Math-Net.Ru

Общероссийский математический портал

Шунь-Лун Ло, Нань Ли, Шуан-Шуан Фу, О квантовости
квантовых ансамблей, *ТМФ*, 2011, том 169, номер 3, 413–
430

DOI: <https://doi.org/10.4213/tmf6738>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.210.77.194

26 апреля 2023 г., 12:15:27

© 2011 г. Шунь-Лун Ло*, Нань Ли*, Шуан-Шуан Фу*

О КВАНТОВОСТИ КВАНТОВЫХ АНСАМБЛЕЙ

Квантовые ансамбли как обобщения квантовых состояний представляют собой универсальный инструмент описания физического или информационного статуса в теории измерений и теории связи ввиду повсеместного присутствия неполной информации и необходимости кодирования классических сообщений в квантовых состояниях. Взаимосвязь между составляющими квантового ансамбля может в большей или меньшей степени проявлять квантовые черты, когда рассматриваемые квантовые состояния не коммутируют, поскольку не существует единого классического базиса, диагонализующего все эти состояния. Эта ситуация резко контрастирует с ситуацией одиночного квантового состояния, которое всегда можно привести к диагональному виду. Чтобы количественно измерять эти квантовые характеристики и, в частности, яснее понимать возможности безопасной передачи данных в квантовой криптографии, основанной на прототипичных квантовых ансамблях, введены коэффициенты качества, определяющие количество квантовости квантового ансамбля, дан обзор некоторых уже известных величин, которые можно интерпретировать как меры квантовости, и исследованы такие их фундаментальные свойства, как субаддитивность и вогнутость. Сравнение показывает, что различные меры приводят к различно упорядоченной квантовости квантовых ансамблей. Это дает возможность до некоторой степени понять весьма трудноуловимую и сложную природу квантовых ансамблей и показывает, что не существует единой меры, позволяющей описать все фундаментальные и тонкие свойства квантовости.

Ключевые слова: квантовый ансамбль, квантовость, квантовые корреляции, клонирование, величина Холево, коммутатор, квантовые измерения.

1. ВВЕДЕНИЕ

Квантовый ансамбль $\{p_j, \rho_j\}$ состоит из семейства квантовых состояний ρ_j , математически представленных операторами плотности в некотором гильбертовом пространстве системы, и соответствующих вероятностей p_j данных состояний. Квантовые ансамбли являются объектами, одновременно важными с точки зрения и фундаментальной науки, и практики в квантовой теории информации, в частности в квантовой теории связи и теории квантовых измерений. Основное различие между одиночным квантовым состоянием и квантовым ансамблем состоит в том, что

*Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing, People's Republic of China. E-mail: luosl@amt.ac.cn

состояния, составляющие квантовый ансамбль, могут не коммутировать и, следовательно, проявлять свои квантовые черты до некоторой степени зависимым образом, что априори невозможно для одиночного квантового состояния. Эта математическая некоммутативность фактически является источником (или, скорее, синонимом) физических квантовых характеристик. Как можно количественно определить такие квантовые характеристики в квантовом ансамбле? В частности, как охарактеризовать ситуацию, в которой два состояния в наибольшей степени являются квантовыми относительно друг друга в количественном отношении?

В настоящей работе, мотивом для написания которой послужили некоторые фундаментальные труды в таких областях квантовой теории информации, как квантовая связь и криптография, а вдохновляющей идеей – пионерские работы по изучению квантовости [1]–[5], мы рассматриваем квантовость ансамблей с различных точек зрения и сравниваем полученные результаты. Мы увидим, что понятие квантового ансамбля одновременно весьма трудноуловимо и весьма содержательно, а различные меры квантовости могут приводить к по-разному упорядоченным квантовым ансамблям, в точности как и трудноуловимое понятие зацепленности, которое при различных мерах зацепленности приводит к разному ее упорядочению [6], [7].

Помимо того что квантовые ансамбли интересны сами по себе с эстетической точки зрения, изучение квантовости квантовых ансамблей имеет практическое значение в квантовой криптографии. Чтобы извлечь секретные ключи, можно использовать некоторые квантовые ансамбли как сигнальные состояния, наиболее чувствительные к перехвату данных, т. е. являющиеся наиболее квантовыми в некотором смысле. Таким образом, желательно найти некоторые величины, синтезирующие квантовость квантовых ансамблей, чтобы лучше понимать и иметь возможность сравнивать безопасность и эффективность квантовых криптографических схем [8]–[13].

Основная идея определения эффективных понятий квантовости восходит к применению понятий возмущения и информации в теории квантовых измерений и квантовой связи. Из общих наблюдений известно, что в то время как семейство классических состояний можно измерять и передавать без возмущений, квантовые состояния “чувствительны к воздействиям”, и в общем случае их невозможно измерить без возмущений, если они не коммутируют. Как следствие степень возмущенности можно использовать для измерения квантовости квантовых ансамблей. Другой интуитивный подход основан на измерении степени коммутативности различных пар квантовых состояний в квантовом ансамбле.

Статья построена следующим образом. В разделе 2 приведены некоторые важные примеры квантовых ансамблей, которые имеют большое значение для знаменитых квантовых криптографических протоколов и применяются для тестирования различных мер квантовости. В разделе 3 впервые введены некоторые естественные меры квантовости в терминах коммутаторов и относительной энтропии квантовых ансамблей, а затем дан обзор некоторых известных мер квантовости ансамблей, которые базируются на доступной информации, безопасности передачи информации и квантовом клонировании. В разделе 4 рассмотрены некоторые фундаментальные свойства меры квантовости, включая вогнутость и субаддитивность. В разделе 5 мы сравниваем различные меры квантовости и обсуждаем возможность их применения для интуитивного понимания природы безопасности квантовых криптографических протоколов. Выводы приведены в разделе 6. Некоторые вспомога-

ные сведения содержатся в приложениях. Основной результат настоящей статьи – это количественный анализ квантовости некоторых важных ансамблей и сравнение различных мер квантовости, включая их фундаментальные свойства. Чтобы упростить изложение, мы ограничиваем рассмотрение кубитными ансамблями чистых состояний с начальным равномерным распределением вероятностей. Мы используем логарифм по основанию 2, таким образом, единицей информации является один бит.

2. ОСНОВНЫЕ КВАНТОВЫЕ АНСАМБЛИ

Прежде чем приступить к обсуждению различных мер квантовости, сначала напомним некоторые важные примеры квантовых ансамблей: ансамбли B92, BB84, кубитная триада, кубитная тетрада и т. д., которые возникли из знаменитых квантовых криптографических схем и применяются для тестирования различных понятий квантовости. Пусть $\{|0\rangle, |1\rangle\}$ – вычислительная база некоторой кубитной системы.

ПРИМЕР 1. Двухкубитный ансамбль B92 $\mathcal{E}_x = \{1/2, 1/2; |\psi_1\rangle, |\psi_2\rangle\}$ состоит из двух чистых состояний с одинаковыми вероятностями. Здесь $\langle\psi_1|\psi_2\rangle = \sin\theta = x$, $\theta \in [0, \pi/2]$ и

$$|\psi_1\rangle = \cos\frac{\theta}{2} \cdot |0\rangle + \sin\frac{\theta}{2} \cdot |1\rangle, \quad |\psi_2\rangle = \sin\frac{\theta}{2} \cdot |0\rangle + \cos\frac{\theta}{2} \cdot |1\rangle.$$

В протоколе B92 извлечения квантового ключа этот ансамбль применяется для кодирования и передачи информации о секретном ключе [10]. Будучи достаточно простым, так как он состоит из двух (в общем случае неортогональных) состояний, такой ансамбль оказывается удивительно богатым и тонким с точки зрения передачи квантовой информации [1].

ПРИМЕР 2. Диагональный ансамбль $\mathcal{E}_{\text{diag}} = \{1/3, 1/3, 1/3; |0\rangle, |1\rangle, |+\rangle\}$ объединяет вычислительную базу $\{|0\rangle, |1\rangle\}$ и диагональный вектор $|+\rangle := (|0\rangle + |1\rangle)/\sqrt{2}$.

ПРИМЕР 3. Ансамбль BB84 $\mathcal{E}_{\text{BB84}} = \{1/4, 1/4, 1/4, 1/4; |0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, в котором $|-\rangle := (|0\rangle - |1\rangle)/\sqrt{2}$, является фундаментальной составляющей первого протокола квантового распределения криптографического ключа [8].

ПРИМЕР 4. Триадный ансамбль

$$\mathcal{E}_{\text{trine}} = \left\{ \frac{1}{3}, \frac{1}{3}, \frac{1}{3}; |0\rangle, \frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle, \frac{1}{2}|0\rangle - \frac{\sqrt{3}}{2}|1\rangle \right\}$$

хорошо изучен в теории квантовых измерений и криптографии [14]–[17], в частности он лежит в основе протокола RBC00 квантового распределения ключа [11], [18].

