Записки научных
семинаров ПОМИ
Том 373, 2009 г.

В. П. Гердт, Ю. Г. Палий, А. М. Хведелидзе

О КОЛЬЦЕ ЛОКАЛЬНЫХ ИНВАРИАНТОВ ПАРЫ ЗАПУТАННЫХ КУБИТОВ

Введение

Согласно квантовой теории нелокальность в квантовом мире проявляет себя существенно отличным от интуитивных классических представлений образом. На заре квантовой эпохи осмысление этого факта породило множество парадоксов, начиная с парадокса Эйнштейна–Подольского–Розена и знаменитого ни живого, ни мертвого кота Шредингера [1, 2, 3]. В конце двадцатого века, с развитием техники эксперимента, когда управление квантовой когерентностью стало реальным, прагматичность мышления изменила подходы, поставив вопросы практического применения квантовой нелокальности. Наступило время решать задачи квантовой теории коммуникаций и создать квантовый компьютер [4].

Отличие квантовых корреляций от классических имеет прозрачную математическую основу. Ее можно сформулировать уже на примере базовых состояний классического и квантового компьютера; битов и кубитов. В то время, как два произвольных n-битовых состояний могут быть переведены одно в другое так называемым "локальным" действием на однобитовые состояния, в квантовом случае это верно лишь для одного кубита. Иными словами, действие "локальных" преобразований перестает быть *транзитивным* для многокубитных систем [5, 6]. Действием локальных преобразований пространство состояний квантовой системы разбивается на классы эквивалентности, причем каждый класс характеризуется определенными свойствами нелокальности [7]. Таким образом, проблема классификации нелокальности в системе n-кубитов сводится к математической задаче описания пространства орбит действия "локальной" группы преобразований пространства состояний [8, 9]. Это пространство орбит, $\mathcal{E}_n$, получило в англоязычной литературе название "*entanglement*

Ключевые слова : полиномиальные инварианты, пространство перепутанности, разложение Хиронаки.

space” – пространство перепутанности (сцепленности) [5, 6]. Математическим аппаратом, применяемым для его характеристики стала классическая теория инвариантов (см. например [10, 11]). В то время как элементами пространства состояний являются матрицы плотности, для отделения орбит, т.е. координатизации пространства $\mathcal{E}_n$, могут быть использованы соответствующие “локально” инвариантные полиномы от элементов матрицы плотности. Пространство сцепленности имеет крайне нетривиальную структуру, как геометрическую так и топологическую [6, 12]. Причем с ростом числа кубитов сложность $\mathcal{E}_n$ резко возрастает. Однако, для простейшей системы 2-кубитов, подход основанный на теории инвариантов, позволяет получить ряд важных алгебраических результатов, проясняющих свойства $\mathcal{E}_2$ [9, 13, 14].

Описание пространства $\mathcal{E}_n$ усложняется еще одним обстоятельством. В силу требований физического характера матрица плотности должна быть неотрицательно определенной [15, 16, 17]. Это означает, что пространство действия группы не есть линейное пространство, как это обычно считается в теории инвариантов, а представляет собой полу-алгебраическое многообразие $\mathfrak{P}_+$. Поэтому применяя классическую теорию инвариантов для описания пространства орбит следует учитывать это обстоятельство. В данной работе задача учета полуалгебраичности многообразия действия локальной группы будет решаться на примере системы двух кубитов. Мы сформулируем условие неотрицательности оператора плотности в виде алгебраическх неравенств от $\mathrm{SU}(2)\otimes SU(2)$ инвариантов, определяющих пространство $\mathfrak{P}_+$ и приведем базис кольца инвариантов $\mathbb{C}[\,\mathfrak{P}_+\,]^{\mathrm{SU}(2)\otimes SU(2)}$, который содержит минимальное число инвариантов, связанных необходимыми неравенствами.

Наш план изложения следующий. Мы начнем в параграфах 2 и 3 с краткого обзора необходимых понятий из квантовой механики в контексте характеристики квантовой сцепленности в терминах теории классических инвариантов. Затем в третьем параграфе выводится система неравенств от операторов Казимира обертывающей алгебры su(4). С учетом этих ограничений в четвертом параграфе будет предъявлен базис кольца локальных инвариантов $\mathbb{C}[\,\mathfrak{P}_+\,]^{\mathrm{SU}(2)\otimes SU(2)}$.

1. Пространство состояний

Наиболее общее состояние n-уровневой квантовой системы, *смешанное состояние*, задается $n \times n$ комплексной матрицей, матрицей плотности ϱ, [15, 16][1] удовлетворяющей следующим условиям:

i. *эрмитовости* – $\varrho = \varrho^+$,
ii. *иметь конечный след* – $\mathrm{Tr}(\varrho) = 1$,
iii. *должна быть неотрицательно определена.*

Таким образом пространство смешанных состояний квантовой n-уровневой системы представляет собой подпространство $\mathfrak{P}_+$, пространства эрмитовых $n\times n$ матриц. Прежде, чем дать характеристику этого пространства начнем с простейшей двухуровневой системы.

1.1. Кубит

В квантовой теории информации выделенное положение занимает двухуровневая квантовая система, которая независимо от конкретной физической реализации носит унифицированное название – *кубит*. Состояние кубита дается в виде матрицы плотности, совпадающей со стандартной матрицей плотности нерелятивистского спина-1/2

$$\varrho = \frac{1}{2}\left(1 + \boldsymbol{\alpha}\cdot\boldsymbol{\sigma}\right), \tag{1.1}$$

где $\boldsymbol{\sigma}$ – набор матриц Паули[2] и $\boldsymbol{\alpha}$ дается математическим ожиданием $\langle\boldsymbol{\sigma}\rangle$, определенным в виде

$$\boldsymbol{\alpha} = \mathrm{Tr}\left(\boldsymbol{\sigma}\varrho\right),$$

В представлении (1.1) требования (i.) и (ii.) учтены в самой конструкции, а условие (iii.) ограничивает пространство параметров единичным шаром

$$\boldsymbol{\alpha}^2 \leq 1, \tag{1.2}$$

в то время как для чистых состояний кубита ожидание $\boldsymbol{\alpha}$ описывает 2-сферу Блоха

$$\boldsymbol{\alpha}^2 = 1. \tag{1.3}$$

1.2. Кудит

[1] При этом специальный класс идемпотентных матриц плотности $\varrho^2 = \rho$, соответствует так называемым *чистым состояниям*, описание которых сводятся к использованию лучей в гильбертовом пространстве. Смешанное состояние является смесью чистых состояний.

