что полугруппа $S_h(t)$, $t \geq 0$, в пространстве $\mathcal{H}$ не является суммируемой по Абелю к оператору I при $t \rightarrow +0$, поскольку для всякого ненулевого вектора $u \in \mathcal{H}_\mathcal{E}$ удовлетворяющего условию $\{(h, e_k)\} \notin l_1$, согласно лемме 4.4 выполняется неравенство $u \neq \lim_{\lambda \rightarrow +\infty} \lambda R(\lambda)u = 0$.

6. СЛУЧАЙНЫЕ СДВИГИ И ИХ МАТЕМАТИЧЕСКИЕ ОЖИДАНИЯ

В этом разделе исследуем случайные сдвиги в пространстве H и их математические ожидания.

Пусть H — вещественное сепарабельное гильбертово пространство. Исследуем операторы сдвига S_h на случайный вектор $h \in H$, распределение которого на пространстве H задается некоторой гауссовской мерой или однопараметрическим семейством (полугруппой) гауссовских мер.

Для каждого вектора $h \in H$ определено преобразование сдвига U_h пространства $\mathcal{H}$, действующее на произвольный элемент $u \in \mathcal{H}$ по формуле $U_h u(x) = u(x + h)$. Для каждого ортонормированного базиса $\mathcal{E}$ пространства H и каждого вектора $h \in H$ определим преобразование сдвига $U_{\mathcal{E},h}$ пространства $\mathcal{H}_\mathcal{E}$ по формуле $U_{\mathcal{E},h} = U_h|_{\mathcal{H}_\mathcal{E}}$.

Пусть ν — центрированная гауссовская мера на гильбертовом пространстве H , обладающая ядерным ковариационным оператором D . Тогда D — неотрицательный оператор с ортонормированным базисом из собственных векторов $\mathcal{F}$. Гауссовская мера ν на гильбертовом пространстве H , обладающая ядерным ковариационным оператором, является счетно-аддитивной. Заметим (см. [7, теоремы 2.1, 2.3]), что гауссовская мера γ , определенная на σ -алгебре $\mathcal{C}(H)$ (минимальной σ -алгебре, содержащей цилиндрических подмножеств пространства H , порождаемых функционалами из H) при условии ядерности ковариационного оператора D имеет единственное счетно-аддитивное продолжение до меры на σ -алгебре $\mathcal{B}(H)$ борелевских подмножеств пространства H .

Для каждой центрированной гауссовской меры ν с ядерным ковариационным оператором D определим однопараметрическое семейство гауссовских мер γ_t , $t \geq 0$, на пространстве H , по следующему правилу:

$$\nu_t(A) = \gamma\left(\frac{1}{\sqrt{t}}A\right), \quad A \in \mathcal{B}(H).$$

Тогда при каждом $t \geq 0$ мера ν_t имеет преобразование Фурье

$$\tilde{\nu}_t(\xi) = \exp\left(-\frac{t}{2}D\xi^2\right),$$

т.е. ν_t — гауссовская мера на пространстве H с нулевым средним и ядерным ковариационным оператором tD . Семейство гауссовских мер ν_t , $t \geq 0$, образует однопараметрическую полугруппу относительно операции свертки:

$$\nu_t * \nu_s = \nu_{t+s} \quad \forall t, s \in \mathbb{R}_+$$

(см. [4]); при этом каждая мера ν_t , $t \geq 0$, является счетно-аддитивной мерой.

Пусть $\mathcal{E}$ — ортонормированный базис из собственных векторов неотрицательного ядерного оператора $\mathbf{D}$, являющегося ковариационным оператором центрированной гауссовской меры ν . По введенному однопараметрическому семейству гауссовских мер ν_t , $t \geq 0$, определим однопараметрическое семейство $\mathcal{U}_{\nu, \mathcal{E}}(t)$, $t \geq 0$, преобразований пространства $\mathcal{H}_{\mathcal{E}}$ как результат усреднения случайного преобразования сдвига $\mathbf{U}_{\mathcal{E}, h}$, распределение случайного параметра $h \in H$ которого в каждый момент времени $t \geq 0$ задается мерой ν_t на пространстве H . Тогда в каждый момент времени $t \geq 0$ образ $\mathcal{U}_{\nu, \mathcal{E}}(t)u$ элемента $u \in H$ определяется равенством

$$\mathcal{U}_{\nu, \mathcal{E}}(t)u = \int_H \mathbf{U}_{\mathcal{E}, h} u d\nu_t(h).$$

При каждом значении $t \geq 0$ вектор $\mathcal{U}_{\nu, \mathcal{E}}(t)u$ определяется как интеграл Петтиса:

$$(\mathcal{U}_{\nu, \mathcal{E}}(t)u, v)_{\mathcal{H}_{\mathcal{E}}} = \int_H (\mathbf{U}_{\mathcal{E}, h} u, v)_{\mathcal{H}_{\mathcal{E}}} d\nu_t(h) \quad \forall u, v \in \mathcal{H}_{\mathcal{E}}. \quad (12)$$

Лемма 6.1. *Если $u, v \in \mathcal{H}_{\mathcal{E}}$ и $\mathbf{D}$ — ядерный оператор в пространстве H , то при любом $t \geq 0$ числовая функция $\phi(h) = (\mathbf{U}_{\mathcal{E}, h} u, v)_{\mathcal{H}_{\mathcal{E}}}$, $h \in H$, является ограниченной измеримой относительно меры ν_t (относительно σ -алгебры $\mathcal{C}(H)$ цилиндрических подмножеств) функцией $H \rightarrow \mathbb{C}$.*

Доказательство. Пусть $t \geq 0$. Сначала докажем, что функция ϕ определена на H и ограничена. Пусть $u, v \in \mathcal{H}_{\mathcal{E}}$. При каждом $h \in H$ имеем $\mathbf{U}_{\mathcal{E}, h} u \in \mathcal{H}_{\mathcal{E}}$, а числовая функция $\phi(h) = (\mathbf{U}_{\mathcal{E}, h} u, v)_{\mathcal{H}_{\mathcal{E}}}$, $h \in H$, ограничена условием

$$|\phi(h)| \leq \|u\|_{\mathcal{H}_{\mathcal{E}}} \|v\|_{\mathcal{H}_{\mathcal{E}}}.$$

Докажем ν_t -измеримость функции ϕ . Рассмотрим сначала действие оператора $\mathcal{U}_{\nu, \mathcal{E}}(t)$ на индикаторную функцию u измеримого бруса $\Pi \in \mathcal{P}_{\mathcal{E}}$ и рассмотрим скалярное произведение (12) в предположении, что элемент v является индикаторной функцией измеримого бруса $\Pi' \in \mathcal{P}_{\mathcal{E}}$.

Поскольку $\mathbf{U}_{\mathcal{E}, h} u$ и v — индикаторные функции брусков из класса $\mathcal{P}_{\mathcal{E}}$, то функция ϕ является произведением счетного множества цилиндрических функций вида $\phi_j(h)$, зависящих только от величины $h_j = (h, e_j)$, $j \in \mathbb{N}$ (при каждом $j \in \mathbb{N}$ имеем $\phi_j(h) = |[a_j, b_j] \cap [a'_j + h_j, b'_j + h_j]|$). Тогда

$$\phi(h) = \prod_{j=1}^{\infty} \phi_j(h), \quad h \in H,$$

причем при любом $h \in H$ последнее произведение сходится, поскольку брусы Π , Π' являются абсолютно измеримыми. Цилиндрические функции ϕ_j являются ν_t -измеримыми, поэтому функция ϕ также ν_t -измерима (см. [3, теорема 2.1.5]).

Любой элемент $\mathcal{H}_{\mathcal{E}}$ может быть аппроксимирован линейной комбинацией индикаторов измеримых брусков. Поэтому при произвольных $u, v \in \mathcal{H}_{\mathcal{E}}$ функция ϕ ν_t -измерима, поскольку является равномерным пределом последовательности ν_t -измеримых функций. $\square$

Следствие 6.1. *При любом $t \geq 0$ определен оператор $\mathcal{U}_{\nu, \mathcal{E}}(t) \in B(\mathcal{H}_{\mathcal{E}})$, норма которого не превосходит единицы.*

Доказательство. Пусть $u, v \in \mathcal{H}_{\mathcal{E}}$ и $t \geq 0$. Ограниченная измеримая функция $\phi(h)$, $h \in H$, интегрируема по гауссовской мере ν_t . Правая часть выражения (12) определена при всех $u, v \in \mathcal{H}_{\mathcal{E}}$ и в силу неравенства

$$\int_H (\mathbf{U}_{\mathcal{E}, h} u, v)_{\mathcal{H}_{\mathcal{E}}} d\nu_t(h) \leq \|v\|_{\mathcal{H}_{\mathcal{E}}} \|\mathbf{U}_{\mathcal{E}, h} u\|_{\mathcal{H}_{\mathcal{E}}} \|\nu_t\|_{var} = \|u\|_{\mathcal{H}_{\mathcal{E}}} \|v\|_{\mathcal{H}_{\mathcal{E}}}$$

является непрерывной полуторалинейной формой. Следовательно, при любом $t \geq 0$ определен ограниченный линейный оператор

$$\mathcal{U}_{\nu, \mathcal{E}}(t) = \int_H \mathbf{U}_{\mathcal{E}, h} d\nu_t(h). \quad \square$$

По однопараметрическому семейству гауссовских мер ν_t , $t \geq 0$, определим однопараметрическое семейство $\mathcal{U}_\nu(t)$, $t \geq 0$, преобразований пространства $\mathcal{H}$ по следующему правилу: в каждый момент времени $t \geq 0$ образ $\mathcal{U}_\nu(t)u$ элемента $u \in H$ определяется равенством

$$\mathcal{U}_\nu(t)u = \int_H U_h u d\nu_t(h). \quad (13)$$

Лемма 6.2. *Если $u, v \in \mathcal{H}$ и D — ядерный оператор в пространстве H , то при любом $t \geq 0$ числовая функция $\phi(h) = (U_h u, v)_\mathcal{H}$, $h \in H$, является ограниченной и измеримой относительно меры ν_t (относительно σ -алгебры $\mathcal{C}(H)$ цилиндрических множеств пространства H).*

Доказательство. Сначала изучим действие оператора $\mathcal{U}_\nu(t)$ на функцию $u \in \mathcal{H}_\mathcal{E}$ и рассмотрим выражение (14) в предположении, что $v \in \mathcal{H}_\mathcal{F}$, где $\mathcal{E}, \mathcal{F}$ — некоторые ОНБ в пространстве H .

Если $\mathcal{H}_\mathcal{E} \perp \mathcal{H}_\mathcal{F}$, то, поскольку эти пространства инвариантны относительно операторов U_h при любом $h \in H$, имеем $(U_h u, v)_\mathcal{H} = 0$ для всех $h \in H$. Следовательно, $(\mathcal{U}_\nu(t)u, v) = 0$ при любом $t \in \mathbb{R}$ и имеет место непрерывность числовой функции $(\mathcal{U}_\nu(t)u, v)$, $t \in \mathbb{R}$.

В случае произвольного расположения пространств $\mathcal{H}_\mathcal{E}$ и $\mathcal{H}_\mathcal{F}$ в пространстве $\mathcal{H}$ пространство $\mathcal{H}_\mathcal{F}$ можно разложить в прямую сумму $\mathcal{H}_\parallel \oplus \mathcal{H}_\perp$, где $\mathcal{H}_\parallel = \mathcal{H}_\mathcal{F} \cap \mathcal{H}_\mathcal{E}$ и $\mathcal{H}_\perp = \mathcal{H}_\mathcal{F} \cap \mathcal{H}_\mathcal{E}^\perp$.

Пространство $\mathcal{H}_\mathcal{E}$ инвариантно относительно сдвига на произвольный вектор пространства H . Поэтому для любых векторов $u \in \mathcal{H}_\mathcal{E}$ и $v = v_\parallel \oplus v_\perp \in \mathcal{H}_\mathcal{F}$ справедливы равенства

$$(\mathcal{U}_\nu(t)u, v) = (\mathcal{U}_\nu(t)u, v_\parallel + v_\perp) = (\mathcal{U}_\nu(t)u, v_\parallel) + (\mathcal{U}_\nu(t)u, v_\perp) = (\mathcal{U}_\nu(t)\chi_\Pi, v_\parallel), \quad t \in \mathbb{R}.$$

Измеримость последней функции следует из уже доказанной в лемме 6.1 измеримости функции $(\mathcal{U}_\nu(t)u, v)$ относительно σ -алгебры $\mathcal{C}(H)$ при произвольном выборе $u, v \in \mathcal{H}_\mathcal{E}$, поскольку $u, v_\parallel \in \mathcal{H}_\mathcal{E}$.

Если u, v — произвольные функции из $\mathcal{H}$, то они могут быть приближены по норме пространства $\mathcal{H}$ линейными комбинациями функций из пространств $\mathcal{H}_\mathcal{E}$, $\mathcal{E} \in \mathcal{S}$. Поэтому функция ϕ является ν_t -измеримой как равномерный предел последовательности ν_t -измеримых функций.

При каждом $h \in H$ числовая функция $\phi(h) = (U_h u, v)_\mathcal{H}$, $h \in H$, очевидно, ограничена условием $|\phi(h)| \leq \|u\|_\mathcal{H} \|v\|_\mathcal{H}$. $\square$

Теорема 6.1. *При каждом значении $t \geq 0$ и при любом $u \in \mathcal{H}$ вектор $\mathcal{U}_\nu(t)u$ определяется как интеграл Петтиса:*

$$(\mathcal{U}_\nu(t)u, v)_\mathcal{H} = \int_H (U_h u, v)_\mathcal{H} d\nu_t(h) \quad \forall u, v \in \mathcal{H}. \quad (14)$$

Доказательство. Ограниченная измеримая функция $\phi(h) = (U_h u, v)_\mathcal{H}$, $h \in H$, интегрируема по мере ν_t с вариацией, равной единице. Поэтому правая часть выражения (14) определена при всех $u, v \in \mathcal{H}_\mathcal{E}$ и в силу неравенства

$$\int_H (U_h u, v)_\mathcal{H} d\nu_t(h) \leq \|v\|_\mathcal{H} \|U_h u\|_\mathcal{H} \|\nu_t\|_{var} = \|u\|_\mathcal{H} \|v\|_\mathcal{H}$$

является непрерывной полуторалинейной формой. $\square$

Следствие 6.2. *Пусть ν — гауссовская мера на пространстве H с ядерным ковариационным оператором. Тогда при любом $t \geq 0$ равенство (14) определяет оператор $\mathcal{U}_\nu(t) \in B(\mathcal{H}_\mathcal{E})$, норма которого не превосходит единицы.*

Теорема 6.2 (см. [10, лемма 7]). *Пусть ν — гауссовская мера на пространстве H с ядерным ковариационным оператором. Тогда однопараметрическое семейство операторов*

$$\mathcal{U}_\nu(t), \quad t \geq 0, \quad \mathcal{U}_\nu(t)\mathcal{U}_\nu(s) = \mathcal{U}_\nu(t+s) \quad \forall t, s \in \mathbb{R}_+,$$

является полугруппой сжимающих операторов в пространстве $\mathcal{H}$.

Доказательство. Рассмотрим выражение (14) при $t = s + r$. Поскольку меры ν_t, ν_s являются вероятностными мерами на σ -алгебре борелевских подмножеств пространства H , то согласно [3, предложение 3.3.1] мера $\nu_t \otimes \nu_s$ является вероятностной мерой на алгебре борелевских подмножеств пространства $H \times H$. Мера $\nu_t * \nu_s$ является образом меры $\nu_t \otimes \nu_s$ на $H \times H$ при отображении $\phi : H \times H \rightarrow H$, действующем по правилу $\phi(x, y) = x + y$.

Согласно формуле (14) справедливо равенство

$$(\mathcal{U}_\nu(s+r)u, v)_\mathcal{H} = \int_H (\mathbf{U}_h u, v)_\mathcal{H} d\nu_{s+r}(h).$$

Фиксировав векторы $u, v \in \mathcal{H}$, определим функцию $f_{u,v}(h) = (\mathbf{U}_h u, v)_\mathcal{H}$, $h \in H$. Функция $f_{u,v}$ измерима относительно σ -алгебры $\mathcal{C}(H)$ и ограничена на H по лемме 6.2. Тогда

$$(\mathcal{U}_\nu(s+r)u, v)_\mathcal{H} = \int_H f_{u,v}(h) d\nu_{s+r}(h).$$

В силу полугруппового свойства семейства мер ν_t , $t \geq 0$, справедливо равенство $\nu_{s+r} = \nu_s * \nu_r$, поэтому

$$\int_H f_{u,v}(h) d\nu_{s+r}(h) = \int_{H \times H} f_{u,v}(x+y) d(\nu_s \otimes \nu_r)(x, y).$$

Поскольку функция $f_{u,v}$ измерима относительно σ -алгебры $\mathcal{C}(H)$ и ограничена, то функция $f_{u,v}(x+y)$, $(x, y) \in H \times H$, ограничена и измерима на $H \times H$ относительно σ -алгебры $\mathcal{C}(H) \otimes \mathcal{C}(H)$ (см. [3, 3.9.1]), ибо $f_{u,v}(x+y) = f_0 \circ F(x, y)$, где $F(x, y) = (x+y, y)$, $(x, y) \in H \times H$, и $f_0(x, y) = f_{u,v}(x)$, $(x, y) \in H \times H$, т.е. функция $f_{u,v}(x+y)$, $(x, y) \in H \times H$ на $H \times H$ является композицией двух измеримых отображений. Поэтому в силу теоремы Фубини (см. [3, 3.4.4])

$$\begin{aligned} \int_{H \times H} f_{u,v}(x+y) d(\nu_s \otimes \nu_r)(x, y) &= \\ &= \int_H \left[\int_H f_{u,v}(x+y) d\nu_s(x) \right] d\nu_r(y) = \int_H \left[\int_H f_{u,v}(x+y) d\nu_r(y) \right] d\nu_s(x). \end{aligned}$$

С другой стороны,

$$\begin{aligned} (\mathcal{U}_\nu(s)\mathcal{U}_\nu(r)u, v)_\mathcal{H} &= \int_H (\mathbf{U}_h \mathcal{U}(r)u, v)_\mathcal{H} d\nu_s(h) = \\ &= \int_H (\mathcal{U}_{\nu, \mathcal{E}}(r)(\mathbf{U}_h u), v)_\mathcal{H} d\nu_s(h) = \int_H \left[\int_H (\mathbf{U}_\sigma(\mathbf{U}_h u), v)_\mathcal{H} d\nu_r(\sigma) \right] d\nu_s(h) = \\ &= \int_H \left[\int_H (\mathbf{U}_{h+\sigma} u, v)_\mathcal{H} d\nu_r(\sigma) \right] d\nu_s(h) = \int_H \left[\int_H f_{u,v}(h+\sigma) d\nu_r(\sigma) \right] d\nu_s(h). \end{aligned}$$

Поэтому $\mathcal{U}_\nu(s)\mathcal{U}_\nu(r) = \mathcal{U}_\nu(s+r)$ для всех $r, s \geq 0$. $\square$

Приведем условия сильной непрерывности полугруппы $\mathcal{U}_\nu$, которая является результатом усреднения операторов случайного сдвига $\mathbf{U}_h$ по однопараметрической полугруппе мер ν_t , $t \in \mathbb{R}$.

Теорема 6.3 (см. [13]). Пусть $\mathbf{D}$ — неотрицательный оператор в пространстве H с ортонормированным базисом собственных векторов $\mathcal{E}$, который невырожден и таков, что $\mathbf{D}^{1/4}$ является ядерным. Пусть $\nu_t \mathbf{D}$, $t \geq 0$, — полугруппа (относительно свертки) гауссовских мер на гильбертовом пространстве H с ковариационным оператором $t\mathbf{D}$. Тогда однопараметрическое семейство преобразований $\mathcal{U}_\nu$ пространства $\mathcal{H}$ является сильно непрерывной полугруппой сжимающих самосопряженных преобразований пространства $\mathcal{H}_\mathcal{E}$.

Следствие 6.3. *Сильно непрерывная полугруппа $\mathcal{U}_{\nu, \mathcal{E}}$ сжимающих операторов в пространстве $\mathcal{H}_{\mathcal{E}}$ обладает плотно определенным замкнутым неположительным генератором $\Delta_{\nu, \mathcal{E}}$.*

Замечание 6.1. Если D — оператор конечного ранга $m \in \mathbb{N}$, то $\mathcal{U}_{\nu, \mathcal{E}}$ унитарно эквивалентна полугруппе, разрешающей уравнение диффузии в конечномерном пространстве размерности m .

Лемма 6.3. *Пусть выполнены условия теоремы 6.2 и пусть $\mathcal{F}$ — некоторый ортонормированный базис в пространстве H . Тогда линейное подпространство $\mathcal{H}_{\mathcal{F}}$ пространства $\mathcal{H}$ инвариантно относительно преобразований $\mathcal{U}_{\nu}(t)$, $t \geq 0$.*

Доказательство. Пусть $u \in \mathcal{H}_{\mathcal{F}}$ и $v \in \mathcal{H}_{\mathcal{F}}^{\perp}$. Тогда для любого $t \geq 0$ справедливо равенство

$$\mathcal{U}_{\nu}(t)(u, v)_{\mathcal{H}} = \int_H (U_h u, v)_{\mathcal{H}} d\nu_t(h) = 0,$$

поскольку подпространства $\mathcal{H}_{\mathcal{F}}$ и $\mathcal{H}_{\mathcal{F}}^{\perp}$ инвариантны относительно каждого из преобразований U_h , $h \in H$. $\square$

Исследуем свойства полугруппы $\mathcal{U}_{\nu}$ на инвариантных подпространствах $\mathcal{H}_{\mathcal{F}}$ пространства $\mathcal{H}$.