ПРИМЕР 5. Тетрадный ансамбль $\mathcal{E}_{\text{tetrad}} = \{p_j, |\psi_j\rangle\}$, где $p_j = 1/4$, $j = 1, 2, 3, 4$, и

$$\begin{aligned} |\psi_1\rangle &= |0\rangle, & |\psi_2\rangle &= \sqrt{\frac{1}{3}}|0\rangle + \sqrt{\frac{2}{3}}|1\rangle, \\ |\psi_3\rangle &= \sqrt{\frac{1}{3}}|0\rangle + e^{2\pi i/3}\sqrt{\frac{2}{3}}|1\rangle, & |\psi_4\rangle &= \sqrt{\frac{1}{3}}|0\rangle + e^{4\pi i/3}\sqrt{\frac{2}{3}}|1\rangle, \end{aligned}$$

является простейшим случаем симметричного информационно полного (СИП) множества (или множества лучей, расположенных под равными углами) [19]. СИП-множество в гильбертовом пространстве $\mathbb{C}^d$ – это множество, состоящее из d^2 чистых состояний $|\psi_j\rangle$ таких, что

$$|\langle\psi_j|\psi_k\rangle|^2 = \frac{1}{d+1}, \quad j \neq k.$$

Несмотря на кажущуюся простоту устройства СИП-множества, доказательство самого его существования в случае произвольной размерности является выдающейся нерешенной задачей [19]. СИП-множества были построены аналитически при размерностях $d = 2, 3, \dots, 15, 19, 24, 35, 48$, а численные примеры показывают, что при $d \leq 67$ СИП-множества существуют [20]. В частности, при $d = 2$ существует явный СИП-ансамбль $\mathcal{E}_{\text{tetrad}}$, который называется тетрадным, так как четыре состояния образуют вершины некоторого правильного тетраэдра [15].

ПРИМЕР 6. Ансамбль из шести состояний

$$\mathcal{E}_{\text{six}} = \left\{ \frac{1}{6}, \frac{1}{6}, \frac{1}{6}, \frac{1}{6}, \frac{1}{6}, \frac{1}{6}; |0_x\rangle, |1_x\rangle, |0_y\rangle, |1_y\rangle, |0_z\rangle, |1_z\rangle \right\}$$

состоит из собственных состояний трех операторов Паули σ_x , σ_y и σ_z . Точнее, если положить $|0_z\rangle = |0\rangle$ и $|1_z\rangle = |1\rangle$, то

$$|0_x\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \quad |1_x\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}, \quad |0_y\rangle = \frac{|0\rangle + i|1\rangle}{\sqrt{2}}, \quad |1_y\rangle = \frac{|0\rangle - i|1\rangle}{\sqrt{2}}.$$

Этот квантовый ансамбль является в высшей степени симметричным и применяется в протоколе из шести состояний в квантовой криптографии [21]–[23]. Он также является простейшим примером так называемых взаимно несмещенных баз [20], [24].

Квантовый ансамбль называется классическим, если состояния, содержащиеся в нем, образуют коммутирующее семейство. В противном случае он называется истинно квантовым ансамблем. Интуитивно ясно, что все безусловно надежные протоколы квантовых распределений ключей должны включать некоторые квантовые ансамбли, проявляющие истинную квантовость.

3. МЕРЫ КВАНТОВОСТИ

В этом разделе изучаются некоторые меры, позволяющие количественно измерить квантовость квантовых ансамблей с разных точек зрения: в терминах коммутаторов, квантовых корреляций, доступной информации, безопасности передачи информации, квантового клонирования.

3.1. В терминах коммутаторов. Простейший способ исследования квантовости квантового ансамбля состоит в использовании попарных коммутаторов квантовых состояний. Для квантового ансамбля $\mathcal{E} = \{p_j, \rho_j\}$ величина

$$Q_{\text{comm}}(\mathcal{E}) := - \sum_{j,k} p_j p_k \text{tr}[\rho_j, \rho_k]^2$$

есть средняя некоммутативность пар состояний в ансамбле, таким образом, ее можно в некоторой степени рассматривать как меру квантовости. Здесь знак минус обусловлен тем, что коммутатор $[\rho_j, \rho_k] := \rho_j \rho_k - \rho_k \rho_j$ двух самосопряженных операторов является кососопряженным, откуда следует, что величина $[\rho_j, \rho_k]^2$ неположительна. Для ансамблей в примерах 1–6 вычисления дают следующие результаты:

$$\begin{aligned} Q_{\text{comm}}(\mathcal{E}_x) &= x^2(1-x^2), & Q_{\text{comm}}(\mathcal{E}_{\text{diag}}) &= \frac{2}{9}, & Q_{\text{comm}}(\mathcal{E}_{\text{BB84}}) &= \frac{1}{4}, \\ Q_{\text{comm}}(\mathcal{E}_{\text{trine}}) &= \frac{1}{4}, & Q_{\text{comm}}(\mathcal{E}_{\text{tetrad}}) &= \frac{1}{3}, & Q_{\text{comm}}(\mathcal{E}_{\text{six}}) &= \frac{1}{3}. \end{aligned}$$

Мера Q_{comm} замечательна тем, что она совершенно понятна интуитивно и в то же время может быть непосредственно вычислена, что сильно контрастирует с остальными мерами, которые содержат оптимизацию по измерениям и не поддаются аналитическим вычислениям в общем случае. Несмотря на простоту меры Q_{comm} ее значения совпадают со значениями меры Q_{FS} (довольно сложная мера, которую весьма трудно вычислять, см. п. 3.4) для большинства ансамблей, рассмотренных в настоящей статье.

3.2. В терминах квантовых корреляций. Квантовый ансамбль $\mathcal{E} = \{p_j, \rho_j\}$ можно отождествить с классически-квантовым двухчастным состоянием

$$\rho_{\mathcal{E}} := \sum_j p_j |j\rangle\langle j| \otimes \rho_j.$$

Здесь $\{|j\rangle\}$ – любое ортонормированное множество некоторой вспомогательной системы a . Корреляции в этом двухчастном состоянии кодируют связи между различными состояниями, составляющими ансамбль. Соответственно, можно изучать квантовость квантового ансамбля $\mathcal{E}$, рассматривая квантовые корреляции в состоянии $\rho_{\mathcal{E}}$ [25]. Более точно, проводя локальное измерение фон Неймана $\Pi = \{\Pi_k\}$ на системе $\{\rho_j\}$, получим классическое двухчастное состояние (классически-классическое состояние, точное определение и характеристики которого даны в работе [26])

$$\Pi(\rho_{\mathcal{E}}) := \sum_k (\mathbf{1} \otimes \Pi_k) \rho_{\mathcal{E}} (\mathbf{1} \otimes \Pi_k),$$

которое “классифицирует” исходное двухчастное квантовое состояние $\rho_{\mathcal{E}}$. Здесь $\mathbf{1}$ – единичный оператор для системы $\{|j\rangle\langle j|\}$.

Теперь можно естественным образом определить меры квантовости для ансамбля $\mathcal{E}$ через какую-нибудь разумную меру “расстояния” между состоянием $\rho_{\mathcal{E}}$ и его классической редукцией $\Pi(\rho_{\mathcal{E}})$, порожденной измерением фон Неймана Π , с последующим вычислением точной нижней грани по всем измерениям фон Неймана. В частности, применяя понятие квантовой относительной энтропии, можно определить

$$Q_{\text{corr}}(\mathcal{E}) := \inf_{\Pi} D(\rho_{\mathcal{E}} | \Pi(\rho_{\mathcal{E}})).$$

Здесь величина $D(\rho | \sigma) := \text{tr}(\rho \log \rho - \rho \log \sigma)$ является квантовой относительной энтропией квантовых состояний. Введенное выше определение Q_{corr} не зависит от выбора ортонормированного множества $\{|j\rangle\}$ благодаря унитарной инвариантности квантовой относительной энтропии.

В качестве альтернативы как меру квантовости также можно интерпретировать величину

$$Q_I(\mathcal{E}) := \inf_{\Pi} \{I(\rho_{\mathcal{E}}) - I(\Pi(\rho_{\mathcal{E}}))\}.$$

Здесь $I(\rho) := S(\rho^a) + S(\rho^b) - S(\rho)$ является квантовой взаимной информацией в двухчастном состоянии ρ с маргинальными состояниями ρ^a и ρ^b . Мера квантовости $Q_I(\mathcal{E})$ фактически является квантовой несогласованностью состояния $\rho_{\mathcal{E}}$ при проведении измерения фон Неймана в системе $\{\rho_j\}$ [27], [28].