[2] Явный вид матриц Паули дается формулами (4.24), приведенными в параграфе 4.

Аналогично состоянию кубита вводится понятие “*кудита*” – состояния d – уровневой системы. Обобщение представления (1.1) на случай кудита имеет вид [18]

$$\varrho = \frac{1}{d}\left(\mathbb{I}_d + \sqrt{\frac{d(d-1)}{2}}\,\boldsymbol{\xi}\cdot\boldsymbol{\lambda}\right) \tag{1.4}$$

с (d^2-1)-мерным вектором Блоха $\boldsymbol{\xi} = \langle\boldsymbol{\lambda}\rangle \in \mathbb{R}^{d^2-1}$. В разложении (1.4) компоненты вектора $\boldsymbol{\lambda} = (\lambda_1, \lambda_2, \dots, \lambda_{d^2-1})$ представляют собой базис алгебры $\mathrm{su}(d)$, нормированный условием

$$\lambda_i\lambda_j = \frac{2}{d}\delta_{ij}\mathbb{I}_d + (d_{ijk} + i\,f_{ijk})\lambda_k,$$

δ_{ij} – символ Кронекера. d_{ijk} и f_{ijk} – структурные константы алгебры, полностью симметричные и антисимметричные, соответственно:

$$d_{abc} = \frac{1}{4}\,\mathrm{Tr}(\{\lambda_a,\lambda_b\}\lambda_c), \quad f_{abc} = -\frac{i}{4}\,\mathrm{Tr}([\lambda_a,\lambda_b]\lambda_c),$$

где

$$\{\lambda_a,\lambda_b\} = \lambda_a\lambda_b + \lambda_b\lambda_a, \quad [\lambda_a,\lambda_b] = \lambda_a\lambda_b - \lambda_b\lambda_a.$$

Как и в случае кубита, свойства (i.) и (ii.) матрицы плотности кудита уже учтены в декомпозиции (1.4). Однако требование неотрицательности (iii.) накладыает на вектор Блоха более изощренные чем (1.2) ограничения. Полная характеристика пространства вектора Блоха, $\mathbf{B}(\mathbb{R}^{d^2-1})$, в случае кудита произвольной размерности является открытой проблемой. Известны некоторые общие свойства этого множества, в частности, можно показать, что $\mathbf{B}(\mathbb{R}^{d^2-1})$ представляет собой выпуклое подмножество единичного d^2-1-мерного шара

$$\boldsymbol{\xi}^2 \le 1, \tag{1.5}$$

причем все чистые состояния сосредоточены на его поверхности. Более точно, чистые состояния кудита определяются уравнением

$$\boldsymbol{\xi}^2 = 1, \quad \boldsymbol{\xi}\vee\boldsymbol{\xi} = \boldsymbol{\xi}, \tag{1.6}$$

где

$$(\boldsymbol{\xi}\vee\boldsymbol{\xi})_k := \sqrt{\frac{d(d-1)}{2}}\,\frac{1}{d-2}\,d_{ijk}\xi_i\xi_j.$$

1.3. Композиционные состояния

С точки зрения квантовой теории информации наибольший интерес представляют многокудитные композиционные состояния. Согласно постулату квантовой теории о составных системах [4], пространство системы, полученной объединением систем A и B, описываемых гильбертовыми пространствами $\mathcal{H}_A$ и $\mathcal{H}_B$, является подпространством их тензорного произведения

$$\mathcal{H} \subset \mathcal{H}_A \otimes \mathcal{H}_B. \tag{1.7}$$

Тензорное произведение в (1.7) в сочетании с *принципом суперпозиции* являются источником возникновения корреляций в объединенной системе, которые *не имеют классического аналога.* Если смешанное состояние ϱ, составленное из систем A и B может быть представлено (не обязательно единственным образом) как выпуклое множество произведений состояний [7]

$$\varrho = \sum_{j=1}^{M} \omega_j\, \varrho_i^A \otimes \varrho_i^B, \quad \omega_i > 0, \quad \sum_{i=1}^{M} \omega_i = 1, \tag{1.8}$$

индивидуальных матриц подсистем, ϱ_i^A и ϱ_i^B, то состояние называется *сепарабельным* [7]. Для таких состояний связи между подсистемами соответствуют классически мыслимым корреляциям. Но состояния (1.8) далеко не исчерпывают возможных состояний составной системы. Состояния, не представимые в виде (1.8), называются *запутанными или сцепленными (entangled).*

Общий вид матрицы плотности объединенной системы r-дита и s-дита удобно записывать в так называемой форме Фано [19, 20]

$$\varrho = \frac{1}{rs}\left(\mathbb{I}_{rs} + \sum_{i=1}^{r^2-1} a_i\, \lambda_i \otimes \mathbb{I}_s + \sum_{i=1}^{s^2-1} b_i\, \mathbb{I}_r \otimes \tau_i + \sum_{i=1}^{r^2-1}\sum_{j=1}^{s^2-1} c_{ij} \lambda_i \otimes \tau_j\right), \tag{1.9}$$

В (1.9) матрицы λ_i и τ_i образуют базисы в алгебре $\mathrm{su}(r)$ и $\mathrm{su}(s)$ соответственно. Вещественную матрицу $C = ||c_{ij}||$ размера $(r^2-1)\times(s^2-1)$ принято называть *корреляционной матрицей.* Смысл параметров $\boldsymbol{a} = (a_1, \dots, a_{r^2-1})$ и $\boldsymbol{b} = (b_1, \dots, b_{s^2-1})$ становится ясным если выполнить операцию частичного взятия следа [5] по состояниям одной из подсистем

$$\varrho^{(A)} := \mathrm{Tr}_B(\varrho) = \frac{1}{r}(\mathbb{I}_r + \boldsymbol{a}\cdot\boldsymbol{\lambda}), \quad \varrho^{(B)} := \mathrm{Tr}_A(\varrho) = \frac{1}{s}(\mathbb{I}_s + \boldsymbol{b}\cdot\boldsymbol{\tau}). \tag{1.10}$$

Векторы $\boldsymbol{a}$ и $\boldsymbol{b}$ соответствуют блоховским векторам подсистем, описываемых матрицами $\varrho^{(A)}$ и $\varrho^{(B)}$ соответственно.