Замечание 6.2. Пусть $\mathcal{E}$ — ортонормированный базис из собственных векторов ковариационного оператора D меры ν и $\mathcal{F}$ — такой ортонормированный базис в пространстве, что $\mathcal{H}_{\mathcal{E}} \perp \mathcal{H}_{\mathcal{F}}$. Тогда согласно лемме 6.3 для любого $t > 0$ справедливо равенство

$$(u, \mathcal{U}_{\nu}(t)v)_{\mathcal{H}} = 0 \quad \forall u \in \mathcal{H}_{\mathcal{F}}, \quad \forall v \in \mathcal{H}_{\mathcal{E}}. \quad (15)$$

Лемма 6.4. *Пусть ν — гауссовская мера на пространстве H с ядерным неотрицательным ковариационным оператором D , имеющим базис из собственных векторов $\mathcal{E}$. Тогда если $u \in \mathcal{H}_{\mathcal{F}}$, то*

$$\lim_{t \rightarrow +0} (\mathcal{U}_{\nu}(t)u, u) \leq \nu(L_1(H, \mathcal{F})) \|u\|_{\mathcal{H}}^2.$$

Доказательство. Сначала покажем, что если $\mathcal{F}$ — некоторый ортонормированный базис в пространстве H , то множество $L_1(H, \mathcal{F})$ измеримо относительно меры ν . Функция $g(h) = \sum_{k=1}^{\infty} |(f_k, h)|$, $h \in H$, измерима относительно борелевской σ -алгебры $\mathcal{B}(H)$ в силу [3, лемма 2.1.6], поэтому множества $G_n = \{h \in H : g(h) \leq n\}$, $n \in \mathbb{N}$, измеримы относительно меры ν . Тогда множество $L_1(H, \mathcal{F}) = \bigcup_{n=1}^{\infty} G_n$ является ν -измеримым в силу [3, лемма 2.1.7].

Пусть u — индикаторная функция измеримого бруса из класса $\mathcal{P}_{\mathcal{F}}$ с ребрами, сонаправленными с векторами базиса $\mathcal{H}_{\mathcal{F}}$. Тогда, как показано в доказательстве леммы 4.2 (см. также лемму 4.4) для любого вектора $h \in H$, не лежащего в $L_1(H, \mathcal{F})$, при всех $t > 0$ справедливо равенство

$$(U_{\sqrt{t}h}u, u)_{\mathcal{H}} = 0. \quad (16)$$

Если u — линейная комбинация индикаторных функций измеримых брусов из класса $\mathcal{P}_{\mathcal{F}}$, при всех $t > 0$ равенство (16) справедливо при всех $h \in H$, $h \notin L_1(H, \mathcal{F})$, за исключением, быть может, конечного числа векторов.

Пусть $u \in \mathcal{H}_{\mathcal{F}}$ и $t > 0$. Тогда для любого $\varepsilon > 0$ и любого $t > 0$ найдется такое конечное число векторов $M \in H$, что для любого вектора $h \in H$, $h \notin (L_1(H, \mathcal{F}) \cup M)$, справедливо неравенство

$$\left| (U_{\sqrt{t}h}u, u)_{\mathcal{H}} \right| \leq \varepsilon. \quad (17)$$

Поскольку

$$(u, \mathcal{U}_{\nu}(t)u) = \int_H (u, U_{\sqrt{t}h}u) d\nu(h) = \int_{\substack{h \in H: \\ h \in L_1(H, \mathcal{F})}} (u, U_{\sqrt{t}h}u) d\nu(h) + \int_{\substack{h \in H: \\ h \notin L_1(H, \mathcal{F})}} (u, U_{\sqrt{t}h}u) d\nu(h),$$

то в силу равенства (17) для любого $t > 0$ справедлива оценка

$$\left| (u, \mathcal{U}_\nu(t)u)_{\mathcal{H}} \right| \leq \varepsilon + \left| \int_{\substack{h \in H: \\ h \in L_1(H, \mathcal{F})}} (u, \mathbf{U}_{\sqrt{t}h}u) d\nu(h) \right| = \varepsilon + \|u\|_{\mathcal{H}}^2 \nu(\{h \in H : h \in L_1(H, \mathcal{F})\}),$$

откуда в силу произвольности числа $\varepsilon > 0$ следует утверждение леммы. $\square$

Теорема 6.4. Пусть ν — гауссовская мера на пространстве H с ядерным ненулевым ковариационным оператором $\mathbf{D}$, имеющим базис из собственных векторов $\mathcal{E}$. Тогда полугруппа $\mathcal{U}_\nu$ не является сильно непрерывной на пространстве $\mathcal{H}$.

Доказательство. Покажем, что найдется такой ОНБ $\mathcal{F}$, что $\nu(L_1(H, \mathcal{F})) < 1$. Предположим противное, что для любого ОНБ $\mathcal{F}$ выполняется $\nu(L_1(H, \mathcal{F})) = 1$.

Пусть $e_1 \in \mathcal{E}$ — собственный вектор оператора $\mathbf{D}$ и пусть $\mathbf{D}e_1 = d_1 e_1$, $d_1 > 0$. Пусть $\mathcal{F}$ — такой ОНБ, что $e_1 \notin L_1(H, \mathcal{F})$, т.е. $\{f_k, e_1\} \notin l_1$. Тогда для любого $x \in H$, $x \in L_1(H, \mathcal{F})$, и любого числа $s \neq 0$ выполняется условие $x + se_1 \notin L_1(H, \mathcal{F})$. Оценим значение меры ν на множестве

$$M_1(s) = \{se_1 + x, x \in L_1(H, \mathcal{F})\} = \mathbf{U}_{se_1} L_1(H, \mathcal{F}), \quad s \geq 0.$$

Согласно предположению $\nu(M_f(0)) = \nu(L_1(H, \mathcal{F})) = 1$.

Так как e_1 — собственный вектор корреляционного оператора $\mathbf{D}$ гауссовской меры ν , отвечающий собственному значению $d_1 > 0$, то гауссовская мера ν имеет логарифмическую производную по направлению вектора e_1 , которая является ограниченной непрерывной функцией на пространстве H . Следовательно, функция

$$\nu(M_1(s)) = \nu(\mathbf{U}_{se_1}(M_1(0))) = (\mathbf{U}_{-se_1}\nu)(M_1(0)), \quad s \in \mathbb{R},$$

дифференцируема по параметру s . Следовательно, существует такое число $\delta_1 > 0$, что

$$\nu(\mathbf{U}_{\delta_1 e_1} M_1(0)) = \nu(M_1(\delta_1)) \geq \frac{1}{2}.$$

Поскольку

$$M_1(\delta_1) \subset \{h \in H : h \notin L_1(H, \mathcal{F})\},$$

ибо $h \notin L_1(H, \mathcal{F})$ для любого $h \in M_f(\delta_f)$, то

$$\nu(\{h \in H : h \notin \mathcal{H}_{\mathcal{F}}\}) \geq \nu(M_1(\delta_1)) \geq \frac{1}{2}.$$

Следовательно, предположение о том, что $\nu(L_1(H, \mathcal{F})) = 1$ для любого $\mathcal{F}$, не верно.

Поэтому найдется такой ОНБ $\mathcal{F}_0$, что $\nu(L_1(H, \mathcal{F}_0)) = \delta_0 < 1$ и, согласно лемме 6.4 для любого $u \in \mathcal{H}_{\mathcal{F}_0}$ выполняется неравенство

$$\lim_{t \rightarrow +0} (\mathcal{U}_\nu(t)u, u) \leq \delta_0 \|u\|_{\mathcal{H}}^2.$$

Следовательно,

$$\lim_{t \rightarrow +0} (\mathcal{U}_\nu(t)u, u) < (\mathcal{U}_\nu(0)u, u)$$

для любого $u \in \mathcal{H}_{\mathcal{F}_0}$, и полугруппа $\mathcal{U}_\nu$ не является сильно непрерывной. $\square$

Пример 6.1. Пусть $\mathbf{D}$ — вырожденный неотрицательный оператор в пространстве H ранга m и $\{e_1, \dots, e_m\}$ — набор его собственных векторов, отвечающих ненулевым собственным значениям. Пусть $\nu_{\mathbf{D}}$ — центрированная гауссовская мера с ковариационным оператором $\mathbf{D}$ и $\mathcal{U}_\nu$ — полугруппа неотрицательных сжимающих операторов, сильно непрерывная на пространстве $\mathcal{H}_{\mathcal{E}}$ в силу теоремы 5.3. Если $\mathcal{F}$ — такой ОНБ пространства H , что $e_j \notin L_1(H, \mathcal{F})$ для всех $j = 1, \dots, m$, то

$$\nu(\{h \in H : h \notin L_1(H, \mathcal{F})\}) = 1,$$

поскольку $\nu(\{\text{lin}(e_1, \dots, e_m)\}) = 1$. Тогда для любого $u \in \mathcal{H}_{\mathcal{F}}$ и любого $t > 0$ выполняется равенство $(u, \mathcal{U}_{\nu}(t)u)_{\mathcal{H}} = 0$, т.е. полугруппа $\mathcal{U}_{\nu}$ не является сильно непрерывной на пространстве $\mathcal{H}$.

Благодарности. Автор благодарит Г. Г. Амосова, М. М. Галламова, Д. В. Завадского, Л. С. Ефремову, Ю. Н. Орлова, О. Г. Смолянова, Е. Т. Шавгулидзе и Н. Н. Шамарова за обсуждения затронутых в статье проблем.

СПИСОК ЛИТЕРАТУРЫ

1. Амосов Г. Г., Сакбаев В. Ж. Геометрические свойства векторных состояний и разложение состояний в интегралы Петтиса// Алгебра и анализ. — 2015. — 27, № 4. — С. 1–14.
2. Амосов Г. Г., Сакбаев В. Ж. Об аналогах спектрального разложения квантового состояния// Мат. заметки. — 2013. — 93, № 3. — С. 323–332.
3. Богачев В. И. Основы теории меры. Т. 1. — М.-Ижевск: РХД, 2003.
4. Богачев В. И. Гауссовские меры. — М.: Физматлит, 1997.
5. Вейль А. Интегрирование в топологических группах и его применение. — М.: ИЛ, 1950.
6. Вершик А. М. Существует ли мера Лебега в бесконечномерном пространстве?// Тр. Мат. ин-та им. В. А. Стеклова РАН. — 2007. — 259. — С. 256–281.
7. Го Х. С. Гауссовские меры в банаховых пространствах. — М.: Мир, 1979.
8. Ефремова Л. С., Сакбаев В. Ж. Понятие взрыва множества решений дифференциальных уравнений и усреднение случайных полугрупп// Теор. мат. физ. — 2015. — 185, № 2. — С. 252–271.
9. Орлов Ю. Н., Сакбаев В. Ж., Смолянов О. Г. Случайные неограниченные операторы и формулы Фейнмана// Изв. РАН. Сер. мат. — 2016. — 80, № 6. — С. 141–172.
10. Сакбаев В. Ж. Усреднение случайных блужданий и меры на гильбертовом пространстве, инвариантные относительно сдвига// Теор. мат. физ. — 2017. — 191, № 3. — С. 473–502.
11. Сакбаев В. Ж. О законе больших чисел для композиций независимых случайных полугрупп// Изв. вузов. Сер. мат. — 2016. — 10. — С. 86–91.
12. Сакбаев В. Ж., Смолянов О. Г. Аналоги формул Фейнмана для некорректных задач, связанных с уравнением Шредингера// Докл. РАН. — 2016. — 471, № 3. — С. 275–280.
13. Сакбаев В. Ж. Случайные блуждания и меры на гильбертовом пространстве, инвариантные относительно сдвигов и поворотов// Итоги науки и техн. Совр. мат. прилож. Темат. обзоры. — 2017. — 140. — С. 88–118.
14. Хилле Э., Филлипс Р. Функциональный анализ и полугруппы. — М.: ИЛ, 1962.
15. Baker R. «Lebesgue measure» on R^{∞} // Proc. Am. Math. Soc. — 1991. — 113, № 4. — С. 1023–1029.
16. Sakbaev V. Zh., Volovich I. V. Self-adjoint approximations of the degenerate Schrödinger operator// *p*-Adic Numbers Ultrametric Anal. Appl. — 2017. — 9, № 1. — С. 39–52.

В. Ж. Сакбаев

Московский физико-технический институт (государственный университет)

E-mail: fumi2003@mail.ru



КВАНТОВЫЕ ПОТОЧНЫЕ ШИФРЫ: НЕВОЗМОЖНОСТЬ БЕЗУСЛОВНОЙ СТОЙКОСТИ

© 2018 г. П. А. ТРЕГУБОВ, А. С. ТРУШЕЧКИН

Аннотация. Поточные шифры образуют один из двух больших классов шифров с закрытым ключом в классической криптографии. В этой работе вводится понятие квантового поточного шифра. Специальные виды квантовых поточных шифров уже предлагались различными исследователями. Мы доказываем общий результат о невозможности существования безусловно стойкого квантового поточного шифра, если длина сообщения намного превышает длину ключа. Анализируются индивидуальные и коллективные атаки против квантового поточного шифра. Устанавливается связь между задачей угадывания противником ключа и различением случайных квантовых состояний.

Ключевые слова: квантовая криптография, поточные шифры, безусловная стойкость, различение квантовых состояний.

AMS Subject Classification: 81P68

1. ВВЕДЕНИЕ

Настоящая работа посвящена задаче секретной связи двух доверяющих друг другу субъектов. В этой задаче одна легитимная сторона связи, называемая «отправителем», должна отправить другой легитимной стороне, называемой «получателем», некоторое секретное сообщение. Канал связи, по которому передается сообщение, прослушивается противником. Поэтому отправитель применяет к сообщению определенное преобразование (называемое криптографическим преобразованием или шифром), зависящее от некоторой информации, называемой ключом. То, что получается в результате преобразования, называется шифртекстом, который и передается по каналу связи. Получатель, также зная ключ, применяет к шифртексту обратное преобразование и восстанавливает исходное сообщение. Предполагается, что противник знает криптографическое преобразование (вид функции), но не знает ключ. Шифр называется совершенно стойким, если знание шифртекста не позволяет противнику получить какую-либо информацию об исходном сообщении. Исходное сообщение в непреобразованном виде также называется открытым текстом.

Таким образом, для осуществления секретной связи легитимные стороны должны обладать общей секретной информацией — ключом. Для простоты будем предполагать, что ключ и сообщение — двоичные строки. Согласно фундаментальному результату Шеннона (см. [7]; современное изложение см., например, в [1]), шифр может быть совершенно стойким только тогда, когда длина сообщения не превосходит длину ключа. Это является существенным ограничением для использования совершенно стойких шифров, поскольку встает задача распределения ключей: легитимные стороны должны постоянно каким-то образом согласовывать новые общие секретные ключи в условиях, когда канал связи между ними прослушивается. В силу того, что передаваемое сообщение не должно быть длиннее ключа, невозможно зашифровать полезное сообщение и вместе с ним новый ключ той же длины.

В настоящее время для распределения ключей используется так называемая криптография с открытым ключом (см. [1, 8]). Она не является совершенно стойкой, а основана на предположении об ограниченности вычислительных мощностей противника и вычислительной сложности решения определенных математических задач, таких, как, например, задача разложения больших

целых чисел на простые сомножители. Однако большинство задач, используемых в настоящее время в криптографии с открытым ключом, может быть эффективно разрешимо на квантовом компьютере (см. [5, 21]), что создает угрозу для таких криптографических систем.

Квантовая криптография призвана устранить эту угрозу благодаря тому, что способна (в теории) обеспечить безусловную стойкость секретной связи, т.е. стойкость без каких-либо предположений о вычислительных мощностях и технологиях противника. В настоящее время квантовая криптография — активно развивающаяся область. Наиболее известный и проработанный раздел квантовой криптографии — это квантовое распределение ключей. В нем легитимные участники связи могут, используя прослушиваемый квантовый канал связи, сгенерировать общий секретный ключ. Предполагается, что легитимные участники перед началом протокола квантового распределения ключей обладают некоторым коротким общим секретным ключом, который они используют для аутентификации друг друга. Поскольку квантовое распределение ключей позволяет распределить ключ большей длины, нежели начальный, то часть нового ключа может быть оставлена для аутентификации в следующем сеансе.

В основе квантовой криптографии (см. [5, 9, 12]) лежит принцип, что измерение (прослушивание) квантового сигнала влечет его возмущение (изменение состояния), поэтому прослушивание квантового канала противником будет обнаружено. В случае обнаружения прослушивания протокол распределения ключей прерывается, созданный ключ для шифрования секретных сообщений не используется. Системы квантового распределения ключей реализованы на практике в различных странах, включая Россию, США, ЕС, Швейцарию, Китай, Японию (см. [2, 3, 10, 11, 17, 20, 22]).

Представляет интерес рассмотрение другой задачи в рамках квантовой криптографии: не задачи квантового распределения ключей для их последующего использования в классических шифрах, а задачи непосредственного квантового шифрования, т.е. кодирования секретного сообщения в квантовые состояния. Также предполагается, что это преобразование зависит от ключа, известного легитимным участникам, но не противнику. Замысел состоит в следующем. Легитимный получатель сообщения, зная ключ, знает, какие наблюдаемые надо измерить для восстановления сообщения. Противник, не знающий ключ и, следовательно, правильные наблюдаемые, проводит с большой вероятностью измерения неправильных наблюдаемых и тем самым не получает никакой информации.

В этой работе рассматривается концепция квантового поточного шифра, обобщающая классические поточные шифры. Известен специальный вид квантового поточного шифра Y00, использующий когерентные состояния (см. [24]). В последующей серии работ (см., например, [13]) было показано, что этот шифр более устойчив к некоторым известным атакам, нежели классические поточные шифры. Однако остается открытым вопрос о том, могут ли подобные шифры обеспечить безусловную стойкость. В этой статье мы доказываем, что если длина сообщения намного больше длины ключа, то квантовый поточный шифр так же, как и классический, не может обеспечить безусловную стойкость.

Более общей мотивацией к этой работе служит исследование псевдослучайных последовательностей квантовых состояний. Псевдослучайные числовые последовательности играют важную роль в классической информатике и, в частности, криптографии. Представляет интерес изучение квантовых псевдослучайных последовательностей, изучение того, может ли соединение квантового принципа неопределенности с псевдослучайностью дать синергетический эффект.

Дальнейший текст организован следующим образом. Раздел 2 посвящен классическим поточным шифрам. Вводится определение безусловной стойкости и приводится доказательство известного факта, что классический поточный шифр не может быть безусловно стойким, если длина передаваемого сообщения превышает длину ключа. В разделе 3 дается определение квантового поточного шифра и безусловной стойкости для него. В разделах 4 и 5 анализируются соответственно индивидуальные и коллективные атаки на квантовые поточные шифры. Показано, что качественного улучшения по сравнению с классическими поточными шифрами достичь не удастся: передавать сообщения существенно большей длины, нежели ключ, с безусловной стойкостью, также не удастся.

2. КЛАССИЧЕСКИЕ ПОТОЧНЫЕ ШИФРЫ

Определение 1. *Классическим поточным шифром* будем называть отображение вида

$$(m, k) \mapsto (m_1 \oplus x_1(k), m_2 \oplus x_2(k), \dots, m_n \oplus x_n(k)) = e, \quad (1)$$

где $m = (m_1, \dots, m_n) \in \{0, 1\}^n$ — сообщение, $k \in \mathcal{K}$ — ключ ($\mathcal{K}$ — некоторое конечное множество), $(x_1(k), x_2(k), \dots)$ — некоторая псевдослучайная двоичная последовательность, зависящая от ключа (называется *гаммой*), $\oplus$ — сложение по модулю два. В этом определении e представляет собой шифртекст.

Обозначим через M , K и E соответственно открытое сообщение, ключ и шифртекст как случайные величины, $X_i = x_i(K)$. Везде будем предполагать, что K распределен равномерно на множестве $\mathcal{K}$ и не зависит от M . Распределение M может быть произвольным и заранее неизвестным. Распределение E определяется на основе распределений M и K и формулы (1).

Отметим, что произвольность распределения M может быть связана как с тем, что оно точно не известно (например, оно может быть связано со статистическими свойствами естественного языка, которые известны только приблизительно), так и с возможным частичным знанием противника о сообщении. Так, например, далее будем рассматривать атаку на основе известного открытого текста, когда противнику известна часть сообщения. Можно сказать, что распределение величины M отражает априорное вероятностное знание противника о том, какое сообщение может быть послано.

Обозначим через $H(\cdot)$, $H(\cdot, \cdot)$, $H(\cdot | \cdot)$, $I(\cdot; \cdot)$ соответственно энтропию Шеннона, совместную и условную энтропии и взаимную информацию:

$$\begin{aligned} H(M) &= - \sum_{m \in \mathcal{M}} p_M(m) \log p_M(m), \\ H(E) &= - \sum_{e \in \mathcal{E}} p_E(e) \log p_E(e), \\ H(M, E) &= - \sum_{m \in \mathcal{M}} \sum_{e \in \mathcal{E}} p_{ME}(m, e) \log p_{ME}(m, e), \\ H(M|E) &= H(M, E) - H(E), \\ I(M; E) &= H(M) - H(M|E). \end{aligned}$$

Здесь и далее $\log$ означает двоичный логарифм.