Для ансамблей, приведенных в примерах 1–4, имеем [25]

$$Q_{\text{corr}}(\mathcal{E}_{1/\sqrt{2}}) = \frac{1}{2}, \quad Q_{\text{corr}}(\mathcal{E}_{\text{diag}}) = \frac{1}{3}, \quad Q_{\text{corr}}(\mathcal{E}_{\text{BB84}}) = \frac{1}{2}, \quad Q_{\text{corr}}(\mathcal{E}_{\text{trine}}) = 0.541.$$

Для тетрадного ансамбля и ансамбля из шести состояний получим

$$Q_{\text{corr}}(\mathcal{E}_{\text{tetrad}}) = 0.689, \quad Q_{\text{corr}}(\mathcal{E}_{\text{six}}) = \frac{2}{3}.$$

Кстати, в этом контексте также можно использовать относительную энтропию квантовых ансамблей [29] для определения меры квантовости:

$$Q_{\mathcal{D}}(\mathcal{E}) := \inf_{\Pi} \mathcal{D}(\mathcal{E}|\Pi(\mathcal{E})).$$

Здесь точная нижняя грань берется по всем измерениям фон Неймана $\Pi = \{\Pi_k\}$, а $\Pi(\mathcal{E}) = \{p_j, \Pi(\rho_j)\}$, где $\Pi(\rho_j) := \sum_k \Pi_k \rho_j \Pi_k$, есть классический квантовый ансамбль, так как $\{\Pi(\rho_j)\}$ – коммутирующее семейство. Относительная энтропия двух квантовых ансамблей $\mathcal{E} = \{p_i, \rho_i\}$ и $\mathcal{F} = \{q_j, \sigma_j\}$ определяется как [29]

$$\mathcal{D}(\mathcal{E}|\mathcal{F}) := \inf_c \sum_{i,j} c_{ij} D(\rho_i|\sigma_j),$$

где точная нижняя грань берется по всем двумерным распределениям вероятностей $c = \{c_{ij}\}$ с маргинальными распределениями $p_i = \sum_j c_{ij}$ и $q_j = \sum_i c_{ij}$. Распределение c можно интерпретировать как спаривание между $p := \{p_i\}$ и $q := \{q_i\}$. Относительная энтропия $\mathcal{D}(\mathcal{E}|\mathcal{F})$ квантовых ансамблей сводится к относительной энтропии квантовых состояний, если оба ансамбля $\mathcal{E}$ и $\mathcal{F}$ вырождаются в множества с одним квантовым состоянием. Вычисление меры $Q_{\mathcal{D}}$ весьма сложно из-за неоднозначности спаривания, и мы не будем его здесь проводить.

3.3. В терминах доступной информации. Знаменитый результат, полученный в контексте квантовых ансамблей, – это неравенство Холево, дающее фундаментальный предел доступной информации, которую можно извлечь из квантового ансамбля посредством измерений [14]. Основной трудностью при оценке доступной информации является то, что она не поддается аналитическим вычислениям в общем случае, несмотря на многочисленные исследования в этом направлении [14]–[17], [30]–[34]. Неравенство Холево строгое, если квантовые состояния в ансамбле не коммутируют. Таким образом, разрыв между верхней границей Холево и доступной информацией является естественной характеристикой качества при вычислении квантовости квантового ансамбля [1]. Для определенности для квантового

ансамбля $\mathcal{E} = \{p_j, \rho_j\}$ будем считать, что граница Холево есть

$$\chi(\mathcal{E}) := S\left(\sum_j p_j \rho_j\right) - \sum_j p_j S(\rho_j),$$

а доступная информация равна $\chi_0(\mathcal{E}) := \sup_M I(M(\mathcal{E}))$. Здесь $S(\rho) := -\operatorname{tr} \rho \log \rho$ есть энтропия фон Неймана, $M = \{M_k\}$ – общее квантовое измерение (положительная операторнозначная мера), а $I(M(\mathcal{E})) := H(p) + H(q) - H(T)$ – взаимная информация Шеннона для распределения вероятностей двухчастного состояния $T = \{t_{jk}\}$, где

$$t_{jk} := p_j \operatorname{tr} \rho_j M_k, \quad p_j := \sum_k t_{jk}, \quad q_k := \sum_j t_{jk}$$

и $H(p) := -\sum_j p_j \log p_j$ – энтропия Шеннона. Из неравенства Холево [14] следует, что $\chi_0(\mathcal{E}) \leq \chi(\mathcal{E})$, а равенство возможно тогда и только тогда, когда все состояния в ансамбле коммутируют.

Теперь меру квантовости можно определить как [1] $Q_{\text{Hol}}(\mathcal{E}) := \chi(\mathcal{E}) - \chi_0(\mathcal{E})$. Ясно, что $Q_{\text{Hol}}(\mathcal{E}) = 0$ тогда и только тогда, когда ансамбль $\mathcal{E}$ классический.

Для ансамбля B92 из примера 1 мера его квантовости $Q_{\text{Hol}}(\mathcal{E}_x)$ была вычислена в работе [1]:

$$Q_{\text{Hol}}(\mathcal{E}_x) = 1 - \frac{1}{2}(1+x) \log(1+x) - \frac{1}{2}(1-x) \log(1-x) - \\ - \frac{1}{2}(1+y) \log(1+y) - \frac{1}{2}(1-y) \log(1-y), \quad y = \sqrt{1-x^2}.$$

В частности, при $x = 1/\sqrt{2}$ эта величина достигает максимума, $Q_{\text{Hol}}(\mathcal{E}_{1/\sqrt{2}}) = 0.202$. Следовательно, при измерении с помощью Q_{Hol} два чистых квантовых состояния будут максимально квантовыми, когда они развернуты на угол 45° , что для нас весьма привлекательно, поскольку два чистых состояния являются классическими, когда они либо ортогональны друг другу (развернуты на угол 90°) либо совпадают (развернуты на угол 0°), таким образом, естественно ожидать, что они будут максимально квантовыми относительно друг друга, когда степень их перекрытия лежит посередине между двумя крайними значениями, т.е. между 0° и 90° [1].

Для диагонального ансамбля из примера 2 можно считать, что $\chi_0(\mathcal{E}_{\text{diag}}) = 2/3$, $\chi(\mathcal{E}_{\text{diag}}) = \log 3 - 2/3$. Следовательно, $Q_{\text{Hol}}(\mathcal{E}_{\text{diag}}) = 0.252$.

Для ансамбля BB84 из примера 3, который является действительным симметричным ансамблем в смысле работы [33], его доступная информация дается выражением $\chi_0(\mathcal{E}_{\text{BB84}}) = 1/2$ [33]. Однако ясно, что $\chi(\mathcal{E}_{\text{BB84}}) = 1$, следовательно,

$$Q_{\text{Hol}}(\mathcal{E}_{\text{BB84}}) = \chi(\mathcal{E}_{\text{BB84}}) - \chi_0(\mathcal{E}_{\text{BB84}}) = \frac{1}{2}.$$

Для триадного ансамбля $\mathcal{E}_{\text{trine}}$ (см. пример 4) из результатов, полученных в работе [33], следует, что доступная информация равна $\chi_0(\mathcal{E}_{\text{trine}}) = \log(3/2) = 0.585$, а границу Холево можно оценить как $\chi(\mathcal{E}_{\text{trine}}) = 1$. Следовательно,

$$Q_{\text{Hol}}(\mathcal{E}_{\text{trine}}) = \chi(\mathcal{E}_{\text{trine}}) - \chi_0(\mathcal{E}_{\text{trine}}) = 2 - \log 3 = 0.415.$$

Для тетрадного ансамбля $\mathcal{E}_{\text{tetrad}}$ (см. пример 5) из результатов, полученных в работе [15], следует, что доступная информация равна $\chi_0(\mathcal{E}_{\text{tetrad}}) = \log(4/3)$. Легко оценить границу Холево: $\chi(\mathcal{E}_{\text{tetrad}}) = 1$. Следовательно,

$$Q_{\text{Hol}}(\mathcal{E}_{\text{tetrad}}) = \chi(\mathcal{E}_{\text{tetrad}}) - \chi_0(\mathcal{E}_{\text{tetrad}}) = \log 3 - 1 = 0.585.$$

Для ансамбля из шести состояний из результатов работы [15] следует, что доступная информация может быть получена с помощью некоторой положительной операторнозначной меры с четырьмя элементами ранга 1. Отсюда и из прямого, но весьма скучного анализа (детали см. в приложении A) имеем $\chi_0(\mathcal{E}_{\text{six}}) = 1/3$. С другой стороны, ясно, что $\chi(\mathcal{E}_{\text{six}}) = 1$. Следовательно,

$$Q_{\text{Hol}}(\mathcal{E}_{\text{six}}) = \chi(\mathcal{E}_{\text{six}}) - \chi_0(\mathcal{E}_{\text{six}}) = \frac{2}{3}.$$

3.4. В терминах безопасности передачи информации. В работах [1]–[4] было начато изучение квантовости множества квантовых состояний в терминах трудности передачи состояния через классический канал связи. Для квантового ансамбля $\mathcal{E}$ было введено понятие доступной точности, которое определяется как

$$F(\mathcal{E}) := \sup_{M, \{\sigma_k\}} \sum_{j,k} p_j \text{tr}(\rho_j M_k) \text{tr}(\sigma_k \rho_j).$$

Здесь $M = \{M_k\}$ – общее квантовое измерение. Эта средняя точность представляет собой вероятность того, что прослушивающее устройство останется незамеченным после атаки на канал связи, осуществленной с помощью стратегии перехвата с повторной передачей (intercept–resend). Чем меньше эта величина, тем больше чувствительность ансамбля к измерению. Следовательно, величину $Q_{\text{FS}}(\mathcal{E}) := 1 - F(\mathcal{E})$ можно считать мерой квантовости квантового ансамбля $\mathcal{E}$.