Свойство зацепленности матрицы плотности (1.9) и более общих многокудитных систем может быть сформулировано в терминах инвариантов связанных с действием так называемой локальной группы [9]. В следующем пункте будут приведены соответствующие определения.

2. Пространство сцепленности

2.1. Локальная инвариантность

На пространстве матриц плотности N-уровневой квантовой системы существует отношение эквивалентности порожденное присоединенным действием группы $\mathrm{SU}(n)$

$$\varrho \quad \rightarrow \quad \varrho' = U^{\dagger} \varrho U. \tag{2.11}$$

В системе, полученной объединение r-подсистем, каждая из которых имеет соответственно $n_1, n_2, \ldots, n_r$ уровней, нелокальные свойства определяются соответствующим разбиением операторов действия (2.11). Из всех унитарных действий выделяется так называемая группа *локальных унитарных преобразований* (Local Unitary Transformations (LUT))

$$\mathrm{SU}(n_1) \otimes \mathrm{SU}(n_2) \otimes \cdots \otimes \mathrm{SU}(n_r), \tag{2.12}$$

действующих независимо на операторы плотности каждой из подсистем

$$\varrho^{(n_i)} \quad \rightarrow \quad \varrho^{(n_i)\,\prime} = g^{\dagger} \varrho^{(n_i)}\, g \quad g \in SU(n_i), \quad i = 1, 2, \ldots, r. \tag{2.13}$$

Оставшиеся преобразования

$$\frac{\mathrm{SU}(n)}{\mathrm{SU}(n_1) \otimes \mathrm{SU}(n_2) \otimes \cdots \otimes \mathrm{SU}(n_r)}, \quad n = n_1 \cdots n_r \tag{2.14}$$

принадлежат классу нелокальных преобразований. Два состояния, связанные преобразованием из группы LUT имеют одинаковые нелокальные свойства.

Как было отмечено во Введении, действие группы локальных преобразований на пространстве матриц плотности не является транзитивным. Поэтому эквивалентность состояний на основе действия (2.12) приводит к разбиению пространства матриц плотности на соответствующие классы (орбиты). Объединение этих классов, т.е., пространство орбит, принято называть пространством сцепленности, $\mathcal{E}_n$.

2.2. Пространство орбит и локальные полиномиальные инварианты

Мотивом исследования геометрии $\mathcal{E}_n$ является необходимость выработки качественных критериев и определения количественных мер степени нелокальности [6, 12]. Каноническим методом изучения пространства орбит $\mathcal{E}_n$ является теория инвариантов [11]. Начиная с работ [9], в этом направлении был получен ряд интересных результатов, проясняющих математическое содержание явления сцепленности. Наибольший прогресс был достигнут для чистых состояний. Здесь, в качестве примера, можно привести построение рядов Гильберта для многочастичных систем кубитов [21] и классификацию чистых сцепленных состояний на основе теории гипердетерминантов [22].

Анализ пространства орбит в случае смешанных состояний носит значительно более сложный характер. Общие вопросы построения базиса кольца локальных инвариантов для смешанных состояний были рассмотрены в работах [13, 14]. С этой целью использовались и алгоритмические методы компьютерной алгебры [23], [24][3]

Согласно теории инвариантов [11] кольцо полиномиальных инвариантов $\mathbb{C}[V]^G$ линейного пространства V над полем комплексных чисел $\mathbb{C}$ относительно действия группы G является градуированной алгеброй

$$\mathbb{C}[V]^G = \bigoplus_{k=1}^{\infty} A_k,$$

где A_k есть пространство однородных инвариантных многочленов степени k. Специальные унитарные группы Ли $\mathrm{SU}(n)$ принадлежат к

[3]К сожалению, надо отметить, что применение существующих алгоритмических методов, в том числе техники базисов Гребнера [25], для анализа кольца инвариантов многокудитовых систем оказывается, вычислительно, мало эффективным ввиду резкого возрастания числа требуемых алгебраических операций с ростом числа кудитов.

редуктивным алгебраическим группам. Их кольцо инвариантов является конечно порожденным [11], а $\mathbb{C}[V]^G$ является алгеброй Коэна–Маколея [26]. Однако непосредственное применение этой конструкции к задачам квантовой сцепленности осложнено тем, что в данном случае пространство V, на котором определено действие группы G не является линейным пространством. Как отмечалось во введении в силу физических требований матрица плотности должна быть неотрицательно определенной и поэтому пространство представления является нелинейным, полуалгебраическим многообразием.

Для данной проблемы предлагается следующее решение, Поясним его на примере пары кубитов. Начнем с построения кольца инвариантов $\mathbb{C}[\,\mathcal{H}_{4\times 4}\,]^{\mathrm{SU}(2)\otimes\mathrm{SU}(2)}$ для присоединенного действия на пространстве 4×4 эрмитовых матриц $\mathcal{H}_{4\times 4}$. Для определения интересующего нас кольца, $\mathbb{C}[\,\mathfrak{P}_+\,]^{\mathrm{SU}(2)\otimes\mathrm{SU}(2)}$, заметим, что пространство неотрицательно определенных матриц $\mathfrak{P}_+$ есть инвариантное подпространство $\mathcal{H}_{4\times 4}$ относительно действия группы $\mathrm{SU}(4)$. Как показано ниже, данное подмножество $\mathfrak{P}_+$ может быть представлено в виде набора полиномиальных неравенств[4]

$$P_a(\mathfrak{C}_2,\mathfrak{C}_3,\mathfrak{C}_4)\geq 0,\quad a=1,2,3 \tag{2.15}$$

от трех инвариантов группы $\mathrm{SU}(4)$. С другой стороны поскольку $\mathfrak{C}_2,\mathfrak{C}_3,\mathfrak{C}_4$ одновременно являются и инвариантами группы $\mathrm{SU}(2)\otimes\mathrm{SU}(2)$, то в $\mathbb{C}[\,\mathcal{H}_{4\times 4}\,]^{\mathrm{SU}(2)\otimes\mathrm{SU}(2)}$ можно построить базис, который включает эти инварианты. Тем самым, имея этот базис и учитывая неравенства (2.15), интересующее нас кольцо $\mathbb{C}[\,\mathfrak{P}_+\,]^{\mathrm{SU}(2)\otimes\mathrm{SU}(2)}$ оказывается полностью охарактеризованым.