Если для всех распределений величины M выполнено $I(M; E) = 0$, то шифр называется *совершенно стойким* (см. [7]). Если же

$$I(M; E) \leq \varepsilon, \quad (2)$$

где ε — заданная достаточно малая величина, то шифр не является совершенно стойким, однако можно говорить о *безусловной* стойкости шифра, поскольку условие (2) гарантирует, что информация противника об открытом сообщении достаточно мала (не превышает заданного допустимого порога) вне зависимости от его вычислительных мощностей.

Примером совершенно стойкого шифра является одноразовый блокнот. В нем $\mathcal{K} = \{0, 1\}^n$, т.е. длина ключа (как двоичной строки) равна длине сообщения. Тогда ключ можно записать в виде $k = (k_1, \dots, k_n)$, $k_i \in \{0, 1\}$. Далее, $x_i(k) = k_i$. Ключ может использоваться только один раз.

В одноразовом блокноте ключ имеет ту же длину, что и открытый текст. Известно, что выполнение неравенства $|\mathcal{K}| \equiv l \geq n$ является необходимым условием совершенной стойкости шифра (см. [1, 7]). Более того,

$$H(M|E) \leq H(K). \quad (3)$$

В самом деле,

$$H(M|E) = H(M, E) - H(E) \leq H(K, E) - H(E) = H(K|E) \leq H(K), \quad (4)$$

где первое неравенство имеет место в силу того, что открытый текст M однозначно восстанавливается по ключу K и шифртексту E . Следовательно, в предположении $H(M) = n$, имеет место

неравенство

$$I(M; E) = H(M) - H(M|E) \geq n - H(K), \quad (5)$$

т.е. при длине ключа, меньшей n , информация противника существенна и безусловная стойкость в смысле (2) (при $\varepsilon < 1$) также не может быть обеспечена.

Итак, поточный шифр не является безусловно стойким при $\varepsilon < 1$. Покажем теперь это другим способом. Одним из видов атаки на шифры является атака на основе известного открытого текста. Предположим, что противнику известны $t < n$ битов открытого текста в специально подобранных позициях. Тогда, зная также и шифртекст, он может восстановить соответствующие биты гаммы. Противник может использовать это знание для определения ключа и последующего дешифрования оставшихся $n - t$ неизвестных ему битов открытого текста.

Теорема 1.

$$\sum_{t=1}^n H(X_{t+1} | X_1, \dots, X_t) \leq \log |\mathcal{K}| \equiv l. \quad (6)$$

Доказательство. Имеем

$$l \geq H(X_1, \dots, X_n) = \sum_{t=1}^n H(X_{t+1} | X_1, \dots, X_t). \quad (7)$$

Здесь неравенство верно в силу того, что последовательность $X = (X_1, X_2, \dots)$, будучи функцией ключа K , не может иметь неопределенность большую, чем $H(K)$, которая, в свою очередь, не превосходит l . $\square$

Рассмотрим неравенство (6). Допустим, в последовательности X существуют члены, которые нельзя предсказать с большей вероятностью успеха, нежели простое угадывание, даже при условии знания всех предыдущих членов последовательности, т.е. $H(X_{t+1} | X_1, \dots, X_t) = 1$. Неравенство (6) утверждает, что таких членов не может быть больше, чем длина ключа l . Если их ровно l (обозначим номера этих членов $i_1 < \dots < i_l$), то остальные члены последовательности с достоверностью предсказуемы при условии знания предыдущих членов ($H(X_{t+1} | X_1, \dots, X_t) = 0$). Таким образом, противнику достаточно знать ровно l бит открытого текста в позициях с непредсказуемыми членами для того чтобы узнать остальную часть гаммы и, следовательно, открытого текста:

$$\begin{aligned} H(X_1, \dots, X_n | X_{i_1}, \dots, X_{i_l}) &= H(X_1, \dots, X_n) - H(X_{i_1}, \dots, X_{i_l}) = \\ &= H(X_1, \dots, X_n) - H(X_{i_1}) - H(X_{i_2} | X_{i_1}) - \dots - H(X_{i_l} | X_{i_2}, \dots, X_{i_{l-1}}) \leq \\ &\leq H(X_1, \dots, X_n) - H(X_{i_1} | X_1, \dots, X_{i_1-1}) - \dots - H(X_{i_l} | X_1, \dots, X_{i_l-1}) = l - l = 0. \end{aligned}$$

Если же в некоторых позициях имеет место промежуточная ситуация

$$0 < H(X_{t+1} | X_1, \dots, X_t) < 1,$$

то данные рассуждения верны «в среднем», поскольку суммарная неопределенность членов последовательности X при условии знания предыдущих членов последовательности не может превышать l . Если противник знает порядка l позиций с наиболее непредсказуемыми членами, то с высокой вероятностью он правильно определяет и остальную последовательность.

В следующем разделе мы покажем, что переход к квантовому поточному шифру не меняет ситуацию существенно: противнику по-прежнему достаточно знать порядка l битов открытого текста в специально подобранных позициях.

3. КВАНТОВЫЕ ПОТОЧНЫЕ ШИФРЫ

Определение 2 (см. также [14]). *Квантовым поточным шифром* будем называть отображение вида

$$(m, k) \mapsto (\psi_1(m_1, k), \psi_2(m_2, k), \dots, \psi_n(m_n, k)), \quad (8)$$

где $m = (m_1, \dots, m_n) \in \{0, 1\}^n$ — открытое сообщение, $k \in \mathcal{K}$ — ключ ($\mathcal{K}$ — некоторое конечное множество), $\{\psi_i(0, k), \psi_i(1, k)\}$ при всех i и k — ортонормированные базисы в гильбертовом пространстве $\mathbb{C}^2$.

Снова предполагаем, что отправитель и получатель имеют общий неизвестный противнику секретный ключ k , который распределен равномерно на $\mathcal{K}$. Отправитель зашифровывает сообщение m в квантовые состояния кубитов согласно (8) и посылает эти состояния получателю. Получатель проводит измерения каждого кубита в базисах $\{\psi_i(0, k), \psi_i(1, k)\}$ и таким образом восстанавливает сообщение m . Если же последовательность квантовых состояний (8) измеряет не легитимный получатель, а противник, то он не должен получить информацию об m с точностью до заданного пренебрежимо малого уровня. А именно, потребуем, чтобы для любой наблюдаемой противника на пространстве $\mathbb{C}^{2^n}$ было выполнено неравенство

$$I(M; X) \leq \varepsilon, \quad (9)$$

где X — результат измерения противником выбранной наблюдаемой.

В последних двух разделах этой статьи рассматриваются два типа атак противника на квантовые поточные шифры. В разделе 4 мы рассмотрим случай, когда противник измеряет кубиты по отдельности (в квантовой криптографии такие атаки называются индивидуальными). В разделе 5 мы рассмотрим более общий случай атаки, когда противник может проводить коллективные измерения над произвольным количеством кубитов сразу (коллективные атаки). Везде будем предполагать, что классические вычислительные мощности противника неограниченны.

4. ИНДИВИДУАЛЬНЫЕ АТАКИ

Введем следующие обозначения. Пусть ρ — квантовое состояние, т.е. положительный оператор с единичным следом в некотором (конечномерном) гильбертовом пространстве $\mathcal{H}$. *Энтропией фон Неймана* называется величина

$$H(\rho) = -\text{Tr } \rho \log \rho.$$

Пусть дана составная система с гильбертовым пространством $\mathcal{H}_A \otimes \mathcal{H}_B$ и состоянием ρ_{AB} . Введем обозначения

$$\rho_A = \text{Tr}_B \rho_{AB}, \quad \rho_B = \text{Tr}_A \rho_{AB},$$

где Tr_A и Tr_B — частичные следы. Тогда условная энтропия и взаимная информация определяются формулами

$$H(A|B) = H(\rho_{AB}) - H(\rho_B) \equiv H(AB) - H(B), \quad (10)$$

$$I(A; B) = H(A) - H(A|B) = H(B) - H(B|A). \quad (11)$$

Если система трехчастичная с гильбертовым пространством $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C$ и состоянием ρ_{ABC} , то можно определить условную взаимную информацию:

$$I(A; B|C) = H(A|C) - H(A|BC) = H(B|C) - H(B|AC).$$

Произвольную классическую случайную величину X , принимающую значения на множестве мощности d с вероятностями $\{p(x)\}_{x \in \mathcal{X}}$ можно отождествить с квантовым состоянием

$$\rho_X = \sum_{x \in \mathcal{X}} p(x) |x\rangle \langle x|,$$

где $\{|x\rangle\}_{x \in \mathcal{X}}$ — некоторый выделенный ортонормированный базис в d -мерном гильбертовом пространстве. В этом случае энтропия фон Неймана ρ_X совпадает с энтропией Шеннона X .

Классически-квантовое состояние имеет вид

$$\rho_{XA} = \sum_{x \in \mathcal{X}} p(x) |x\rangle \langle x| \otimes \rho_A^x,$$

где ρ_A^x — квантовые состояния. Тогда, очевидно, $\text{Tr}_A \rho_{XA} = \rho_X$. Таким образом, классические случайные величины и квантовые состояния можно рассматривать в рамках единого формализма.

Сначала для простоты предположим, что противнику известны все n битов сообщения. Из неравенства (15), которое мы собираемся доказать, будет следовать оценка на реальное количество битов сообщения, которое противнику достаточно знать для взлома шифра (чтения по крайней мере некоторых из оставшихся битов сообщения). Без ограничения общности можно считать, что $m_i = 0$ для всех i : если для некоторого i имеет место $m_i = 1$, то противник может осуществить унитарное преобразование из $\psi_i(1, k)$ в $\psi_i(0, k)$. Поэтому первый аргумент в обозначении $\psi_i(m_i, k)$ мы можем опустить и считать, что $\psi_i(k) \equiv \psi_i(0, k)$. Введём также обозначения

$$\psi(k) = \psi_1(k) \otimes \psi_2(k) \otimes \dots \otimes \psi_n(k), \quad \rho(k) = |\psi(k)\rangle \langle \psi(k)|, \quad \rho = 2^{-l} \sum_{k \in \mathcal{K}} \rho(k), \quad (12)$$

Q_i — квантовая система, соответствующая i -му кубиту, $Q = (Q_1, \dots, Q_n)$.

Пусть противник проводит над всеми кубитами некоторое измерение, которое задается вероятностной операторнозначной мерой $M = \{M_x\}_{x \in \mathcal{X}}$. Случайную величину, соответствующую результату измерения, обозначим X . Тогда определим величины $H(Q|X)$ и $I(Q; X)$ — количество информации, которое дает результат измерения о посланном состоянии, следующим образом. Совместное распределение вероятностей ключа и результата измерения определяется формулой

$$p(k, x) = 2^{-l} \text{Tr } \rho(k) M_x.$$

Стандартным образом можно определить условную вероятность $p(k|x)$ и распределение вероятностей результата измерения $p(x) = \text{Tr } \rho M_x$. Распределение вероятностей ключа, очевидно, есть $p(k) = 2^{-l}$. Тогда

$$\begin{aligned} \rho_x &= \sum_{k \in \mathcal{K}} p(k|x) \rho(k), \\ H(Q|X) &= \sum_{x \in \mathcal{X}} p(x) H(\rho_x), \end{aligned} \quad (13)$$

$$I(Q; X) = H(Q) - H(Q|X) = H(\rho) - \sum_{x \in \mathcal{X}} p(x) H(\rho_x) \quad (14)$$

— фундаментальная в квантовой теории информации величина, возникающая, в частности, в задаче кодирования классически-квантового канала (иногда называется хи-величиной; см. [6]).

Величины $H(Q|X)$ и $I(Q; X)$ можно задать и при помощи общих определений (10) и (11). Эти определения предполагают существование совместного состояния Q и X , причем частичное состояние Q должно быть ρ . В общем случае состояние квантовой системы после измерения меняется, что, на первый взгляд, препятствует определению величин $H(Q|X)$ и $I(Q; X)$ по формулам (10) и (11). Однако мы можем себе представить, что отправитель приготовил каждый кубит в двух копиях: одну копию он отправил по квантовому каналу (которая и была перехвачена и измерена противником), вторую оставил себе в нетронутном виде (которые тогда мы и обозначим $Q_1, \dots, Q_n$). После этого применение формул (10) и (11) корректно. Покажем эквивалентность формул (10) и (11) с одной стороны и (13) и (14) — с другой. Совместное состояние Q и X имеет вид

$$\rho_{QX} = \sum_k p(k) \rho(k) \otimes \sum_x p(x|k) |x\rangle \langle x| = \sum_x p(x) \left[\sum_k p(k|x) \rho(k) \right] \otimes |x\rangle \langle x| = \sum_x p(x) \rho_x \otimes |x\rangle \langle x|.$$

Выпишем спектральное разложение ρ_x :

$$\rho_x = \sum_y q_y^x |e_y^x\rangle \langle e_y^x|,$$

где $|e_y^x\rangle$ — единичные векторы. Очевидно, $|e_y^x\rangle \otimes |x\rangle$ — собственные векторы оператора ρ_{QX} , отвечающие собственным значениям $p(x)q_y^x \equiv p(x, y)$. Величины $p(x, y)$ можно интерпретировать как

совместное распределение вероятностей случайной величины X и некоторой случайной величины Y (такой, что $p(y|x) = q_y^x$). Тогда

$$H(QX) = H(XY) = H(X) + H(Y|X),$$

$$H(Q|X) = H(QX) - H(X) = H(Y|X) = - \sum_{xy} p(x)p(y|x) \log p(y|x) = - \sum_x p(x)H(\rho_x),$$

что и требовалось доказать. Энтропию $H(\rho_x)$ будем обозначать $H(Q|X = x)$.

Докажем теорему, из которой будет следовать невозможность существования безусловно стойкого квантового поточного шифра (в смысле неравенства (9)).

Теорема 2. *Существуют такая наблюдаемая для кубита (вероятностная операторнозначная мера на $\mathbb{C}^2$) M_1 и такие отображения исходов прошедших измерений $x_i \in \{0, 1\}$ на множество вероятностных операторнозначных мер для кубита*

$$x_1 \mapsto M_2(x_1), \quad (x_1, x_2) \mapsto M_3(x_1, x_2), \quad \dots, \quad (x_1, \dots, x_{n-1}) \mapsto M_n(x_1, \dots, x_{n-1}),$$

что

$$\sum_{t=1}^n H(\rho_t | X_1, \dots, X_{t-1}) \leq \log |\mathcal{K}| \equiv l. \quad (15)$$

Здесь X_i — двоичная случайная величина, соответствующая результату измерения наблюдаемой $M_i(X_1, \dots, X_{i-1})$ над i -м кубитом.

В формуле (15) и далее по определению полагаем, что при $t = 0$ кортеж $(X_1, \dots, X_{t-1})$ пуст, т.е. $H(\rho_0 | X_1, \dots, X_{0-1}) = H(\rho_0)$.

Доказательство. Рассмотрим величину $I(Q_1, \dots, Q_n; X_1, \dots, X_n)$. С одной стороны,

$$I(Q_1, \dots, Q_n; X_1, \dots, X_n) = H(Q_1, \dots, Q_n) - H(Q_1, \dots, Q_n | X_1, \dots, X_n) \leq H(Q_1, \dots, Q_n) \leq l.$$

Первое неравенство здесь имеет место в силу неотрицательности условной энтропии для классически-квантового состояния $(X_1, \dots, X_n, Q_1, \dots, Q_n)$. Второе неравенство имеет место в силу того, что в сумме (12) 2^l членов и все $\rho(k)$ — чистые состояния. Равенство $H(\rho) = l$ достигается, когда все $\psi(k)$ попарно ортогональны.

С другой стороны,

$$\begin{aligned} I(Q_1, \dots, Q_n; X_1, \dots, X_n) &= H(X_1, \dots, X_n) - H(X_1, \dots, X_n | Q_1, \dots, Q_n) = \\ &= \sum_{t=1}^n \left[H(X_t | X_1, \dots, X_{t-1}) - H(X_t | Q_1, \dots, Q_n, X_1, \dots, X_{t-1}) \right] \geq \\ &\geq \sum_{t=1}^n \left[H(X_t | X_1, \dots, X_{t-1}) - H(X_t | Q_t, X_1, \dots, X_{t-1}) \right] = \\ &= \sum_{t=1}^n I(Q_t; X_t | X_1, \dots, X_{t-1}). \end{aligned}$$

Наконец, покажем, что подходящим выбором наблюдаемых (зависимых от предыдущих исходов) можно добиться выполнения равенства

$$I(Q_t; X_t | X_1, \dots, X_{t-1}) = H(Q_t | X_1, \dots, X_{t-1}), \quad (16)$$

что и завершит доказательство теоремы. Пусть $p(x_1, \dots, x_{t-1})$ — распределение $(X_1, \dots, X_{t-1})$. Тогда

$$I(Q_t; X_t | X_1, \dots, X_{t-1}) = \sum_{x_1, \dots, x_{t-1} \in \{0,1\}} p(x_1, \dots, x_{t-1}) I(Q_t; X_t | X_1 = x_1, \dots, X_{t-1} = x_{t-1}),$$

$$\begin{aligned}
I(Q_t; X_t \mid X_1 = x_1, \dots, X_{t-1} = x_{t-1}) &= \\
&= H(Q_t \mid X_1 = x_1, \dots, X_{t-1} = x_{t-1}) - H(Q_t \mid X_t, X_1 = x_1, \dots, X_{t-1} = x_{t-1}).
\end{aligned}$$

Обозначим квантовое состояние t -го кубита при условии $(X_1 = x_1, \dots, X_{t-1} = x_{t-1})$, т.е. состояния, на основе которого рассчитывается $H(Q_t \mid X_1 = x_1, \dots, X_{t-1} = x_{t-1})$, как $\rho_{Q_t|x_1, \dots, x_{t-1}}$. Выпишем его спектральное разложение:

$$\rho_{Q_t|x_1, \dots, x_{t-1}} = \sum_{y=0,1} p(y \mid x_1, \dots, x_{t-1}) |e_y(x_1, \dots, x_{t-1})\rangle \langle e_y(x_1, \dots, x_{t-1})|.$$

Выберем тогда двоичную наблюдаемую

$$\begin{aligned}
M_t(x_1, \dots, x_{t-1}) &= \{M_t^0(x_1, \dots, x_{t-1}), M_t^1(x_1, \dots, x_{t-1})\}, \\
M_t^y(x_1, \dots, x_{t-1}) &|e_y(x_1, \dots, x_{t-1})\rangle \langle e_y(x_1, \dots, x_{t-1})|.
\end{aligned}$$

В этом случае

$$\rho_{Q_t X_t|x_1, \dots, x_{t-1}} = \sum_{y=0,1} p(y|x_1, \dots, x_{t-1}) |e_y(x_1, \dots, x_{t-1})\rangle \langle e_y(x_1, \dots, x_{t-1})| \otimes |y\rangle \langle y|,$$

поэтому

$$\begin{aligned}
H(Q_t, X_t \mid X_1 = x_1, \dots, X_{t-1} = x_{t-1}) &= H(Q_t \mid X_1 = x_1, \dots, X_{t-1} = x_{t-1}) = \\
&= - \sum_{y=0,1} p(y \mid x_1, \dots, x_{t-1}) \log p(y \mid x_1, \dots, x_{t-1}),
\end{aligned}$$

т.е.

$$\begin{aligned}
H(Q_t \mid X_t, X_1 = x_1, \dots, X_{t-1} = x_{t-1}) &= H(Q_t, X_t \mid X_1 = x_1, \dots, X_{t-1} = x_{t-1}) - \\
&- H(Q_t \mid X_1 = x_1, \dots, X_{t-1} = x_{t-1}) = 0,
\end{aligned}$$

откуда и следует (16). $\square$

Следствие. Если в квантовом поточном шифре существуют такие l позиций $i_1 < \dots < i_l$, что

$$H(\rho_{i_j} \mid X_{i_1}, \dots, X_{i_{j-1}}) = 1, \quad j = 1, \dots, l,$$

для измерений, описанных в доказательстве теоремы 2, то

$$H(\rho_t \mid X_{i_1}, \dots, X_{i_j}) = 0$$

для всех t .

Если условие следствия выполнено, то противник полностью узнает базисы, а значит, и сообщение, если ему известны биты сообщения в позициях $i_1, \dots, i_l$.

Однако условие следствия может быть и не выполнено. В этом случае возникает теоретическая возможность обеспечения условия (9) при некоторых $\varepsilon < 1$ и $n > l$. Однако на практике интересен случай $n \gg l$ и очень малых ε . В этом случае теорема 2 говорит о том, что средняя энтропия

$$\frac{1}{n} \sum_{t=1}^n H(\rho_t \mid X_1, \dots, X_t) \leq \frac{l}{n},$$

т.е. близка к нулю. Это означает, что зная порядка l бит сообщения, противник с большой вероятностью может узнать по крайней мере один неизвестный ему бит сообщения, что нарушает условие $\varepsilon < 1$. Таким образом, переход к квантовому поточному шифру не позволяет достичь качественного превосходства над классическими поточными шифрами.

5. КОЛЛЕКТИВНЫЕ АТАКИ

Несмотря на то, что уже доказана невозможность безусловной стойкости для квантового поточного шифра с $n \gg l$ к индивидуальным атакам, представляет интерес исследовать возможности более общих атак — коллективных, когда противник может проводить коллективные измерения над произвольным количеством кубитов сразу.