В частности, для квантового ансамбля $\mathcal{E}_x$ из примера 1 из результатов, полученных в работе [3], следует, что $F(\mathcal{E}_x) = (1 + \sqrt{1 - x^2 + x^4})/2$, таким образом, $Q_{\text{FS}}(\mathcal{E}_x) = (1 - \sqrt{1 - x^2 + x^4})/2$. В противоположность к мере Q_{clon} (см. далее п. 3.5), но в соответствии с мерой Q_{Hol} эта величина достигает максимального значения $Q_{\text{FS}}(\mathcal{E}_{1/\sqrt{2}}) = 0.067$ при $x = 1/\sqrt{2}$.

Для диагонального ансамбля из примера 2 получим $Q_{\text{FS}}(\mathcal{E}_{\text{diag}}) = 0.127$. Для ансамбля $\mathcal{E}_{\text{BB84}}$, триадного ансамбля $\mathcal{E}_{\text{trine}}$ и тетрадного ансамбля $\mathcal{E}_{\text{tetrad}}$ доступные точности были вычислены в работе [3]:

$$F(\mathcal{E}_{\text{BB84}}) = \frac{3}{4}, \quad F(\mathcal{E}_{\text{trine}}) = \frac{3}{4}, \quad F(\mathcal{E}_{\text{tetrad}}) = \frac{2}{3}.$$

Соответственно получим следующие меры квантовости:

$$Q_{\text{FS}}(\mathcal{E}_{\text{BB84}}) = \frac{1}{4}, \quad Q_{\text{FS}}(\mathcal{E}_{\text{trine}}) = \frac{1}{4}, \quad Q_{\text{FS}}(\mathcal{E}_{\text{tetrad}}) = \frac{1}{3}.$$

Для ансамбля из шести состояний $\mathcal{E}_{\text{six}}$ из результатов работы [4] следует, что доступная точность равна $F(\mathcal{E}_{\text{six}}) = 2/3$, а мера квантовости $Q_{\text{FS}}(\mathcal{E}_{\text{six}}) = 1/3$.

3.5. В терминах квантового клонирования. Из знаменитой теоремы о запрете клонирования следует, что нельзя клонировать множество неортогональных чистых состояний [35]–[37] благодаря их внутренним квантовым характеристикам. В более общей формулировке множество некоммутирующих квантовых состояний не допускает распространения [38]–[42], однако эти состояния могут быть клонированы или распространены приближенно. Таким образом, способности к клонированию и распространению можно интерпретировать как меры квантовости квантовых ансамблей [2], [5]. Здесь мы рассмотрим только подход, основанный на клонировании.

Следуя работам [1], [2], будем считать, что $\mathcal{E} = \{p_j, \rho_j\}$ – квантовый ансамбль, состоящий из чистых состояний, $\rho_j = |\psi_j\rangle\langle\psi_j|$. Пусть U – любой унитарный оператор, переводящий состояние $|\psi_j\rangle \otimes |0\rangle$ в чистое двухчастное состояние $|\Psi_j\rangle$ с идентичными маргинальными состояниями (это симметричное ограничение вводится для удобства). Тогда можно использовать среднюю доступную точность

$$F_{\text{clon}}(\mathcal{E}) := \max_U \sum_j p_j |\langle \Psi_j | \psi_j \otimes \psi_j \rangle|^2$$

для определения меры квантовости как $Q_{\text{clon}}(\mathcal{E}) := 1 - F_{\text{clon}}(\mathcal{E})$. Чем больше F_{clon} , тем меньше квантовость ансамбля $\mathcal{E}$.

Для квантового ансамбля $\mathcal{E}_x$ из примера 1 известно, что [1], [2], [43]

$$F_{\text{clon}}(\mathcal{E}_x) = \frac{1}{2}(1 + x^3 + (1 - x^2)\sqrt{1 + x^2}),$$

следовательно,

$$Q_{\text{clon}}(\mathcal{E}_x) = \frac{1}{2}(1 - x^3 - (1 - x^2)\sqrt{1 + x^2}), \quad Q_{\text{clon}}(\mathcal{E}_{1/\sqrt{2}}) = 0.017.$$

Однако максимальное значение $Q_{\text{clon}}(\mathcal{E}_x) = 0.019$ достигается при $x = 1/\sqrt{3}$. Следовательно, при измерении с помощью Q_{clon} два чистых квантовых состояния будут максимально квантовыми, когда они развернуты на угол $\arcsin(1/\sqrt{3}) = 54.7^\circ$, что резко противоречит Q_{Hol} -калибровке.

Так как вычисление меры Q_{clon} в общем случае сталкивается со значительными трудностями, для удобства численных вычислений, следуя уравнениям (39) и (40) в работе [43], мы ограничимся упрощенной версией меры Q_{clon} , т. е. ограничим унитарный оператор U в определении $F_{\text{clon}}(\mathcal{E})$ следующим симметричным анзацем (напомним, что в настоящей работе мы имеем дело только с ансамблями, состоящими из кубитных состояний):

$$U|00\rangle = a|00\rangle + b(|01\rangle + |10\rangle) + c|11\rangle, \quad U|10\rangle = c|00\rangle + b(|01\rangle + |10\rangle) + a|11\rangle,$$

где a, b, c – действительные числа. Доступную точность и меру квантовости обозначим через $F'_{\text{clon}}(\mathcal{E})$ и $Q'_{\text{clon}}(\mathcal{E})$ соответственно. Из условия нормировки и унитарности оператора U , получим ограничения $a^2 + 2b^2 + c^2 = 1$, $ac + b^2 = 0$.

Оказывается, что для ансамбля B92 из примера 1 $Q'_{\text{clon}}(\mathcal{E}_x) = Q_{\text{clon}}(\mathcal{E}_x)$. Для других ансамблей прямые, но весьма скучные численные расчеты дают

$$\begin{aligned} Q'_{\text{clon}}(\mathcal{E}_{\text{diag}}) &= 0.099, & Q'_{\text{clon}}(\mathcal{E}_{\text{BB84}}) &= 0.324, & Q'_{\text{clon}}(\mathcal{E}_{\text{trine}}) &= 0.324, \\ Q'_{\text{clon}}(\mathcal{E}_{\text{tetrad}}) &= 0.344, & Q'_{\text{clon}}(\mathcal{E}_{\text{six}}) &= 0.348. \end{aligned}$$

4. ОСНОВНЫЕ СВОЙСТВА КВАНТОВОСТИ

Здесь и далее мы обозначаем через Q любую из ранее введенных мер. Из приведенных выше определений мы имеем следующие основные свойства для всех мер квантовости, введенных в предыдущем разделе.

Свойство 1. Мера $Q(\mathcal{E}) = 0$ тогда и только тогда, когда $\mathcal{E}$ является классическим ансамблем в том смысле, что квантовые состояния в ансамбле коммутируют друг с другом; в частности, если ансамбль вырождается до одиночного квантового состояния, то его квантовость исчезает.

Свойство 2. Меры $Q(\mathcal{E})$ являются унитарно инвариантными в том смысле, что $Q(\mathcal{E}) = Q(U\mathcal{E}U^\dagger)$ для любого унитарного оператора U . Здесь $U\mathcal{E}U^\dagger = \{p_j, U\rho_j U^\dagger\}$.

Свойство 3. Меры $Q(\mathcal{E})$ являются субаддитивными: $Q(\mathcal{E} \otimes \mathcal{F}) \leq Q(\mathcal{E}) + Q(\mathcal{F})$ для любых двух квантовых ансамблей $\mathcal{E} = \{p_i, \rho_i\}$ и $\mathcal{F} = \{q_j, \sigma_j\}$. Здесь тензорное произведение двух ансамблей определяется как $\mathcal{E} \otimes \mathcal{F} := \{p_i q_j, \rho_i \otimes \sigma_j\}$.

Свойство 4. Меры $Q(\mathcal{E})$ (за исключением Q_{comm}) являются вогнутыми в том смысле, что

$$Q\left(\bigcup_k \lambda_k \mathcal{E}_k\right) \geq \sum_k \lambda_k Q(\mathcal{E}_k).$$

Здесь

$$\bigcup_k \lambda_k \mathcal{E}_k := \{\lambda_k p_{jk}, \rho_{jk}\}$$

является чем-то вроде выпуклой комбинации семейства квантовых ансамблей $\mathcal{E}_k = \{p_{jk}, \rho_{jk}\}$, а $\{\lambda_k\}$ – распределение вероятностей, т.е. $\sum_k \lambda_k = 1$, $\lambda_k \geq 0$.

