Math-Net.Ru

Общероссийский математический портал

А. А. Разборов, О квантовой коммуникационной сложности симметрических предикатов, *Изв. РАН. Сер. матем.*, 2003, том 67, выпуск 1, 159–176

DOI: <https://doi.org/10.4213/im422>

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: 3.80.181.102

26 апреля 2023 г., 10:53:21

УДК 510.52

А. А. Разборов

О квантовой коммуникационной сложности симметрических предикатов

С точностью до логарифмического множителя определяется коммуникационная сложность вычисления произвольной, зависящей лишь от $|x \cap y|$, функции $f(x, y)$, $x, y \subseteq [n]$, с допустимой вероятностью ошибки, отделенной от $1/2$. Более точно, для предиката D на множестве $\{0, 1, \dots, n\}$ полагаем

$$\begin{aligned}\ell_0(D) &\stackrel{\text{def}}{=} \max\{\ell \mid 1 \leq \ell \leq n/2 \wedge D(\ell) \neq D(\ell-1)\}, \\ \ell_1(D) &\stackrel{\text{def}}{=} \max\{n-\ell \mid n/2 \leq \ell < n \wedge D(\ell) \neq D(\ell+1)\}.\end{aligned}$$

Тогда квантовая коммуникационная сложность функции $f_D(x, y) = D(|x \cap y|)$ в этой модели равна (с точностью до логарифмического множителя) величине $\sqrt{n\ell_0(D) + \ell_1(D)}$. В частности, сложность предиката, называемого *дисъюнкцией*, оказывается равной $\Omega(\sqrt{n})$. Полученный результат выполняется как в модели с предварительным зацеплением, так и в модели без такого зацепления.

Библиография: 26 наименований.

§ 1. Введение

С момента, когда модель коммуникационной сложности была впервые рассмотрена в работе [25], она развилась в важное самостоятельное направление теории вычислительной сложности, позволяющее, в частности, взглянуть с единой точки зрения на целый ряд разнородных понятий. В этой модели участвуют два игрока, по традиции называемые *Алиса* и *Боб*. У Алисы имеется некоторый элемент x из фиксированного конечного множества X , у Боба – другой элемент $y \in Y$, и их задача состоит в вычислении некоторого (данного заранее) булевого предиката $f: X \times Y \rightarrow \{0, 1\}$ путем обмена сообщениями. Сложность измеряется суммарной битовой длиной пересланных сообщений, и так же, как и во многих других разделах теории вычислительной сложности, при этом различают детерминированные и вероятностные алгоритмы.

Точно так же, как в теории сложности булевых схем часто рассматривают симметрические булевы функции, значительный интерес в теории коммуникационной сложности представляют *симметрические предикаты*, определяемые как такие f , для которых x и y – конечные множества и значение f задается формулой

Работа выполнена во время командировки в Институт перспективных исследований (Принстон, США), поддержанной Фондом им. фон Неймана.

$f_D(x, y) = D(|x \cap y|)$, где D – некоторый булев предикат, определенный на целых числах. Два наиболее часто встречающихся в научной литературе представителя этого класса – это предикат DISJ_n ($D(s) \equiv (s = 0)$), называемый *дизъюнктивность*, и функция IP_n ($D(s) \equiv s \pmod{2}$), называемая *скалярное произведение MOD 2*. Из классической нижней оценки Мелхорна–Шмидта [19], основанной на ранге соответствующей матрицы, вытекает точная нижняя оценка¹ $\Omega(n)$ детерминированной коммуникационной сложности обоих предикатов DISJ_n и IP_n .

Что касается вероятностных алгоритмов, допускающих ошибку с вероятностью ε , где $\varepsilon < 1/2$ – произвольная абсолютная константа, в работах [4], [10] [24] была доказана нижняя оценка $\Omega(n)$ сложности функции IP_n ; статья [4] также содержала нижнюю оценку $\Omega(\sqrt{n})$ для DISJ_n . Последняя оценка была усилена до точной оценки $\Omega(n)$ в работе [18]; более простое доказательство последнего результата было впоследствии представлено в [23].

Модель *квантовой* коммуникационной сложности была предложена в работе [26]. Предположим, что Алиса и Боб могут использовать дополнительные возможности, предоставляемые законами квантовой механики, и для достижения своей цели вместо обмена классическими битами информации могут использовать кубиты. Могут ли они за счет этого уменьшить количество пересылаемой информации?

Г. Бурман, Р. Клиф и А. Вигдерсон [3] заметили, что основанная на ранге матрицы нижняя оценка для детерминированных протоколов распространяется на квантовый случай (так что, в конце концов, было бы неудивительно, если бы для случая безошибочных протоколов ответ на поставленный вопрос оказался бы отрицательным). В частности, для точного (с вероятностью 1) вычисления обоих предикатов DISJ_n и IP_n требуется пересылка по крайней мере $\Omega(n)$ кубитов. В работе [7] эта нижняя оценка была обобщена на более сильную модель с предварительным зацеплением (prior entanglement), ранее предложенную в [8] (в этой модели Алиса и Боб с самого начала обладают неограниченным запасом пар Эйнштейна–Подольского–Розена, “зацепленных” в том смысле, что Алиса имеет доступ к первой компоненте каждой пары, а Боб – ко второй).

Существенно более интересен вопрос о коммуникационной сложности в модели, допускающей небольшую ошибку. И. Кремер [17], опираясь на некоторые идеи из основополагающей работы [26], доказал точную нижнюю оценку $\Omega(n)$ для предиката IP_n . В работе [9] его результат был обобщен на модель с предварительным зацеплением. Х. Клаук [14] рассмотрел пороговые предикаты ($D(s) \equiv (s \geq \ell)$) и предикаты точного равенства ($D(s) \equiv (s = \ell)$) и в обоих случаях установил нижнюю оценку $\Omega(\ell / \log \ell)$ (в модели без предварительного зацепления). Единственная общая нижняя оценка для предиката DISJ_n (соответствующего случаю $\ell = 0$), известная до настоящей работы, имела вид $\Omega(\log n)$ [1], [7]; можно также отметить некоторые частные результаты в этом направлении, такие как оценки для прото-

¹Широко используемое в теории вычислительной сложности обозначение $\Omega(f(n))$ двойственно привычному $O(f(n))$ и обозначает произвольную функцию $g(n)$ такую, что для некоторой абсолютной константы $\varepsilon > 0$ при всех n выполнено $g(n) \geq \varepsilon f(n)$.

колов с фиксированным числом раундов [15], для протоколов с экспоненциально малой вероятностью ошибки [7] и для протоколов некоторого весьма специального вида [13].

Для верхних оценок в работе [3] была установлена тесная взаимосвязь между квантовым поиском и квантовым обменом информацией. Именно в ней было показано, что всякий алгоритм квантового поиска для произвольной булевой функции g можно превратить в квантовый коммуникационный алгоритм для вычисления ассоциированного предиката $f_g(x, y) = g(x \cap y)$ так, что сложность при этом увеличивается не более чем на логарифмический множитель. Применяя это общее сведение к алгоритму квантового поиска Гровера [12], немедленно получаем верхнюю оценку $O(\sqrt{n} \log n)$ квантовой коммуникационной сложности предиката *дизъюнктивность* в модели с небольшой допустимой ошибкой (в работе [13] эта оценка была слегка усилена до $O(\sqrt{n} \exp(\log^* n))$). В [2] было доказано, что сложность квантового поиска для любой симметрической булевой функции g с точностью до мультипликативной константы равна ее *приближенной степени* $\widetilde{\deg}(g)$, определяемой как минимальная возможная степень вещественного полинома, приближающего функцию g на множестве $\{0, 1\}^n$ в ℓ_∞ -норме с точностью до $1/3$. В сочетании с редукцией из [3], отсюда следует верхняя оценка $O(\widetilde{\deg}(g) \log n)$ квантовой коммуникационной сложности предиката $f_g(x, y)$ в модели с небольшой допустимой ошибкой.