Предполагаем, что противнику известны t битов сообщения. Пусть для простоты это будут первые t битов сообщения $m_1, \dots, m_t$. Снова без ограничения общности можно считать, что $m_i = 0$ для всех $i = 1, \dots, t$ и обозначить $\psi_i(k) \equiv \psi_i(0, k)$.

Будем рассматривать состояния $\psi_i(k)$ специального вида:

$$\psi_i(k) = \begin{pmatrix} \cos \varphi_i(k) \\ \sin \varphi_i(k) \end{pmatrix} \equiv |\varphi_i(k)\rangle,$$

где $\varphi_i(k) \in \left\{0, \frac{\pi}{h}, \frac{2\pi}{h}, \dots, \frac{(h-1)\pi}{h}\right\}$ генерируются псевдослучайным образом из ключа $k \in \mathcal{K}$.

Здесь натуральное число $h \geq 3$ — количество базисов, которые используются для шифрования сообщений. Пусть

$$|\psi(k)\rangle = |\varphi_1(k)\rangle \otimes \dots \otimes |\varphi_t(k)\rangle. \quad (17)$$

Задача, которую мы будем решать, заключается в следующем: какова вероятность при заданном t , что противник сумеет определить ключ k (и, следовательно, правильно измерить последние $n - t$ кубитов и узнать неизвестную ему часть сообщения). В этом разделе некоторые наши рассуждения будут носить эвристический характер. Справедливость этой части рассуждений будет проверена численно. Основная цель этого раздела — это установление связи между задачей взлома генераторов псевдослучайных квантовых состояний и задачей различения квантовых состояний, хорошо известной в квантовой теории информации.

Противник действует следующим образом. Сначала он сохраняет в квантовой памяти t первых кубитов, затем проводит над ними измерение произвольной (специально им подобранной) наблюдаемой вида $M = \{M_k\}_{k \in \mathcal{K}}$. Результат измерения k противник интерпретирует как значение секретного ключа. Обозначим через

$$p_{\text{угад}} = \text{Tr} |\psi(k)\rangle \langle \psi(k)| M_k$$

вероятность правильного угадывания ключа, а через $p_{\text{ош}} = 1 - p_{\text{угад}}$ — вероятность ошибки. Для простоты будем также предполагать, что $\mathcal{K} = \{0, 1\}^l$.

Утверждение 1.

1) Имеет место неравенство

$$p_{\text{угад}} \leq 2^{t-l}. \quad (18)$$

Как следствие, если $t \ll l$, то противник имеет лишь пренебрежимо малую вероятность правильного угадывания ключа.

2) Если последовательность квантовых состояний $\psi_1(k), \psi_2(k), \dots$ «похожа на истинно случайную» (т.е. при анализе ее статистических свойств с ней можно работать как с истинно случайной), то

$$p_{\text{угад}} \geq \left(1 + \frac{2^l - 1}{2^t}\right)^{-1}. \quad (19)$$

Как следствие, если $t \geq l$, то

$$p_{\text{угад}} \geq \frac{1}{2}. \quad (20)$$

Если же $t \gg l$, то

$$p_{\text{угад}} \approx 1 - 2^{l-t} \approx 1,$$

т.е. противник практически достоверно угадывает ключ.

Доказательство. Задача угадывания ключа в данной постановке сводится к задаче различения 2^l квантовых состояний $|\psi(k)\rangle$ (см. (17)) при $k \in \{0, 1\}^l$. Это наблюдение, связывающее задачу взлома квантового поточного шифра с задачей различения квантовых состояний, является основным.

Воспользуемся известной нижней оценкой вероятности ошибки (см. [19]):

$$p_{\text{ош}} \geq 1 - \frac{d}{2^l}, \quad (21)$$

где $1/2^l$ — априорная вероятность каждого из состояний (17), а d — размерность линейной оболочки 2^l состояний $|\psi(k)\rangle$, $k \in \{0, 1\}^l$. Очевидно, $d \leq 2^t$, откуда и следует формула (18).

Перейдем теперь к доказательству второго пункта утверждения, которое носит эвристический характер. Воспользуемся нижней оценкой на вероятность правильного угадывания квантового состояния при оптимальном измерении (см. [16]):

$$p_{\text{угад}} = 1 - p_{\text{ош}} \geq \frac{1}{2^l} \sum_{k \in \mathcal{K}} \frac{1}{\sum_{k' \in \mathcal{K}} |\langle \psi(k) | \psi(k') \rangle|^2} = \frac{1}{2^l} \sum_k \frac{1}{1 + \sum_{k' \neq k} |\langle \psi(k) | \psi(k') \rangle|^2}. \quad (22)$$

Далее,

$$\langle \psi(k) | \psi(k') \rangle = \langle \varphi_1(k) | \varphi_1(k') \rangle \langle \varphi_2(k) | \varphi_2(k') \rangle \cdots \langle \varphi_t(k) | \varphi_t(k') \rangle.$$

Теперь воспользуемся тем, что последовательность псевдослучайных квантовых состояний $\psi_1(k), \psi_2(k), \dots$ похожа на истинно случайную в том смысле, что углы $\varphi_i(k)$ можно считать независимыми и равномерно распределенными на $\left\{0, \frac{\pi}{h}, \frac{2\pi}{h}, \dots, \frac{(h-1)\pi}{h}\right\}$ (т.е. $\varphi_i(k_j)$ и $\varphi_j(k')$ независимы, если $k \neq k'$ или $i \neq j$). Будем тогда ассоциировать $p_{\text{угад}}$ с математическим ожиданием M правой части (22):

$$p_{\text{угад}} \geq \frac{1}{2^l} \sum_k M \frac{1}{1 + \sum_{k' \neq k} |\langle \psi(k) | \psi(k') \rangle|^2} \geq \frac{1}{2^l} \sum_k \frac{1}{1 + \sum_{k' \neq k} M |\langle \psi(k) | \psi(k') \rangle|^2}. \quad (23)$$

Последнее неравенство здесь следует из того, что среднее гармоническое всегда не превышает среднего арифметического. Далее,

$$M |\langle \psi(k) | \psi(k') \rangle|^2 = \prod_{i=1}^n M |\langle \varphi_i(k) | \varphi_i(k') \rangle|^2$$

в силу независимости величин $|\langle \varphi_i(k) | \varphi_i(k') \rangle|^2$, $i = 1, \dots, t$. Наконец, ввиду того что $\varphi_i(k)$ и $\varphi_i(k')$ независимы и равномерно распределены на $\left\{0, \frac{\pi}{h}, \frac{2\pi}{h}, \dots, \frac{(h-1)\pi}{h}\right\}$, нетрудно показать, что

$$M |\langle \varphi_i(k) | \varphi_i(k') \rangle|^2 = \frac{1}{2}$$

при любом натуральном $h \geq 2$. Следовательно,

$$M |\langle \psi(k) | \psi(k') \rangle|^2 = 2^{-t}.$$

Подстановка этого результата в (23) и дает формулу (19). $\square$

Поскольку формула (19) получена эвристически, то целесообразно проверить ее справедливость численно, сравнив результаты вычислений по формуле (19) с результатами вычислений по строгой оценке (22).

В качестве генератора псевдослучайных чисел будем использовать линейный конгруэнтный метод с обрезанием:

$$\begin{aligned} \varphi_i(k) &= (\lfloor h2^{-l}x_i \rfloor \bmod h) \frac{\pi}{h}, \quad i = 1, 2, \dots, \\ x_i &= 5x_{i-1} + 1 \bmod 2^l, \quad i = 2, 3, \dots, \\ x_1 &= k \in \{0, 1, \dots, 2^l - 1\}. \end{aligned} \quad (24)$$

ТАБЛИЦА 1. Зависимость оценки снизу (22) вероятности угадывания противником ключа при различном числе известных битов сообщения t для различного числа базисов h , используемых для шифрования сообщения. Во всех случаях длина ключа была выбрана $l = 10$ бит, в качестве генератора случайных чисел использовался линейный конгруэнтный метод с обрезанием (24).

t	Формула (19)	$h = 4$	$h = 8$	$h = 16$
1	$1,951 \times 10^{-3}$	$1,949 \times 10^{-3}$	$1,953 \times 10^{-3}$	$1,953 \times 10^{-3}$
2	$3,895 \times 10^{-3}$	$3,891 \times 10^{-3}$	$3,906 \times 10^{-3}$	$3,906 \times 10^{-3}$
3	$7,759 \times 10^{-3}$	$7,752 \times 10^{-3}$	$7,806 \times 10^{-3}$	$7,812 \times 10^{-3}$
4	$1,540 \times 10^{-2}$	$1,538 \times 10^{-2}$	$1,560 \times 10^{-2}$	$1,562 \times 10^{-2}$
5	$3,033 \times 10^{-2}$	$3,030 \times 10^{-2}$	$3,116 \times 10^{-2}$	$3,124 \times 10^{-2}$
6	$5,888 \times 10^{-2}$	$5,882 \times 10^{-2}$	$6,214 \times 10^{-2}$	$6,239 \times 10^{-2}$
7	0,111	0,111	0,123	0,124
8	0,200	0,200	0,232	0,234
9	0,334	0,333	0,395	0,403
10	0,500	0,500	0,559	0,565
11	0,667	0,667	0,722	0,726
12	0,800	0,800	0,850	0,853
13	0,889	0,889	0,920	0,920
14	0,941	0,941	0,960	0,959
15	0,970	0,970	0,980	0,979
16	0,9846	0,9846	0,9910	0,9911
17	0,9923	0,9922	0,9968	0,9972
18	0,9961	0,9961	0,9988	0,9991
19	0,9981	0,9981	0,9996	0,9998
20	0,9990	0,9990	0,9999	1,0000

Подчеркнем, что для наших целей проверки справедливости формулы (19) криптографическая стойкость генератора псевдослучайных чисел не существенна. Мы выбрали линейный конгруэнтный метод с обрезанием как один из простейших генераторов.

Результаты вычислений по строгой оценке (22) для длины ключа $l = 10$ и различном числе базисов h , используемых для шифрования, приведены в табл. 1 и на рис. 1.

Видим, что результаты вычислений по эвристической формуле (19) находятся в хорошем согласии с результатами вычислений по строгой оценке (22). При количестве базисов $h = 4$ совпадение практически идеальное. При большем h эвристическая формула дает несколько более заниженную (т.е. более пессимистическую для противника) оценку вероятности успеха, нежели (22). Это связано с тем, что чем больше h , тем больше бит требуется для задания каждого угла φ_i , следовательно, раскрывается больше информации о ключе. Однако мы видим и то, что результаты для $h \geq 8$ практически не отличаются друг от друга, т.е. при увеличении h величина нижней оценки вероятности успешного угадывания не стремится к единице, а стабилизируется на определенном уровне. Это связано с тем, что квантовые состояния $|\varphi\rangle$ и $|\varphi'\rangle$ при близких φ и φ' сложно различить, поэтому противник получает мало информации о младших битах, задающих угол.

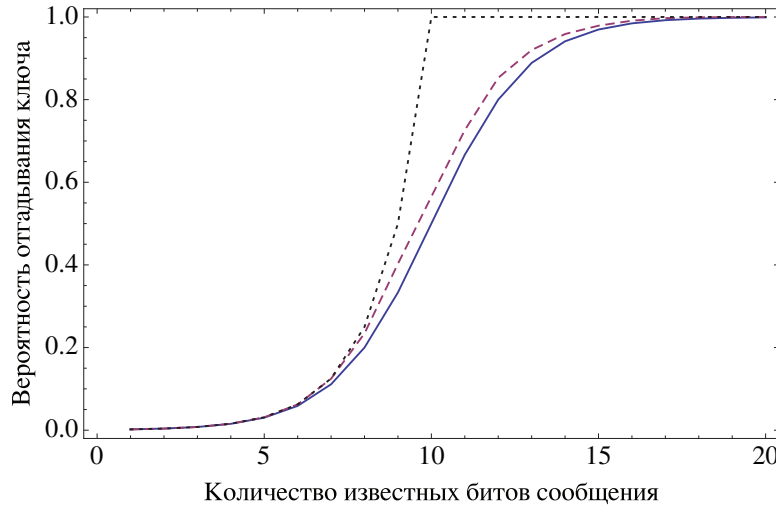


Рис. 1. Зависимость оценки снизу (22) вероятности угадывания противником ключа при различном числе известных битов сообщения t . Сплошная линия — случай $h = 4$ базисов, используемых для шифрования сообщения; в выбранном масштабе совпадает с линией нижней границы (19), полученной эвристически (см. числовые данные в табл. 1). Пунктирная линия с крупными штрихами — случай $h = 16$ базисов; в выбранном масштабе совпадает с линией $h = 8$. Пунктирная линия с мелкими штрихами — верхняя граница вероятности угадывания (18).

Поэтому при $h \geq 8$ дальнейшее уменьшение шага π/h в задании угла не приводит к раскрытию существенной дополнительной информации о ключе.

Также интересно заметить (см. табл. 1), что в некоторых случаях эвристическая нижняя оценка (19), полученная в допущении, что углы $\varphi_i(k)$ истинно случайные, оказалась даже несколько выше (т.е. оптимистичнее для противника), чем результат точного вычисления для псевдослучайных углов при $h = 4$. Возможно, это связано с тем, что для выбранного генератора количества возникновений каждого значения $\pi j/h$ в периоде 2^l псевдослучайной последовательности в точности равны, тогда как истинно случайные последовательности сбалансированы лишь приблизительно (в среднем). То же касается и последовательных пар углов $(\varphi_i, \varphi_{i+1})$ для $h = 4$.

В заключение отметим, что, как показано в [16], неравенство (19), а следовательно, и (20), в пределе $l \rightarrow \infty$, $n \rightarrow \infty$, $t \rightarrow \infty$, $t - l = \text{const}$, могут быть усилены, если воспользоваться теоремой Марченко—Пастура (см. [4]). Необходимо отметить, что в [16] рассматриваются случайные квантовые состояния, равномерно распределенные на всем множестве состояний определенной размерности. Это позволяет применить теорему Марченко—Пастура в исходном виде. Мы же рассматриваем состояния в виде тензорного произведения (17), в котором углы φ_i распределены равномерно на дискретном множестве и независимо (продолжаем работать в допущении, что углы $\varphi_i(k)$ можно считать истинно случайными). Теорема Марченко—Пастура в исходной формулировке в этом случае неприменима. Однако, несколько адаптировав для нашего случая доказательства из [15], можно доказать справедливость распределения Марченко—Пастура и для случайных состояний вида (17). Также справедливость закона Марченко—Пастура для состояний вида (17) проверена нами и численно. Тогда, как показано в [16], в пределе $l \rightarrow \infty$, $n \rightarrow \infty$, $t \rightarrow \infty$, $t - l = \text{const}$, имеет место оценка

$$p_{\text{угад}} \geq \begin{cases} 2^{n-l} \left[1 - 2^{t-l} \left(1 - \frac{64}{9\pi^2} \right) \right], & t < l, \\ 1 - 2^{l-t} \left(1 - \frac{64}{9\pi^2} \right), & t \geq l. \end{cases}$$

В частности, $p_{\text{угад}} > 0,720$ при $t \geq l$.

6. ОБСУЖДЕНИЕ И ЗАКЛЮЧЕНИЕ

При обобщении понятий из классической информатики на квантовый случай обычно пытаются ответить на вопрос о том, может ли переход к квантовым носителям информации дать определенные преимущества перед классическими системами. В нашем исследовании квантовых поточных шифров мы выяснили, что они не дают существенного преимущества перед классическими аналогами, если нам необходима безусловная стойкость: как и в классическом случае, они не способны ее обеспечить, если длина сообщения существенно превышает длину ключа (что обычно требуется на практике).

Это означает, что при рассмотрении квантовых поточных шифров, в частности шифра Y00, речь может идти только о стойкости в более слабом смысле, например в вычислительном. Так, в [13] показано, что шифр Y00 более стоек против определенного вида атаки, нежели аналогичный классический поточный шифр.

Обсудим обобщение неравенства (3), фундаментального для классической криптографии, на случай квантовых поточных шифров. Если в этом неравенстве под E понимать квантовую память противника, в которой он сохранил все переданные состояния $\psi_1(m_1, k), \dots, \psi_n(m_n, k)$ (Q в обозначениях раздела 4), то неравенство остается верным, поскольку все свойства энтропии, использованные в выводе (4), верны и в квантовом случае. Это соответствует случаю коллективной атаки, так как предполагает, что противник может осуществлять произвольные действия с большой квантовой системой Q как целым. Если же противник ограничен индивидуальными атаками, то в качестве E стоит взять результаты его измерений $X_1, \dots, X_n$. В этом случае может нарушаться первое равенство в (4), поскольку ключа и результатов измерений наблюдаемых, выбранных без знания ключа, может быть недостаточно для восстановления открытого текста. Несмотря на то что, как показали результаты раздела 4, при длинном и частично известном противнику открытом тексте квантовый поточный шифр не может быть стойким даже против индивидуальных атак, все же представляет интерес вопрос, возможно ли нарушение фундаментального классического неравенства (3) хотя бы на небольшую величину.

Отметим также недавние работы [18, 23], в которых разработаны протоколы квантового распределения ключей, использующих генераторы псевдослучайных чисел. Представляет интерес дальнейшее исследование возможных применений псевдослучайных квантовых состояний в квантовой информатике.

Благодарности. Авторы признательны Е. О. Киктенко, Д. А. Кронбергу, Ю. А. Курочкину, Н. Люткенхаусу (N. Lütkenhaus), А. К. Фёдорову и П. А. Яськову за ценные консультации и обсуждения.

СПИСОК ЛИТЕРАТУРЫ

1. Алфёров А. П., Zubov A. Ю., Кузьмин А. С., Черёмушкин А. В. Основы криптографии. — М.: Гелиос АРФ, 2002.
2. Балыгин К. А. и др. Практическая квантовая криптография // Письма в ЖЭТФ. — 2017. — 105, № 9. — С. 570–576.
3. Киктенко Е. О. и др. Демонстрация сети квантового распределения ключа в городских оптоволоконных линиях связи // Квант. электр. — 2017. — 47, № 9. — С. 798–802.
4. Марченко В. А., Пастур Л. А. Распределение собственных значений в некоторых ансамблях случайных матриц // Мат. сб. — 1966. — 72 (114), № 4. — С. 507–536.
5. Нильсен М., Чанг И. Квантовые вычисления и квантовая информация. — М.: Мир, 2006.
6. Холево А. С. Квантовые системы, каналы, информация. — М.: МЦНМО, 2010.
7. Шеннон К. Теория связи в секретных системах // В сб.: Шеннон К. Работы по теории информации и кибернетике. — М.: ИЛ, 1963. — С. 333–369.
8. Шнайер Б. Прикладная криптография. — М.: ТРИУМФ, 2003.
9. Bennett C. H., Brassard G. Quantum cryptography: public key distribution and coin tossing // Proc. IEEE Int. Conf. on Computers, Systems, and Signal Processing/ Bangalore, India. — 1984. — С. 175–179.
10. Chen T.-Y. et al. Metropolitan all-pass and inter-city quantum communication network // Opt. Express. — 2009. — 17, № 26. — С. 27217–27225.

11. *Elliott C. et al.* Current status of the DARPA quantum network// Proc. SPIE. — 2005.— 5815.— С. 138–149.
12. *Gisin N., Ribordy G., Tittel W., Zbinden H.* Quantum cryptography// Rev. Mod. Phys. — 2002. — 74, № 1. — С. 145–195.
13. *Hirota O., Kurosawa K.* Immunity against correlation attack on quantum stream cipher by Yuen 2000 protocol// Quant. Inform. Process. — 2007. — 6, № 2. — С. 81–91.
14. *Kato K.* Quantum enigma cipher as a generalization of the quantum stream cipher// Proc. SPIE. — 2016. — 9980. — С. 998005.
15. *Lytova A.* Central limit theorem for linear eigenvalue statistics for a tensor product version of sample covariance matrices// J. Theor. Probab. — 2017; <https://doi.org/10.1007/s10959-017-0741-9>
16. *Montanaro A.* On the distinguishability of random quantum states// Commun. Math. Phys. — 2007. — 273, № 3. — С. 619–636.
17. *Peev M. et al.* The SECOQC quantum key distribution network in Vienna// New J. Phys. — 2009. — 11. — P. 075001.
18. *Price A. B., Rarity J. G., Erven C.* Quantum key distribution without sifting// <https://arxiv.org/abs/1707.03331>
19. *Qiu D., Li L.* Minimum-error discrimination of quantum states: New bounds and comparison// Phys. Rev. A. — 2010. — 81, № 4. — С. 042329.
20. *Sasaki M. et al.* Field test of quantum key distribution in the Tokyo QKD Network// Opt. Express. — 2011. — 19, № 11. — С. 10387–10409.
21. *Shor P. W.* Algorithms for quantum computation: discrete logarithms and factoring// Found. Comput. Sci. Conf. Publ. — 1994. — с. 124–134.
22. *Stucki D. et al.* Long-term performance of the SwissQuantum quantum key distribution network in a field environment// New J. Phys. — 2011. — 13. — С. 123001.
23. *Trushechkin A. S., Tregubov P. A., Kiktenko E. O., Kurochkin Y. V., Fedorov A. K.* Quantum key distribution protocol with pseudorandom bases// <https://arxiv.org/abs/1706.00611>
24. *Yuen H.* A new approach to quantum cryptography, I. General principles and key generation// arxiv.org/abs/quant-ph/0311061.