Доказательство этих свойств приведено в приложении Б.

5. СРАВНЕНИЕ МЕР

Для понимания различных мер квантовости мы изобразили их графически для ансамбля B92 $\mathcal{E}_x$ на рисунке. В таблице представлены численные результаты в битах.

	Q_{comm}	Q_{corr}	Q_{Hol}	Q_{FS}	Q'_{clon}
$\mathcal{E}_{1/\sqrt{2}}$	1/4	1/2	0.202	0.067	0.017
$\mathcal{E}_{\text{diag}}$	2/9	1/3	0.252	0.127	0.099
$\mathcal{E}_{\text{BB84}}$	1/4	1/2	1/2	1/4	0.324
$\mathcal{E}_{\text{trine}}$	1/4	0.541	0.415	1/4	0.324
$\mathcal{E}_{\text{tetrad}}$	1/3	0.689	0.585	1/3	0.344
$\mathcal{E}_{\text{six}}$	1/3	2/3	2/3	1/3	0.348

Любая мера квантовости Q приводит к упорядочению множества квантовых ансамблей: будем говорить, что квантовый ансамбль $\mathcal{E}_1$ менее квантовый, чем квантовый ансамбль $\mathcal{E}_2$ (относительно меры Q), если $Q(\mathcal{E}_1) < Q(\mathcal{E}_2)$. Поскольку мы теперь имеем несколько мер квантовости, естественно посмотреть, все ли они приводят

Графики зависимости различных мер от x для ансамбля B92 $\mathcal{E}_x$. Для всех мер, кроме $Q_{\text{clon}}(\mathcal{E}_x)$, графики качественно схожи, максимальные величины равны 0.25 для $Q_{\text{comm}}(\mathcal{E}_x)$, 0.5 для $Q_{\text{corr}}(\mathcal{E}_x)$, 0.202 для $Q_{\text{Hol}}(\mathcal{E}_x)$ и 0.067 для $Q_{\text{FS}}(\mathcal{E}_x)$, и все они достигаются при $x = 1/\sqrt{2}$. Для $Q_{\text{clon}}(\mathcal{E}_x)$ максимальное значение равно 0.019 и достигается при $x = 1/\sqrt{3}$.

к одинаково упорядоченным квантовым ансамблям. Примечательно, что любые две меры, введенные в разделе 3, несовместимы в том смысле, что они приводят к по-разному упорядоченным ансамблям.

Рассмотрим ансамбль $\mathcal{E}_x$ с переменным x . Мера $Q'_{\text{clon}}(\mathcal{E}_x)$ достигает своего максимума при $x = 1/\sqrt{3}$, тогда как все другие меры достигают своего максимума при $x = 1/\sqrt{2}$. Отсюда следует, что Q'_{clon} несовместима с любой другой мерой квантовости. Например, $Q'_{\text{clon}}(\mathcal{E}_{1/\sqrt{3}}) > Q'_{\text{clon}}(\mathcal{E}_{1/\sqrt{2}})$, тогда как $Q_{\text{Hol}}(\mathcal{E}_{1/\sqrt{3}}) < Q_{\text{Hol}}(\mathcal{E}_{1/\sqrt{2}})$. Эта несовместимость отчетливо видна на графиках, представленных на рисунке, при $x \in [1/\sqrt{3}, 1/\sqrt{2}]$.

Сравнивая ансамбли $\mathcal{E}_{1/\sqrt{2}}$ и $\mathcal{E}_{\text{diag}}$, видим, что мера Q_{comm} несовместима с мерами Q_{Hol} , Q'_{clon} и Q_{FS} . Сравнивая ансамбли $\mathcal{E}_{1/\sqrt{2}}$ и $\mathcal{E}_{\text{trine}}$, видим, что мера Q_{comm} несовместима с Q_{corr} . Сравнивая ансамбли $\mathcal{E}_{\text{BB84}}$ и $\mathcal{E}_{\text{trine}}$, видим, что мера Q_{Hol} несовместима с Q_{FS} . Сравнивая $\mathcal{E}_{1/\sqrt{2}}$ и $\mathcal{E}_{\text{diag}}$, видим, что мера Q_{Hol} несовместима с Q_{corr} . Сравнивая $\mathcal{E}_{1/\sqrt{2}}$ и $\mathcal{E}_{\text{BB84}}$, видим, что мера Q_{FS} несовместима с Q_{corr} . Все это показывает, что меры квантовости, рассмотренные в настоящей работе, попарно несовместимы.

Весьма интересно и примечательно, что, как это следует из таблицы, для большинства рассмотренных примеров меры Q_{FS} и Q_{comm} дают одно и то же значение. Вычисления для первой из этих мер, как правило, весьма затруднительны, тогда как значения второй меры всегда довольно легко вычислить аналитически. Для более глубокого сравнения этих двух мер квантовости рассмотрим действительный

симметричный ансамбль $\mathcal{E}_{\text{sym},n} := \{p_j, |\psi_j\rangle\}$, где

$$p_j = \frac{1}{n}, \quad |\psi_j\rangle = \cos \frac{j\pi}{n} \cdot |0\rangle + \sin \frac{j\pi}{n} \cdot |1\rangle, \quad j = 1, 2, \dots, n.$$

Тогда при $n \geq 3$ имеем $Q_{\text{FS}}(\mathcal{E}_{\text{sym},n}) = 1/4$ [3]. С другой стороны, пусть $\rho_j = |\psi_j\rangle\langle\psi_j|$. Тогда можно непосредственно рассчитать, что

$$\text{tr}[\rho_j, \rho_k]^2 = -\frac{1}{2} \sin^2 \left(\frac{2j\pi}{n} - \frac{2k\pi}{n} \right),$$

откуда следует, что

$$Q_{\text{comm}}(\mathcal{E}_{\text{sym},n}) = - \sum_{j,k=1}^n p_j p_k \text{tr}[\rho_j, \rho_k]^2 = \sum_{j,k=1}^n \frac{1}{2n^2} \sin^2 \left(\frac{2j\pi}{n} - \frac{2k\pi}{n} \right) = \frac{1}{4}.$$

Таким образом, две меры Q_{FS} и Q_{comm} также совпадают для всех действительных симметричных ансамблей.

В заключение заметим, что все меры, рассмотренные в настоящей работе, приводят к по-разному упорядоченным квантовым ансамблям, и это не удивительно, так как квантовый ансамбль как целое является весьма сложным понятием с физической точки зрения, и нет никакой надежды раскрыть все его тайны через единственное окно (т.е. не существует единственной величины, которая отражала бы все его фундаментальные свойства). Таким образом, необходимо исследовать меры квантовости с разных точек зрения.

6. ОБСУЖДЕНИЕ РЕЗУЛЬТАТОВ

Помимо обзора различных мер квантовости, известных в литературе, мы собрали и вычислили меры для некоторых основных квантовых ансамблей, возникающих из квантовой криптографии, изучили их фундаментальные свойства и провели их сравнительный анализ. Далее мы построили очень интуитивную и простую меру квантовости, основанную на коммутаторах, и изучили ее замечательные свойства. Мы показали, что, как правило, различные меры приводят к по-разному упорядоченным квантовым ансамблям. Одна какая-либо мера может отражать одну какую-либо грань квантовости, и не существует единственной меры, которая полностью удовлетворяла бы всем поставленным целям.

В квантовой криптографии отличие квантовости от нуля в конечном счете обеспечивает безопасность квантового распределения ключа. Задача, как максимально использовать и исследовать эту квантовость, составляет основу квантового распределения ключа. Количественная оценка квантовости не только интересна сама по себе, но и имеет практическое значение для построения квантовых протоколов.

Следует подчеркнуть, что квантовость ансамбля полностью отличается от еще одного важного и хорошо изученного понятия различимости, или избирательности квантовых состояний [32], [44], [45]. Например, для ансамбля, состоящего из ортогональных квантовых состояний, его квантовость равна нулю, а его различимость максимальна, в то время как для ансамбля, состоящего из тождественных квантовых состояний, его квантовость все еще равна нулю, но его различимость минимальна (равна нулю). Однако понятия квантовости и различимости также тесно связаны, и дальнейшее изучение их взаимодействия и взаимосвязей будет иметь большое значение.