В настоящей статье доказывается, что для произвольного симметрического предиката $f_D(x, y)$ такой коммуникационный алгоритм практически оптимален с точностью до одного “вырожденного” случая. Более точно, пусть

$$\ell_0(D) \stackrel{\text{def}}{=} \max\{\ell \mid 1 \leq \ell \leq n/2 \wedge D(\ell) \neq D(\ell - 1)\} \quad (1.1)$$

и

$$\ell_1(D) \stackrel{\text{def}}{=} \max\{n - \ell \mid n/2 \leq \ell < n \wedge D(\ell) \neq D(\ell + 1)\}, \quad (1.2)$$

и пусть $g_D(x_1, \dots, x_n) = D(|x|)$; тогда классический результат Р. Патури [22] утверждает, что $\deg(g_D) = \theta(\sqrt{n(\ell_0(D) + \ell_1(D))})$, откуда на основе результатов [3] вытекает верхняя оценка $O((\sqrt{n\ell_0(D)} + \sqrt{n\ell_1(D)}) \log n)$ квантовой коммуникационной сложности функции f_D в модели с небольшой ошибкой. Эта оценка легко усиливается до $O((\sqrt{n\ell_0(D)} + \ell_1(D)) \log n)$; если значение $|x \cap y|$ велико, то применяется очевидный алгоритм, в котором Алиса просто пересылает Бобу все x . Докажем нижнюю оценку $\Omega(\sqrt{n\ell_0(D)} + \ell_1(D))$, совпадающую с последней, с точностью до логарифмического множителя (теорема 2.1). Эта нижняя оценка распространяется на модель с предварительным зацеплением.

Для доказательства этого результата (п. 5.2) используется многомерное обобщение обычного метода отклонений (discrepancy). Иными словами, мы одновременно измеряем математические ожидания элементов коммуникационной матрицы по отношению сразу к нескольким вероятностным распределениям на ее позициях. Таким способом нам удастся свести интересующую нас задачу к классической проблеме в теории приближений дискретными полиномами, которая (весьма

кстати) была решена в упомянутой выше работе [22] (см. п. 5.3). Другая отличительная черта нашего подхода состоит в более систематическом применении спектральных (в отличие от комбинаторных) методов, чем в предыдущих работах на данную тему (важность такого подхода особенно отчетливо проявляется в модели с предварительным запутыванием). В частности, мы доказываем общую нижнюю оценку квантовой коммуникационной сложности произвольной булевой функции в терминах приближенной следовой нормы ее коммуникационной матрицы (п. 5.1).

Далее сформулируем и докажем основной результат. По мере возможности будем стараться формулировать в разумной общности те вспомогательные утверждения в доказательстве, которые могут представлять независимый интерес.

§ 2. Модель квантовой коммуникационной сложности и основной результат

Известны несколько эквивалентных определений модели квантового обмена информацией; будем следовать работе [7], так как содержащийся в ней вариант определения этой модели наиболее удобен.

Пусть X, Y – конечные множества и $f: X \times Y \rightarrow \{0, 1\}$ – произвольный булев предикат. Пусть $\mathcal{H}_A, \mathcal{C}, \mathcal{H}_B$ – конечномерные гильбертовы пространства (соответствующие кубитам, находящимся в распоряжении Алисы, кубитам, составляющим информационный канал, и кубитам Боба). Следуя работе [7], потребуем, чтобы $\mathcal{C}$ состоял из единственного кубита (иными словами, $\dim(\mathcal{C}) = 2$ и векторы $|0\rangle, |1\rangle$ образуют его ортонормированный базис).

Модели с предварительным запутыванием и без него различаются лишь выбором заранее подготовленного унитарного вектора $\text{Input}(x, y) \in \mathcal{H}_A \otimes \mathcal{C} \otimes \mathcal{H}_B$, с которого начинается обмен информацией. Отложим его определение и опишем вначале, как этот обмен происходит. *Коммуникационный протокол длины c* с полностью определяется системой унитарных операторов $U_1, U_2, \dots, U_c$, где U_i действует в пространстве $\mathcal{H}_A \otimes \mathcal{C}$ при четном i и в пространстве $\mathcal{C} \otimes \mathcal{H}_B$ – при нечетном i . Выходной (унитарный) вектор $\text{Output}(x, y)$ задается формулой

$$\text{Output}(x, y) \stackrel{\text{def}}{=} \dots (U_3 \otimes I_B)(I_A \otimes U_2)(U_1 \otimes I_B) \text{Input}(x, y), \quad (2.1)$$

где I_A, I_B – тождественные операторы на $\mathcal{H}_A$ и $\mathcal{H}_B$ соответственно. *Вероятность утвердительного ответа* рассматриваемого протокола на входе (x, y) – это результат измерения $\text{Output}(x, y)$ по отношению к кубиту $\mathcal{C}$, равный возведенной в квадрат ℓ_2 -норме его ортогональной проекции на $\mathcal{H}_A \otimes |1\rangle \otimes \mathcal{H}_B$.

Теперь опишем входной вектор $\text{Input}(x, y)$. В модели без предварительного запутывания $\mathcal{H}_A$ обладает ортонормированным базисом $\{|a, x\rangle \mid a \in W_A, x \in X\}$, где W_A – некоторое конечное множество (соответствующее чистым состояниям внутренних вычислений, производимых Алисой) с выделенным элементом 0 (начальное состояние). Аналогично, $\mathcal{H}_B$ обладает ортонормированным базисом $\{|y, b\rangle \mid b \in W_B, y \in Y\}$, и $\text{Input}(x, y) \stackrel{\text{def}}{=} |0, x\rangle|0\rangle|y, 0\rangle$.

В модели с предварительным заплетением (см. также замечание 2.4 ниже) $\mathcal{H}_A$ обладает базисом $\{|a, x, e\rangle \mid a \in W_A, x \in X, e \in E\}$, а $\mathcal{H}_B$ – базисом $\{|e, y, b\rangle \mid b \in W_B, y \in Y, e \in E\}$, где E – еще одно конечное множество, соответствующее всевозможным чистым состояниям заплетенной системы пар Эйнштейна–Подольского–Розена. Начальное состояние в этом случае задается формулой

$$\text{Input}(x, y) \stackrel{\text{def}}{=} \frac{1}{|E|^{1/2}} \sum_{e \in E} |0, x, e\rangle |0\rangle |e, y, 0\rangle. \quad (2.2)$$

Важно отметить, что в этой модели ничего не известно о $|E|$; в частности, эта величина никак не должна входить в окончательные оценки.

Протокол *вычисляет* $f(x, y)$ с ошибкой ε , если вероятность утвердительно-го ответа на входе (x, y) не превышает ε всякий раз, когда $f(x, y) = 0$, и не менее $1 - \varepsilon$, если $f(x, y) = 1$. Обозначим через $Q_\varepsilon(f)$ (соответственно, $Q_\varepsilon^*(f)$) наименьшее c , для которого существует квантовый коммуникационный протокол длины c без предварительного заплетения (соответственно, с таковым), вычисляющий f с ошибкой ε . Пусть $Q(f) \stackrel{\text{def}}{=} Q_{1/3}(f)$ и $Q^*(f) \stackrel{\text{def}}{=} Q_{1/3}^*(f)$.

Фиксируем теперь произвольное натуральное n , и пусть $D: \{0, 1, \dots, n\} \rightarrow \{0, 1\}$ – некоторый булев предикат. Пусть $f_{n,D}(x, y) \stackrel{\text{def}}{=} D(|x \cap y|)$, где $x, y \subseteq [n] \stackrel{\text{def}}{=} \{1, 2, \dots, n\}$. Зададим $\ell_0(D)$ и $\ell_1(D)$ формулами (1.1), (1.2) (если ℓ с такими свойствами не существует, естественным образом полагаем $\ell_\varepsilon(D) \stackrel{\text{def}}{=} 0$). Основным результатом настоящей работы является следующая теорема.