Согласно анализу, изложенному в последующих параграфах данной работы, базис кольца может быть выбран так, что лишь первичные инварианты степени 2, 3 и один вторичный инвариант степени 4 в разложении Хиронаки [11] оказываются связанными полиномиальными ограничениями типа (2.15).

3. Неотрицательность оператора плотности

Для выполнения нашей программы построения оптимального однородного базиса кольца $\mathbb{C}[\,\mathfrak{P}_+\,]^{\mathrm{SU}(2)\otimes\mathrm{SU}(2)}$ начнем с требования неотрицательности матрицы плотности. Это условие будет представлено в

[4]Наиболее близкую, к изложенной здесь, формулировку пространства $\mathfrak{P}_+$ можно найти в [27, 28, 29].

форме неравенств, ограничивающих значения инвариантов присоединенного действия группы $\mathrm{SU}(n)$, действующей в $\mathfrak{P}_+$.

3.1 Пространство $\mathfrak{P}_+$ в терминах операторов Казимира $\mathrm{SU}(n)$

Эрмитов оператор тогда и только тогда является неотрицательно определенным, если все его характеристические числа неотрицательны. Условие неотрицательности характеристических чисел для эрмитового оператора может быть сформулировано в терминах коэффициентов характеристического уравнения:

$$|\mathbb{I}_n\, x - \varrho| = x^n - S_1 x^{n-1} + S_2 x^{n-2} - \ldots + (-1)^n S_n = 0. \tag{3.16}$$

Коэффициенты S_k в уравнении (3.16) есть суммы главных миноров k-го порядка:

$$S_k = \sum_{1\leq i_1<\ldots<i_k\leq n} \varrho \begin{pmatrix} i_1 & \ldots & i_k \\ i_1 & \ldots & i_k \end{pmatrix}, \quad k = 1, \ldots, n.$$

Поскольку оператор ϱ эрмитов, все его характеристические числа вещественны. Если они неотрицательны, то все S_k также неотрицательны так как они являются симметрическими функциями корней x_k характеристического уравнения

$$S_k = \sum_{1\leq i_1\leq\ldots\leq i_k\leq n} \prod_{j=1}^{k} x_{i_j}\,.$$

Однако верно также и обратное утверждение: из неотрицательности S_k следует неотрицательность x_k. Доказательство этого наблюдения [27] следует из теоремы Декарта [30], согласно которой число положительных корней (с учетом их кратностей) равно числу перемен знака в последовательности коэффициентов в уравнении (3.16).

Таким образом, неотрицательность матрицы плотности может быть записана в инвариантном виде как условие неотрицательности коэффициентов ее характеристического уравнения

$$S_k \geq 0, \quad k = 1, \ldots, n. \tag{3.17}$$

Приведем явный вид нескольких первых коэффициентов S_k, в терминах n-мерного блоховского вектора $\boldsymbol{\xi}$ [27, 28]:

$$
\begin{aligned}
S_2 &= \frac{1}{2!}\frac{n-1}{n}(1-\boldsymbol{\xi}\cdot\boldsymbol{\xi}),\\
S_3 &= \frac{1}{3!}\frac{(n-1)(n-2)}{n^2}(1-3\,\boldsymbol{\xi}\cdot\boldsymbol{\xi}+2\,(\boldsymbol{\xi}\vee\boldsymbol{\xi})\cdot\boldsymbol{\xi}),\\
S_4 &= \frac{1}{4!}\frac{(n-1)(n-2)(n-3)}{n^3}(1-6\,\boldsymbol{\xi}\cdot\boldsymbol{\xi}+8\,(\boldsymbol{\xi}\vee\boldsymbol{\xi})\cdot\boldsymbol{\xi}\\
&\quad+3\frac{n-1}{n-3}(\boldsymbol{\xi}\cdot\boldsymbol{\xi})^2-6\frac{n-2}{n-3}(\boldsymbol{\xi}\vee\boldsymbol{\xi})\cdot(\boldsymbol{\xi}\vee\boldsymbol{\xi})).
\end{aligned}
$$

Кроме ограничения снизу для коэффициентов S_k существует и ограничение сверху, вытекающее из условий нормировки $\mathrm{Tr}(\varrho) = 1$, $\mathrm{Tr}(\varrho^k) \le 1$, при $k \ge 2$, причем знак равенства соответствует случаю чистых состояний. Максимальные значения S_k достигаются при равных собственных значениях x_i оператора плотности.

Окончательно, условия неотрицательности и нормированности оператора плотности n-уровневой смешанной системы записываются в форме следующих неравенств

$$
0 \le \frac{k!\,n^{k-1}}{(n-1)(n-2)\dots(n-k+1)}\,S_k \le 1, \qquad k=2,\dots,n. \tag{3.18}
$$

Коэффициенты характеристического уравнения S_k, $k = 1,\dots,n$ являются инвариантами относительно присоединенного действия группы $\mathrm{SU}(n)$, они алгебраически независимы и могут быть представлены в виде полиномов от операторов Казимира группы $\mathrm{SU}(n)$.

Ниже мы рассмотрим случай четырехуровневой системы, связанный с интересующей нас 2-кубитной системой, и перепишем ограничения (3.18) непосредственно в терминах операторов Казимира обертывающей алгебры $\mathrm{su}(4)$.

3.2. Ограничения на инварианты $\mathrm{su}(4)$

Группа $SU(4)$ имеет три оператора Казимира, которые в компонентах 15-мерного вектора Блоха $\boldsymbol{\xi}$ (см, разложение матрицы плотности (1.4) записываются следующим образом

$$
\mathfrak{C}_2 = \boldsymbol{\xi}\cdot\boldsymbol{\xi}, \tag{3.19}
$$

$$
\mathfrak{C}_3 = \boldsymbol{\xi}\vee\boldsymbol{\xi}\cdot\boldsymbol{\xi}, \tag{3.20}
$$

$$
\mathfrak{C}_4 = \boldsymbol{\xi}\vee\boldsymbol{\xi}\cdot\boldsymbol{\xi}\vee\boldsymbol{\xi}. \tag{3.21}
$$

