ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Январь—март 2006. Серия 1. Том 13, № 1. 45–64

УДК 519.72

О МОДЕЛИРОВАНИИ КВАНТОВЫХ И КЛАССИЧЕСКИХ БИНАРНЫХ ПРОГРАММ*)

А. Ф. Гайнутдинова

Рассматриваются сложностные классы, определяемые на основе бинарных программ. Доказываются основные соотношения между классами сложности, определяемые вероятностными и квантовыми бинарными программами (как один раз, так и много раз измеряемыми), вычисляющими с изолированной и неизолированной ошибкой. Для доказательства разработаны метод «линейного моделирования» квантовой бинарной программы и метод «квантового моделирования» вероятностной бинарной программы.

Введение

История квантовых вычислений берёт своё начало с 80-х годов прошлого века, когда Ю. И. Манин [8] и Р. Фейнман [13] высказали идею, что поскольку моделирование квантовых процессов на классических компьютерах является сложной задачей, то, возможно, использование квантовых эффектов может оказаться полезным для решения классических задач. В последние годы в области теории квантовых вычислений опубликован ряд книг, в частности, на русском языке вышли книги [3, 6].

В 90-х годах прошлого века построены эффективные квантовые алгоритмы решения некоторых известных задач. В частности, были предложены полиномиальный квантовый алгоритм Шора [20] факторизации чисел и алгоритм Гровера [14] поиска в неупорядоченной базе данных. В связи с этим важным является исследование сравнительной сложности классических моделей вычислений и их квантовых аналогов. В частности, исследуются различные вычислительные модели с ограничениями (например, конечные автоматы [12, 16], схемы с ограничениями [17, 21]). Одной из таких моделей являются бинарные программы — модель для вычисления булевых функций. Интерес к данной модели, в частности,

*)Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований (проект 03-01-00769).

обусловлен тем, что логарифм сложности бинарной программы соответствует объему памяти машины Тьюринга, а максимальная длина вычислительного пути — времени вычисления. Модель квантовой бинарной программы, определенная как обобщение соответствующей вероятностной забывающей модели, впервые была определена в [9]. Эта модель определяется как последовательность унитарных эволюций квантовой системы с заключительным измерением. В настоящей статье такие бинарные программы называем один раз измеряемыми квантовыми бинарными программами. Известная модель перестановочных бинарных программ, рассмотренная в [1], является частным случаем такой модели. Напомним, что класс функций, вычислимых перестановочными бинарными программами полиномиальной сложности, совпадает с классом функций, вычислимых схемами из функциональных элементов логарифмической глубины полиномиальной сложности [1]. В [4] был приведен пример функции, для которой квантовые бинарные программы могут быть экспоненциально экономнее как детерминированных, так и вероятностных «стабильных» бинарных программ. Под «стабильными» понимаются бинарные программы, у которых преобразования, соответствующие одному и тому же значению входной переменной, не зависят от номера уровня, на котором они применяются.

В настоящей статье рассматривается модель квантовой бинарной программы, допускающей измерение текущей конфигурации после каждого вычислительного шага. Такие бинарные программы называем много раз измеряемыми квантовыми бинарными программами. При этом модель один раз измеряемых квантовых бинарных программ является частным случаем модели много раз измеряемых квантовых бинарных программ.

В статье рассматриваются сложностные классы, определяемые на основе бинарных программ. Доказываются основные соотношения между классами сложности, определяемые вероятностными и квантовыми бинарными программами (как один раз, так и много раз измеряемыми), вычисляющими с изолированной и неизолированной ошибкой. Для доказательства разработаны метод «линейного моделирования» квантовой бинарной программы и метод «квантового моделирования» вероятностной бинарной программы. Результаты, представленные в данной статье, докладывались на VIII Международном семинаре «Дискретная математика и ее приложения» в феврале 2004 г. [5].