П. А. Трегубов

Акционерное общество «Сбербанк-Технологии»

E-mail: pavel_tregubov@mail.ru

А. С. Трушечкин

Математический институт им. В. А. Стеклова РАН;

Национальный исследовательский ядерный университет «МИФИ»;

Национальный исследовательский технологический университет «МИСиС»;

Российский квантовый центр

E-mail: trushechkin@mi.ras.ru



ПРИМЕНЕНИЕ И ИССЛЕДОВАНИЕ КВАНТОВЫХ БЛУЖДЕНИЙ

© 2018 г. Л. Е. ФЕДИЧКИН, Ф. П. МЕЩАНИНОВ

Аннотация. В работе рассматриваются непрерывные унитарные квантовые блуждания одной частицы и замкнутых систем, а также обсуждаются более реалистичные подходы к моделированию квантовых блужданий.

Ключевые слова: квантовые блуждания, поиск в базе данных, квантовые вычисления.

AMS Subject Classification: 60K99, 81Q99

СОДЕРЖАНИЕ

1. Унитарные квантовые блуждания	105
2. Квантовые блуждания открытых систем	111
Список литературы	115

1. УНИТАРНЫЕ КВАНТОВЫЕ БЛУЖДЕНИЯ

Квантовые блуждания являются прямыми аналогами классических случайных блужданий; те и другие делятся на два типа: непрерывные по времени и дискретные. Далее для краткости мы будем называть их просто непрерывными и дискретными блужданиями. Часто квантовые блуждания рассматривают в качестве инструмента для построения алгоритмов, работающих значительно быстрее, чем их классические аналоги. Одними из самых известных алгоритмов на квантовых блужданиях являются квантовый метод Монте-Карло по схеме марковской цепи, алгоритм Гровера и алгоритм Амбайниса поиска в базе данных. Также была построена модель искусственного интеллекта, принимающая решения на основе квантовых блужданий по графу из ячеек памяти (см. [7]).

Наиболее простые модели и алгоритмы, основанные на них, рассматривают графы, на которых происходит блуждание, как замкнутые системы. Это значит, что в любой момент времени состояние системы можно описать некоторым вектором $|\psi\rangle$. Если говорить о непрерывных по времени случайных блужданиях, то эволюция системы будет описываться уравнением Шредингера, а в случае дискретных блужданий шаг блужданий осуществляется применением соответствующего оператора, как правило, не зависящего от номера шага.

Более реалистичные модели учитывают внешние шумы феноменологически, как это сделано в [2, 12], вводя вероятность и оператор ошибки, вносимой шумами при блужданиях.

Наиболее реалистичный подход к моделированию квантовых блужданий с исследованием влияния отдельных источников шума демонстрируется в [10, 11, 16, 17].

1.1. Непрерывные унитарные квантовые блуждания. В данном разделе рассматриваются непрерывные унитарные квантовые блуждания одной частицы. Квантовые и классические

блуждания на полных графах $G = (V, E)$ с N узлами описываются похожими системами дифференциальных уравнений. Вводится матрица смежности

$$A_{jk} = \begin{cases} 1, & (j, k) \in E, \\ 0, & (j, k) \notin E. \end{cases}$$

Непрерывные случайные блуждания являются марковским процессом с фиксированной вероятностью перехода частицы в примыкающий узел в единицу времени γ . Эволюция распределения вероятностей по графу описывается системой дифференциальных уравнений первого порядка:

$$\frac{dp_j(t)}{dt} = \gamma \sum_k L_{jk} p_k(t), \quad j = \overline{1, N},$$

где $p_j(t)$ — вероятность нахождения в j -м узле в момент времени t . Оператор L задается равенством $L = A - D$, где $D_{j,k} = \delta_{j,k} \deg(j)$, $j, k \in \overline{1, N}$. Для того, чтобы процесс был марковским и сохранял вероятность, требуется, чтобы сумма элементов в любом столбце матрицы L равнялась нулю.

Квантовые непрерывные блуждания происходят в N -мерном гильбертовом пространстве с базисными векторами $|j\rangle$, где j — узел графа G . Разложим вектор состояния системы по данному базису:

$$|\psi(t)\rangle = \sum_j q_j(t) |j\rangle, \quad (1)$$

где введено обозначение $q_i(t) = \langle i | \psi(t) \rangle$. Пусть H — гамильтониан системы; тогда эволюция распределения амплитуд вероятностей $q_j(t)$ определяется системой уравнений

$$\frac{dq_j(t)}{dt} = -i \sum_k H_{jk} q_k(t), \quad j = \overline{1, N}. \quad (2)$$

Наличие в системе уравнений (2) мнимой единицы, а также то обстоятельство, что в квантовом случае $p_j(t) = |q_j(t)|^2$, обуславливает существенное отличие квантовых непрерывных блужданий от их классического аналога.

В качестве гамильтониана системы можно взять $H = -\gamma L$, однако стоит отметить, что лапласиан дает не единственный возможный гамильтониан, так как для унитарности процесса от гамильтониана требуется только эрмитовость. При этом его вид должен также отображать структуру графа. В случае, если граф регулярный, можно выбрать в качестве альтернативного гамильтониана $H = -\gamma A$, и квантовая динамика при этом не изменится. Однако для нерегулярных графов подобная замена может привести к совершенно иной динамике эволюции состояния системы.

Приведенная модель квантовых блужданий применяется в [8, 9].

В [8] вводится алгоритм поиска по базе данных. Для того чтобы произвести поиск по графу, введем гамильтониан оракула, выделяющий искомый узел w :

$$H_w = -|w\rangle \langle w|.$$

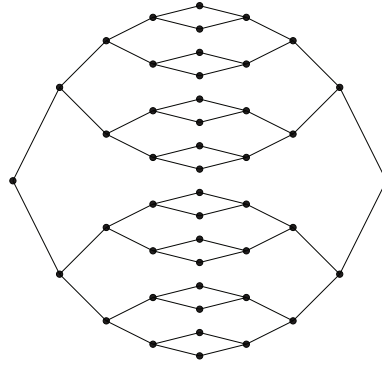
Тогда для построения алгоритма поиска рассмотрим не зависящий от времени гамильтониан

$$H = -\gamma L - |w\rangle \langle w|.$$

Так как все графы в [8] являются регулярными, в дальнейшем будет производиться замена данного гамильтониана на более удобные для анализа выражения. За начальное состояние системы возьмем

$$|s\rangle = \frac{1}{\sqrt{N}} \sum_j |j\rangle.$$

Система эволюционирует некоторое время T , а затем измеряют ее в базисе $|1\rangle, \dots, |N\rangle$. В [8] подбирают значения параметра γ , при котором вероятность успеха $|\langle w | \psi(T) \rangle|^2$ будет максимально близка к 1 при как можно меньшем T .

Рис. 1. Граф G_4 (см. [9])

Сначала рассмотрим две системы, размерность которых растет с увеличением числа узлов в графе: гиперкуб и полный граф. Для полного графа в гамильтониан вместо лапласиана подставим проектор $N |s\rangle \langle s|$. От этого собственные векторы гамильтониана не меняются, меняются собственные значения, но упрощается анализ. В [8] показано, что при выполнении условий $N \gg 1$ и $\gamma N = 1$ переход от $|s\rangle$ к $|w\rangle$ происходит за время $\pi N/2$. При рассмотрении гиперкуба размерности n и с количеством узлов $N = 2^n$ в [8] приведен явный вид матрицы смежности графа:

$$A = \sum_{i=1}^n \sigma_x^i,$$

где σ_x^i — матрица Паули X , действующая на i -й бит. Здесь принимается, что узлы пронумерованы n -битными строками, а элемент матрицы смежности между двумя узлами не равен нулю только в том случае, если номера узлов отличаются ровно в одном бите. Оптимальное значение γ составляет

$$\gamma = \frac{2}{n} + O(n^{-2}),$$

и при данном γ через время порядка $\sqrt{N}$ вероятность найти узел w имеет значение порядка единицы.

В качестве систем, размерность которых не зависит от числа узлов и является фиксированной, в [8] приведены d -размерные решетки. При размерностях $d > 4$ достигается максимально возможное ускорение, т.е. время действия алгоритма пропорционально $\sqrt{N}$, в то время как при $d = 4$ время выполнения алгоритма составляет $O(\sqrt{N} \log^{3/2} N)$.

Та же модель непрерывных квантовых блужданий применяется в [9] при анализе квантовых блужданий по графам G_n . Данные графы представляют из себя два двоичных сбалансированных дерева глубиной n с 2^n узлами n -го уровня, причем узлы на самом высоком уровне у этих двух деревьев совпадают.

Граф G_4 изображен на рис. 1.

В [9] исследуется зависимость вероятности оказаться в крайнем правом узле от времени при условии, что блуждания стартуют из крайнего левого узла. Узлы G_n можно сгруппировать по столбцам, номер j которых меняется от 0 до $2n$. Пусть $H = -\gamma A$, где A — матрица смежности графа G_n . При указанном начальном условии эволюция системы происходит в $(2n + 1)$ -мерном подпространстве $(2^{n+1} + 2^n - 2)$ -мерного гильбертова пространства, натянутом на векторы $|\text{col } j\rangle$, представляющие собой равновзвешенную суперпозицию всех узлов в столбце j :

$$|\text{col } j\rangle = \frac{1}{N_j} \sum_{a \in \text{столбцу } j} |a\rangle.$$

N_j — количество узлов в j -м столбце. В [9] доказано, что в пределе больших значений n волновой пакет распространяется от одного конца графа к другому со скоростью, примерно равной $2\sqrt{2}\gamma$. Определяя предельное распределение, зависящее от начального состояния $|a\rangle$, формулой

$$\chi_b = \lim_{T \rightarrow \infty} \frac{1}{T} \int_0^T \left| \langle b | \exp[-iHt] | a \rangle \right|^2 dt,$$

авторы работы [9] доказывают, что в пределе $t \rightarrow \infty$ вероятность оказаться в крайнем правом узле не меньше $1/(2n+1)$, в то время как в классических блужданиях при любых временах та же вероятность не превосходит 2^{-n} .

1.2. Дискретные унитарные квантовые блуждания. Дискретные квантовые блуждания одной частицы в замкнутых системах можно разделить на два типа: с дополнительным регистром-монеткой и без него. Оба вида блужданий рассмотрены в [3–5].

В [3, 5] предлагаются алгоритмы поиска на двумерной решетке размером $\sqrt{N} \times \sqrt{N}$. Для удобства вводится обозначение $n = \sqrt{N}$, а каждому узлу присваиваются координаты x и y , принимающие значения из $\overline{0, n-1}$. Сетка является «замкнутой», т.е. $(n, y) = (0, y)$, $(x, n) = (x, 0)$. Для задания квантовых блужданий вводится дополнительный регистр — регистр-монетка — с четырьмя базисными состояниями: $|\Leftarrow\rangle$, $|\Downarrow\rangle$, $|\Rightarrow\rangle$ и $|\Uparrow\rangle$. Таким образом, состояние системы является линейной комбинацией состояний $|i, j, d\rangle$, где $i, j \in \{0, \dots, n-1\}$, $d \in \{\Leftarrow, \Downarrow, \Rightarrow, \Uparrow\}$. Шаг данных квантовых блужданий осуществляется через применение оператора

$$U = S \cdot (I \otimes C),$$

где S — оператор сдвига частицы, действующий следующим образом:

$$|i, j, \Rightarrow\rangle \rightarrow |i+1, j, \Leftarrow\rangle, \quad |i, j, \Leftarrow\rangle \rightarrow |i-1, j, \Rightarrow\rangle, \quad |i, j, \Uparrow\rangle \rightarrow |i, j+1, \Downarrow\rangle, \quad |i, j, \Downarrow\rangle \rightarrow |i-1, j, \Uparrow\rangle,$$

а C — унитарное преобразование регистра-монетки.

Часто в качестве оператора подбрасывания монетки выбирают преобразование Гровера

$$D = \begin{pmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{pmatrix}.$$

За начальное состояние принимается

$$|\psi(0)\rangle = \frac{1}{2n} \sum_{i,j} \left(|i, j, \Rightarrow\rangle + |i, j, \Leftarrow\rangle + |i, j, \Uparrow\rangle + |i, j, \Downarrow\rangle \right),$$

а в помеченных узлах вместо преобразования C используется $-I$.

В [5] доказано, что через $O(\sqrt{N \log N})$ шагов вероятность попасть в помеченный узел равна $O(1/\log N)$, если помеченных узлов не более двух, поэтому в этой же статье предлагается сделать усиление амплитуды, занимающее время $O(\sqrt{\log N})$. В [3] же предлагается отказаться от данной процедуры, так как вероятность оказаться от помеченного узла на расстоянии $O(N^{1/4})$ близка к единице, если в графе имеется всего один помеченный узел. Вместо проведения процедуры усиления амплитуды предлагается обработать классическим образом окрестность из $O(\sqrt{N})$ узлов. Также в [5] доказано, что для аналогичного поиска одного помеченного узла в сетке с размерностью $d > 2$ достигается максимальное ускорение, т.е. время поиска равно $O(\sqrt{N})$.

В [4] рассмотрены бесконечные, полубесконечные и конечные блуждания по прямой с квантовым «подбрасыванием» монетки. Дополнительный регистр, очевидно, теперь имеет пространство размерности 2, и за базисные состояния можно принять $|\Leftarrow\rangle$ и $|\Rightarrow\rangle$. Оператором, действующим на пространство состояний монетки, был выбран оператор Адамара H , действующий по правилу

$$H|\Rightarrow\rangle = \frac{1}{\sqrt{2}}(|\Rightarrow\rangle + |\Leftarrow\rangle), \quad H|\Leftarrow\rangle = \frac{1}{\sqrt{2}}(|\Rightarrow\rangle - |\Leftarrow\rangle).$$

Такие блуждания называются *адамаровыми*. Оператор сдвига S определяется равенствами

$$S|x, \Rightarrow\rangle = |x+1, \Rightarrow\rangle, \quad S|x, \Leftarrow\rangle = |x-1, \Leftarrow\rangle,$$

а оператор шага блужданий U определяется так же, как и в [3].

В бесконечных блужданиях за начальное состояние принимается $|0, \Rightarrow\rangle$. Под бесконечными блужданиями понимается то, что время блужданий не ограничено. Для рассмотрения полубесконечных блужданий введем проекторы на состояния с заданным $|x\rangle$:

$$\Pi_{\text{yes}}^x = |x\rangle\langle x| \otimes I, \quad \Pi_{\text{no}}^x = I \otimes I - \Pi_{\text{yes}}^x.$$

Полубесконечные квантовые блуждания осуществляются согласно следующим инструкциям:

- (i) привести систему в начальное состояние $|1, \Rightarrow\rangle$;
- (ii) применить U ;
- (iii) применить оператор Π_{yes}^0 или Π_{no}^0 ;
- (iv) если блуждающая частица оказывается в точке 0, то прервать процесс. В противном случае повторить с пункта (ii).

Конечные квантовые блуждания отличаются от полубесконечных только тем, что после измерения в точке 0 проводятся измерения в некоторой точке n с $n > 1$.

Рассмотрим двухкомпонентный вектор амплитуд в разложении состояния системы $|\Psi(t)\rangle$ по базисным векторам:

$$\Psi(x, t) = \begin{pmatrix} \psi_{\Rightarrow}(x, t) \\ \psi_{\Leftarrow}(x, t) \end{pmatrix},$$

где $\psi_{\Rightarrow}(x, t)$, $\psi_{\Leftarrow}(x, t)$ — амплитуды при $|x, \Rightarrow\rangle$ и $|x, \Leftarrow\rangle$ в момент времени t соответственно. Тогда пусть

$$p_{\Rightarrow}(t) = \left| \langle \psi_{\Rightarrow}(x, t) | \Psi(t) \rangle \right|^2, \quad p_{\Leftarrow}(t) = \left| \langle \psi_{\Leftarrow}(x, t) | \Psi(t) \rangle \right|^2.$$

Введем обозначение $\alpha = x/t$. Следующие три теоремы доказываются в [4] только для $x = t \bmod 2$, так как амплитуды для остальных $|x\rangle$ равны нулю.

Теорема 1. Пусть $n = \alpha t \rightarrow \infty$ при фиксированном α . Если $1/\sqrt{2} < |\alpha| < 1$, то существует $c > 1$, для которого

$$p_{\Rightarrow} = O(c^{-n}), \quad p_{\Leftarrow} = O(c^{-n}).$$

Теорема 2. Пусть ϵ — некоторая константа, $\alpha \in \left(\frac{-1}{\sqrt{2}} - \epsilon, \frac{1}{\sqrt{2}} + \epsilon\right)$. Тогда при $t \rightarrow \infty$ для любого x имеем

$$p_{\Leftarrow}(x, t) \sim \frac{2}{\pi \sqrt{1 - 2\alpha^2 t}} \cos^2\left(-\omega t + \frac{\pi}{4} - \rho\right),$$

$$p_{\Rightarrow}(x, t) \sim \frac{2(1 + \alpha)}{\pi(1 - \alpha) \sqrt{1 - 2\alpha^2 t}} \cos^2\left(-\omega t + \frac{\pi}{4}\right),$$

где

$$\omega = \alpha\rho + \theta, \quad \rho = \arg(-B + \sqrt{\Delta}), \quad \theta = \arg(B + 2 + \sqrt{\Delta}),$$

$$B = \frac{2\alpha}{1 - \alpha}, \quad \Delta = B^2 - 4(B + 1).$$

Теорема 3. Пусть π_t — равномерное распределение вероятностей на $\mathbb{Z} \cap (-t/\sqrt{2}, t/\sqrt{2})$. Обозначим через $P(x, t)$ вероятность найти частицу в точке x в момент времени t , а через $P(\cdot, t)$ — распределение вероятностей. Существует такое δ , что для всех достаточно больших t выполнено неравенство

$$\|P(\cdot, t) - \pi_t\| < \delta.$$

В [4] в полубесконечных блужданиях рассматривается только вероятность p_{∞} обнаружить частицу в точке 0 в любой момент времени и доказывается следующее утверждение.

Теорема 4. $p_{\infty} = 2/\pi$.

При рассмотрении конечных блужданий для любых $n > 1$ введем вероятность p_n того, что частица окажется слева от начальной точки, и вероятность q_n того, что частица окажется справа. В [4] доказана следующая теорема.

Теорема 5. $\lim_{n \rightarrow \infty} p_n = \frac{1}{\sqrt{2}}.$

Один из алгоритмов поиска в базе данных, основанный на дискретных квантовых блужданиях, рассмотрен в [1]. Допустим, что имеются некоторый граф $G = (V, E)$ с множеством вершин $V = \{v_1, \dots, v_n\}$ и «робот», блуждающий по этому графу. Для поиска по базе данных мы должны уметь вычислять произвольную булеву функцию $f : \{0, 1\}^n \rightarrow \{0, 1\}$, аргумент которой пространственно разнесен по графу, т.е. если $X = (x_1, \dots, x_n)$ — аргумент функции $f(X)$, то каждой вершине графа v_i присвоено некоторое x_i . Чтобы обойти ряд проблем, полагаем, что робот знает все о графе, кроме значений x_i .

В любой момент времени состояние системы можно описать вектором

$$\sum_{i,z} \alpha_{i,z} |v_i, z\rangle,$$

где z — битовая строка произвольной длины, отображающая внутреннее состояние робота. Эволюция системы осуществляется через чередующиеся последовательности шагов алгоритма $U^{(i)}$ и вызова оракула O^i :

$$U^{(1)} \rightarrow O^{(1)} \rightarrow \dots \rightarrow U^{(T)} \rightarrow O^{(T)}. \quad (3)$$

Оракул преобразует состояние $|v_i, z\rangle$ в $|v_i, z \oplus x_i\rangle$, причем x_i складывается по модулю 2 с первым битом в z , а результат записывается туда же; $U^{(i)}$ — произвольная унитарная матрица, не зависящая от X и «локально» действующая на G .

Обозначим через $\alpha_{i,z}^{(t)}$ коэффициент при $|v_i, z\rangle$ после t итераций в (3). Функция f посчитана верно с вероятностью $1 - \varepsilon$, если после T шагов выполнено условие

$$\sum_{i,z: z=f(X)} \left| \alpha_{i,z}^{(T)} \right|^2 \geq 1 - \varepsilon.$$

В классическом случае говорят, что стохастическая матрица действует локально на граф G , если вероятность переносится только вдоль его ребер, однако в квантовом случае все несколько сложнее из-за наличия интерференции. Поэтому вводится понятие C -локальных операторов.

Определение 1. Оператор U называется C -локальным, если базисные состояния можно разбить на поднаборы $P_1, \dots, P_q$ так, что:

- (i) $U_{i,z \rightarrow i^*, z^*} = 0$ при любых $|v_i, z\rangle$ и $|v_{i^*}, z^*\rangle$, принадлежащих разным P_j ;
- (ii) для любого j все базисные состояния в P_j либо из одной вершины, либо из двух соседних.

Затем определяется функция $OR(x_1, \dots, x_n)$, принимающая значение 1, если хотя бы один из x_i равен 1, и значение 0 в противном случае.

Отдельно рассмотрены случаи сетки с размерностями $d \geq 3$ и $d = 2$.