ТЕОРЕМА 2.1. *Для любого булевого предиката $D: \{0, 1, \dots, n\} \rightarrow \{0, 1\}$ имеет место оценка*

$$\Omega(\sqrt{n\ell_0(D)} + \ell_1(D)) \leq Q^*(f_{n,D}) \leq Q(f_{n,D}) \leq O((\sqrt{n\ell_0(D)} + \ell_1(D)) \log n).$$

Пусть $\text{DISJ}_n(x, y) \stackrel{\text{def}}{=} x \cap y = \emptyset$.

СЛЕДСТВИЕ 2.2. $Q^*(\text{DISJ}_n) \geq \Omega(\sqrt{n})$.

Доказательство нижней оценки существенно использует высокую симметрию предиката $f_{n,D}$. В частности, для доказательства необходимо, чтобы x и y были одной и той же фиксированной мощности k . Формулируем следующий вспомогательный результат ввиду того, что, несмотря на некоторую техничность, он все же может представлять самостоятельный интерес.

Пусть $k \leq n$ и $D: \{0, 1, \dots, k\} \rightarrow \{0, 1\}$. Предположим, что $X = Y \stackrel{\text{def}}{=} [n]^k$ – множество всех k -элементных подмножеств множества $[n]$ и $f_{n,k,D}: X \times Y \rightarrow \{0, 1\}$, $f_{n,k,D}(x, y) \stackrel{\text{def}}{=} D(|x \cap y|)$ (таким образом, $f_{n,D} = f_{n,n,D}$).

ТЕОРЕМА 2.3. *Пусть выполнены неравенства $k \leq n/4$, $\ell \leq k/4$ и $D: \{0, 1, \dots, k\} \rightarrow \{0, 1\}$ – произвольный предикат такой, что $D(\ell) \neq D(\ell - 1)$. Тогда $Q^*(f_{n,k,D}) \geq \Omega(\sqrt{k\ell})$.*

ЗАМЕЧАНИЕ 2.4. А. Наяк и Я. Ши заметили, что теоремы 2.1, 2.3 обобщаются на еще более сильную модель, в которой предварительное зацепление не обязательно сводится к парам Эйнштейна–Подольского–Розена. Более формально, в этой модели (ранее рассмотренной, например, в работе [21]) входной вектор имеет вид

$$\text{Input}(x, y) \stackrel{\text{def}}{=} \sum_{e \in E} \lambda_e |0, x, e\rangle |0\rangle |e, y, 0\rangle, \quad (2.3)$$

где $\{\lambda_e \mid e \in E\}$ – произвольный унитарный вектор (случай (2.2) пар Эйнштейна–Подольского–Розена соответствует вектору $\lambda_e = \frac{1}{|E|^{1/2}}$). С любезного разрешения А. Наяка и Я. Ши приводим в п. 5.1 изменения, необходимые для получения такого обобщения (см. ниже замечание 5.6).

§ 3. Предварительные сведения

В этом параграфе приведены некоторые необходимые определения и известные ранее результаты.

3.1. Квантовый поиск и квантовый обмен информацией. Точное определение *квантового разрешающего дерева* может быть найдено, например, в [6]. Для булевой функции $g(x_1, \dots, x_n)$ через $Q_{\text{DT}}(g)$ обозначим минимальное число вопросов, необходимых для вычисления g с помощью квантового разрешающего дерева с ошибкой, не превышающей $1/3$ на любом входе $x \in \{0, 1\}^n$.

Через $f_g: \mathcal{P}([n]) \times \mathcal{P}([n]) \rightarrow \{0, 1\}$ обозначим предикат $f_g(x, y) \stackrel{\text{def}}{=} g(x \cap y)$, где $x \cap y$ отождествляется с его характеристической функцией.

ПРЕДЛОЖЕНИЕ 3.1 [3]. *Для всякой булевой функции $g(x_1, \dots, x_n)$ имеет место оценка $Q(f_g) \leq O(Q_{\text{DT}}(g) \log n)$.*

3.2. Матричные нормы. Весь содержащийся в этом пункте материал – классический и может быть найден, например, в учебнике [5].

Если мы откажемся от обозначений Дирака (см. п. 5.2), все векторы будут представляться в виде вектор-столбцов. Для комплексного вектора ξ (комплексной матрицы A) через $x^* \stackrel{\text{def}}{=} (\bar{x})^\top$ (соответственно, $A^* \stackrel{\text{def}}{=} (\bar{A})^\top$) обозначим его комплексно-сопряженный вектор (соответственно, матрицу). Пусть $\|\xi\| \stackrel{\text{def}}{=} (\xi^* \xi)^{1/2}$ – ℓ_2 -норма вектора ξ .

Для комплексной матрицы A через $\|A\|$ обозначим ее *операторную норму*, определяемую как $\|A\| \stackrel{\text{def}}{=} \max\{\|A\xi\|: \|\xi\| \leq 1\}$. Эквивалентным образом, $\|A\| = \max\{\|\eta^\top A\xi\|: \|\eta\|, \|\xi\| \leq 1\}$.

Для двух комплексных матриц A, B одного и того же размера $m \times n$ через $\langle A, B \rangle$ обозначим их покомпонентное скалярное произведение, т.е.

$$\langle A, B \rangle \stackrel{\text{def}}{=} \text{Tr}(A^* B) = \sum_{i=1}^m \sum_{j=1}^n \bar{a}_{ij} b_{ij},$$

через $\|A\|_F$ обозначим *фробениусову норму*, соответствующую этому скалярному произведению:

$$\|A\|_F \stackrel{\text{def}}{=} \left(\sum_{i=1}^m \sum_{j=1}^n |a_{ij}|^2 \right)^{1/2}.$$

Необходимо также определить *следовую норму* $\|A\|_{\text{tr}}$:

$$\|A\|_{\text{tr}} \stackrel{\text{def}}{=} \max_B \{ |\langle A, B \rangle| : \|B\| \leq 1 \},$$

где B – элемент множества всех (комплексных) матриц того же размера, что и A .

Следующее предложение включает некоторые базисные свойства введенных норм.

ПРЕДЛОЖЕНИЕ 3.2. 1. Пусть $\|\cdot\|$ – любая из трех норм $\|\cdot\|$, $\|\cdot\|_F$ или $\|\cdot\|_{\text{tr}}$, и пусть A – комплексная $(m \times n)$ -матрица. Тогда выполнено следующее:

- (a) $\|A^*\| = \|A^\perp\| = \|A\|$;
- (b) если B – подматрица матрицы A , то $\|B\| \leq \|A\|$;
- (c) $\|\cdot\|$ инвариантна относительно левых и правых унитарных преобразований, т.е. для любой унитарной $(m \times m)$ -матрицы U и любой унитарной $(n \times n)$ -матрицы V выполнено $\|UAV\| = \|A\|$.

2. Пусть теперь B – еще одна комплексная $(n \times k)$ -матрица и AB обозначает обыкновенное матричное умножение. Тогда:

- (a) $\|AB\| \leq \|A\| \cdot \|B\|$;
- (b) $\|AB\|_{\text{tr}} \leq \|A\|_F \cdot \|B\|_F$ (неравенство Гёльдера; см., например, [5, следствие IV.2.6]).

3. $\|A\| \leq \|A\|_F \leq (\min\{m, n\})^{1/2} \cdot \|A\|$.

4. Для любой квадратной $(n \times n)$ -матрицы A имеет место неравенство $\|A\|_{\text{tr}} \geq \sum_{i=1}^n |a_{ii}|$.