1. Основные определения

Детерминированная бинарная программа (BP — branching program) над множеством переменных $X = \{x_1, \ldots, x_n\}$ — это ориентированный

ациклический граф с конечными вершинами, помеченными 0 или 1 (будем называть их *отвергающими* и *принимающими* вершинами соответственно). Каждая внутренняя вершина помечена булевской переменной $x \in X$ и имеет две исходящие дуги, помеченные 0 и 1. Вероятностная программа вычисляет булеву функцию $f : \{0,1\}^n \to \{0,1\}$ следующим образом. Вычисление значения $f(\sigma)$ для входного набора $\sigma \in \{0,1\}^n$ начинается в выделенной начальной вершине. Для каждой внутренней вершины, помеченной переменной x_j, осуществляется переход из этой вершины либо по 0-дуге, либо по 1-дуге в соответствии со значением σ_j, которое принимает переменная x_j во входном наборе. Значение функции f для входа σ — это значение, приписанное достигнутой вершине.

Вероятностная бинарная программа (PBP) была впервые определена Ф. Аблаевым и М. Карпинским [10] как естественное обобщение детерминированной бинарной программы. В статье будем пользоваться следующим определением.

Вероятностная бинарная программа (PBP) — это бинарная программа, в которой каждая внутренняя вершина имеет выходную степень не менее 2. При этом из каждой внутренней вершины выходит два типа дуг, которые помечены 0 или 1. Каждой дуге e приписана такая вероятность $p(e)$, $p(e)$ — рациональное число, $0 \leqslant p(e) \leqslant 1$, что для каждой вершины сумма вероятностей всех дуг, исходящих из этой вершины и помеченных 0 (или 1), равна 1. Вычисление на входном наборе $\sigma \in \{0,1\}^n$ осуществляется следующим образом. На каждом шаге, начиная с выделенной начальной вершины, PBP P считывает значение переменной, приписанной вершине, и в зависимости от значения считанной переменной переходит в следующие вершины либо по 0-дугам, либо по 1-дугам с вероятностями, приписанными соответствующим дугам. Вероятность $Pr^P_{acc}(\sigma)$ принятия PBP P входа σ — это вероятность того, что вычисление на входе σ приведёт в конечную вершину, помеченную 1.

В [18] определена модель квантовой бинарной программы (QBP) как обобщение вероятностной бинарной программы. В ней, в отличие от вероятностной модели, каждой дуге e приписана не вероятность $p(e)$, а амплитуда $w(e)$ ($w(e)$ — комплексное число, $0 \leqslant |w(e)| \leqslant 1$) такая, что если $E_0(v)$ ($E_1(v)$) — множество дуг, выходящих из вершины v, помеченных 0 (или 1), то $\sum\limits_{e \in E_0(v)} |w(e)|^2 = 1$ $\left(\sum\limits_{e \in E_1(v)} |w(e)|^2 = 1 \right)$. Множество всех вершин квантовой бинарной программы разбито на три непересекающихся подмножества: Q_{acc}, Q_{rej} и Q_{non} («принимающих», «отвергающих» и «продолжающих»). Вычисление на входном наборе $\sigma \in \{0,1\}^n$ осуществ-

ляется следующим образом. На каждом шаге работы QBP P находится в суперпозиции всех своих вершин, где каждая вершина представлена с соответствующей амплитудой. Бинарная программа начинает работу с начальной суперпозиции, в которой начальная вершина бинарной программы представлена с амплитудой 1, остальные амплитуды равны нулю. Каждый шаг работы состоит из двух частей — измерения и преобразования. Сначала производится измерение текущей суперпозиции. При этом вероятность оказаться в вершине равна квадрату соответствующей амплитуды. Если результатом измерения является вершина из множества Q_{acc} (Q_{rej}), то вычисление заканчивается и выдается ответ 1 (или 0). Если результатом измерения является вершина из множества Q_{non}, то работа квантовой бинарной продолжается. Преобразование, выполняемое бинарной программой, должно быть унитарным, или, иначе говоря, должно удовлетворять соотношению:

$$\sum_{v} \delta(v_1, a, v)^* \delta(v_2, a, v) = \begin{cases} 1, & v_1 = v_2, \\ 0, & v_1 \neq v_2, \end{cases}$$

где $\delta(v, a, v') = w(e)$ — амплитуда дуги e с пометкой $a, (a \in \{0, 1\})$, ведущей из вершины v в вершину v'. Вероятность $Pr^P_{acc}(\sigma)$ принятия QBP P входа σ — это вероятность того, что вычисление на входе σ приведет в вершину из множества Q_{acc}.