ПРИЛОЖЕНИЕ А

Вычислим в явном виде доступную информацию $\chi_0(\mathcal{E}_{\text{six}}) = 1/3$. Пусть $p_j := 1/6$ для всех $j = 1, \dots, 6$ и

$$\begin{aligned} \rho_1 &:= |0_z\rangle\langle 0_z|, & \rho_2 &:= |1_z\rangle\langle 1_z|, & \rho_3 &:= |0_x\rangle\langle 0_x|, \\ \rho_4 &:= |1_x\rangle\langle 1_x|, & \rho_5 &:= |0_y\rangle\langle 0_y|, & \rho_6 &:= |1_y\rangle\langle 1_y|. \end{aligned}$$

Тогда ансамбль из шести состояний можно переписать как $\mathcal{E}_{\text{six}} = \{p_j, \rho_j\}$. Из результатов работы [15], следует, что доступная информация может быть получена с помощью положительной операторнозначной меры $M = \{M_k = |\psi_k\rangle\langle\psi_k|\}$ с четырьмя элементами ранга 1, которые без потери общности можно параметризовать как

$$|\psi_k\rangle := a_k \cos \frac{\theta_k}{2} \cdot |0\rangle + a_k e^{i\varphi_k} \sin \frac{\theta_k}{2} \cdot |1\rangle, \quad a_k \in \mathbb{R}, \quad \theta_k \in [0, \pi], \quad \varphi_k \in [0, 2\pi),$$

где $k = 1, 2, 3, 4$. Из условия полноты $\sum_{k=1}^4 M_k = \mathbf{1}$ получим

$$\begin{aligned} \sum_{k=1}^4 a_k^2 \cos^2 \frac{\theta_k}{2} &= 1, & \sum_{k=1}^4 a_k^2 \sin^2 \frac{\theta_k}{2} &= 1, \\ \sum_{k=1}^4 a_k^2 e^{i\phi_k} \sin \theta_k &= 0, & \sum_{k=1}^4 a_k^2 e^{-i\phi_k} \sin \theta_k &= 0. \end{aligned}$$

Эти ограничения эквивалентны следующим условиям:

$$\sum_{k=1}^4 a_k^2 = 2, \quad \sum_{k=1}^4 a_k^2 \cos \theta_k = 0, \quad \sum_{k=1}^4 a_k^2 \sin \theta_k \cos \varphi_k = 0, \quad \sum_{k=1}^4 a_k^2 \sin \theta_k \sin \varphi_k = 0.$$

Теперь положим

$$x_k := \frac{1}{2} \cos \theta_k, \quad y_k := \frac{1}{2} \sin \theta_k \cos \varphi_k, \quad z_k := \frac{1}{2} \sin \theta_k \sin \varphi_k$$

и получим, что $x_k^2 + y_k^2 + z_k^2 = 1/4$ при $k = 1, 2, 3, 4$ и

$$\sum_{k=1}^4 a_k^2 = 2, \quad \sum_{k=1}^4 a_k^2 x_k = 0, \quad \sum_{k=1}^4 a_k^2 y_k = 0, \quad \sum_{k=1}^4 a_k^2 z_k = 0.$$

Теперь можно вычислить взаимную информацию Шеннона:

$$I(M(\mathcal{E}_{\text{six}})) := H(p) + H(q) - H(T), \quad T = \{t_{jk}\}, \quad t_{jk} := p_j \operatorname{tr} \rho_j M_k,$$

где $p_j := \sum_k t_{jk}$ и $q_k := \sum_j t_{jk}$. Непосредственные вычисления дают

$$\begin{aligned} t_{1k} &= \frac{a_k^2}{6} \left(\frac{1}{2} + x_k \right), & t_{2k} &= \frac{a_k^2}{6} \left(\frac{1}{2} - x_k \right), & t_{3k} &= \frac{a_k^2}{6} \left(\frac{1}{2} + y_k \right), \\ t_{4k} &= \frac{a_k^2}{6} \left(\frac{1}{2} - y_k \right), & t_{5k} &= \frac{a_k^2}{6} \left(\frac{1}{2} + z_k \right), & t_{6k} &= \frac{a_k^2}{6} \left(\frac{1}{2} - z_k \right), \end{aligned}$$

кроме того, $q_k = a_k^2/2$ при $k = 1, 2, 3, 4$ и $p_j = 1/6$ при $j = 1, \dots, 6$. Получаем

$$H(T) = H(p) + H(q) - 1 + \sum_{k=1}^4 \frac{a_k^2}{6} \left(H\left(\frac{1}{2} + x_k\right) + H\left(\frac{1}{2} + y_k\right) + H\left(\frac{1}{2} + z_k\right) \right).$$

Следовательно,

$$I(M(\mathcal{E}_{\text{six}})) = 1 - \sum_{k=1}^4 \frac{a_k^2}{6} \left(H\left(\frac{1}{2} + x_k\right) + H\left(\frac{1}{2} + y_k\right) + H\left(\frac{1}{2} + z_k\right) \right)$$

и

$$\chi_0(\mathcal{E}_{\text{six}}) = \sup_M I(M(\mathcal{E}_{\text{six}})) = 1 - \inf \sum_{k=1}^4 \frac{a_k^2}{6} \left(H\left(\frac{1}{2} + x_k\right) + H\left(\frac{1}{2} + y_k\right) + H\left(\frac{1}{2} + z_k\right) \right),$$

где точная нижняя грань берется по параметрам a_k, x_k, y_k, z_k , подчиняющихся ограничениям $\sum_{k=1}^4 a_k^2 = 2$, $\sum_{k=1}^4 a_k^2 x_k = 0$, $\sum_{k=1}^4 a_k^2 y_k = 0$ и $\sum_{k=1}^4 a_k^2 z_k = 0$.

Рассмотрим функцию $f(x, y, z) := H(1/2 + x) + H(1/2 + y) + H(1/2 + z)$ при $x^2 + y^2 + z^2 = 1/4$. Минимальное значение этой функции равно $f_{\min} = 2$. Таким образом,

$$I(M(\mathcal{E}_{\text{six}})) = 1 - \sum_{k=1}^4 \frac{a_k^2}{6} f(x_k, y_k, z_k) \leq 1 - \sum_{k=1}^4 \frac{a_k^2}{6} f_{\min} = \frac{1}{3}.$$

Легко проверить, что последнее равенство достигается, например, при $a_k = 1/\sqrt{2}$, $y_k = z_k = 0$, $k = 1, 2, 3, 4$, и $x_1 = x_2 = 1/2$, $x_3 = x_4 = -1/2$. Таким образом, мы доказали, что $\chi_0(\mathcal{E}_{\text{six}}) = 1/3$.

ПРИЛОЖЕНИЕ Б

Докажем свойства различных мер квантовости.

Субаддитивность. Напомним, что тензорное произведение двух ансамблей $\mathcal{E} = \{p_i, \rho_i\}$ и $\mathcal{F} = \{q_j, \sigma_j\}$ определяются как $\mathcal{E} \otimes \mathcal{F} := \{p_i q_j, \rho_i \otimes \sigma_j\}$. Покажем, что меры Q_{comm} , Q_{corr} , Q_{Hol} , Q_{FS} и Q_{clon} субаддитивны в том смысле, что

$$Q(\mathcal{E} \otimes \mathcal{F}) \leq Q(\mathcal{E}) + Q(\mathcal{F}).$$

Для меры Q_{comm} простые алгебраические вычисления приводят к соотношениям

$$Q_{\text{comm}}(\mathcal{E}) = 2 \sum_{i, i'} p_i p_{i'} (\text{tr} \rho_i^2 \rho_{i'}^2 - \text{tr}(\rho_i \rho_{i'}))^2,$$

$$Q_{\text{comm}}(\mathcal{F}) = 2 \sum_{j, j'} q_j q_{j'} (\text{tr} \sigma_j^2 \sigma_{j'}^2 - \text{tr}(\sigma_j \sigma_{j'}))^2,$$

$$Q_{\text{comm}}(\mathcal{E} \otimes \mathcal{F}) = 2 \sum_{i, i', j, j'} p_i p_{i'} q_j q_{j'} (\text{tr} \rho_i^2 \rho_{i'}^2 \cdot \text{tr} \sigma_j^2 \sigma_{j'}^2 - \text{tr}(\rho_i \rho_{i'})^2 \text{tr}(\sigma_j \sigma_{j'}))^2.$$

Теперь из монотонного возрастания элементарной функции $f(s, t) = s + t - st$ при $s, t \in [0, 1]$ и неравенств $\text{tr}(\rho_i \rho_{i'})^2 \leq \text{tr} \rho_i^2 \rho_{i'}^2$ и $\text{tr}(\sigma_j \sigma_{j'})^2 \leq \text{tr} \sigma_j^2 \sigma_{j'}^2$, получим для любых i, i', j, j' неравенство

$$\text{tr} \rho_i^2 \rho_{i'}^2 \cdot \text{tr} \sigma_j^2 \sigma_{j'}^2 - \text{tr}(\rho_i \rho_{i'})^2 \text{tr}(\sigma_j \sigma_{j'})^2 \leq \text{tr}(\rho_i^2 \rho_{i'}^2) - \text{tr}(\rho_i \rho_{i'})^2 + \text{tr}(\sigma_j^2 \sigma_{j'}^2) - \text{tr}(\sigma_j \sigma_{j'})^2,$$

откуда следует, что $Q_{\text{comm}}(\mathcal{E} \otimes \mathcal{F}) \leq Q_{\text{comm}}(\mathcal{E}) + Q_{\text{comm}}(\mathcal{F})$.