ЗАМЕЧАНИЕ 3.3. Если $\sigma_1(A) \geq \sigma_2(A) \geq \dots \geq \sigma_p(A)$, $p = \min\{m, n\}$, – сингулярные числа матрицы A , то $\|A\| = \sigma_1(A)$, $\|A\|_F = (\sum_{t=1}^p \sigma_t^2(A))^{1/2}$ и $\|A\|_{\text{tr}} = \sum_{t=1}^p \sigma_t(A)$, что в сочетании с предложением 3.2, 1,(c) и теоремой о сингулярной декомпозиции влечет все нетривиальные утверждения в этом предложении. В нашем доказательстве, однако, характеристизация через сингулярные числа не используется.

ЗАМЕЧАНИЕ 3.4. Из предложения 3.2, 1,(c) вытекает, что операторная, фробениусова или следовая норма корректно определена для операторов, действующих из одного (конечномерного) гильбертового пространства в другое.

Помимо этого, необходимо определить ℓ_1 -норму и ℓ_∞ -норму покомпонентно:

$$\ell_1(A) \stackrel{\text{def}}{=} \sum_{1 \leq i \leq m} \sum_{1 \leq j \leq n} |a_{ij}|,$$

$$\ell_\infty(A) \stackrel{\text{def}}{=} \max_{1 \leq i \leq m} \max_{1 \leq j \leq n} |a_{ij}|.$$

Разумеется, эти нормы не инвариантны относительно унитарных преобразований. Следующее (очевидное) наблюдение, однако, позволит нам по крайней мере в какой-то степени связать их с унитарно инвариантными нормами:

$$|\langle A, B \rangle| \leq \ell_1(A) \cdot \ell_\infty(B).$$

3.3. Декомпозиция квантовых коммуникационных протоколов.

ПРЕДЛОЖЕНИЕ 3.5 (см. [26], [17]). Пусть P – квантовый коммуникационный протокол длины s и U_P – соответствующий унитарный оператор, являющийся композицией в правой части (2.1). Тогда найдутся линейные операторы A_u на $\mathcal{H}_A$ и B_u на $\mathcal{H}_B$ ($u \in \{0, 1\}^c$) такие, что для любых векторов $a \in \mathcal{H}_A$, $b \in \mathcal{H}_B$ имеет место разложение

$$U_P(|a\rangle|0\rangle|b\rangle) = \sum_{u \in \{0, 1\}^c} |A_u(a)\rangle|u_c\rangle|B_u(b)\rangle.$$

Более того, $\|A_u\|, \|B_u\| \leq 1$ для любого $u \in \{0, 1\}^c$.

ДОКАЗАТЕЛЬСТВО. В этом предложении сравнительно новым является лишь последнее замечание об оценке операторной нормы. Эта оценка, однако, непосредственно вытекает из предложения 3.2, 2.(а) и того факта, что A_u , B_u являются композициями унитарных операторов и операторов проекции на подпространства $\mathcal{H}_A \otimes |\varepsilon\rangle \otimes \mathcal{H}_B$, $\varepsilon \in \{0, 1\}$.

3.4. Симметрические функции и предикаты. Для булевого предиката $D: \{0, 1, \dots, n\} \rightarrow \{0, 1\}$ обозначим через $\widetilde{\deg}(D)$ *приближенную степень* этого предиката, определяемую как минимальную степень вещественного полинома $f(x)$ от одной переменной такого, что для любого $s \in \{0, 1, \dots, n\}$ выполнено $|f(s) - D(s)| \leq 1/3$. Пусть $g_D(x_1, \dots, x_n)$ – симметрическая булева функция, заданная формулой

$$g_D(x) \stackrel{\text{def}}{=} D\left(\sum_{i=1}^n x_i\right)$$

(отметим, что $f_{n,D}(x, y) = f_{g_D}(x, y)$). В работе [20] было замечено, что $\widetilde{\deg}(D) = \widetilde{\deg}(g_D)$, где $\widetilde{\deg}(g)$ – минимальная степень вещественного полинома от n переменных, приближающего g на множестве $\{0, 1\}^n$ относительно ℓ_∞ -нормы с точностью до $1/3$.

ПРЕДЛОЖЕНИЕ 3.6 [22]. $\widetilde{\deg}(D) = \theta(\sqrt{n(\ell_0(D) + \ell_1(D))})$.

В [2] доказано, что $\Omega(\widetilde{\deg}(g))$ в общем случае является нижней оценкой на $Q_{\text{ДТ}}(g)$. В той же работе было установлено, что для симметрических функций эта нижняя оценка точна.

ПРЕДЛОЖЕНИЕ 3.7 [2]. $Q_{\text{DT}}(g_D) \leq O(\widetilde{\deg}(D))$.

Предположим теперь, что $X = Y \stackrel{\text{def}}{=} [n]^k$. Для $0 \leq s \leq k$ обозначим через $J_{n,k,s}$ $(0, 1)$ -матрицу размера $\binom{n}{k} \times \binom{n}{k}$, строки и столбцы которой индексированы элементами $[n]^k$,

$$(J_{n,k,s})|_{xy} \stackrel{\text{def}}{=} \begin{cases} 1, & \text{если } |x \cap y| = s, \\ 0 & \text{в противном случае.} \end{cases}$$

Спектр этих матриц описывается так называемыми *полиномами Хана* (см., например, [11]). Эти полиномы, будучи классическими объектами, были открыты бесчисленное число раз в самых различных контекстах; численное выражение, наиболее удобное для наших целей, было предложено Д. Кнутом [16]; отметим, что оно было получено путем прямого вычисления собственных значений.

ПРЕДЛОЖЕНИЕ 3.8 [16]. При $k \leq n/2$ матрицы $J_{n,k,s}$, $0 \leq s \leq k$, обладают общей системой собственных пространств $E_0, E_1, \dots, E_k$. Собственное значение матрицы $J_{n,k,s}$, соответствующее собственному пространству E_t , вычисляется по формуле

$$\sum_{i=\max\{0, s+t-k\}}^{\min\{s, t\}} (-1)^{t-i} \binom{t}{i} \binom{k-i}{s-i} \binom{n-k-t+i}{k-s-t+i}.$$

§ 4. Верхняя оценка

В этом параграфе покажем, что верхняя оценка $Q(f_{n,D}) \leq O((\sqrt{n\ell_0(D)} + \ell_1(D)) \log n)$ в теореме 2.1 почти непосредственно вытекает из известных результатов, собранных в § 3.

Фиксируем предикат $D: \{0, 1, \dots, n\} \rightarrow \{0, 1\}$. По определению значение D постоянно в интервале $[\ell_0(D), n - \ell_1(D)]$. Заменяя в случае необходимости D на его отрицание, без ограничения общности можно предполагать, что в этом интервале D тождественно равен нулю. Тогда $D = D_0 \vee D_1$, где $D_0^{-1}(1) \subseteq [0, \ell_0(D) - 1]$ и $D_1^{-1}(1) \subseteq [n - \ell_1(D) + 1, n]$. Мы также имеем $f_D = f_{D_0} \vee f_{D_1}$, т.е. Алиса и Боб вычисляют функции f_{D_0} , f_{D_1} по отдельности.

Для вычисления f_{D_0} применяется редукция из предложения 3.1; с учетом предложений 3.7, 3.6 получаем оценку

$$Q(f_{D_0}) \leq O(Q_{\text{DT}}(g_{D_0}) \log n) \leq O(\widetilde{\deg}(D_0) \log n) \leq O(\sqrt{n\ell_0(D)} \log n).$$

Для вычисления f_{D_1} Алиса и Боб используют следующий очевидный (классический) протокол. Алиса, прежде всего, проверяет выполнение неравенства $|x| \leq n - \ell_1(D)$. Если $|x| \leq n - \ell_1(D)$, то заведомо выполнено равенство $f_{D_1}(x, y) = 0$, и Алиса сразу объявляет результат. В противном случае она пересылает Бобу все x целиком. На это потребуется не более $\log_2 \left(\sum_{k=n-\ell_1(D)+1}^n \binom{n}{k} \right)$ бит информации,

что в силу неравенства $\ell_1(D) \leq n/2$ оценивается как $O(\ell_1(D) \log n)$. После этого Боб вычисляет $f_{D_1}(x, y)$.