Модель квантовой бинарной программы, определенная в работе [19], в основном аналогична модели из [18]. Отличие состоит в том, что в графе, определяющем бинарную программу, допускаются циклы.

Сложность $\mathrm{Size}(P)$ бинарной программы P — это число её внутренних вершин.

Длина $\mathrm{Depth}(P)$ бинарной программы P равна числу дуг самого длинного пути из начальной вершины в конечную.

Длина бинарной программы очевидным образом оценивает время, требуемое для вычисления функции f в худшем случае. Сложность бинарной программы оценивает память, затрачиваемую в процессе вычисления.

Бинарная программа называется *уровневой*, если множество её вершин разбито на уровни $0, 1, \ldots$ таким образом, что для каждого i дуги, исходящие из вершин уровня i, ведут только в вершины уровня $i + 1$.

Известно, что каждая бинарная программа P может быть преобразована в уровневую бинарную программу P', вычисляющую ту же самую функцию. При этом длина вероятностной бинарной программы не изменится, а сложность возрастет не более чем в квадрат [11].

Ширина $\mathrm{Width}(P)$ уровневой бинарной программы P — это максимальное число вершин на уровне, взятое по всем уровням программы P.

Уровневая бинарная программа называется *забывающей*, если во всех вершинах одного уровня считывается одна и та же переменная. Известно [1], что уровневая бинарная программа может быть преобразована в забывающую путем полиномиального увеличения длины и удвоения ширины.

Всюду в статье рассматриваются бинарные программы полиномиальной сложности. Поскольку в результате указанного выше преобразования бинарной программы в уровневую забывающую программу получается программа полиномиальной сложности, далее мы рассматриваем только такие бинарные программы. Без ограничения общности считаем, что на каждом уровне бинарной программы содержится одинаковое число вершин, перенумерованных числами $1, \ldots, d$ (будем называть их состояниями). Тогда в процессе вычисления макросостояние бинарной программы может быть описано при помощи вектора ψ распределения состояний на уровне, и шаг работы бинарной программы состоит в преобразовании вектора ψ. Поэтому уровневые забывающие бинарные программы можно рассматривать как частный случай линейных бинарных программ, которые мы определим в следующем разделе.

2. Линейное представление бинарных программ

Пусть $\mathcal{A}^d$ — d-мерное линейное нормированное пространство над полем $\mathcal{K}$. В статье мы используем обозначения, принятые в теории квантовых вычислений. Элемент a пространства $\mathcal{A}^d$ будем обозначать через $|a\rangle$, где $|\,\rangle$ обозначает кет-вектор — вектор-столбец в обозначениях Дирака. Через $\langle\,|$ обозначается вектор-строка (бра-вектор). Для вектора $|a\rangle = (a_1, \ldots, a_d) \in \mathcal{A}^d$ будем использовать нормы: $||\,|a\rangle||_1 = \sum\limits_{i=1}^{d} |a_i|$, $||\,|a\rangle||_2 = \sqrt{\sum\limits_{i=1}^{d} |a_i|^2}$.

Оператор проекции. Пусть $\mathcal{A}^d = W_1 \oplus \cdots \oplus W_k$, $k \leqslant d$, — ортогональная декомпозиция пространства $\mathcal{A}^d$ на подпространства $W_1, \ldots, W_k$. Тогда произвольный элемент $|a\rangle \in \mathcal{A}^d$ может быть однозначно представлен как линейная суперпозиция проекций элемента $|a\rangle$ на подпространства $W_1, \ldots, W_k$: $|a\rangle = |a_{W_1}\rangle + \cdots + |a_{W_k}\rangle$, где $|a_{W_1}\rangle \in W_1, \ldots, |a_{W_k}\rangle \in W_k$. В этом случае преобразования $P_{W_1}(|a\rangle) = |a_{W_1}\rangle, \ldots, P_{W_k}(|a\rangle) = |a_{W_k}\rangle$ называются *операторами проекции* на подпространства $W_1, \ldots, W_k$ соответственно.