Поскольку соответствующие коэффициенты S_2, S_3, S_4 выражаются через операторы Казимира

$$\begin{aligned} S_2 &= \frac{3}{8}(1-\mathfrak{C}_2),\\ S_3 &= \frac{1}{16}(1-3\mathfrak{C}_2+2\mathfrak{C}_3),\\ S_4 &= \frac{1}{256}((1-3\mathfrak{C}_2)^2+8\mathfrak{C}_3-12\mathfrak{C}_4), \end{aligned}$$

то система (3.18) для 4-х уровневой системы может быть записана в виде следующих ограничений на SU(4) инварианты

$$\begin{aligned} &0 \le \mathfrak{C}_2 \le 1\\ &0 \le 3\mathfrak{C}_2 - 2\mathfrak{C}_3 \le 1,\\ &0 \le (1-3\mathfrak{C}_2)^2 + 8\mathfrak{C}_3 - 12\mathfrak{C}_4 \le 1. \end{aligned} \tag{3.22}$$

Неравенства (3.22) выделяют в пространстве инвариантов $\mathfrak{C}_2, \mathfrak{C}_3, \mathfrak{C}_4$ ограниченную область, изображенную на рисунке 1.

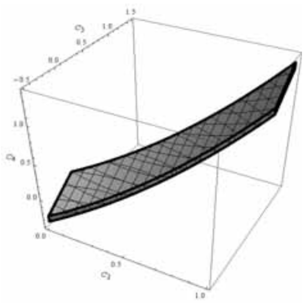

Рис. 1. Область допустимых значений операторов Казимира $\mathfrak{C}_2, \mathfrak{C}_3, \mathfrak{C}_4$.

4. Кольцо локальных инвариантов $\mathbb{C}[\mathfrak{P}_+]^{\mathrm{SU}(2)\otimes SU(2)}$

Пусть матрица плотности двух кубитов параметризована в форме Фано [18, 19]:

$$\varrho = \frac{1}{4}\left[\mathbb{I}_2\otimes\mathbb{I}_2 + \boldsymbol{a}\cdot\boldsymbol{\sigma}\otimes\mathbb{I}_2 + \mathbb{I}_2\otimes\boldsymbol{b}\cdot\boldsymbol{\sigma} + c_{ij}\,\sigma_i\otimes\sigma_j\right], \tag{4.23}$$

где трех-компонентные векторы $\boldsymbol{a} = (a_1, a_2, a_3)$ и $\boldsymbol{b} = (b_1, b_2, b_3)$ являются блоховскими векторами индивидуальных кубитов, σ_i, $i = 1, 2, 3$ – матрицы Паули образующие базис алгебры su(2):

$$\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{4.24}$$

Корреляционная матрица C пары кубитов имеет 9 элементов c_{ij}, $i, j = 1, 2, 3$.

Следуя намеченной в пункте 2.2 программе, на первом этапе построения кольца инвариантов $\mathbb{C}[\mathfrak{P}]^{\mathrm{SU}(2)\otimes \mathrm{SU}(2)}$ мы не будем накладывать ограничений на параметры $\boldsymbol{a}, \boldsymbol{b}$ и C, следующих из условия неотрицательности матрицы плотности, а отождествим пространство параметров с $\mathbb{R}^{15}$. Вместе с этим мы линеаризуем присоединенное действие (2.13) локальной группы $\mathrm{SU}(2) \otimes \mathrm{SU}(2)$

$$V_A \ \to \ V'_A = L_{AB} V_B \quad A, B = 1, \dots, 15, \tag{4.25}$$

с 15×15 матрицей $L \in \mathrm{SU}(2) \otimes \mathrm{SU}(2) \otimes \overline{\mathrm{SU}(2) \otimes \mathrm{SU}(2)}$.

Таким образом, предварительная задача состоит в построении кольца инвариантов линейного действия группы $\mathrm{SU}(2) \otimes \mathrm{SU}(2) \otimes \overline{\mathrm{SU}(2) \otimes \mathrm{SU}(2)}$ в линейном пространстве $\mathbb{R}^{15}$. Линеаризация действия позволяет воспользоваться подсказкой о структуре кольца, следующей из формулы Молина для производящей функции инвариантов представления π_G компактной группы G [24]:

$$M(q) = \int\limits_G \mathrm{d}\,\mu_G \, \frac{1}{\det || \,\mathrm{id} - q\pi_G ||}, \tag{4.26}$$

где интеграл берется по группе с мерой Хаара $\mathrm{d}\,\mu_G$.

Функция Молина позволяет извлечь следующую информацию о структуре кольца инвариантов. Во-первых, ее формальное разложение по степеням параметра q, так называемый ряд Гильберта–Пуанкаре:

$$M(q) = \sum_{k \geq 0} d_k q^k \ \in \ \mathbb{Z}[q],$$

говорит о размерности, d_k, пространства однородных инвариантов порядка k. Во-вторых, эта функция, будучи рациональной, допускает (не единственным образом !) при $q < 1$, представление в виде

$$M(q) = \frac{\sum\limits_{k=0}^{r} q^{\deg J_k}}{\Pi_{m=1}^{n}(1 - q^{\deg K_m})},$$

Согласно которому можно судить о числе и порядке *первичных* $K_i,\ i = 1, 2, \dots , n$, и *вторичных* $J_i,\ i = 1, 2, \dots , r$, инвариантов алгебры Коэна–Маколея

$$\mathbb{C}[V]^G = \bigoplus_{k=0}^{r} J_k\, \mathbb{C}[K_1, K_2, \dots , K_n].$$

Как показывают расчеты, для смешанного состояния двух кубитов функция Молина может быть записана в виде [13, 14]:

$$M(q) = \frac{1 + q^4 + q^5 + 3q^6 + 2q^7 + 2q^8 + 3q^9 + q^{10} + +q^{11} + q^{15}}{(1 - q)(1 - q^2)^3(1 - q^3)^2(1 - q^4)^3(1 - q^6)}, \quad (4.28)$$

Согласно результату (4.28), базис кольца состоит из 10 *первичных инвариантов* степени $1, 2, 2, 2, 3, 3, 4, 4, 4, 6$ и 15 *вторичных инвариантов* степени $4, 5, 6, 6, 6, 7, 7, 8, 8, 10, 11, 15$.