§ 5. Нижняя оценка

В этом параграфе докажем оценки из теоремы 2.1 и теоремы 2.3. Вначале с помощью непосредственной сводимости покажем, как первая оценка вытекает из второй.

ОПРЕДЕЛЕНИЕ 5.1. Для булева предиката D , определенного на $\{0, 1, \dots, n\}$, и $0 \leq r \leq n$ предикат $D - r: \{0, 1, \dots, n - r\} \rightarrow \{0, 1\}$ задается следующим образом: $(D - r)(s) \stackrel{\text{def}}{=} D(r + s)$. Пусть также $D|_k$ – ограничение D на $\{0, 1, \dots, k\}$, $k \leq n$.

ЛЕММА 5.2. Для любого предиката D , определенного на $\{0, 1, \dots, n\}$, и любых целых чисел k, r , удовлетворяющих неравенствам $0 \leq r \leq n$, $k \leq n - r$, выполнена оценка $Q^*(f_{n,D}) \geq Q^*(f_{n-r,k,(D-r)|_k})$.

ДОКАЗАТЕЛЬСТВО. Для вычисления $f_{n-r,k,(D-r)|_k}: [n-r]^k \times [n-r]^k \rightarrow \{0, 1\}$ Алиса и Боб используют оптимальный протокол для $f_{n,D}: \mathcal{P}([n]) \times \mathcal{P}([n]) \rightarrow \{0, 1\}$. С этой целью они, используя отображение $\phi(x) \stackrel{\text{def}}{=} x \cup \{n - r + 1, \dots, n\}$, просто трансформируют свои входные подмножества $x, y \in [n - r]^k$ в $\phi(x), \phi(y) \in \mathcal{P}([n])$ и применяют к паре $\phi(x), \phi(y)$ протокол для вычисления $f_{n,D}$.

ДОКАЗАТЕЛЬСТВО НИЖНЕЙ ОЦЕНКИ ИЗ ТЕОРЕМЫ 2.1 ПО МОДУЛЮ ТЕОРЕМЫ 2.3. Необходимо доказать две различные оценки: $Q^*(f_{n,D}) \geq \Omega(\sqrt{n\ell_0(D)})$ и $Q^*(f_{n,D}) \geq \Omega(\ell_1(D))$; они доказываются на основании сводимости из леммы 5.2 (хотя и с различными значениями параметров r, k). Эти параметры должны удовлетворять следующим двум условиям:

$$k \leq (n - r)/4, \quad (\ell - r) \leq k/4 \quad (5.1)$$

(возникающим из предположений теоремы 2.3), где $\ell \stackrel{\text{def}}{=} \ell_0(D)$ в случае первой оценки и $\ell \stackrel{\text{def}}{=} n - \ell_1(D)$ – в случае второй. Если эти два условия выполнены, то теорема 2.3 влечет оценку $Q^*(f_{n,D}) \geq \Omega(\sqrt{k(\ell - r)})$.

В случае $\ell \leq n/16$ (что возможно лишь при $\ell = \ell_0(D)$) просто полагаем $r \stackrel{\text{def}}{=} 0$ и $k \stackrel{\text{def}}{=} n/4$. При этом оценка теоремы 2.3 преобразуется в $\Omega(\sqrt{n\ell})$, т.е. в точности в требуемую оценку.

В случае $\ell \geq n/16$ мы полагаем $r \stackrel{\text{def}}{=} \frac{16\ell - n}{15}$ и $k \stackrel{\text{def}}{=} \frac{4}{15}(n - \ell)$, после чего неравенства (5.1) преобразуются в равенства. Тогда $\ell - r \geq \Omega(n - \ell)$ и теорема 2.3 по-прежнему влечет доказываемую оценку $Q^*(f_{n,D}) \geq \Omega(n - \ell)$.

Оставшаяся часть статьи посвящена доказательству теоремы 2.3. Доказательство разбивается на три практически независимых куска.

5.1. Нижняя оценка через приближенную следовую норму.

ОПРЕДЕЛЕНИЕ 5.3. Для вещественной матрицы M определим ее ε -приближенную следовую норму как

$$\|M\|_{\text{tr}}^\varepsilon \stackrel{\text{def}}{=} \min\{\|P\|_{\text{tr}} : \ell_\infty(M - P) \leq \varepsilon\}$$

(здесь P принимает значения из множества всех вещественных матриц того же размера, что и M).

ОПРЕДЕЛЕНИЕ 5.4. Для предиката $f: X \times Y \rightarrow \{0, 1\}$ через M_f обозначим его коммуникационную $(0, 1)$ -матрицу $(M_f)_{xy} \stackrel{\text{def}}{=} f(x, y)$.

ТЕОРЕМА 5.5. Для любого предиката $f: X \times Y \rightarrow \{0, 1\}$, где $|X| = |Y| = N$, и любого $\varepsilon > 0$ выполнено $Q_\varepsilon^*(f) \geq \Omega(\log(\|M_f\|_{\text{tr}}^\varepsilon / N))$.

ДОКАЗАТЕЛЬСТВО. Зафиксируем коммуникационный протокол с предварительным зацеплением длины c , вычисляющий предикат f с вероятностью ошибки, не превышающей ε . Пусть p_{xy} – вероятность утвердительного ответа на входе (x, y) ; представим эти вероятности в виде $(N \times N)$ -матрицы P . Тогда, очевидно, $\ell_\infty(M_f - P) \leq \varepsilon$, и необходимо лишь показать, что $\|P\|_{\text{tr}} \leq N \exp(O(c))$.

Применим декомпозицию из предложения 3.5 ко входному вектору (2.2). Получим

$$\text{Output}(x, y) = \frac{1}{|E|^{1/2}} \sum_{e \in E} \sum_{u \in \{0, 1\}^c} A_u |0, x, e\rangle |u_c\rangle B_u |e, y, 0\rangle$$

и, далее,

$$\begin{aligned} p_{xy} &= \frac{1}{|E|} \left\| \sum_{e \in E} \sum_{u \in \Pi} A_u |0, x, e\rangle B_u |e, y, 0\rangle \right\|^2 \\ &= \frac{1}{|E|} \sum_{e, f \in E} \sum_{u, v \in \Pi} (\langle f, x, 0 | A_v | A_u | 0, x, e \rangle \cdot \langle f, y, 0 | B_v | B_u | 0, y, e \rangle), \end{aligned}$$

где $\Pi \stackrel{\text{def}}{=} \{u \in \{0, 1\}^c \mid u_c = 1\}$.

Определим теперь матрицы A, B размера $N \times (|E|^2 \times |\Pi|^2)$, полагая $a_{x, (efuv)} \stackrel{\text{def}}{=} \langle f, x, 0 | A_v | A_u | 0, x, e \rangle$ и $b_{y, (efuv)} \stackrel{\text{def}}{=} \langle f, y, 0 | B_v | B_u | 0, y, e \rangle$. Тогда $P = \frac{1}{|E|} AB^\perp$ и из предложения 3.2, 2.(b) вытекает

$$\|P\|_{\text{tr}} \leq \frac{1}{|E|} \|A\|_{\text{F}} \|B\|_{\text{F}}. \quad (5.2)$$

Для оценки фробениусовых норм $\|A\|_{\text{F}}, \|B\|_{\text{F}}$ разобьем эти матрицы на $N|\Pi|^2$ блоков и интерпретируем каждый блок как матрицу размера $|E| \times |E|$. Более точно, для фиксированных $x \in X$ и $u, v \in \Pi$ обозначим через A^{xuv} квадратную матрицу размера $|E| \times |E|$, заданную формулой $a_{ef}^{xuv} \stackrel{\text{def}}{=} a_{x, (efuv)} = \langle f, x, 0 | A_v | A_u | 0, x, e \rangle$. Тогда

$$\|A\|_{\text{F}}^2 \leq N |\Pi|^2 \max_{x, u, v} \|A^{xuv}\|_{\text{F}}^2. \quad (5.3)$$