Для меры Q_{corr} предположим, что Π и Π' – оптимальные измерения фон Неймана такие, что $Q_{\text{corr}}(\mathcal{E}) = D(\rho_{\mathcal{E}}|\Pi(\rho_{\mathcal{E}}))$ и $Q_{\text{corr}}(\mathcal{F}) = D(\rho_{\mathcal{F}}|\Pi'(\rho_{\mathcal{F}}))$. Тогда

$$\begin{aligned} Q_{\text{corr}}(\mathcal{E} \otimes \mathcal{F}) &\leq D(\rho_{\mathcal{E} \otimes \mathcal{F}}|\Pi \otimes \Pi'(\rho_{\mathcal{E} \otimes \mathcal{F}})) = D(\rho_{\mathcal{E}} \otimes \rho_{\mathcal{F}}|\Pi(\rho_{\mathcal{E}}) \otimes \Pi'(\rho_{\mathcal{F}})) = \\ &= D(\rho_{\mathcal{E}}|\Pi(\rho_{\mathcal{E}})) + D(\rho_{\mathcal{F}}|\Pi'(\rho_{\mathcal{F}})) = Q_{\text{corr}}(\mathcal{E}) + Q_{\text{corr}}(\mathcal{F}). \end{aligned}$$

Для меры Q_{Hol} по определению имеем

$$\begin{aligned} \chi(\mathcal{E} \otimes \mathcal{F}) &= S\left(\sum_{i,j} p_i q_j \rho_i \otimes \sigma_j\right) - \sum_{i,j} p_i q_j S(\rho_i \otimes \sigma_j) = \\ &= S\left(\sum_i p_i \rho_i \otimes \sum_j q_j \sigma_j\right) - \sum_{i,j} p_i q_j (S(\rho_i) + S(\sigma_j)) = \\ &= S\left(\sum_i p_i \rho_i\right) + S\left(\sum_j q_j \sigma_j\right) - \sum_i p_i S(\rho_i) - \sum_j q_j S(\sigma_j) = \chi(\mathcal{E}) + \chi(\mathcal{F}). \end{aligned}$$

С другой стороны, пусть M_1 и M_2 – оптимальные положительные операторнозначные меры, достигающиеся на $\chi_0(\mathcal{E})$ и $\chi_0(\mathcal{F})$ соответственно. Тогда

$$\chi_0(\mathcal{E} \otimes \mathcal{F}) = \sup_M I(M(\mathcal{E} \otimes \mathcal{F})) \geq I(M_1(\mathcal{E}) \otimes M_2(\mathcal{F})) = \chi_0(\mathcal{E}) + \chi_0(\mathcal{F}),$$

откуда следует субаддитивность меры $Q_{\text{Hol}} := \chi - \chi_0$.

Для меры Q_{FS} из результатов, полученных в работе [46], следует, что доступную точность можно записать как $F(\mathcal{E} \otimes \mathcal{F}) = F(\mathcal{E})F(\mathcal{F})$. Таким образом, для меры $Q_{\text{FS}} = 1 - F$ имеем

$$Q_{\text{FS}}(\mathcal{E} \otimes \mathcal{F}) = Q_{\text{FS}}(\mathcal{E}) + Q_{\text{FS}}(\mathcal{F}) - Q_{\text{FS}}(\mathcal{E})Q_{\text{FS}}(\mathcal{F}) \leq Q_{\text{FS}}(\mathcal{E}) + Q_{\text{FS}}(\mathcal{F}).$$

Для меры Q_{clon} можно непосредственно показать, что имеет место неравенство $F_{\text{clon}}(\mathcal{E} \otimes \mathcal{F}) \geq F_{\text{clon}}(\mathcal{E})F_{\text{clon}}(\mathcal{F})$, следовательно, в силу $Q_{\text{clon}} = 1 - F_{\text{clon}}$ имеем

$$Q_{\text{clon}}(\mathcal{E} \otimes \mathcal{F}) \leq Q_{\text{clon}}(\mathcal{E}) + Q_{\text{clon}}(\mathcal{F}) - Q_{\text{clon}}(\mathcal{E})Q_{\text{clon}}(\mathcal{F}) \leq Q_{\text{clon}}(\mathcal{E}) + Q_{\text{clon}}(\mathcal{F}).$$

Вогнутость. Для квантовых ансамблей $\mathcal{E}_k = \{p_{jk}, \rho_{jk}\}$ и распределения вероятностей $\{\lambda_k\}$ их λ -комбинация определяется как $\bigcup_k \lambda_k \mathcal{E}_k := \{\lambda_k p_{jk}, \rho_{jk}\}$. Это в некотором роде выпуклая комбинация ансамблей, где ансамбль $\mathcal{E}_k$ имеет вероятность λ_k . Покажем, что меры Q_{corr} , Q_{Hol} , Q_{FS} и Q_{clon} вогнуты:

$$Q\left(\bigcup_k \lambda_k \mathcal{E}_k\right) \geq \sum_k \lambda_k Q(\mathcal{E}_k).$$

Мера Q_{comm} , однако, не является вогнутой.

Вогнутость меры Q_{corr} следует из соотношений

$$\begin{aligned} Q_{\text{corr}}\left(\bigcup_k \lambda_k \mathcal{E}_k\right) &= \inf_{\Pi} \sum_{j,k} \lambda_k p_{jk} (S(\Pi(\rho_{jk})) - S(\rho_{jk})), \\ Q_{\text{corr}}(\mathcal{E}_k) &= \inf_{\Pi} \sum_j p_{jk} (S(\Pi(\rho_{jk})) - S(\rho_{jk})). \end{aligned}$$

Для меры Q_{Hol} из вогнутости энтропии фон Неймана следует, что

$$\begin{aligned}\chi\left(\bigcup_k \lambda_k \mathcal{E}_k\right) &= S\left(\sum_{j,k} \lambda_k p_{jk} \rho_{jk}\right) - \sum_{j,k} \lambda_k p_{jk} S(\rho_{jk}) \geq \\ &\geq \sum_k \lambda_k S\left(\sum_j p_{jk} \rho_{jk}\right) - \sum_{j,k} \lambda_k p_{jk} S(\rho_{jk}) \geq \\ &\geq \sum_k \lambda_k \left(S\left(\sum_j p_{jk} \rho_{jk}\right) - \sum_j p_{jk} S(\rho_{jk})\right) = \sum_k \lambda_k \chi(\mathcal{E}_k).\end{aligned}$$

С другой стороны, пусть M – оптимальная положительная операторнозначная мера, достигающаяся на $\chi_0(\bigcup_k \lambda_k \mathcal{E}_k)$. Тогда из общей выпуклости квантовой относительной энтропии следует, что

$$\begin{aligned}\chi_0\left(\bigcup_k \lambda_k \mathcal{E}_k\right) &= I\left(M\left(\bigcup_k \lambda_k \mathcal{E}_k\right)\right) = \\ &= I\left(\bigcup_k \lambda_k M(\mathcal{E}_k)\right) \leq \sum_k \lambda_k I(M(\mathcal{E}_k)) \leq \sum_k \lambda_k \chi_0(\mathcal{E}_k),\end{aligned}$$

а отсюда немедленно следует вогнутость меры $Q_{\text{Hol}} = \chi - \chi_0$.

Вогнутость меры $Q_{\text{FS}} = 1 - F$ следует из соотношений

$$\begin{aligned}F\left(\bigcup_k \lambda_k \mathcal{E}_k\right) &= \sup_{M, \{\sigma_{lk}\}} \sum_{j,l,k} \lambda_k p_{jk} \text{tr}(\rho_{jk} M_l) \text{tr}(\sigma_l \rho_{jk}) \leq \\ &\leq \sum_k \lambda_k \sup_{M, \{\sigma_{lk}\}} \sum_{j,l} p_{jk} \text{tr}(\rho_{jk} M_l) \text{tr}(\sigma_l \rho_{jk}) = \sum_k \lambda_k F(\mathcal{E}_k).\end{aligned}$$

Для меры Q_{clon} напомним, что в настоящей работе рассматриваются только ансамбли чистых состояний. Пусть $\rho_{jk} = |\psi_{jk}\rangle\langle\psi_{jk}|$. Тогда из соотношений

$$\begin{aligned}F_{\text{clon}}\left(\bigcup_k \lambda_k \mathcal{E}_k\right) &= \sup_U \sum_{j,k} \lambda_k p_{jk} |\langle\Psi_{jk}|\psi_{jk} \otimes \psi_{jk}\rangle|^2 \leq \\ &\leq \sum_k \lambda_k \sup_{U_k} \sum_j p_{jk} |\langle\Psi_{jk}|\psi_{jk} \otimes \psi_{jk}\rangle|^2 = \sum_k \lambda_k F_{\text{clon}}(\mathcal{E}_k)\end{aligned}$$

следует вогнутость меры $Q_{\text{clon}} = 1 - F_{\text{clon}}$.