Рассмотрим случай $d \geq 3$. Для проведения алгоритма необходимо выполнить разбиение сетки. Для этого берется некоторое большое l_0 , выбираются $\beta \in (2/3, 1)$ и $\mu \in (1/3, 1/2)$, удовлетворяющие требованию $\mu\beta \geq 1/3$, после чего строится последовательность l_R , элементы которой связаны соотношением

$$l_R = l_{R-1} \left[l_{R-1}^{1/\beta-1} \right].$$

Также вводится величина $n_R = l_R^d$. Для простоты полагаем, что для некоторого R выполнено $n = n_R$, т.е. подкуб $L_d(n_R)$ имеет ребра длины l_R . Обозначим через $v(C)$ узел подкуба C с минимальным значением всех координат.

Введем два алгоритма, реализуемых при поиске одной помеченной вершины.

Алгоритм 1 (A_R). Алгоритм ищет помеченный узел в подкубе C размера n_R и увеличивает вероятность того, что при измерении выпадет правильный результат. Начальное состояние по умолчанию: $|v(C), 0\rangle$.

- В случае $R = 0$:
 - 1) Используя классические C -локальные операции, перебрать все узлы в C в произвольном порядке. На каждом узле $v_i \in C$ использовать преобразование $|v_i, z\rangle \rightarrow |v_i, z \oplus x_i\rangle$.
 - 2) Вернуться к $v(C)$.
- В случае $R \geq 1$:
 1. Вызвать алгоритм U_R .
 2. Пусть m_R — минимальное m , при котором $2m + 1 > (n_R/n_{R-1})^\mu$. Провести m_R раз следующую итерацию: вызвать W_R , затем U_R^{-1} , после чего вызвать S_R и U_R .

Алгоритм 2 (U_R). Алгоритм ищет помеченный узел в подкубе C . Начальное состояние по умолчанию: $|v(C), 0\rangle$.

1. Разбить C на n_R/n_{R-1} меньших подкубов $C_1, \dots, C_{n_R/n_{R-1}}$, каждый из n_{R-1} вершин.
2. Для любого $j \in \overline{1, d}$ обозначим через V_j набор «угловых» вершин $v(C_i)$, отличающихся от $v(C)$ только в первых j координатах. Пусть для любого $j \in \overline{1, d}$

$$|V_j\rangle = \frac{1}{l_R^{\frac{j}{2}}} \sum_{v(C_i) \in V_j} |v(C_i), 0\rangle.$$

Применить последовательность преобразований $Z_1, \dots, Z_d$, где Z_i — унитарное преобразование, переводящее $|V_{j-1}\rangle$ в $|V_j\rangle$, применяющее C -локальное преобразование, переносящее амплитуду только вдоль j -й координаты.

3. Рекурсивно вызвать алгоритм A_{R-1} .

Шаг 2 алгоритма 1 выполняет ту же функцию в данном алгоритме, что и итерация Гровера в алгоритме Гровера. Преобразование W_R имеет вид

$$|v_i, z\rangle \rightarrow (-1)^z |v_i, z\rangle,$$

а S_R заменяет $|v_i, z\rangle$ на $-|v_i, z\rangle$, если $z = 0$ и $v_i = v(C)$ для некоторого подкуба C , и ничего не делает в противном случае.

Следует обратить внимание, что шаг 3 в алгоритме 2 выполняет поиск в подкубах $C_1, \dots, C_{n_R/n_{R-1}}$ в суперпозиции.

Пусть дан единственный помеченный узел $v(C_{i^*})$. Назовем *успешным* такое выполнение алгоритмов A_R и U_R , при котором измерение в стандартном базисе дает результат $|v(C_{i^*})\rangle$. Вероятность успешного выполнения алгоритма A_R составляет $\Omega(1/n_R^{1-2\mu})$. Для достижения вероятности успеха $\Omega(1)$ данный алгоритм запускают $O(n_R^{1/2-\mu})$ раз.

Время выполнения алгоритма поиска составляет $O(\sqrt{n})$ на сетке размерности $d \geq 3$ и $O(\sqrt{n} \log^{3/2} n)$ на двумерной сетке. Поиск в двумерном случае отличается только способом разбиения на подкубы.

2. КВАНТОВЫЕ БЛУЖДЕНИЯ ОТКРЫТЫХ СИСТЕМ

Все указанные выше работы моделируют, как уже было сказано, квантовые блуждания замкнутых систем. Далее мы рассмотрим более реалистичные подходы к моделированию квантовых блужданий.

В [12] исследуются дискретные квантовые блуждания по нескольким графам, среди которых линейный и кольцевой. Как и в [5], используется регистр-монетка. За базисные состояния системы принимаются чистые состояния $|x, a\rangle$, где $|a\rangle$ — одно из состояний дополнительного регистра, а $|x\rangle$ указывает положение на графе.

При рассмотрении линейного и кольцевого графов пространство состояний монетки натягивается на векторы $|\rightarrow\rangle$ и $|\leftarrow\rangle$. Оператор шага блужданий U определяется так же, как и в [4].

Для моделирования процессов декогеренции эволюцию матрицы плотности записывают в виде соотношения

$$\rho(t+1) = (1-p)U\rho(t)U^\dagger + p \sum_i \mathbb{P}_i U \rho(t) U^\dagger \mathbb{P}_i^\dagger. \quad (4)$$

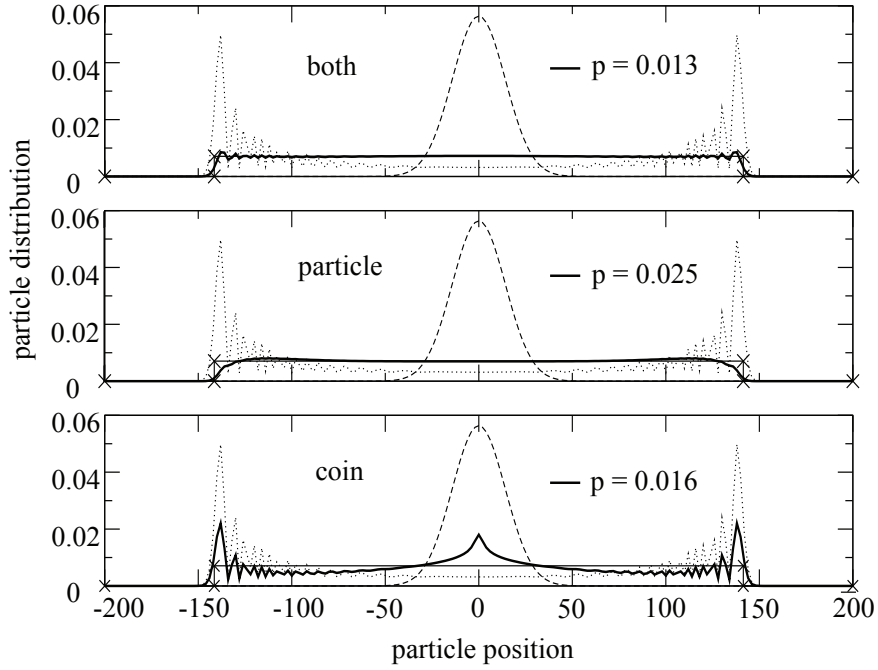


Рис. 2. Распределение положения частицы на прямой после 200 шагов в классических равновзвешенных блужданиях (пунктир), чистых квантовых адамаровых блужданиях (точки) и квантовых адамаровых блужданиях незамкнутой системы при различных значениях p (сплошная линия). См. [12].

Через p обозначена вероятность наступления события, соответствующего нарушению когерентности, в единицу времени, $\mathbb{P}_i$ — проектор, представляющий результат воздействия внешних шумов. В [12] указывается, что при применении различных наборов $\{\mathbb{P}_i\}_i$ получают качественно похожие формы перехода $\sigma_p(T)$ стандартного отклонения $\sigma(T)$ положения частицы от начального положения при отсутствии декогеренции к классическому отклонению. Если $p = 0$, то

$$\sigma_p(T) = \sigma(T) = \sqrt{\langle x^2 \rangle} \propto T,$$

в то время как при $p = 1$ отклонение становится классическим и пропорциональным $\sqrt{T}$. Однако для случая, когда состояние частицы подвержено декогеренции, стремящейся локализовать её в стандартном базисе, наблюдается близкое к равномерному распределение вероятностей между точками $x = -T/2$ и $x = T/2$.

Вычисляя отклонение распределения от равномерного

$$\nu(p, T) = \sum_x \left| P(x, p, T) - P_u(T) \right|,$$

где $P_u(T) = \sqrt{2}/T$ при $-T/\sqrt{2} \geq x \geq T/\sqrt{2}$, а $P(x, p, T)$ — вероятность обнаружить частицу в точке x в момент времени T , можно найти оптимальную вероятность p_u , при которой распределение будет максимально равномерным на $\mathbb{Z} \cap [-T/\sqrt{2}, T/\sqrt{2}]$. Стоит отметить, что p_u зависит от T . Если потере когерентности подвержено также состояние монетки, то получается наиболее близкое к равномерному распределение, но функция $\nu(p, T)$ более чувствительна к значениям p , чем при потере когерентности только у состояния частицы. Если же процессам потери когерентности подвержена только монетка, то никакого усиления равномерности не наблюдается.

При рассмотрении квантовых блужданий частицы по кольцевому графу с числом узлов N в качестве меры прогресса блуждания удобно использовать время перемешивания. В данном случае процесс эволюции состояния системы не дает какого-либо предельного распределения вероятностей при $T \rightarrow \infty$, поэтому приходится ввести усредненные по времени вероятности

$$\overline{P(x, p, T)} = \frac{1}{N} \sum_{t=0}^{T-1} P(x, p, t).$$

Тогда время перемешивания определяется следующим выражением:

$$M_\epsilon = \min \left\{ T \mid \forall t > T : \sum_x \left| \overline{P(x, p, t)} - P_u \right| < \epsilon \right\},$$

где $P_u = 1/N$. В [12] приводятся оценки времени перемешивания, полученные численным путем, при наличии декогеренции и её отсутствии. Так, для $N = 2k + 1$ время перемешивания $M_\epsilon \sim N/\epsilon$. При малой декогеренции наблюдается ускорение выхода распределения на равномерное. Например, если разрушается только когерентность состояния монетки, то для четных N на участке $p < 2/N$ время перемешивания удовлетворяет равенству $M_\epsilon \simeq N/(4p\epsilon)$ при N , не кратных 4, а при кратных 4 время перемешивания составляет примерно $N/(16p\epsilon)$. Минимальное M_ϵ при этом удовлетворяет неравенству $M_\epsilon \gtrsim N^2/32\epsilon$. При воздействии шумов на состояния, отвечающие положению частицы на графе, если $p < 16/N^2$, то $M_\epsilon \simeq 1/(N/2 - 1)$ для N , кратных 2, и $M_\epsilon \simeq 1/(N/4 + 3)$ при N , кратных 4. В данном случае $M_\epsilon^{(\min)} \sim \alpha N/\epsilon$, причем соответствующее значение декогеренции $p^{(\min)} = 16/N^2$. На кольце с нечетным количеством узлов распределение усредненных по времени вероятностей ведет себя похожим образом, включая линейный спад M_ϵ на участке $0 \geq p \gtrsim 16/N^2$ и поведение $M_\epsilon^{\min} \sim \alpha N/\epsilon$ при одновременном нарушении когерентности состояний монетки и частицы. На рис. 3 приведены зависимости времен перемешивания от p при воздействии шумов на состояния монетки, частицы, а также на оба состояния.

Аналогичный подход применяется в [2] при рассмотрении непрерывных квантовых блужданий по гиперкубу. Попытаемся вывести супероператор, который имел бы тот же смысл в непрерывной динамике, что и супероператор в уравнении (4). Будем искать оператор, удовлетворяющий условию

$$S_{t+dt} = S_t \left[e^{-iHdt} \otimes e^{iHdt} \right] \left[(1 - pdt)I + pdt(\mathbb{P}) \right],$$

где H — гамильтониан системы. Из данного уравнения тривиальным способом выводится дифференциальное уравнение на S_t , решением которого является

$$S_t = \exp \left(\left[i(I \otimes H - H \otimes I) - pI \otimes I + p(\mathbb{P}) \right] t \right).$$

Оператор декогеренции определяется равенством

$$\mathbb{P} = \frac{1}{n} \sum_{1 \leq i \leq n} \left[\Pi_0^i \otimes \Pi_0^i + \Pi_1^i \otimes \Pi_1^i \right],$$

где Π_j^i — проектор i -го кубита на состояние $|j\rangle$, $j \in \overline{0, 1}$. Введем обозначение $\tilde{\sigma}_x = \frac{k}{n}\sigma_x$, и пусть недекогерирующий гамильтониан системы равен

$$H = \sum_{j=1}^n I \otimes \dots \tilde{\sigma}_x \dots \otimes I, \quad (5)$$

где $\tilde{\sigma}_x$ стоит на j -м месте. Тогда каждый кубит имеет энергию k/n , и энергия всей системы равна k . Благодаря форме гамильтониана (5) и проекторов Π_j^i оператор S_t можно представить в виде тензорного произведения

$$S_t = [e^A]^{\otimes n}$$

при

$$A = \frac{t}{n} \left[(I \otimes in\tilde{\sigma}_x) - (in\tilde{\sigma}_x \otimes I) - p(I \otimes I) + p(\Pi_1 \otimes \Pi_1) + p(\Pi_0 \otimes \Pi_0) \right].$$

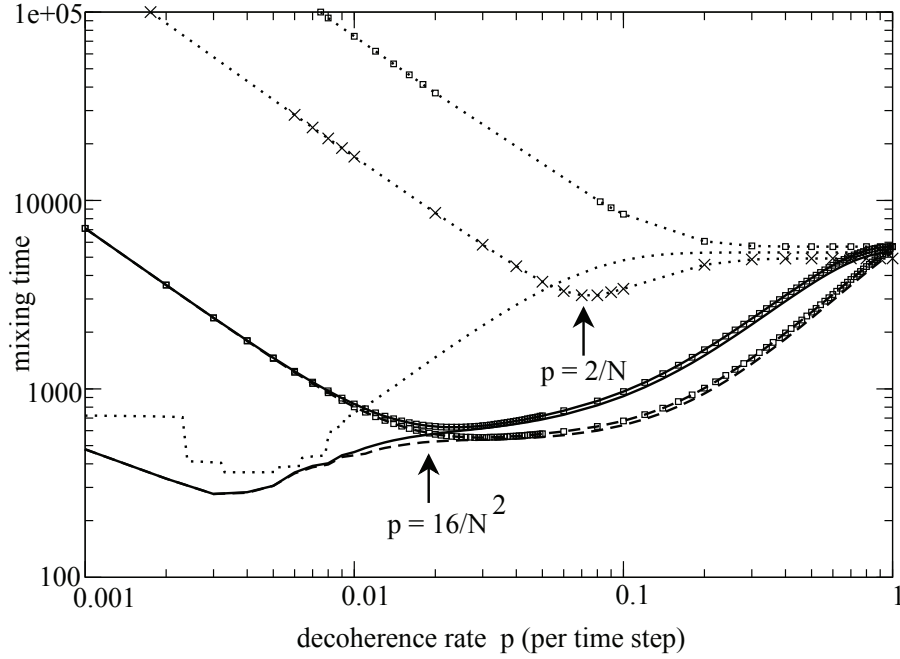


Рис. 3. Численные зависимости времен перемешивания на кольцевом графе с размером $N = 29$ и $N = 20$ ($\square$) при подверженных декогеренции состояниях монетки (точки), частицы (пунктир) или обоих состояниях одновременно (сплошная линия). Также $N = 28$ ($\times$) для монетки. Двойной логарифмический масштаб. См. [12].

В [2] производится анализ поведения однокубитной системы под действием супероператора e^A . За начальное состояние $|\psi_0\rangle$ примем $|0\rangle$. Введем обозначения

$$\alpha = \sqrt{p^2 - 16k^2}, \quad \beta = -i\alpha.$$

Тогда вероятности получить при измерении состояния системы $|0\rangle$ и $|1\rangle$ в момент времени t равны

$$P[0] = \frac{1}{2} + \frac{1}{2} \exp\left(-\frac{pt}{2n}\right) \left[\cos\left(\frac{\beta t}{2n}\right) + \frac{p}{\beta} \sin\left(\frac{\beta t}{2n}\right) \right],$$

$$P[1] = 1 - P[0].$$

При $p < 4k$, $p = 4k$ и $p > 4k$ система ведет себя по-разному. Для нахождения времени перемешивания решается уравнение $P[0] = 1$.

В случае $p < 4k$ можно наблюдать экспоненциальное затухание колебаний распределения вероятностей, но это происходит при $t \rightarrow \infty$. Следует обратить внимание на периодическое возникновение равномерного распределения. Соответствующие времена тоже называются временами перемешивания и определяются следующим выражением:

$$t_{\text{mix}} = \frac{n}{\beta} \left[2\pi c - \arccos\left(\frac{p^2}{8k^2} - 1\right) \right], \quad c \in \mathbb{Z}_+.$$

Найдем моменты времени, в которые состояние этой малой системы наиболее близко к $|0\rangle$. Так как большая система стартует с состояния $|0\rangle^{\otimes n}$, данные моменты времени будут приблизительно соответствовать времени, за которое система перейдет из состояния $|0\rangle^{\otimes n}$ в наиболее близкое к

состоянию $|1\rangle^{\otimes n}$. Решениями являются

$$t_{\text{hit}} = 2n\pi \left(\frac{2c+1}{\beta} \right).$$

Если $p = 4k$, то колебания распределения вероятностей отсутствуют, и само распределение экспоненциально по времени стремится к равномерному.

При $p > 4k$ большая система приходит к равномерному распределению за время $\Theta(n \log n)$, как и в классическом случае.

Практическая значимость непрерывных квантовых блужданий в открытых системах для вычислений демонстрируется в [15] при рассмотрении метода Монте-Карло по схеме марковской цепи. Рассматривается обратимая марковская цепь P со стационарным распределением π . В классическом случае время перемешивания, являющееся временем работы данного алгоритма, составляет $O(\delta^{-1} \log(1/\pi^*))$, где $\pi^* = \min_j \pi_j$, а δ — щель в спектре P . В [15] доказаны следующие факты:

- 1) квантовые блуждания с наличием шумов всегда приходят к предельному распределению;
- 2) время перемешивания является устойчивой величиной, не зависящей от вида декогеренции;
- 3) время перемешивания декогерентного квантового блуждания на периодической решетке $\mathbb{Z}_n^d$ составляет $O(nd \log d)$ или, если выразить через δ и π^* , $O(\sqrt{\delta^{-1}} \log(1/\pi^*))$.

В [10, 11, 16] рассмотрены квантовые блуждания по кольцевому графу, к узлам которого подсоединены точечные контакты. Считается, что других источников шума в системе не существует, и моделируется влияние точечных контактов на эволюцию квантового состояния частицы в графе. В [11, 16] дано общее описание системы. Узлы графа пронумерованы от 0 до $N-1$. Время перемешивания определяется условием

$$T_{\text{mix}} = \min \left\{ t : \sum_{j=0}^{N-1} P_j(t) < \varepsilon \right\}.$$

В [11, 16] показано, что в пределе $\Gamma N \rightarrow 0$ время перемешивания T_{mix} стремится к a/Γ , при $\Gamma \rightarrow \infty$ время перемешивания выходит на асимптоту $T_{\text{mix}} = b\Gamma$, где Γ — уровень шума, а a и b — некоторые константы. В [11] даны оценки времени перемешивания в обоих пределах, а именно:

$$\begin{aligned} \frac{\Gamma N^2}{\pi^2} \ln \left(\frac{2}{N\varepsilon} \right) < T_{\text{mix}} < \frac{\Gamma N^2}{2} \ln \left(\frac{2+\varepsilon}{\varepsilon} \right), \quad \Gamma N \rightarrow 0, \\ T_{\text{mix}} < \frac{1}{\Gamma} \ln \left(\frac{N}{\varepsilon} \right) \left[1 + \frac{2}{N-2} \right], \quad \Gamma \rightarrow \infty. \end{aligned}$$

В [10] показано, что минимальное время перемешивания выходит на асимптоту

$$T_{\text{mix}} = n \ln n \cdot f \left(\frac{\varepsilon}{N} \right)$$

при $N \rightarrow \infty$, а оптимальный уровень шума $\Gamma_{\text{mix min}}$ стремится к $\tilde{f} \left(\frac{\varepsilon}{N} \right) \frac{1}{N}$ при $N \rightarrow \infty$, где $\tilde{f} \left(\frac{\varepsilon}{N} \right)$ и $f \left(\frac{\varepsilon}{N} \right)$ — некоторые функции.

СПИСОК ЛИТЕРАТУРЫ

1. Aaronson S., Ambainis A. Quantum search of spatial regions // Proc. 44 Annual IEEE Symp. Foundations of Computer Science. — 2003. — С. 200–209.
2. Alagic G., Russell A. Decoherence in quantum walks on the hypercube // Phys. Rev. A. — 2005. — 72, № 6. — С. 062304.
3. Ambainis A. et al. Search by quantum walks on two-dimensional grid without amplitude amplification // Conf. on Quantum Computation, Communication, and Cryptography. — Berlin–Heidelberg: Springer-Verlag, 2012. — С. 87–97.