Линейная бинарная программа над пространством $\mathcal{A}^d$ ширины d глубины l ((d,l)-LBP) — это тройка $LP = \big(|a_0\rangle, T, M_{acc}\big)$, где $|a_0\rangle \in \mathcal{A}^d$ — начальный вектор, $T = \{\langle i_j, W_j(0), W_j(1)\rangle\}_{j=1}^{l}$ — последовательность линейных преобразований пространства $\mathcal{A}^d$, где $W_j(0), W_j(1)$ — матрицы порядка d, M_{acc} — матрица порядка d проекции на *подпространство принимающих состояний*.

На входном наборе $\sigma = (\sigma_1, \ldots, \sigma_n)$ программа LP производит вычисление следующим образом:

- Вычисление начинается из начального вектора $|a_0\rangle$.
- На j-м шаге ($j = 1, \ldots, l$) линейная программа считывает значение входной переменной $x_{i_j} = \sigma_{i_j}$ и преобразует текущий вектор $|a\rangle$ в вектор $|a'\rangle = W_j(\sigma_{i_j})|a\rangle$.
- После l-го (последнего) шага получается результирующий вектор $|a_l(\sigma)\rangle = W_l(\sigma_{i_l}) \cdots W_1(\sigma_{i_1})|a_0\rangle$. Вектор $|a_l(\sigma)\rangle$ проектируется на подпространство принимающих состояний, в результате чего получаем финальный вектор $|a_{final}(\sigma)\rangle = M_{acc}|a_l(\sigma)\rangle$.

Для входного набора $\sigma = (\sigma_1, \ldots, \sigma_n)$ определим два значения $Pr1_{acc}^{LP}(\sigma)$ и $Pr2_{acc}^{LP}(\sigma)$, получаемые из финального вектора $|a_{final}(\sigma)\rangle$ следующим образом:

$$Pr1_{acc}^{LP}(\sigma) = ||\,|a_{final}(\sigma)\rangle||_1, \quad Pr2_{acc}^{LP}(\sigma) = ||\,|a_{final}(\sigma)\rangle||_2^2.$$

Линейную бинарную программу будем называть *линейной бинарной программой LBP типа* I (LBP *типа* II), если она использует значение $Pr1_{acc}^{LP}(\sigma)$ ($Pr2_{acc}^{LP}(\sigma)$) в качестве вероятности принятия слова σ.

Детерминированная и вероятностная забывающие программы являются частным случаем линейной бинарной программы. А именно:

Детерминированая вероятностная программа ширины d глубины l ((d,l)-ВР) $P = \big(|a_0\rangle, T, M_{acc}\big)$ — это LBP типа I , где $|a_0\rangle$ — булевский вектор с единственной ненулевой компонентой, соответствующей начальной вершине нулевого уровня; $T = \{\langle i_j, W_j(0),\ W_j(1)\rangle\}_{j=1}^{l}$, где $W_j(0), W_j(1)$ ($j = 1, \ldots, l$) — булевские матрицы, каждый столбец которых содержит ровно одну единицу. А именно, в матрице $W_{i_j}(\sigma), \sigma \in \{0,1\}$ единица находится на пересечении s-го столбца и s'-ой строки, если в бинарной программе есть дуга из вершины s $(j-1)$-го уровня вершину s' j-го уровня, помеченного σ. M_{acc} — булевская диагональная матрица, в которой $M_{acc}(i,i) = 1$ тогда и только тогда, когда вершина i l-го уровня является принимающей вершиной.