Еще более подробная информация о зависимости инвариантов от коэффициентов разложения матрицы плотности (4.23) может быть извлечена с помощью так называемых много-параметрических производящих функций [24]. В этом случае производящая функция $F(a, b, c)$ зависит не от одного параметра q, а от трех, поскольку теперь вклад в формулу Молина от каждой из переменной $\boldsymbol{a}, \boldsymbol{b}$ и c_{ij} входит с весом, задаваемым независимым параметрами, a, b и c соответственно. Интересно, что производящая функция $F(a, b, c)$ была построена уже в середине 70-х годов [31, 32], в связи с так называемой проблемой “*недостающего индекса*,” возникшей при классификации спектров ядер (соответствующую математическую формулировку проблемы и ее решение см., например, в [31]).

Далее в изложении мы будем в основном следовать указанной работе. Рассмотрим пространство всех многочленов от 15-ти переменных $a_i, b_i, c_{ij}\ i, j = 1, 2, 3,$. В силу присоединенного действия группы локальных преобразований, пространство параметров Блоха разбивается на неприводимые представления группы $SO(3) \otimes SO(3)$. Точнее, переменные a_i, b_i и c_{ij} преобразуются по неприводимым представлениям $D_1 \times D_0, D_0 \times D_1, D_1 \times D_1$, соответственно. Подпространство $P_{s,t,q}[a_i, b_i, c_{ij}]$ однородных многочленов степеней s, t, q от переменных a_i, b_i, c_{ij} инвариантно относительно действия $\mathrm{SU}(3) \otimes \mathrm{SU}(3)$. Поэтому инварианты могут быть классифицированы в терминах степеней однородности переменных, $C^{(s\,t\,q)}$.

Введем следующие набор инвариантов, следуя конструкции, предложенной в работе [32]:[5]

3 инварианта 2-го порядка

$$C^{(002)} = c_{ij}c_{ij}, \quad C^{(200)} = a_i a_i, \quad C^{(020)} = b_i b_i, \tag{4.29}$$

2 инварианта 3-го порядка

$$C^{(003)} = \frac{1}{3!}\epsilon_{ijk}\epsilon_{\alpha\beta\gamma}c_{i\alpha}c_{j\beta}c_{k\gamma}, \quad C^{(111)} = a_i c_{ij} b_j, \tag{4.30}$$

4 инварианта 4-го порядка

$$C^{(004)} = c_{i\alpha}c_{i\beta}c_{j\alpha}c_{j\beta}, \tag{4.31}$$

$$C^{(202)} = a_i a_j c_{i\alpha}c_{j\alpha}, \tag{4.32}$$

$$C^{(022)} = b_\alpha b_\beta c_{i\alpha}c_{i\beta}, \tag{4.33}$$

$$C^{(112)} = \epsilon_{ijk}\epsilon_{\alpha\beta\gamma}a_i b_\alpha c_{j\beta}c_{k\gamma} \tag{4.34}$$

1 инвариант 5-го порядка

$$C^{(113)} = a_i c_{i\alpha}c_{\beta\alpha}c_{\beta j}b_j, \tag{4.35}$$

4 инварианта 6-го порядка

$$C^{(123)} = \epsilon_{ijk}b_i c_{\alpha j}a_\alpha c_{\beta k}c_{\beta l}b_l, \tag{4.36}$$

$$C^{(204)} = a_i c_{i\alpha}c_{j\alpha}c_{j\beta}c_{k\beta}a_k, \tag{4.37}$$

$$C^{(024)} = b_i c_{\alpha i}c_{\alpha j}c_{\beta j}c_{\beta,k}b_k, \tag{4.38}$$

$$C^{(213)} = \epsilon_{\alpha\beta\gamma}a_\alpha c_{\beta i}b_i c_{\gamma j}c_{\delta j}a_\delta, \tag{4.39}$$

[5]Во всех нижеприведенных выражениях подразумевается суммирование по повторяющимся индексам от одного до трех.

2 инварианта 7-го порядка

$$C^{(214)} = \epsilon_{ijk} b_i c_{\alpha j} a_\alpha c_{\beta k} c_{\beta l} c_{\gamma l} a_l, \tag{4.40}$$

$$C^{(124)} = \epsilon_{\alpha\beta\gamma} a_\alpha c_{\beta j} b_j c_{\gamma k} c_{\delta k} c_{\delta l} b_l, \tag{4.41}$$

2 инварианта 8-го порядка

$$C^{(125)} = \epsilon_{ijk} b_i c_{\alpha j} c_{\alpha l} b_l c_{\beta k} c_{\beta m} c_{\gamma m} a_\gamma, \tag{4.42}$$

$$C^{(215)} = \epsilon_{\alpha\beta\gamma} a_\alpha c_{\beta i} c_{\delta i} a_\delta c_{\gamma k} c_{\varrho k} c_{\varrho l} b_l, \tag{4.43}$$

2 инварианта 9-го порядка

$$C^{(306)} = \epsilon_{\alpha\beta\gamma} a_\alpha c_{\beta i} c_{\delta i} a_\delta c_{\gamma j} c_{\varrho j} c_{\varrho k} c_{\sigma k} a_\sigma, \tag{4.44}$$

$$C^{(036)} = \epsilon_{ijk} b_i c_{\alpha j} c_{\alpha l} b_l c_{\beta k} c_{\beta m} c_{\gamma m} c_{\gamma s} b_s, \tag{4.45}$$

Из данных инвариантов и будет сформирован базис кольца

$$\mathbb{C}[\,\mathfrak{P}_+\,]^{\mathrm{SU}(2)\otimes \mathrm{SU}(2)}.$$

Одним из критериев его построения мы выбираем принцип, согласно которому минимальное число элементов базиса входит в определяющие уравнения пространства $\mathfrak{P}_+$. Поскольку пространство $\mathfrak{P}_+$ задается значениями операторов Казимира группы SU(4) (3.19)–(3.21), найдем их разложение по инвариантам (4.29)–(4.34):

$$\mathfrak{C}_2 = \frac{1}{3}\,(C^{(200)} + C^{(020)} + C^{(002)}), \tag{4.46}$$

$$\mathfrak{C}_3 = C^{(111)} - C^{(003)}, \tag{4.47}$$

$$\mathfrak{C}_4 = \frac{1}{6}\,[2(C^{(200)}C^{(020)} + C^{(202)} + C^{(022)} - C^{(112)}) + (C^{(002)})^2 - C^{(004)}]. \tag{4.48}$$

Из уравнений (4.46)–(4.48), следует, что операторы Казимира $\mathfrak{C}_2$, $\mathfrak{C}_3$, $\mathfrak{C}_4$ можно рассматривать в качестве базисных инвариантов вместо инвариантов $C^{(002)}$, $C^{(003)}$ и $C^{(112)}$.