Для оценки $\|A^{xuv}\|_F$ сначала используем утверждение 3 предложения 3.2:

$$\|A^{xuv}\|_F \leq |E|^{1/2} \|A^{xuv}\|. \quad (5.4)$$

Наконец, мы утверждаем, что

$$\|A^{xuv}\| \leq 1. \quad (5.5)$$

В самом деле, рассмотрим произвольные векторы η, ξ длины $|E|$ такие, что $\|\eta\|, \|\xi\| \leq 1$. Тогда

$$\eta^\top A^{xuv} \xi = \left\langle \sum_{f \in E} \eta_f f, x, 0 \middle| A_v \middle| A_u \middle| 0, x, \sum_{e \in E} \xi_e e \right\rangle,$$

и ввиду того, что $\|A_u\|, \|A_v\| \leq 1$, имеем

$$\begin{aligned} \|\eta^\top A^{xuv} \xi\| &\leq \left\| A_u \middle| 0, x, \sum_{e \in E} \xi_e e \right\rangle \left\| \left\| A_v \middle| 0, x, \sum_{f \in E} \eta_f f \right\rangle \right\| \\ &\leq \left\| \middle| 0, x, \sum_{e \in E} \xi_e e \right\rangle \right\| \left\| \middle| 0, x, \sum_{f \in E} \eta_f f \right\rangle \right\| = \|\xi\| \|\eta\| \leq 1. \end{aligned}$$

Неравенство (5.5) доказано. Отсюда и из неравенств (5.4), (5.3) вытекает оценка $\|A\|_F \leq N^{1/2} |\Pi| |E|^{1/2}$; аналогичная оценка справедлива также для $\|B\|_F$. Подставляя эти оценки в (5.2), получаем $\|P\|_{\text{tr}} \leq N |\Pi|^2 \leq N \exp(O(c))$, что завершает доказательство теоремы 5.5.

ЗАМЕЧАНИЕ 5.6 (А. Наяк, Я. Ши). Теорема 5.5 (и, следовательно, все нижние оценки, доказанные с ее помощью) обобщается на случай произвольного зацепления, при котором входной вектор задается в виде (2.3). Чтобы убедиться в этом, отметим, прежде всего, следующее обобщение неравенства в правой части предложения 3.2, 3:

$$\|LA\|_F \leq \|L\|_F \|A\| \quad (5.6)$$

(исходное утверждение соответствует случаю $L = I_{\min\{m,n\}}$). Для $\hat{a}_{x,(efuv)} \stackrel{\text{def}}{=} \lambda_e a_{x,(efuv)}$ и $\hat{b}_{y,(efuv)} \stackrel{\text{def}}{=} \lambda_f b_{y,(efuv)}$ мы имеем $\hat{P} = \hat{A} \hat{B}^\top$, где $\hat{P}$ – матрица вероятностей по отношению к исходному вектору (2.3); кроме того, $\|\hat{P}\|_{\text{tr}} \leq \|\hat{A}\|_F \|\hat{B}\|_F$. Как и ранее, $\|\hat{A}\|_F^2 \leq N |\Pi|^2 \max_{x,u,v} \|\hat{A}^{xuv}\|_F^2$. Нам, однако, известно, что $\hat{A}^{xuv} = L A^{xuv}$, где L – диагональная матрица с элементами $\{\lambda_e \mid e \in E\}$. Поскольку вектор λ унитарен, $\|L\|_F = 1$ и из (5.6) вытекает неравенство $\|\hat{A}^{xuv}\|_F \leq \|A^{xuv}\| \leq 1$. Оставшиеся вычисления проводятся так же, как и в исходном доказательстве.

5.2. Метод многомерных отклонений. Этот пункт составляет ядро всего нашего доказательства, поэтому мы начнем с краткого неформального описания метода, основанного на оценке обыкновенного (одномерного) отклонения.

Предположим, что мы хотим получить нижнюю оценку для приближенной следовой нормы (или любой другой приближенной нормы) матрицы M . Иными словами, мы хотим вывести противоречие из существования декомпозиции $M = P + \Delta$, где $\|P\|_{\text{tr}}$ и $\ell_\infty(\Delta)$ малы. Обыкновенный метод отклонений [26], [17] для решения этой задачи состоит в следующем. Предположим для простоты, что $M - (\pm 1)$ -матрица, рассмотрим произвольное вероятностное распределение μ на ее позициях и образуем адамарово произведение $M \circ \mu$ $((M \circ \mu)_{ij} \stackrel{\text{def}}{=} M_{ij}\mu_{ij})$. Тогда $\langle M, M \circ \mu \rangle = 1$ и $|\langle \Delta, M \circ \mu \rangle| \leq \ell_1(M \circ \mu) \cdot \ell_\infty(\Delta) = \ell_\infty(\Delta)$. Следовательно, если $|\langle P, M \circ \mu \rangle|$ мало для любой матрицы P с малой следовой нормой (иными словами, $M \circ \mu$ имеет *малое отклонение* по отношению к таким матрицам), то наша цель достигнута.

Следующий логический шаг в этом направлении был сделан Х. Клауком [14, теорема 4], заметившим, что “тестовая матрица”, по отношению к которой измеряется отклонение, не обязана иметь специфический вид $M \circ \mu$. Коль скоро μ – произвольная матрица с $\ell_1(\mu) = 1$, обладающая свойством малого отклонения, мы все еще можем установить искомую нижнюю оценку для любой матрицы M , для которой $|\langle M, \mu \rangle|$ достаточно велико.

Хорошо известно, что даже в такой обобщенной форме одномерный метод отклонений не применим, например, к предикату *дизъюнктность*. Для преодоления этой трудности в настоящей статье мы делаем еще один шаг и вместо линейного функционала $X \mapsto \langle X, \mu \rangle$ для единственной “тестовой матрицы” μ рассматриваем многомерный “оператор следа” $X \mapsto (\langle X, \mu_1 \rangle, \dots, \langle X, \mu_r \rangle)$ для целого семейства матриц $\mu_1, \dots, \mu_r$, обладающих свойством $\ell_1(\mu_s) \leq 1$. Для успешного применения спектральных методов нам придется потребовать, чтобы $\mu_1, \dots, \mu_r$ были попарно коммутирующими вещественными симметрическими матрицами (хотя, на самом деле, было бы достаточно лишь потребовать наличия одновременного сингулярного разложения $U\mu_1V, \dots, U\mu_rV$ для произвольных унитарных матриц U, V).

ОПРЕДЕЛЕНИЕ 5.7. *r-мерный тест на отклонения* по определению состоит из попарно коммутирующих вещественных симметрических матриц $\mu_1, \dots, \mu_r$ со свойством $\ell_1(\mu_s) \leq 1$, $1 \leq s \leq r$, одного и того же размера $N \times N$, а также ортогонального разложения

$$\mathbb{R}^N = E_1 \oplus E_2 \oplus \dots \oplus E_k \quad (5.7)$$

пространства $\mathbb{R}^N$ в прямую сумму их общих собственных пространств $E_1, E_2, \dots, E_k$.

Отметим, что коммутативность сама по себе уже влечет существование по крайней мере одного разложения вида (5.7). Для нас, однако, существенно, что $k \ll N$ (или, иными словами, среди собственных значений матриц μ_s много совпадающих), и по этой причине мы предпочитаем явно фиксировать интересующее нас разложение в определении.

Для данного теста на отклонения $(\mu_1, \dots, \mu_r, E_1, \dots, E_k)$ обозначим через λ_{st} собственное значение матрицы μ_s , соответствующее собственному пространству E_t . Следом E_t назовем r -мерный вектор λ^t , определяемый естественным образом как $(\lambda^t)_s \stackrel{\text{def}}{=} \lambda_{st}$. Пусть $\text{Trace}(\bar{\mu}, \bar{E}) \stackrel{\text{def}}{=} \{\lambda^t \in \mathbb{R}^r \mid 1 \leq t \leq k\}$ – множество всех таких векторов.