4. *Ambainis A. et al.* One-dimensional quantum walks// Proc. 33 Annual ACM Symp. on Theory of Computing. — 2001. — quantph/0104137. — С. 37–49.
5. *Ambainis A., Kempe J., Rivosh A.* Coins make quantum walks faster// Proc. SODA 2005 — 2005. — С. 1099–1108.
6. *Beals R. et al.* Quantum lower bounds by polynomials// J. ACM. — 2001. — 48, № 4. — С. 778–797.
7. *Briegel H. J., De las Cuevas G.* Projective simulation for artificial intelligence// Sci. Reports. — 2012. — 2. — С. 400.
8. *Childs A. M., Goldstone J.* Spatial search by quantum walk// Phys. Rev. A. — 2004. — 70, № 2. — С. 022314.
9. *Childs A. M., Farhi E., Gutmann S.* An example of the difference between quantum and classical random walks// Quantum Inform. Process. — 2002. — 1, № 1. — С. 35–43.
10. *Fedichkin L., Meshchaninov F.* Quantum-classical crossover in quantum walks mixing time// Proc. Int. Conf. on Micro- and Nano-Electronics, 2016. — Int. Soc. for Optics and Photonics, 2016. — С. 102242M-6.
11. *Fedichkin L., Solenov D., Tamon C.* Mixing and decoherence in quantum walks on cycles// Quantum Inform. Comput. — 2006. — 6, № 3. — С. 263–276.
12. *Kendon V., Tregenna B.* Decoherence can be useful in quantum walks// Phys. Rev. A. — 2003. — 67, № 4. — С. 042315.
13. *Melnikov A. A., Fedichkin L. E.* Quantum walks of interacting fermions on a cycle graph// Sci. Reports. — 2016. — 6. — С. 34226.
14. *Melnikov A. A., Fedichkin L. E.* Continuous-time quantum walk of two interacting fermions on a cycle graph// Proc. Int. Conf. on Micro- and Nano-Electronics, 2016. — Int. Soc. for Optics and Photonics, 2016. — С. 102242L-6.
15. *Richter P. C.* Quantum speedup of classical mixing processes// Phys. Rev. A. — 2007. — 76, № 4. — С. 042306.
16. *Solenov D., Fedichkin L.* Continuous-time quantum walks on a cycle graph// Phys. Rev. A. — 2006. — 73, № 1. — С. 012313.
17. *Solenov D., Fedichkin L.* Nonunitary quantum walks on hypercycles// Phys. Rev. A. — 2006. — 73, № 1. — С. 012308.

Л. Е. Федичкин

Компания НИКС;

Физико-технологический институт РАН;

Московский физико-технический институт (государственный университет)

E-mail: leonidf@gmail.com

Ф. П. Мещанинов

Физико-технологический институт РАН

Московский физико-технический институт (государственный университет)

E-mail: meshchaninov@phystech.edu



ТЕНЗОРНЫЕ ПРОИЗВЕДЕНИЯ КВАНТОВЫХ ОТОБРАЖЕНИЙ

© 2018 г. С. Н. ФИЛИПPOB

Аннотация. В работе исследуются свойства тензорной степени квантовых отображений Φ . В частности, приводится обзор свойств положительности унитарных и неунитарных кубитных отображений $\Phi^{\otimes 2}$. Для произвольных конечномерных систем представлена связь между положительной и вполне положительной делимостью динамических отображений $\Phi_t^{\otimes 2}$ и Φ_t . Найден критерий аннигиляции перепутанности произвольным кубитным отображением $\Phi^{\otimes 2}$.

Ключевые слова: квантовый канал, вполне положительность, положительное отображение, делимость, тензорное произведение.

AMS Subject Classification: 15A69, 46L06

1. Введение. Линейные отображения естественным образом возникают в задачах квантовой эволюции операторов плотности (см. [9, 27, 39]), поскольку основные квантовые уравнения движения являются линейными дифференциальными уравнениями первого порядка по времени. В данной работе рассматриваются конечномерные квантовые системы, состояния которых задаются линейными операторами плотности $\varrho(t) \in \mathcal{B}(\mathcal{H})$, где $\mathcal{H}$ — конечномерное гильбертово (унитарное) пространство, $\dim \mathcal{H} = d < \infty$, $\mathcal{B}(\mathcal{H})$ — множество операторов, действующих на $\mathcal{H}$. Оператор плотности $\varrho(t)$ является эрмитовым ($\varrho^\dagger(t) = \varrho(t)$) и неотрицательно определённым ($\langle \psi | \varrho^\dagger(t) | \psi \rangle \geq 0$ для всех $|\psi\rangle \in \mathcal{H}$; здесь и далее мы пользуемся стандартными обозначениями Дирака) и обладает единичным следом ($\text{tr}[\varrho(t)] = 1$).

При отсутствии начальных корреляций между квантовой системой и её окружением эволюция описывается динамическим отображением $\varrho(t) = \Phi_t[\varrho(0)]$, где Φ_t — вполне положительное, сохраняющее след отображение, называемое *квантовым каналом* (см., например, [27]). Физическое требование вполне положительности вместо простой положительности отображения заключается в том, что рассматриваемая система может изначально находиться в перепутанном (сцепленном, зацепленном, запутанном) состоянии с другой (вспомогательной) системой (см. [31, 48, 49]). Вспомогательная система может обладать произвольной размерностью (k), и она претерпевает тривиальную эволюцию, задаваемую тождественным отображением Id_k . Матрица плотности исходного перепутанного состояния должна переходить в матрицу плотности, поэтому отображение $\Phi_t \otimes \text{Id}_k$ должно быть положительным для любого k ; это и есть определение вполне положительности отображения Φ_t . Примечательно, что для вполне положительных отображений существует удобный критерий, основанный на изоморфизме Чоя—Ямиolkовского (см. [10, 12, 32]), в то время как для положительных отображений такого критерия в общем случае не найдено.

Существование перепутанных состояний подразумевает структуру тензорного произведения у пространства $\mathcal{H}$. Под *перепутанным состоянием* двусоставной системы понимается оператор плотности $\varrho_{AB} \in \mathcal{B}(\mathcal{H}_A) \otimes \mathcal{B}(\mathcal{H}_B)$, не допускающий представления в виде замыкания выпуклой суммы тензорных произведений локальных операторов плотности (см. [53]), т.е.

$$\varrho_{AB} \neq \sum_k p_k \varrho_A^{(k)} \otimes \varrho_B^{(k)}. \quad (1)$$

Состояния, описываемые правой частью уравнения (1), называются *сепарабельными* (распутанными, расцепленными) и могут быть приготовлены с помощью локальных операций и классической коммуникации в удалённых лабораториях A и B .

Допустим, что физические носители информации (A и B) эволюционируют независимо. Это происходит, в частности, при распространении квантового сигнала от источника к двум удалённым приёмникам A и B по индивидуальным линиям связи. В этом случае динамическое отображение задаётся локальным квантовым каналом вида $\Phi_1^A \otimes \Phi_2^B$. Легко показать, что $\Phi_1^A \otimes \Phi_2^B$ является вполне положительным тогда и только тогда, когда и Φ_1^A , и Φ_2^B являются вполне положительными.

Другой важный случай тензорного отображения возникает при передаче информации, закодированной в нескольких физических носителях, через один и тот же канал связи Φ . При отсутствии эффектов памяти, последовательная пересылка n физических носителей через канал приведёт к отображению $\Phi^{\otimes n}$. Именно такие тензорные конструкции используются в определениях пропускных способностях квантовых каналов (см. [28]). Очевидно, что $\Phi^{\otimes n}$ является вполне положительным тогда и только тогда, когда Φ является вполне положительным. Таким же свойством инвариантности к тензорному произведению обладают каналы, разрушающие перепутанность (см. [2, 3, 30, 33, 45, 50]). Однако свойство положительности не является инвариантным по отношению к тензорному произведению, т.е. $\Phi^{\otimes n}$ может не быть положительным, даже если линейное отображение Φ является положительным (см. [1, 17, 22, 38]). Аналогично, отображения $\Phi^{\otimes n}$ и $\Phi^{\otimes m}$, $m > n \geq 2$, могут по-разному действовать на перепутанные состояния: $\Phi^{\otimes n}$ может приводить к аннигиляции перепутанности (см. [14, 15, 19, 21–23, 37]) или абсолютной сепарабельности выходного состояния (см. [18]), в то время как $\Phi^{\otimes m}$ этими свойствами не обладает.

Свойства положительности и вполне положительности промежуточных отображений (см. [54]) $\Theta_{t,t+s} = \Phi_{t+s} \circ \Phi_t^{-1}$, $s > 0$, часто используются для характеристики марковости динамического процесса Φ_t (см. [8, 13, 43]). В частности, если $\Theta_{t,t+s}$ является вполне положительным для любых $t, s \geq 0$, то процесс Φ_t называют *вполне положительно делимым* (марковским), а соответствующее кинетическое уравнение имеет вид уравнения Горини—Коссаковского—Сударшана—Линдблада (см. [25, 34]) с зависящими от времени коэффициентами (скорости декогеренции остаются при этом неотрицательными; см. [26]). Если $\Theta_{t,t+s}$ является положительным для всех $t, s \geq 0$, но не является вполне положительным для некоторых $t, s \geq 0$, то процесс Φ_t называют *слабо немарковским* (см. [11, 42, 55]). Если $\Theta_{t,t+s}$ не является положительным для некоторых $t, s \geq 0$, то процесс Φ_t называют *существенно немарковским* (см. [11]). Физическое различие между перечисленными процессами наглядно демонстрируется в моделях столкновений, где квантовая система последовательно взаимодействует с микроскопическими частицами резервуара (см. [41, 47, 56, 57]). Марковские процессы могут быть легко реализованы с помощью факторизованного состояния резервуара (см. [20]) в непрерывном или стробоскопическом пределе (см. [24, 35, 36]), в то время как для немарковских (слабо или существенно) процессов необходимо скоррелированное окружение (см. [20, 46]) (корреляции могут быть как квантовыми, так и классическими).

Данная работа посвящена анализу однопараметрических семейств отображений Φ_t , $t \geq 0$, $\Phi_0 = \text{Id}$, и их тензорных произведений $\Phi_t^{\otimes 2}$.

Допустим, что Φ_t является полугруппой с некоторым линейным генератором $\mathcal{L}$, т.е. $\Phi_t = \exp(\mathcal{L}t)$. В [5] показано, что положительность отображения $\exp(\mathcal{L}t)^{\otimes 2}$ эквивалентна вполне положительности отображения $\exp(\mathcal{L}t)$ (в этом случае генератор $\mathcal{L}$ задается уравнением Горини—Коссаковского—Сударшана—Линдблада с постоянными коэффициентами). В данной работе показано, что если Φ_t не является полугруппой, то отмеченное свойство не имеет места. Первой целью данной работы является установление соответствия между свойствами положительности отображения Φ_t и отображения $\Phi_t^{\otimes 2}$.

В свете вышеприведенных примеров совершенно неудивительно, что процессы Φ_t и $\Phi_t^{\otimes n}$ могут обладать разной делимостью. Второй целью данной работы является установление соответствия между свойствами делимости отображения Φ_t и отображения $\Phi_t^{\otimes 2}$.

Третьей целью данной работы является нахождение условия аннигиляции перепутанности произвольным двухкубитным квантовым каналом $\Phi_t^{\otimes 2}$.

2. Положительность тензорного произведения отображений. Рассмотрим линейное кубитное отображение $\Phi : \mathcal{B}(\mathcal{H}_2) \mapsto \mathcal{B}(\mathcal{H}_2)$. В [38] показано, что $\Phi^{\otimes n}$ является положительным

для любого $n \in \mathbb{N}$ тогда и только тогда, когда Φ является вполне положительным или вполне коположительным (последовательное применение вполне положительного отображения и транспонирования в некотором базисе). Для случая $n = 1$ также известно, что любое положительное отображение $\Phi : \mathcal{B}(\mathcal{H}_2) \mapsto \mathcal{B}(\mathcal{H}_2)$ есть коническая комбинация вполне положительного и вполне коположительного отображений (см. [51]). В недавней работе [17] исследован случай произвольного n . В частности, если Υ — унитарное отображение вида

$$\Upsilon[\varrho] = \frac{1}{2} \left(\text{tr}[\varrho]I + \sum_{j=1}^3 \tilde{\lambda}_j \text{tr}[\sigma_j \varrho] \sigma_j \right), \quad (2)$$

где $\sigma_1, \sigma_2, \sigma_3$ — стандартные операторы Паули, I — тождественный оператор на $\mathcal{H}_2$, то $\Upsilon^{\otimes 2}$ является положительным тогда и только тогда, когда Υ^2 является вполне положительным (см. [17]). Поскольку критерий вполне положительности кубитных отображений известен (см. [44]), получаем, что $\Upsilon^{\otimes 2}$ является положительным тогда и только тогда, когда

$$1 + \tilde{\lambda}_1^2 - \tilde{\lambda}_2^2 - \tilde{\lambda}_3^2 \geq 0, \quad 1 - \tilde{\lambda}_1^2 + \tilde{\lambda}_2^2 - \tilde{\lambda}_3^2 \geq 0, \quad 1 - \tilde{\lambda}_1^2 - \tilde{\lambda}_2^2 + \tilde{\lambda}_3^2 \geq 0.$$

Пример 1. Рассмотрим зависящий от времени диссипатор

$$\mathcal{L}_t[\varrho] = \frac{\alpha}{2} \sum_{k=1}^3 \gamma_k(t) (\sigma_k \varrho \sigma_k - \varrho), \quad (3)$$

где $\alpha > 0$, $\gamma_1(t) = \gamma_2(t) = 1$, $\gamma_3(t) = -\text{th}(t)$. Поскольку отображения $\mathcal{L}_{t_1}$ и $\mathcal{L}_{t_2}$ в разные моменты времени перестановочны, результирующее отображение есть

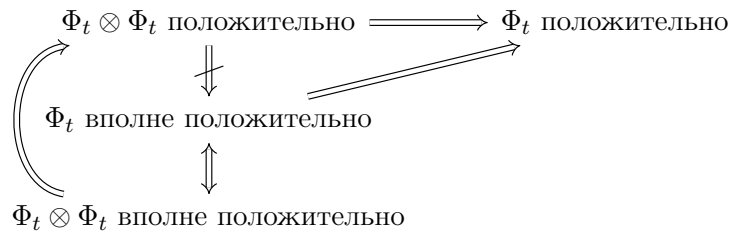
$$\Upsilon_t = \exp \left(\int_0^t \mathcal{L}(t') dt' \right).$$

Нетрудно вычислить

$$\tilde{\lambda}_1(t) = \tilde{\lambda}_2(t) = \text{ch}^\alpha(t) e^{-\alpha t}, \quad \tilde{\lambda}_3(t) = e^{-2\alpha t}.$$

Полученное отображение Υ_t является вполне положительным тогда и только тогда, когда $\alpha \geq 1$, и просто положительным при $\alpha > 0$ (см. [6]). Используя критерий положительности отображения $\Upsilon_t^{\otimes 2}$ (см. [17]), заключаем, что $\Upsilon_t^{\otimes 2}$ является положительным тогда и только тогда, когда $\alpha \geq 1/2$. Таким образом, если $1/2 \leq \alpha < 1$, то все отображения $\{\Upsilon_t^{\otimes 2}\}_{t>0}$ являются положительными, в то время как отображения $\{\Upsilon_t\}_{t>0}$ не являются вполне положительными. Данное обстоятельство показывает, что из положительности отображения $\Upsilon_t^{\otimes 2}$ в общем случае не следует вполне положительность Υ_t в отличие от случая полугруппы, рассмотренного в [5].

Полученные результаты можно представить в виде следующей диаграммы:



В [4] показано, что для любого положительного кубитного отображения Φ , не принадлежащего границе положительных отображений, найдутся такие положительно определённые операторы A и B , что

$$\Phi_A \circ \Phi \circ \Phi_B = \Upsilon, \quad (4)$$

где $\Phi_A[X] = AXA^\dagger$, $\Phi_B[X] = BXB^\dagger$, а Υ имеет вид (2). Ввиду невырожденности операторов A и B отображения $\Phi^{\otimes n}$ и $\Upsilon^{\otimes n}$ имеют одинаковые свойства положительности. В [16] найден явный

вид операторов A и B , а также параметры $\tilde{\lambda}_j$. В частности, для неунитального отображения

$$\Phi[X] = \frac{1}{2} \left(\text{tr}[X](I + t_3\sigma_3) + \sum_{j=1}^3 \lambda_j \text{tr}[\sigma_j \varrho] \sigma_j \right) \quad (5)$$

параметры $\tilde{\lambda}_j$ определяются выражениями

$$\tilde{\lambda}_1 = \frac{2\lambda_1}{\sqrt{(1+\lambda_3)^2 - t_3^2} + \sqrt{(1-\lambda_3)^2 - t_3^2}}, \quad (6)$$

$$\tilde{\lambda}_2 = \frac{2\lambda_2}{\sqrt{(1+\lambda_3)^2 - t_3^2} + \sqrt{(1-\lambda_3)^2 - t_3^2}}, \quad (7)$$

$$\tilde{\lambda}_3 = \frac{4\lambda_3}{\left(\sqrt{(1+\lambda_3)^2 - t_3^2} + \sqrt{(1-\lambda_3)^2 - t_3^2} \right)^2}. \quad (8)$$

В результате мы получаем критерий положительности отображения $\Phi^{\otimes 2}$.

Предложение 1. *Отображение $\Phi^{\otimes 2}$, где Φ задаётся уравнением (5) и $|t_3| + |\lambda_3| < 1$, является положительным тогда и только тогда, когда параметры (6)–(8) удовлетворяют условиям*

$$1 + \tilde{\lambda}_1^2 - \tilde{\lambda}_2^2 - \tilde{\lambda}_3^2 \geq 0, \quad 1 - \tilde{\lambda}_1^2 + \tilde{\lambda}_2^2 - \tilde{\lambda}_3^2 \geq 0, \quad 1 - \tilde{\lambda}_1^2 - \tilde{\lambda}_2^2 + \tilde{\lambda}_3^2 \geq 0.$$

Аналогично, объединяя результаты работ [16, 17], можно получить критерий положительности отображения $\Phi^{\otimes 3}$. Здесь мы не приводим данный критерий ввиду его громоздкости. Необходимые и (отдельно) достаточные условия положительности произвольного кубитного отображения $\Phi^{\otimes n}$ получаются таким же образом.

3. Делимость тензорного произведения отображений. Рассмотренные в предыдущем разделе свойства применимы к промежуточному отображению $\Theta_{t,t+s} = \Phi_{t+s} \circ \Phi_t^{-1}$, преобразующему состояние в момент времени t в состояние в момент времени $t+s$. Очевидно, что если процесс Φ_t является вполне положительно делимым, то вполне положительно делимым будет и процесс $\Phi_t \otimes \text{Id}$. Однако, если процесс Φ_t является просто положительно делимым, то отсюда не следует положительной делимости процесса $\Phi_t \otimes \text{Id}$, поскольку отображение $\Theta_{t,t+s} \otimes \text{Id}$ не всегда является положительным для положительных отображений $\Theta_{t,t+s}$. Этот пример показывает, что добавление к системе тривиальной вспомогательной системы (претерпевающей тождественное преобразование Id) может повлиять на свойство положительной делимости отображения.

Если же перейти на уровень тензорного произведения отображения на себя, то для динамики произвольной конечномерной системы справедлив следующий результат (см. [6]).

Предложение 2. *Однопараметрическое семейство $\{\Phi_t\}_{t \geq 0}$ динамических отображений конечномерной квантовой системы является вполне положительно делимым тогда и только тогда, когда тензорное произведение $\{\Phi_t \otimes \Phi_t\}_{t \geq 0}$ является положительно делимым.*

С другой стороны, $\Theta_{t,t+s} \otimes \Theta_{t,t+s}$ является вполне положительным тогда и только тогда, когда $\Theta_{t,t+s}$ является вполне положительным. Таким образом, мы получаем следующее утверждение.

Предложение 3. *Положительная делимость и вполне положительная делимость конечномерного динамического отображения $\Phi_t \otimes \Phi_t$ эквивалентны.*

Эти результаты можно представить в виде диаграммы:

$$\begin{array}{c} \Phi_t \otimes \Phi_t \text{ положительно делимо} \\ \Updownarrow \\ \Phi_t \text{ вполне положительно делимо} \\ \Updownarrow \\ \Phi_t \otimes \Phi_t \text{ вполне положительно делимо.} \end{array}$$

Поскольку из положительности отображения $\Theta_{t,t+s}^{\otimes n+1}$ следует положительность отображения $\Theta_{t,t+s}^{\otimes n}$, $n \in \mathbb{N}$, то Φ_t является вполне положительно делимым (марковским), если $\Phi_t^{\otimes n}$ с $n \geq 2$ является положительно делимым.

4. Аннигиляция перепутанности тензорным произведением кубитных отображений. Отображение

$$\Phi \otimes \Phi' : \mathcal{B}(\mathcal{H}) \otimes \mathcal{B}(\mathcal{H}') \mapsto \mathcal{B}(\mathcal{H}) \otimes \mathcal{B}(\mathcal{H}')$$

называется *положительным и аннигилирующим перепутанность*, если $\Phi \otimes \Phi'[\varrho]$ является сепарабельным оператором плотности по отношению к разбиению $\mathcal{H}|\mathcal{H}'$ для любых операторов плотности $\varrho \in \mathcal{B}(\mathcal{H}) \otimes \mathcal{B}(\mathcal{H}')$ (см. [22]). Свойства таких отображений были частично исследованы в [14, 15, 21, 23]. В данной работе мы полностью характеризуем двухкубитные отображения

$$\Phi \otimes \Phi' : \mathcal{B}(\mathcal{H}_2) \otimes \mathcal{B}(\mathcal{H}'_2) \mapsto \mathcal{B}(\mathcal{H}_2) \otimes \mathcal{B}(\mathcal{H}'_2),$$

обладающие свойством аннигиляции перепутанности. Поскольку почти все неунитальные положительные кубитные отображения Φ сводятся к унитарным отображениям вида (2) по формуле (4), а отображения Φ_A и Φ_B не изменяют свойство перепутанности, то наша задача сводится к анализу тензорного произведения $\Upsilon \otimes \Upsilon'$. Отображениям Υ и Υ' поставим в соответствие векторы $\lambda = (\tilde{\lambda}_1, \tilde{\lambda}_2, \tilde{\lambda}_3)^\top$ и $\tilde{\lambda} = (\tilde{\lambda}_1, \tilde{\lambda}_2, \tilde{\lambda}_3)^\top$.