Вероятностная бинарная программа ширины d глубины l ((d,l)-PBP) $P = \big(|a_0\rangle, T, M_{acc}\big)$ — это LBP типа I, где $|a_0\rangle$ — стохастический вектор — вектор начального распределения вероятностей состояний, $T = \{\langle i_j, W_j(0), W_j(1)\rangle\}_{j=1}^{l}$, где $W_j(0), W_j(1)$ $(j = 1, \ldots, l)$ — матрицы, стохастические по столбцам. А именно, в матрице $W_{i_j}(\sigma), \sigma \in \{0,1\}$ на пересечении s-го столбца и s'-ой строки находится вероятность перехода из вершины s $(j-1)$-го уровня в вершину s' j-го уровня при значении входной переменной $x_{i_j} = \sigma$. M_{acc} — булевская диагональная матрица, в которой $M_{acc}(i,i) = 1$ тогда и только тогда, когда вершина i l-го уровня является принимающей вершиной.

Отметим, что в соответствие с определением *ширина* линейной бинарной программы — это размерность d пространства состояний $\mathcal{A}^d$, *длина* линейной бинарной программы — это длина l последовательности линейных преобразований.

2.1. Квантовая система

Пусть $\mathcal{H}^d$ — d-мерное гильбертово пространство с нормой $||.||_2$. Пусть QS — квантовая физическая система с d устойчивыми состояниями $\{1, \ldots, d\}$. *Чистое состояние* QS описывается вектором $|\psi\rangle$ единичной длины в гильбертовом пространстве $\mathcal{H}^d$ в базисе $\{|1\rangle, \ldots, |d\rangle\}$ (будем называть его стандартным базисом), где $|i\rangle$ — вектор-столбец, i-ая компонента которого равна единице, остальные равны нулю. То есть $|\psi\rangle = \sum_{i=1}^{d} z_i|i\rangle$ или коротко $|\psi\rangle = (z_1, \ldots, z_d)$.

Всюду далее будем называть $|\psi\rangle$ *конфигурацией*. Комплексное число z_i называется *амплитудой* базисного состояния $|i\rangle$ в конфигурации $|\psi\rangle$.

Эволюция квантовой системы. Эволюция квантовой системы (изменение состояния QS за определенный промежуток времени) задается унитарным оператором и описывается следующим образом. Если $|\psi\rangle$ — конфигурация системы QS на текущем шаге, то на следующем шаге конфигурацией QS будет $|\psi'\rangle$, где $|\psi'\rangle = U|\psi\rangle$ и U — квадратная унитарная матрица порядка d.

Измерение квантовой системы. Извлечение информации о QS из конфигурации $|\psi\rangle$ называется *измерением* и задается оператором проекции.

В статье будем использовать два типа измерений — *промежуточное измерение* и *финальное измерение*. Промежуточное измерение производится на некотором этапе вычислительного процесса, финальное измерение производится по окончании вычисления. Будем задавать их следующим образом (см., например, [15, гл. 1.6]).

Промежуточное измерение. Пусть $|\psi\rangle$ — текущая конфигурация и пусть $\mathcal{H}^d = W_1 \oplus \cdots \oplus W_k$ — ортогональная декомпозиция простран-

ства $\mathcal{H}^d$. Измерение $\mathcal{O} = \{W_1, \ldots, W_k\}$ относительно подпространств $W_1, \ldots, W_k$ состоит в следующем.

1. Выбирается одно из подпространств $W_1, \ldots, W_k$. Вероятность выбора подпространства W_i равна $||P_{W_i}(|\psi\rangle)||_2^2$.

2. После выбора подпространства состояние $|\psi_{W_i}\rangle = P_{W_i}(|\psi\rangle)$ нормализуется. и конфигурацией $|\psi'\rangle$ после измерения становится

$$|\psi'\rangle = \frac{P_{W_i}(|\psi\rangle)}{||P_{W_i}(|\psi\rangle)||_2}$$

   Вся информация, не принадлежащая $|\psi_{W_i}\rangle$, теряется.

3. Как результат измерения $\mathcal{O}$ мы получаем некоторое значение μ, которое называется *исходом измерения*. Всюду в статье μ есть информация о том, какое из подпространств $W_1, \ldots, W_k$ было выбрано в результате измерения, т. е. $\mu = i$, $i \in \{1, \ldots, k\}$.

Промежуточное измерение $\mathcal{O}$ производится на некотором этапе вычисления, и дальнейший процесс вычисления зависит от исхода μ этого промежуточного измерения.