Имея в виду это наблюдение и используя результаты работы [14], в которой было построено кольцо $\mathbb{C}[\mathbb{R}^{16}]^{\mathrm{SU}(2)\otimes SU(2)}$, определим следующий набор, состоящий из 10 *первичных инвариантов*, включая операторы Казимира $\mathfrak{C}_2, \mathfrak{C}_3$,

$$\deg = 4, \quad K_1 = 1, \tag{4.49}$$
$$\deg = 2, \quad K_2 = \mathfrak{C}_2, \qquad K_3 = C^{(200)}, \quad K_4 = C^{(020)}, \tag{4.50}$$
$$\deg = 3, \quad K_5 = \mathfrak{C}_3, \qquad K_6 = C^{(111)}, \tag{4.51}$$
$$\deg = 4, \quad K_7 = C^{(004)}, \qquad K_8 = C^{(202)}, \quad K_9 = C^{(022)}, \tag{4.52}$$
$$\deg = 6, \quad K_{10} = C^{(204)} + C^{(024)}, \tag{4.53}$$

и 15 *вторичных инвариантов* с оператором Казимира $\mathfrak{C}_4$

$$\deg = 4, \quad J_1 = \mathfrak{C}_4, \tag{4.54}$$
$$\deg = 5, \quad J_2 = C^{(113)}, \tag{4.55}$$
$$\deg = 6, \quad J_3 = C^{(204)} - C^{(024)}, J_8 = C^{(124)}, \quad J_9 = C^{(213)}, \tag{4.56}$$
$$\deg = 7, \quad J_{10} = C^{(214)}, \qquad J_{11} = C^{(113)} \tag{4.57}$$
$$\deg = 8, \quad J_{12} = C^{(215)}, \qquad J_{13} = C^{(125)}, \tag{4.58}$$
$$\deg = 9, \quad J_4 = J_1 J_2, \qquad J_{14} = C^{(306)}, \quad J_{15} = C^{(036)}, \tag{4.59}$$
$$\deg = 10, \quad J_5 = J_1 J_3, \tag{4.60}$$
$$\deg = 11, \quad J_6 = J_2 J_3, \tag{4.61}$$
$$\deg = 15, \quad J_7 = J_1 J_2 J_3. \tag{4.62}$$

Таким образом, заключаем, что набор однородных инвариантов (4.49)–(4.62) является базисом кольца $\mathbb{C}[\mathfrak{P}]^{\mathrm{SU}(2)\otimes\mathrm{SU}(2)}$:

$$\mathbb{C}[\mathfrak{P}_+]^{\mathrm{SU}(2)\otimes\mathrm{SU}(2)} = \bigoplus_{k=0}^{15} J_k\, \mathbb{C}[K_1, K_2, \ldots, K_{10}], \tag{4.63}$$

при условии, что два первичных инварианта K_2, K_5 и один вторичный инвариант J_1 удовлетворяют неравенствам (3.22).

5. Заключение

Фундаментальной задачей теории квантовой информации является качественная и количественная характеристика сугубо квантовых корреляций, так называемой запутанности или сцепленности квантовых состояний. Теория инвариантов дает возможность подобной характеристики соответствующего пространства сцепленности, т.е. пространства орбит действия группы локальных преобразований на пространстве состояния составных систем. В интересующем нас случае двух-кубитной системы группой локальных преобразований оператора плотности является группа $\mathrm{SU}(2) \otimes SU(2)$. Ее присоединенное действие на пространстве эрмитовых матриц с единичным следом, отождествленным с $\mathbb{R}^{15}$, задает пространство орбит общего положения

$$\mathcal{O} := \frac{\mathbb{R}^{15}}{\mathrm{SU}(2) \otimes \mathrm{SU}(2)},$$

размерности

$$\dim\, \mathcal{O} = 15 - 2 \times 3 = 9.$$

Однако, определенное таким образом множество не есть еще пространство сцепленности $\mathcal{E}_2$, поскольку из-за условия неотрицательности оператора плотности, пространство физических состояний есть $\mathfrak{P}_+ \subset \mathfrak{R}^{15}$. В настоящей работе было предложено описание пространства $\mathfrak{P}_+$ в виде полиномиальных неравенств на операторы Казимира обертывающей алгебры su(4) и показано, что эти ограничения могут быть учтены в структуре определяющего кольца, $\mathbb{C}[\,\mathfrak{P}_+\,]^{\mathrm{SU}(2)\otimes \mathrm{SU}(2)}$, путем фиксации базиса, в котором первичные инварианты степени 2, 3 и один вторичный инвариант степени 4 в разложении Хиронаки оказываются связаны полиномиальными ограничениями (3.22).

Важно отметить, что без учета неравенств (3.22), использование локальных инвариантов для "координатизации" пространства сцепленности $\mathcal{E}_2$ не является корректным. Анализ следствий из этих ограничений на геометрию пространства сцепленности $\mathcal{E}_2 \subset \mathcal{O}$ мы оставляем для последующих публикаций.

Благодарности

Настоящая работа выполнена при поддержке Российского Фонда Фундаментальных Исследований (грант No. 07-01-00660), Министерства Образования и Науки Российской Федерации (грант No. 5362.2006.2.) и Национального Фонда Науки Грузии (грант GNSF/ST08/4-405).