Предложение 4. Пусть Υ и Υ' — положительные кубитные отображения. Отображение $\Upsilon \otimes \Upsilon'$ является положительным и аннигилирующим перепутанность тогда и только тогда, когда

$$|\tilde{\lambda}^\top P R \tilde{\lambda}'| \leq 1$$

для всех матриц перестановки размера 3×3 и матриц

$$R \in \left\{ I, \text{diag}(1, -1, -1), \text{diag}(-1, 1, -1), \text{diag}(-1, -1, 1) \right\}.$$

Доказательство. Вследствие выпуклой структуры сепарабельных состояний отображение $\Upsilon \otimes \Upsilon'$ является аннигилирующим перепутанность тогда и только тогда, когда $\Upsilon \otimes \Upsilon'[\psi\rangle\langle\psi|]$ сепарабельно для всех чистых состояний $|\psi\rangle$. Разложение Шмидта произвольного двухкубитного чистого состояния $|\psi\rangle$ имеет вид

$$|\psi\rangle = \sqrt{p}|\varphi\rangle \otimes |\chi\rangle + \sqrt{1-p}|\varphi_\perp\rangle \otimes |\chi_\perp\rangle = U \otimes V|\psi_p\rangle,$$

где $0 \leq p \leq 1$,

$$|\psi_p\rangle = \sqrt{p}|0\rangle \otimes |0\rangle + \sqrt{1-p}|1\rangle \otimes |1\rangle$$

и операторы U, V унитарны (матрицы перехода от базиса $\{|0\rangle, |1\rangle\}$ к базису $\{|\varphi\rangle, |\varphi_\perp\rangle\}$, от базиса $\{|0\rangle, |1\rangle\}$ к базису $\{|\chi\rangle, |\chi_\perp\rangle\}$).

Положим $\Phi_U[X] = UXU^\dagger$; тогда

$$\Upsilon \otimes \Upsilon'[\psi\rangle\langle\psi|] = (\Upsilon \circ \Phi_U) \otimes (\Upsilon' \circ \Phi_V)[\psi_p\rangle\langle\psi_p|].$$

Поскольку локальные унитарные операции сохраняют сепарабельность, применим дополнительные унитарные операции $\Phi_{U^\dagger} \otimes \Phi_{V^\dagger}$. При этом $\Upsilon \otimes \Upsilon'[\psi\rangle\langle\psi|]$ является сепарабельным тогда и только тогда, когда

$$(\Phi_{U^\dagger} \circ \Upsilon \circ \Phi_U) \otimes (\Phi_{V^\dagger} \circ \Upsilon' \circ \Phi_V)[\psi_p\rangle\langle\psi_p|]$$

сепарабельно.

Матричное представление

$$M_{ij}(\Upsilon) = \frac{1}{2} \text{tr} [\sigma_i \Upsilon [\sigma_j]], \quad i, j = 0, \dots, 3,$$

отображения $\Phi_{U^\dagger} \circ \Upsilon \circ \Phi_U$ не является диагональным:

$$M(\Phi_{U^\dagger} \circ \Upsilon \circ \Phi_U) = \left(\frac{1}{\mathbf{0}} \middle| \frac{\mathbf{0}^\top}{Q_U^\top} \right) \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \tilde{\lambda}_1 & 0 & 0 \\ 0 & 0 & \tilde{\lambda}_2 & 0 \\ 0 & 0 & 0 & \tilde{\lambda}_3 \end{pmatrix} \left(\frac{1}{\mathbf{0}} \middle| \frac{\mathbf{0}^\top}{Q_U} \right), \quad (9)$$

где Q_U — ортогональная матрица размера 3×3 , отвечающая каналу Φ_U , $\mathbf{0}$ — трёхкомпонентный нулевой столбец. При действии на состояние $|\psi_p\rangle\langle\psi_p|$ только диагональные элементы матриц $M(\Phi_{U^\dagger} \circ \Upsilon \circ \Phi_U)$ и $M(\Phi_{V^\dagger} \circ \Upsilon' \circ \Phi_V)$ имеют значение, поэтому

$$(\Phi_{U^\dagger} \circ \Upsilon \circ \Phi_U) \otimes (\Phi_{V^\dagger} \circ \Upsilon' \circ \Phi_V) [|\psi_p\rangle\langle\psi_p|] = \Upsilon_U \otimes \Upsilon'_V [|\psi_p\rangle\langle\psi_p|],$$

где

$$M(\Upsilon_U) = \text{diag} \left(1, (\mathcal{Q}_U \tilde{\lambda})^\top \right), \quad (\mathcal{Q}_U)_{ij} = |(Q_U^\top)_{ij}|^2, \quad (10)$$

$$M(\Upsilon'_V) = \text{diag} \left(1, (\mathcal{Q}_V \tilde{\lambda}')^\top \right), \quad (\mathcal{Q}_V)_{ij} = |(Q_V^\top)_{ij}|^2. \quad (11)$$

Заметим, что матрицы $\mathcal{Q}_U$ и $\mathcal{Q}_V$ являются бистохастическими. Для краткости введем обозначения $\mu = \mathcal{Q}_U \tilde{\lambda}$ и $\mu' = \mathcal{Q}_V \tilde{\lambda}'$. В базисе $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ оператор плотности $\Upsilon_U \otimes \Upsilon'_V [|\psi_p\rangle\langle\psi_p|]$ имеет так называемый X-вид, следовательно, он является неотрицательно определённым и сепарабельным по критерию Переса—Городецких (см. [29, 40]) тогда и только тогда, когда

$$(1 + \mu_3 \mu'_3)^2 \geq (\mu_1 \mu'_1 \pm \mu_2 \mu'_2)^2 + (2p - 1)^2 [(\mu_3 + \mu'_3)^2 - (\mu_1 \mu'_1 \pm \mu_2 \mu'_2)^2], \quad (12)$$

$$(1 - \mu_3 \mu'_3)^2 \geq (\mu_1 \mu'_1 \pm \mu_2 \mu'_2)^2 + (2p - 1)^2 [(\mu_3 - \mu'_3)^2 - (\mu_1 \mu'_1 \pm \mu_2 \mu'_2)^2]. \quad (13)$$

Условия (12) и (13) автоматически выполняются при $p = 0$ или $p = 1$, поскольку отображения Υ и Υ' положительны, а состояние $|\psi_p\rangle$ в этом случае является факторизованным. Вследствие монотонности по параметру $(2p - 1)^2$ условия (12) и (13) выполняются для всех $0 \leq p \leq 1$ тогда и только тогда, когда они удовлетворяются для $p = 1/2$:

$$|\mu^\top \tilde{P}^{-1} \tilde{R} \tilde{P} \mu'| \leq 1, \quad (14)$$

где $\tilde{R} = I$ или $\tilde{R} = \text{diag}(1, -1, -1)$, а $\tilde{P}$ — матрица перестановки 3×3 . Вспоминая, что $\mu = \mathcal{Q}_U \tilde{\lambda}$ и $\mu' = \mathcal{Q}_V \tilde{\lambda}'$, приводим неравенство (14) к виду

$$|\tilde{\lambda}^\top \mathcal{Q}_U^\top \tilde{P}^{-1} \tilde{R} \tilde{P} \mathcal{Q}_V \tilde{\lambda}'| \leq 1. \quad (15)$$

По теореме Биркгоффа—фон Неймана (см. [7, 52]) бистохастические матрицы $\mathcal{Q}_U^\top$ и $\mathcal{Q}_V$ являются выпуклыми суммами матриц перестановки, и неравенство (15) будет выполняться для всех $\mathcal{Q}_U^\top$ и $\mathcal{Q}_V$ тогда и только тогда, когда условие

$$|\tilde{\lambda}^\top P_1 \tilde{R} P_2 \tilde{\lambda}'| \leq 1 \quad (16)$$

выполняется для всех матриц перестановки P_1 и P_2 . С другой стороны, $\tilde{R} P_2 = P_2 R$, где R — одна из матриц $I, \text{diag}(1, -1, -1), \text{diag}(-1, 1, -1), \text{diag}(-1, -1, 1)$. Обозначая $P_1 P_2 = P$, получаем, что

$$(\Phi_{U^\dagger} \circ \Upsilon \circ \Phi_U) \otimes (\Phi_{V^\dagger} \circ \Upsilon' \circ \Phi_V) [|\psi_p\rangle\langle\psi_p|]$$

сепарабельно, а следовательно, $\Upsilon_1 \otimes \Upsilon_2$ аннигилирует перепутанность тогда и только тогда, когда

$$|\tilde{\lambda}^\top P R \tilde{\lambda}'| \leq 1$$

для всех матриц перестановки размера 3×3 и матриц

$$R \in \left\{ I, \text{diag}(1, -1, -1), \text{diag}(-1, 1, -1), \text{diag}(-1, -1, 1) \right\}.$$

Предложение 4 доказано. $\square$

Следствие 1. Пусть

$$1 \geq \tilde{\lambda}_1 \geq \tilde{\lambda}_2 \geq \tilde{\lambda}_3 \geq 0, \quad 1 \geq \tilde{\lambda}'_1 \geq \tilde{\lambda}'_2 \geq \tilde{\lambda}'_3 \geq 0.$$

Локальное двухкубитное унитарное отображение $\Upsilon \otimes \Upsilon'$ аннигилирует перепутанность тогда и только тогда, когда

$$\tilde{\lambda}^\top \tilde{\lambda}' = \tilde{\lambda}_1 \tilde{\lambda}'_1 + \tilde{\lambda}_2 \tilde{\lambda}'_2 + \tilde{\lambda}_3 \tilde{\lambda}'_3 \leq 1.$$

Следствие 2. Локальное двухкубитное унитарное отображение $\Upsilon^{\otimes 2}$ аннигилирует перепутанность тогда и только тогда, когда

$$\tilde{\lambda}_1^2 + \tilde{\lambda}_2^2 + \tilde{\lambda}_3^2 \leq 1.$$

Следствие 3. Отображение $\Phi^{\otimes 2}$, где Φ задается формулой (5), аннигилирует перепутанность тогда и только тогда, когда

$$\frac{4(\lambda_1^2 + \lambda_2^2)}{\left(\sqrt{(1 + \lambda_3)^2 - t_3^2} + \sqrt{(1 - \lambda_3)^2 - t_3^2}\right)^2} + \frac{16\lambda_3^2}{\left(\sqrt{(1 + \lambda_3)^2 - t_3^2} + \sqrt{(1 - \lambda_3)^2 - t_3^2}\right)^4} \leq 1. \quad (17)$$

5. Заключение. В работе исследованы свойства тензорной степени квантовых отображений Φ , в частности, большинство результатов представлены для $\Phi^{\otimes 2}$. Приведён обзор свойств положительности унитарных кубитных отображений $\Phi^{\otimes 2}$, а исследование неунитарных отображений сведено к унитарным. Для произвольных конечномерных систем показана эквивалентность между положительной и вполне положительной делимостью динамических отображений $\Phi_t^{\otimes 2}$. Таким образом, положительная делимость динамического отображения $\Phi_t^{\otimes 2}$ равносильна вполне положительной делимости (марковости) отображения Φ_t . Для произвольных кубитных отображений Φ и Φ' найден критерий аннигиляции перепутанности отображением $\Phi \otimes \Phi'$. Результаты продемонстрированы на частном случае неунитарного кубитного канала (5).

СПИСОК ЛИТЕРАТУРЫ

1. Филиппов С. Н. Квантовые отображения и характеристизация перепутанных квантовых состояний // Квантовые вычисления / Итоги науки и техн. Сер. Совр. мат. прилож. Темат. обз. — 2017. — М.: ВИНТИ РАН, 2017. — 138. — С. 99–124.
2. Холево А. С. Квантовые теоремы кодирования // Усп. мат. наук. — 1998. — 53, № 6 (324). — С. 193–230.
3. Холево А. С. Каналы, разрушающие сцепленность, в бесконечных размерностях // Пробл. передачи информ. — 2008. — 44, № 3. — С. 3–18.
4. Aubrun G., Szarek S. J. Two proofs of Størmer's theorem // arXiv:1512.03293[math.FA].
5. Benatti F., Floreanini R., Romano R. Complete positivity and dissipative factorized dynamics // J. Phys. A: Math. Gen. — 2002. — 35. — С. L351.
6. Benatti F., Chruściński D., Filippov S. Tensor power of dynamical maps and positive versus completely positive divisibility // Phys. Rev. A. — 2017. — 95. — С. 012112.
7. Birkhoff G. Tres observaciones sobre el algebra lineal // Univ. Nac. Tucumán Rev. Ser. A. — 1946. — 5. — С. 147.
8. Breuer H.-P., Laine E.-M., Piilo J., Vacchini B. Colloquium: Non-Markovian dynamics in open quantum systems // Rev. Mod. Phys. — 2016. — 88. — С. 021002.
9. Breuer H.-P., Petruccione F. The theory of open quantum systems. — New York: Oxford Univ. Press, 2002.
10. Choi M.-D. Completely positive linear maps on complex matrices // Linear Algebra Appl. — 1975. — 10. — С. 285.
11. Chruściński D., Maniscalco S. Degree of non-Markovianity of quantum evolution // Phys. Rev. Lett. — 2014. — 112. — С. 120404.
12. De Pillis J. Linear transformations which preserve Hermitian and positive semidefinite operators // Pac. J. Math. — 1967. — 23. — С. 129.
13. De Vega I., Alonso D. Dynamics of non-Markovian open quantum systems // Rev. Mod. Phys. — 2017. — 89. — С. 015001.
14. Filippov S. N. PPT-inducing, distillation-prohibiting, and entanglement-binding quantum channels // J. Russ. Laser Research. — 2014. — 35. — С. 484.

15. *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. — C. 03003.
16. *Filippov S. N., Frizen V. V., Kolobova D. V.* Ultimate entanglement robustness of two-qubit states to general local noises// arXiv:1708.08208[quant-ph].
17. *Filippov S. N., Magadov K. Yu.* Positive tensor products of qubit maps and n -tensor-stable positive qubit maps// J. Phys. A: Math.Theor. — 2017. — 50. — C. 055301.
18. *Filippov S. N., Magadov K. Yu., Jivulescu M. A.* Absolutely separating quantum maps and channels// New J. Phys. — 2017. — 19. — C. 083010.
19. *Filippov S. N., Melnikov A. A., Ziman M.* Dissociation and annihilation of multipartite entanglement structure in dissipative quantum dynamics// Phys. Rev. A. — 2013. — 88. — C. 062328.
20. *Filippov S. N., Piilo J., Maniscalco S., Ziman M.* Divisibility of quantum dynamical maps and collision models// arXiv:1708.04994[quant-ph].
21. *Filippov S. N., Rybár T., Ziman M.* Local two-qubit entanglement-annihilating channels// Phys. Rev. A. — 2012. — 85. — C. 012303.
22. *Filippov S. N., Ziman M.* Bipartite entanglement-annihilating maps: Necessary and sufficient conditions// Phys. Rev. A. — 2013. — 88. — C. 032316.
23. *Filippov S. N., Ziman M.* Entanglement sensitivity to signal attenuation and amplification// Phys.Rev. A. — 2014. — 90. — C. 010301(R).
24. *Giovannetti V., Palma G. M.* Master equations for correlated quantum channels// Phys. Rev. Lett. — 2012. — 108. — C. 040401.
25. *Gorini V., Kossakowski A., Sudarshan E. C. G.* Completely positive dynamical semigroups of N -level systems// J. Math. Phys. — 1976. — 17. — C. 821.
26. *Hall M. J. W.* Complete positivity for time-dependent qubit master equations// J. Phys. A: Math. Theor. — 2008. — 41. — C. 205302.
27. *Holevo A. S.* Quantum systems, channels, information. — Berlin: Walter de Gruyter, 2012.
28. *Holevo A. S., Giovannetti V.* Quantum channels and their entropic characteristics// Repts. Progr. Phys. — 2012. — 75. — C. 046001.
29. *Horodecki M., Horodecki P., Horodecki R.* Separability of mixed states: necessary and sufficient conditions// Phys. Lett. A. — 1996. — 223. — C. 1.
30. *Horodecki M., Shor P. W., Ruskai M. B.* Entanglement breaking channels// Rev. Math. Phys. — 2003. — 15. — C. 629.
31. *Horodecki R., Horodecki P., Horodecki M., Horodecki K.* Quantum entanglement// Rev. Mod. Phys. — 2009. — 81. — C. 865.
32. *Jamiolkowski A.* Linear transformations which preserve trace and positive semidefiniteness of operators// Repts. Math. Phys. — 1972. — 3. — C. 275.
33. *King C.* Maximization of capacity and l_p norms for some product channels// J. Math. Phys. — 2002. — 43. — C. 1247.
34. *Lindblad G.* On the generators of quantum dynamical semigroups// Commun. Math. Phys. — 1976. — 48. — C. 119.
35. *Lorenzo S., Ciccarello F., Palma G. M.* Composite quantum collision models// arXiv:1705.03215[quant-ph].
36. *Luchnikov I. A., Filippov S. N.* Quantum evolution in the stroboscopic limit of repeated measurements// Phys. Rev. A. — 2017. — 95. — C. 022113.
37. *Moravčíková L., Ziman M.* Entanglement-annihilating and entanglement-breaking channels// J. Phys. A: Math. Theor. — 2010. — 43. — C. 275306.
38. *Müller-Hermes A., Reeb D., Wolf M. M.* Positivity of linear maps under tensor powers// J. Math. Phys. — 2016. — 57. — C. 015202.
39. *Nielsen M. A., Chuang I. L.* Quantum Computation and Quantum Information. — Cambridge: Cambridge Univ. Press, 2000.
40. *Peres A.* Separability criterion for density matrices// Phys. Rev. Lett. — 1996. — 77. — C. 1413.
41. *Rau J.* Relaxation phenomena in spin and harmonic oscillator systems// Phys. Rev. — 1963. — 129. — C. 1880.
42. *Rivas Á., Huelga S. F., Plenio M. B.* Entanglement and non-Markovianity of quantum evolutions// Phys. Rev. Lett. — 2010. — 105. — C. 050403.
43. *Rivas Á., Huelga S. F., Plenio M. B.* Quantum non-Markovianity: characterization, quantification and detection// Repts. Progr. Phys. — 2014. — 77. — C. 094001.

44. *Ruskai M. B., Szarek S., Werner E.* An analysis of completely-positive trace-preserving maps on M_2 // Linear Algebra Appl. — 2002. — 347. — С. 159.
45. *Ruskai M. B.* Qubit entanglement breaking channels// Rev. Math. Phys. — 2003. — 15. — С. 643.
46. *Rybár T., Filippov S. N., Ziman M., Bužek V.* Simulation of indivisible qubit channels in collision models// J. Phys. B: Atomic, Molecular and Optical Physics. — 2012. — 45. — С. 154006.
47. *Scarani V., Ziman M., Štelmachovič P., Gisin N., Bužek V.* Thermalizing quantum machines: Dissipation and entanglement// Phys. Rev. Lett. — 2002. — 88. — С. 097905.
48. *Schrödinger E.* Discussion of probability relations between separated systems// Math. Proc. Cambridge Philos. Soc. — 1935. — 31. — С. 555–563.
49. *Schrödinger E.* Probability relations between separated systems// Math. Proc. Cambridge Philos. Soc. — 1936. — 32. — С. 446–452.
50. *Shor P. W.* Additivity of the classical capacity of entanglement-breaking quantum channels// J. Math. Phys. — 2002. — 43. — С. 4334.
51. *Størmer E.* Positive linear maps of operator algebras// Acta Math. — 1963. — 110. — С. 233.
52. *von Neumann J.* A certain zero-sum two-person game equivalent to an optimal assignment problem// Ann. Math. Stud. — 1953. — 28. — С. 5.
53. *Werner R. F.* Quantum states with Einstein–Podolsky–Rosen correlations admitting a hidden-variable model// Phys. Rev. A. — 1989. — 40. — С. 4277.
54. *Wolf M. M., Cirac J. I.* Dividing quantum channels// Commun. Math. Phys. — 2008. — 279. — С. 147.
55. *Wolf M. M., Eisert J., Cubitt T. S., Cirac J. I.* Assessing non-Markovian quantum dynamics// Phys. Rev. Lett. — 2008. — 101. — С. 150402.
56. *Ziman M., Bužek V.* Open system dynamics of simple collision models// in: *Quantum Dynamics and Information*/ R. Olkiewicz et al., eds. — Singapore: World Scientific, 2011. — С. 199–227.
57. *Ziman M., Štelmachovič P., Bužek V., Hillery M., Scarani V., Gisin N.* Diluting quantum information: An analysis of information transfer in system-reservoir interactions// Phys. Rev. A. — 2002. — 65. — С. 042105.

С. Н. Филиппов

Московский физико-технический институт (государственный университет)

E-mail: sergey.filippov@phystech.edu