Финальное измерение. Вектор текущей конфигурации проектируется на одно из двух подпространств W_{acc}, W_{rej}: $W_{acc} \oplus W_{rej} = \mathcal{H}^d$, $W_{acc} \perp W_{rej}$. Будем называть W_{acc} (W_{rej}) подпространством принимающих (отвергающих) состояний. Оператор проекции на подпространство W_{acc} будем задавать матрицей проекции M_{acc} следующим образом. Пусть $|\psi\rangle$ — конфигурация и пусть подпространство $W_{acc} \subseteq \mathcal{H}^d$ принимающих состояний задается системой $\{|e_i\rangle\}_{i=1}^r$ ортонормированных векторов. *Матрица проекции* на подпространство принимающих состояний M_{acc} — это квадратная матрица порядка d, которая содержит r ненулевых строк $M_{acc}[i_1]$, …, $M_{acc}[i_r]$, определяемых следующим образом: $M_{acc}[i] = (\alpha_1, \ldots, \alpha_d)$, где $|e_i\rangle = \alpha_1|1\rangle + \cdots + \alpha_d|d\rangle$, т. е. $M_{acc}[i]$ — это представление базисного вектора $|e_i\rangle$ в стандартном базисе $\{|1\rangle, \ldots, |d\rangle\}$.

Для конфигурации $|\psi\rangle$ вероятность выбора подпространства принимающих состояний $p_{acc} = ||M_{acc}|\psi\rangle||_2^2$.

2.2. Определение один раз измеряемой квантовой бинарной программы

Модель квантовой бинарной программы, определенная как обобщение уровневой забывающей вероятностной модели, была впервые введена

в работе [9]. В этой модели измерение текущей конфигурации производится один раз по окончании вычислительного процесса. Поэтому такую бинарную программу будем называть один раз измеряемой квантовой бинарной программой(MO–QBP).

Определение. Один раз измеряемая квантовая бинарная программа ширины d и глубины l ((d,l)-MO–QBP) $P = \left(|\psi_0\rangle, T, M_{acc}\right)$ — это LBP типа II, где $|\psi_0\rangle$ — начальная конфигурация P, $||\,|\psi_0\rangle||_2 = 1$, $T = \{\langle j_i, U_i(0), U_i(1)\rangle\}_{i=1}^{l}$ — последовательность d-мерных квантовых преобразований квантовой системы QS с d устойчивыми состояниями, где $U_i(0)$, $U_i(1)$ — унитарные матрицы порядка d, M_{acc} — матрица проекции порядка d на пространство принимающих состояний.

2.3. Представление функций

Бинарная программа P (квантовая или вероятностная) вычисляет функцию f с *неизолированной ошибкой* (unbounded error), если для любого $\sigma \in f^{-1}(1)$ вероятность $Pr_{acc}^{P}(\sigma)$принятия программой P входа σ больше $1/2$ и $Pr_{acc}^{P}(\sigma') < 1/2$ для любого $\sigma' \in f^{-1}(0)$. В этом случае будем также говорить, что P вычисляет функцию f с неизолированной точкой сечения $1/2$.

Бинарная программа P (квантовая или вероятностная) вычисляет функцию f с *изолированной ошибкой* (bounded error), если существует $\varepsilon \in (0, 1/2]$ такое, что для любого входа $\sigma \in f^{-1}(1)$ вероятность $Pr_{acc}^{P}(\sigma)$ принятия программой P входа σ не меньше $1/2 + \varepsilon$ и для любого $\sigma' \in f^{-1}(0)$ вероятность $Pr_{acc}^{P}(\sigma')$ принятия программой P входа σ' не больше $1/2 - \varepsilon$. При этом будем также говорить, что программа P вычисляет f с ε-изолированной точкой сечения $1/2$.

Обозначим через BQP-BP$_{MO}$, PrQP-BP$_{MO}$ классы функций, которые вычислимы с изолированной и неизолированной ошибкой соответственно один раз измеряемыми квантовыми бинарными программами полиномиальной сложности. Через BPP-BP, PP-BP обозначим классы функций, которые вычислимы с изолированной и неизолированной ошибкой соответственно вероятностными бинарными программами полиномиальной сложности.