ОПРЕДЕЛЕНИЕ 5.8. Для множества векторов $T \subseteq \mathbb{R}^r$ и $C > 0$ обозначим через $\text{Conv}_C(T) \stackrel{\text{def}}{=} \{\sum_{\lambda \in T} a_\lambda \lambda : \sum_{\lambda \in T} |a_\lambda| \leq C\}$ выпуклую оболочку множества сегментов $\{[-C, C]\lambda \mid \lambda \in T\}$. Если $\xi \in \mathbb{R}^r$ – еще один вектор в том же пространстве и $\varepsilon > 0$, то $\phi^\varepsilon(\xi, T) \stackrel{\text{def}}{=} \min\{C \mid \rho_\infty(\xi, \text{Conv}_C(T)) \leq \varepsilon\}$, где ρ_∞ – расстояние, соответствующее ℓ_∞ -норме.

ТЕОРЕМА 5.9. Пусть M – квадратная вещественная матрица и $(\mu_1, \dots, \mu_r, E_1, \dots, E_k)$ – произвольный r -мерный тест того же размера. Определим $\xi_M \in \mathbb{R}^r$ формулой $(\xi_M)_s \stackrel{\text{def}}{=} \langle M, \mu_s \rangle$. Тогда

$$\|M\|_{\text{tr}}^\varepsilon \geq \phi^\varepsilon(\xi_M, \text{Trace}(\bar{\mu}, \bar{E})).$$

ДОКАЗАТЕЛЬСТВО. Пусть $\|M\|_{\text{tr}}^\varepsilon = C$; фиксируем разложение $M = P + \Delta$, где $\|P\|_{\text{tr}} = C$ и $\ell_\infty(\Delta) \leq \varepsilon$. Тогда $\xi_M = \xi_P + \xi_\Delta$ и, более того, $|(\xi_\Delta)_s| = |\langle \Delta, \mu_s \rangle| \leq \ell_1(\mu_s) \ell_\infty(\Delta) \leq \varepsilon$ для любого $s \in [r]$, откуда вытекает $\ell_\infty(\xi_\Delta) \leq \varepsilon$. Таким образом, осталось показать, что $\xi_P \in \text{Conv}_C(\text{Trace}(\bar{\mu}, \bar{E}))$.

Выберем произвольную ортогональную матрицу U , соответствующую разложению (5.7), таким образом, что все $(U^\top \mu_s U)$ диагональны. Введем в рассмотрение матрицу $(U^\top P U)$, для всякого $t \in [k]$ обозначим через $(U^\top P U)_t$ ее главную подматрицу, соответствующую собственному пространству E_t , и положим $a_t \stackrel{\text{def}}{=} \text{Tr}((U^\top P U)_t)$. Тогда требуемое свойство $\xi_P \in \text{Conv}_C(\text{Trace}(\bar{\mu}, \bar{E}))$ вытекает из следующих двух утверждений:

$$\xi_P = \sum_{t=1}^k a_t \lambda^t$$

и

$$\sum_{t=1}^k |a_t| \leq C.$$

Оба эти утверждения доказываются с помощью простых матричных преобразований и оценок (для которых существенно используется предложение 3.2):

$$(\xi_P)_s = \langle P, \mu_s \rangle = \langle (U^\top P U), (U^\top \mu_s U) \rangle = \sum_{t=1}^k \text{Tr}((U^\top P U)_t) \lambda_{st} = \sum_{t=1}^k a_t \lambda_{st}$$

и

$$\sum_{t=1}^k |a_t| \leq \sum_{i=1}^N |(U^\top P U)_{ii}| \leq \|(U^\top P U)\|_{\text{tr}} = \|P\|_{\text{tr}} = C.$$

5.3. Завершение доказательства теоремы 2.3. Фиксируем целые числа n и $k \leq n/4$. Пусть $N \stackrel{\text{def}}{=} \binom{n}{k}$, $D: \{0, 1, \dots, k\} \rightarrow \{0, 1\}$ – произвольный предикат и $\ell \leq k/4$ таково, что имеет место $D(\ell) \neq D(\ell - 1)$. Применив теорему 5.5 (и отметив, что вероятность ошибки всегда может быть понижена с $1/3$ до $1/4$ за счет увеличения сложности не более чем на мультипликативную константу), получим

$$Q^*(f_{n,k,D}) \geq \Omega(\log(\|M_{f_{n,k,D}}\|_{\text{tr}}^{1/4}/N)). \quad (5.8)$$

Пусть теперь $\mu_s \stackrel{\text{def}}{=} N^{-1} \binom{k}{s}^{-1} \binom{n-k}{k-s}^{-1} J_{n,k,s}$ и $E_0, \dots, E_k$ – общие собственные пространства этих матриц, фигурирующие в предложении 3.8. Отметим, что $\ell_1(\mu_s) = 1$ и $\langle M_{f_{n,k,D}}, \mu_s \rangle = D(s)$. Применяя теорему 5.9 к $(k/2+1)$ -мерному тесту $(\mu_0, \mu_1, \dots, \mu_{k/2}, E_0, E_1, \dots, E_k)$, получим

$$\|M_{f_{n,k,D}}\|_{\text{tr}}^{1/4} \geq \phi^{1/4}(D|_{k/2}, \text{Trace}(\bar{\mu}, \bar{E})). \quad (5.9)$$

УТВЕРЖДЕНИЕ 5.10. Пусть λ_{st} – собственное значение матрицы μ_s , соответствующее собственному пространству E_t . Тогда:

- 1) $\lambda_{st} = F_t(s)$, где F_t – полином степени t , совпадающий, с точностью до нормализующего множителя, с полиномом Хана;
- 2) всякий раз, когда $k \leq n/4$ и $s \leq k/2$, имеет место оценка $|\lambda_{st}| \leq N^{-1} \exp(-\Omega(t))$.

ДОКАЗАТЕЛЬСТВО. Согласно предложению 3.8 имеем

$$\begin{aligned} \lambda_{st} &= N^{-1} \binom{k}{s}^{-1} \binom{n-k}{k-s}^{-1} \\ &\quad \times \sum_{i=\max\{0, s+t-k\}}^{\min\{s, t\}} (-1)^{t-i} \binom{t}{i} \binom{k-i}{s-i} \binom{n-k-t+i}{k-s-t+i} \\ &= N^{-1} \sum_{i=\max\{0, s+t-k\}}^{\min\{s, t\}} (-1)^{t-i} \binom{t}{i} \frac{\binom{k-i}{s-i}}{\binom{k}{s}} \frac{\binom{n-k-t+i}{k-s-t+i}}{\binom{n-k}{k-s}} \\ &= N^{-1} \sum_{i=0}^t \left((-1)^{t-i} \binom{t}{i} \frac{s(s-1)\dots(s-i+1)}{k(k-1)\dots(k-i+1)} \right. \\ &\quad \left. \times \frac{(k-s)(k-s-1)\dots(k-s-t+i+1)}{(n-k)(n-k-1)\dots(n-k-t+i+1)} \right). \end{aligned}$$

Утверждение 1) непосредственно вытекает из этого представления. Утвержде-

ние 2) также легко из него следует:

$$\begin{aligned}
|\lambda_{st}| &\leq N^{-1} \sum_{i=0}^t \left(\binom{t}{i} \frac{s(s-1)\dots(s-i+1)}{k(k-1)\dots(k-i+1)} \right. \\
&\quad \times \left. \frac{(k-s)(k-s-1)\dots(k-s-t+i+1)}{(n-k)(n-k-1)\dots(n-k-t+i+1)} \right) \\
&\leq N^{-1} \sum_{i=0}^t \binom{t}{i} \left(\frac{s}{k} \right)^i \left(\frac{k-s}{n-k} \right)^{t-i} \\
&= N^{-1} \left(\frac{s}{k} + \frac{k-s}{n-k} \right)^t \leq N^{-1} \left(\frac{1}{2} + \frac{1}{3} \right)^t.
\end{aligned}$$