Литература

1. A. Einstein, B. Podolsky, and N. Rosen, *Can quantum-mechanical description of physical reality be considered complete?* — Phys. Rev. **47** (1935), 777–780.
2. J. Bell, *Speakable and Unspeakable in Quantum Mechanics.* Cambridge University Press, Cambridge (1987).
3. A. Aspect, *Bell's theorem: the naiv view of an experimentalist.* In: *Quantum [Un]speakables: From Bell to Quantum Information*, R. A. Bertlmann and A. Zeilinger (Eds.), Springer Verlag, Berlin (2002).
4. M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information.* Camridge University Press (2000); перевод: М. Нильсен, И. Чанг, *Квантовые вычисления и квантовая информация.* Мир, М. (2006).
5. V. Vedral, *Introduction to Quantum Information Science.* Oxford University Press, New York (2006).
6. I. Bengtsson and K. Źyczkowski, *Geometry of Quantum States. An Introduction to Quantum Entanglement.* Cambridge University Press, 2006.
7. R. F. Werner, *Quantum states with Einstein-Podolski-Rosen correlations admitting a hidden-variable model.* — Phys. Rev. A **40** (1989), 4277.
8. J. Schlienz and G. Mahler, *Description of entanglement.* — Phys. Rev. A **52** (1995), 4396–4404.
9. N. Linden and S. Popescu, *On multi-particle entanglement.*— Fortschr. Phys. **46** (1998), 567–578.
10. H. Weyl, *The Classical Groups: Their Invariants and Representations.* Princeton University Press (1939); перевод: Г. Вейль, *Классические группы, их инварианты и представления.* ИЛ, М. 1947.
11. V. L. Popov and E.B. Vinberg, *Invariant theory*, in Algebraic Geometry IV, Encycl. Math. Sci., Vol. 55, Springer-Verlag (1994) 123–273.
12. M. Kus and K. Zyczkowski, *Geometry of entangled states.* — Phys. Rev. A **63** (2001), 032307 [13 pages].
13. M. Grassl, M. Rötteler, and T. Beth, *Computing local invariants of qubit systems.* — Phys. Rev. A **58** (1998), 1853–1856.
14. R. C. King, T. A. Welsh, and P. D. Jarvis, *The mixed two-qubit system and the structure of its ring of local invariants.* — J. Phys. A: Math. Theor. **40** (2007), 10083–10108.
15. J. von Neumann, *Warscheinlichtkeitstheoritischer aufbau der Quantemechanik.* Göttingen Nachrichten (1927), 245–272.
16. L. D. Landau, *Das dämpfungsproblem in der Wellenmechanik.* — Zeitschrift für Physik **45** (1927), 430–441.
17. K. Blum, *Density Matrix. Theory and Applications.* Plenum Press, New York (1981). перевод: К. Блум, *Теория матрицы плотности и ее приложения.* Мир, М. (1983).
18. F. T. Hioe and J. H. Eberly, *N−Level Coherence Vector and Higher Conservation Laws in Quantum Optics and Quantum Mechanics.* — Phys. Rev. Lett. **47** (1981), 838–841.
19. U. Fano, *Description of states in quantum mechanics by density matrix and operator techniques.* — Rev. Mod. Phys. **29** (1957), 74–93.
20. U. Fano, *Pairs of two-level systems.* — Rev. Mod. Phys. **55** (1983), 855–874.

21. J.-G. Luque and J.-Y. Thibon, *The polynomial invariants of four qubits.* — Phys. Rev. A **63** (2003), 042303 [5 pages].
J.-G. Luque and J.-Y. *Thibon, Algebraic invariants of five qubits.* — J. Phys. A: Math. Gen. **39** (2005), 371–377.
22. A. Miyake, *Classification of multipartite entangled states by multidimensional determinants.* — Phys. Rev. A **67** (2003), 012108 [10 pages].
23. B. Sturmfels, *Algorithms in Invariant Theory.* Springer-Verlag, Wien (1993).
24. H. Derksen and G. Kemper, *Computational Invariant Theory.* Encyclopedia of Mathematical Sciences, vol. 130, Springer-Verlag, Berlin (2002).
25. B. Buchberger, *Gröbner bases – an algorithmic method in polynomial ideal theory.* in: N. K. Bose (ed.): *Multidimensional Systems Theory*, D. Reidel, Dordrecht (1985), 184–232; перевод в кн.: *Компьютерная алгебра. Символьные и алгебраические вычисления.* Мир, М. (1986).
26. M. Hochster and J. Roberts, *Rings of invariants of reductive groups acting on regular rings are Cohen–Macaulay.* — Advances in Mathematics **13** (1974), 125–175.
27. G. Kimura, *The Bloch vector for N-level systems.* — Phys. Lett. A **314** (2003), 339–349.
28. M. S. Byrd and N. Khaneja, *Characterization of the positivity of the density matrix in terms of the coherence vector representation.* — Phys. Rev. A **68** (2003), 062322 [13 pages].
29. S. Kryszewski and M. Zachcial, *Positivity of the $N\times N$ density matrix expressed in terms of polarization operators.* — J. Phys. A: Math. Theor. **39** (2006), 5921–5931.
30. Э. Б. Винберг, *Курс алгебры.* 3-е изд., Издательство "Факториал Пресс," М. (2002).
31. B. R. Judd, W. Miller Jr., J. Patera, and P. Winternitz, *Complete set of commuting operators and $O(3)$ scalars in the enveloping algebra of $SU(3)$.* — J. Math. Phys. **15** (1974), 1787–1799.
32. C. Quesne, *$SU(2)\otimes SU(2)$ scalars in the enveloping algebra of $SU(4)$.* — J. Math. Phys. **17** (1976), 1452–1467.

Gerdt V., Palii Yu., Khvedelidze A. On the ring of local invariants for a pair of the entangled q-bits.

The entanglement characteristics of two q-bits are encoded in the invariants of the adjoint action of the group $\mathrm{SU}(2)\otimes\mathrm{SU}(2)$ on the space of the density matrices $\mathfrak{P}_+$, i.e., space of 4×4 non-negative Hermitian matrices. The corresponding ring $\mathbb{C}[\mathfrak{P}_+]^{\mathrm{SU}(2)\otimes\mathrm{SU}(2)}$ in elements of the density matrix is studied. The special integrity basis for $\mathbb{C}[\mathfrak{P}_+]^{\mathrm{SU}(2)\otimes\mathrm{SU}(2)}$ is described and constraints on its elements due to the semi-definiteness of the density matrix are given explicitly in the form of inequalities. This basis has the property that only a minimal number of primary invariants of degree 2, 3 and one lowest degree 4 secondary invariant that appear

in the Hironaka decomposition of $\mathbb{C}[\mathfrak{P}_+]^{\mathrm{SU}(2)\otimes\mathrm{SU}(2)}$ are subject to the polynomial inequalities.

Объединенный Институт
Ядерных Исследований,
141980 Дубна, Россия

Поступило 21 сентября 2009 г.

Институт Прикладной Физики,
Академия наук Р. Молдовы,
Кишинев, MD-2028, Республика Молдова

Математический Институт им. А. М. Размадзе,
Тбилиси, GE-0193, Грузия