Теорема 1. *Справедливы включения*:

$$\text{PrQP-BP}_{MO} \subseteq \text{PP-BP}, \quad \text{BQP-BP}_{MO} \subseteq \text{PP-BP}.$$

Справедливость теоремы 1 следует из теоремы 2, которая доказывается в следующем разделе.

3. Линейное моделирование квантовой бинарной программы

Теорема 2. *Пусть функция f вычислима с неизолированной (с изолированной) ошибкой (d,l)-*MO–QBP *P. Тогда существует вероятностная забывающая $(4d^2+3,l)$-*PBP *P', вычисляющая функцию f с неизолированной ошибкой.*

Доказательство. Квантовая и вероятностная забывающие бинарные программы имеют три отличия:

1) В вероятностной бинарной программе компоненты текущего вектора состояний и матриц преобразований являются вещественными числами. В квантовой бинарной программой соответствующие элементы являются в общем случае комплексными значениями.

2) В вероятностной модели извлечение результата вычисления производится «линейно». В квантовой модели в определении вероятности принятия входного слова «появляется квадрат».

3) В вероятностной модели текущий вектор состояний является стохастическим вектором, матрицы преобразований — матрицы, стохастические по столбцам, сохраняющие норму $||\cdot||_1$ преобразуемого вектора. В квантовой модели матрицы преобразований — унитарные матрицы, сохраняющие норму $||\cdot||_2$ преобразуемой конфигурации. Для текущего вектора $|\psi\rangle$ распределения амплитуд всегда выполняется равенство $||\,|\psi\rangle||_2 = 1$.

План доказательства теоремы следующий: по квантовой бинарной программе P строится вероятностная бинарная программа P'. Процесс построения P' разбивается на этапы, на каждом из которых преодолевается одно из отмеченных выше отличий, что будет подтверждаться соответствующими леммами.

Будем называть QBP P *вещественнозначной* QBP, если её конфигурации и матрицы преобразований содержат только вещественные значения. В противном случае QBP P будем называть *комплекснозначной* QBP.

1 *этап*. Переход от комплекснозначных амплитуд к вещественным.

Лемма 1. *Если функция f вычислима комплекснозначной (d,l)-*MO–QBP *P, то она вычислима такой вещественнозначной $(2d,l)$-*MO–QBP *P', что*

$$Pr^{P'}_{acc}(\sigma) = Pr^{P}_{acc}(\sigma) \text{ для любого } \sigma \in \{0,1\}^n.$$

Доказательство основано на известном факте, что, используя представление комплексного числа $z = a+ib$ при помощи матрицы $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$

от d-мерного линейного пространства над полем $\mathbf{C}$ можно перейти к $2d$-мерному линейному пространству над полем $\mathbf{R}$ (см., например, [7]).

Пусть z — комплексное число. Обозначим через $\mathrm{Re}(z)$ и $\mathrm{Im}(z)$ его вещественную и мнимую части.

Пусть (d,l)-MO–QBP $P = \big(|\psi_0\rangle, T, M_{acc}\big)$, где $|\psi_0\rangle = (z_1,\ldots,z_d)^T$;

$$M_{acc} = \begin{pmatrix} m_{1,1} & \ldots & m_{1,d} \\ \vdots & \ddots & \vdots \\ m_{d,1} & \ldots & m_{d,d} \end{pmatrix}, \quad T = \{\langle j_i, U_i(0), U_i(1)\rangle\}_{i=1}^{l},$$

$$U_i(\sigma) = \begin{pmatrix} u_{1,1} & \ldots & u_{1,d} \\ \vdots & \ddots & \vdots \\ u_{d,1} & \ldots & u_{d,d} \end{pmatrix}, \quad i = 1,\ldots,l, \quad \sigma \in \{0,1\}.$$

Процесс вычисления функции f на наборе $\sigma = (\sigma_1,\ldots,\sigma_n)$ представляется следующим образом: $|\psi_l(\sigma)\rangle = U_l(\sigma_{i_l})\cdots U_1(\sigma_{i_1})|\psi_0\rangle$. Вероятность $Pr_{acc}^{P}(\sigma)$ принятия набора σ равна $||M_{acc}|\psi_l(\sigma)\rangle||_2^2$.