Из этого утверждения вытекает, что для любого $t_0 \leq k$ выполнена оценка $\{\lambda^t \mid t \leq t_0\} \subseteq P(t_0)$, где $P(t_0)$ – множество всех вещественнозначных функций на $\{0, 1, \dots, k/2\}$, представимых в виде (вещественных) полиномов степени не более t_0 . С другой стороны, $\ell_\infty(\lambda^t) \leq N^{-1} \exp(-\Omega(t_0))$ для любого $t \geq t_0$. Поэтому

$$\forall \xi \in \text{Conv}_C(\text{Trace}(\bar{\mu}, \bar{E})) \quad \rho_\infty(\xi, P(t_0)) \leq N^{-1} C \exp(-\Omega(t_0)). \quad (5.10)$$

Полагаем теперь $t_0 \stackrel{\text{def}}{=} \widetilde{\deg}(D|_{k/2}) - 1$ и $C \stackrel{\text{def}}{=} \phi^{1/4}(D|_{k/2}, \text{Trace}(\bar{\mu}, \bar{E}))$. Отметим, что из $\ell \leq k/4$ на основании предложения 3.6 вытекает неравенство

$$t_0 \geq \Omega(\sqrt{k\ell}). \quad (5.11)$$

Помимо этого, согласно определению приближенной степени имеет место оценка $\rho_\infty(D|_{k/2}, P(t_0)) > 1/3$. С другой стороны, в силу (5.10) имеем

$$\begin{aligned}
\rho_\infty(D|_{k/2}, P(t_0)) &\leq N^{-1} C \exp(-\Omega(t_0)) + \rho_\infty(D|_{k/2}, \text{Conv}_C(\text{Trace}(\bar{\mu}, \bar{E}))) \\
&\leq N^{-1} C \exp(-\Omega(t_0)) + 1/4.
\end{aligned}$$

Сравнивая эти две оценки, с учетом (5.11) получаем

$$\phi^{1/4}(D|_{k/2}, \text{Trace}(\bar{\mu}, \bar{E})) = C \geq N \exp(\Omega(\sqrt{k\ell})). \quad (5.12)$$

Утверждение теоремы 2.3 следует из соотношений (5.8), (5.9) и (5.12).

Автор признателен Андрису Амбайнису и Ави Вигдерсону за несколько полезных обсуждений, Ноге Алону, обратившему внимание автора на работу [16], Хармуту Клауку, указавшему на неточность в предварительном варианте настоящей работы, а также Ашвину Наяку и Яююну Ши за их любезное разрешение включить замечание 5.6.

Список литературы

1. *Ambainis A., Schulman L., Ta-Shma A., Vazirani U., Wigderson A.* The quantum communication complexity of sampling // Proceedings of the 39th IEEE Symposium on Foundations of Computer Science. 1998. P. 342–351.
2. *Beals R., Buhrman H., Cleve R., Mosca M., de Wolf R.* Quantum lower bounds by polynomials // Proceedings of the 39th IEEE Symposium on Foundations of Computer Science. 1998. P. 352–361. Preliminary version available at quant-ph/9802049.
3. *Buhrman H., Cleve R., Wigderson A.* Quantum vs. classical communication and computation // Proceedings of the 30th ACM Symposium on the Theory of Computing. 1998. P. 63–86. Preliminary version available at quant-ph/9802040.
4. *Babai L., Frankl P., Simon J.* Complexity classes in communication complexity theory // Proceedings of the 27th IEEE FOCS. 1986. P. 337–347.
5. *Bhatia R.* Matrix Analysis. Graduate texts in mathematics. V. 169. Berlin–N. Y.: Springer-Verlag, 1997.
6. *Buhrman H., de Wolf R.* Complexity measures and decision tree complexity: a survey // Theoretical Computer Science. 2000.
7. *Buhrman H., de Wolf R.* Communication complexity lower bounds by polynomials // Proceedings of the 16th IEEE Conference on Computational Complexity. 2001. P. 120–130. Preliminary version available at cs.CC/9910010.
8. *Cleve R., Buhrman H.* Substituting quantum entanglement for communication // Phys. Rev. A. 1997. V. 56. P. 1201–1204. Preliminary version available at quant-ph/9704026.
9. *Cleve R., van Dam W., Nielsen M., Tapp A.* Quantum entanglement and the communication complexity of the inner product function // Proceedings of the 1st NASA QCQC Conference. Lecture Notes in Computer Science. V. 1509. N. Y.–Berlin: Springer-Verlag, 1998. P. 61–74. Preliminary version available at quant-ph/9708019.
10. *Chor B., Goldreich O.* Unbiased bits from sources of weak randomness and probabilistic communication complexity // SIAM J. on Computing. 1988. V. 17. № 2. P. 230–261.
11. *Delsarte Ph.* Hahn polynomials, discrete harmonics and t -designs // SIAM J. on Applied Mathematics. 1978. V. 34. № 1. P. 157–166.
12. *Grover L. K.* A fast quantum mechanical algorithm for database search // Proceedings of the 28th ACM Symposium on the Theory of Computing. 1996. P. 212–219. Preliminary version available at quant-ph/9605043.
13. *Høyer P., de Wolf R.* Improved quantum communication complexity bounds for disjointness and equality // Proceedings of the 19th Annual Symposium on Theoretical Aspects of Computer Science. 2002. P. 299–310. Preliminary version available at quant-ph/0109068.
14. *Klauck H.* Lower bounds for quantum communication complexity // Proceedings of the 42nd IEEE Symposium on Foundations of Computer Science. 2001. P. 288–297. Preliminary version available at quant-ph/0106160.
15. *Klauck H., Nayak A., Ta-Shma A., Zuckerman D.* Interaction in quantum communication and the complexity of set disjointness // Proceedings of the 33rd ACM Symposium on the Theory of Computing. 2001. P. 124–133.
16. *Knuth D.* Combinatorial matrices: Manuscript available at <http://www-cs-faculty.stanford.edu/~knuth/preprints.html#unpub>, 1991.
17. *Kremer I.* Quantum communication. Master's thesis. Jerusalem: Hebrew University, 1995.
18. *Kalyanasundaram B., Schnitger G.* The probabilistic communication complexity of set intersection // SIAM J. on Discrete Mathematics. 1992. V. 5. № 4. P. 545–557.

19. *Mehlhorn K., Schmidt E. M.* Las Vegas is better than determinism in VLSI and distributive computing // Proceedings of the 14th ACM STOC. 1982. P. 330–337.
20. *Nisan N., Szegedy M.* On the degree of Boolean functions as real polynomials // Computational complexity. 1994. V. 4. P. 301–313.
21. *Nayak A., Salzman J.* On communication over an entanglement-assisted quantum channel // Proceedings of the 34th ACM Symposium on the Theory of Computing. 2002.
22. *Paturi R.* On the degree of polynomials that approximate symmetric Boolean functions // Proceedings of the 24th ACM Symposium on the Theory of Computing. 1992. P. 468–474.
23. *Razborov A.* On the distributional complexity of disjointness // Theoretical Computer Science. 1992. V. 106. P. 385–390.
24. *Vazirani U.* Towards a strong communication complexity theory of generating quasi-random sequences from two communicating slightly-random sources // Combinatorica. 1987. V. 7. № 4. P. 375–392.
25. *Yao A.* Some complexity questions related to distributive computing // Proceedings of the 11th ACM STOC. 1979. P. 209–213.
26. *Yao A.* Quantum circuit complexity // Proceedings of the 34th IEEE Symposium on Foundations of Computer Science. 1993. P. 352–361.

Математический ин-т им. В. А. Стеклова РАН

Поступило в редакцию
29.IV.2002