Следующий пример показывает, что мера Q_{comm} не является вогнутой. Возьмем $\lambda_1 = \lambda_2 = 1/2$ и предположим, что

$$\mathcal{E}_1 = \left\{\frac{1}{2}, \frac{1}{2}; |0\rangle|0\rangle, |0\rangle|+\rangle\right\}, \quad \mathcal{E}_2 = \left\{\frac{1}{2}, \frac{1}{2}; |1\rangle|0\rangle, |1\rangle|+\rangle\right\}.$$

Тогда непосредственно получаем $Q_{\text{comm}}(\mathcal{E}_1) = Q_{\text{comm}}(\mathcal{E}_2) = 1/4$, но при этом $Q_{\text{comm}}(\bigcup_k \lambda_k \mathcal{E}_k) = 1/8$. Следовательно,

$$\frac{1}{8} = Q_{\text{comm}}\left(\bigcup_k \lambda_k \mathcal{E}_k\right) < \sum_k \lambda_k Q_{\text{comm}}(\mathcal{E}_k) = \frac{1}{4},$$

что противоречит предположению о вогнутости. Конечно, мера Q_{comm} не может быть выпуклой, поскольку квантовость любого ансамбля, состоящего из одного элемента, равна нулю, а любой квантовый ансамбль можно рассматривать как выпуклую комбинацию его элементов, следовательно, мера Q_{comm} , если бы она была выпуклой, всегда была равна нулю.

Благодарности. Работа выполнена при финансовой поддержке NSFC (грант № 10771208), Science Fund for Creative Research Groups (грант № 10721101) и Key Lab of Random Complex Structures and Data Science, CAS (грант № 2008DP173182).

Список литературы

- [1] C. A. Fuchs, *Just two nonorthogonal quantum states*, arXiv: quant-ph/9810032.
- [2] C. A. Fuchs, M. Sasaki, *The quantumness of a set of quantum states*, arXiv: quant-ph/0302108.
- [3] C. A. Fuchs, M. Sasaki, *Quantum Inf. Comput.*, **3**:5 (2003), 377–404.
- [4] C. A. Fuchs, *On the quantumness of a Hilbert space*, arXiv: quant-ph/0404122.
- [5] M. Horodecki, P. Horodecki, R. Horodecki, M. Piani, *Int. J. Quant. Inf.*, **4**:1 (2006), 105–118.
- [6] J. Eisert, M. B. Plenio, *J. Modern Opt.*, **46**:1 (1999), 145–154, arXiv: quant-ph/9807034.
- [7] S. Virmani, M. B. Plenio, *Phys. Lett. A*, **268**:1–2 (2000), 31–34.
- [8] C. H. Bennet, G. Brassard, “Quantum cryptography: public key distribution and coin tossing”, *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* (Bangalore, India, December 10–12, 1984), IEEE, New York, 1984, 175–179.
- [9] A. K. Ekert, *Phys. Rev. Lett.*, **67**:6 (1991), 661–663.
- [10] C. H. Bennett, *Phys. Rev. Lett.*, **68**:21 (1992), 3121–3124.
- [11] S. J. D. Phoenix, S. M. Barnett, A. Chefles, *J. Modern Opt.*, **47**:2–3 (2000), 507–516.
- [12] P. W. Shor, J. Preskill, *Phys. Rev. Lett.*, **85**:2 (2000), 441–444, arXiv: quant-ph/0003004.
- [13] N. Gisin, G. Ribordy, W. Tittel, H. Zbinden, *Rev. Modern Phys.*, **74**:1 (2002), 145–195, arXiv: quant-ph/0101098.
- [14] A. S. Holevo, *Problems Inform. Transmission*, **9**:2 (1973), 110–118.
- [15] E. Davis, *IEEE Trans. Inf. Theory*, **24**:5 (1978), 596–599.
- [16] A. Peres, W. K. Wootters, *Phys. Rev. Lett.*, **66**:9 (1991), 1119–1122.
- [17] P. Hausladen, W. K. Wootters, *J. Modern Opt.*, **41**:12 (1994), 2385–2390.
- [18] J. C. Boileau, K. Tamaki, J. Batuwantudawe, R. Laflamme, J. M. Renes, *Phys. Rev. Lett.*, **94**:4 (2005), 040503, 4 pp., arXiv: quant-ph/0408085.
- [19] J. M. Renes, R. Blume-Kohout, A. J. Scott, C. M. Caves, *J. Math. Phys.*, **45**:6 (2004), 2171–2180, arXiv: quant-ph/0310075.
- [20] A. J. Scott, M. Grassl, *J. Math. Phys.*, **51**:4 (2010), 042203, 16 pp., arXiv: 0910.5784.
- [21] D. Bruß, *Phys. Rev. Lett.*, **81**:14 (1998), 3018–3021, arXiv: quant-ph/9805019.
- [22] H. Bechmann-Pasquinucci, N. Gisin, *Phys. Rev. A*, **59**:6 (1999), 4238–4248, arXiv: quant-ph/9807041.
- [23] Z. Shadman, H. Kampermann, T. Meyer, D. Bruß, *Int. J. Quantum Inf.*, **7**:1 (2009), 297–306.
- [24] W. K. Wootters, B. D. Fields, *Ann. Phys.*, **191**:2 (1989), 363–381.
- [25] S. Luo, N. Li, W. Sun, *Quant. Inf. Processing*, **9**:6 (2010), 711–726.
- [26] S. Luo, *Phys. Rev. A*, **77**:2 (2008), 022301, 5 pp.
- [27] H. Ollivier, W. H. Zurek, *Phys. Rev. Lett.*, **88**:1 (2002), 017901, 4 pp.
- [28] L. Henderson, V. Vedral, *J. Phys. A*, **34**:35 (2001), 6899–6905, arXiv: quant-ph/0105028.

- [29] S. Luo, N. Li, X. Cao, *Period. Math. Hungar.*, **59**:2 (2009), 223–237.
- [30] R. Jozsa, D. Robb, W.K. Wootters, *Phys. Rev. A*, **49**:2 (1994), 668–677.
- [31] L. B. Levitin, “Optimal quantum measurements for two pure and mixed states”, *Quantum Communications and Measurement* (Univ. of Nottingham, Nottingham, July 10–16, 1994), eds. V. P. Belavkin, O. Hirota, R. L. Hudson, Plenum, New York, 1995, 439–448.
- [32] C. A. Fuchs, *Distinguishability and accessible information in quantum theory*, arXiv: quant-ph/9601020.
- [33] M. Sasaki, S. M. Barnett, R. Jozsa, M. Osaki, O. Hirota, *Phys. Rev. A*, **59**:5 (1999), 3325–3335, arXiv: quant-ph/9812062.
- [34] J. Mizuno, M. Fujiwara, M. Akiba, T. Kawanishi, S. M. Barnett, M. Sasaki, *Phys. Rev. A*, **65**:1 (2001), 012315, 10 pp.
- [35] W.K. Wootters, W.H. Zurek, *Nature*, **299** (1982), 802–803.
- [36] D. Dieks, *Phys. Lett. A*, **92**:6 (1982), 271–272.
- [37] H. P. Yuen, *Phys. Lett. A*, **113**:8 (1986), 405–407.
- [38] H. Barnum, C. M. Caves, C. A. Fuchs, R. Jozsa, B. Schumacher, *Phys. Rev. Lett.*, **76**:15 (1996), 2818–2821, arXiv: quant-ph/9511010.
- [39] G. Lindblad, *Lett. Math. Phys.*, **47**:2 (1999), 189–196.
- [40] V. Scarani, S. Iblisdir, N. Gisin, A. Acín, *Rev. Modern Phys.*, **77**:4 (2005), 1225–1256, arXiv: quant-ph/0511088.
- [41] H. Barnum, J. Barrett, M. Leifer, A. Wilce, *Phys. Rev. Lett.*, **99**:24 (2007), 240501, 4 pp., arXiv: 0707.0620.
- [42] A. Kalev, I. Hen, *Phys. Rev. Lett.*, **100**:21 (2008), 210502, 4 pp., arXiv: 0704.1754.
- [43] D. Bruß, D. P. DiVincenzo, A. Ekert, C. A. Fuchs, C. Macchiavello, J. A. Smolin, *Phys. Rev. A*, **57**:4 (1998), 2368–2378, arXiv: quant-ph/9705038.
- [44] A. Chefles, *Contem. Phys.*, **41**:6 (2000), 401–424, arXiv: quant-ph/0010114.
- [45] S. M. Barnett, S. Croke, *Quantum state discrimination*, arXiv: 0810.1970.
- [46] K. M. R. Audenaert, C. A. Fuchs, C. King, A. Winter, *Quantum Inf. Comput.*, **4**:1 (2004), 1–11.

Поступила в редакцию 16.12.2010