Будем строить $(2d,l)$-MO–QBP $P' = \big(|\psi_0'\rangle, T', M_{acc}'\big)$ следующим образом:

$$|\psi_0'\rangle = (\mathrm{Re}(z_1),\mathrm{Im}(z_1),\ldots,\mathrm{Re}(z_d),\mathrm{Im}(z_d))^T,\ T' = \{\langle j_i, U_i'(0), U_i'(1)\rangle\};$$

$$M_{acc}' = \begin{pmatrix} M_{1,1} & \ldots & M_{1,d} \\ \vdots & \ddots & \vdots \\ M_{d,1} & \ldots & M_{d,d} \end{pmatrix}, \quad U_i'(\sigma) = \begin{pmatrix} U_{1,1} & \ldots & U_{1,d} \\ \vdots & \ddots & \vdots \\ U_{d,1} & \ldots & U_{d,d} \end{pmatrix},$$

$$i = 1,\ldots,l, \quad \sigma \in \{0,1\},$$

где $M_{i,j} = \begin{pmatrix} \mathrm{Re}(m_{i,j}) & \mathrm{Im}(m_{i,j}) \\ -\mathrm{Im}(m_{i,j}) & \mathrm{Re}(m_{i,j}) \end{pmatrix}$, $U_{i,j} = \begin{pmatrix} \mathrm{Re}(u_{i,j}) & \mathrm{Im}(u_{i,j}) \\ -\mathrm{Im}(u_{i,j}) & \mathrm{Re}(u_{i,j}) \end{pmatrix}$ — матричное представление комплексных чисел $m_{i,j}$ и $u_{i,j}$ соответственно.

Очевидно, что из $||\,|\psi\rangle||_2 = 1$ следует $||\,|\psi'\rangle||_2 = 1$, из унитарности $U_i(\sigma)$ следует унитарность $U_i'(\sigma)$ и из свойства ортонормированности ненулевых строк матрицы M_{acc} следует ортонормированность ненулевых строк матрицы M_{acc}'.

Из построения следует, что QBP P' принимает входное слово $\sigma \in \{0,1\}^n$ с той же вероятностью, что и исходная QBP P: $Pr_{acc}^{P'}(\sigma) = Pr_{acc}^{P}(\sigma)$. Лемма 1 доказана.

2 *этап.* Переход от LBP типа II к LBP типа I.

В следующей лемме мы установим соотношение сложности между LBP типа I и LBP типа II (между «линейным» и «нелинейным» извлечением результата).

Лемма 2. *Пусть функция f вычислима вещественнозначной (d,l)-MO–QBP P. Тогда она вычислима (d^2,l)-LBP типа* I *LP такой, что*

$$Pr^{LP}_{acc}(\sigma) = Pr^{P}_{acc}(\sigma) \text{ для любого } \sigma \in \{0,1\}^n.$$

Доказательство. Имеем (d,l)-QBP $P = \big(|\psi_0\rangle, T, M_{acc}\big)$. Вероятность $Pr^P_{acc}(\sigma)$ принятия входного набора $\sigma = (\sigma_1, \ldots, \sigma_n)$ равна $||M_{acc}U(\sigma)|\psi_0\rangle||^2_2$, где $U(\sigma) = U_l(\sigma_{i_l}), \cdots, U_1(\sigma_{i_1})$.

Пусть $\{e_1, \ldots, e_r\}$ — множество ортонормированных векторов, определяющих пространство E_{acc} (т. е. e_i — i-я ненулевая строка матрицы M_{acc}).

Тогда $Pr^P_{acc}(\sigma) = \sum\limits_{i=1}^{r} \langle e_i|U(\sigma)|\psi_0\rangle^2$. Используя факт, что $\langle a|b\rangle^2 = \langle a \otimes a|b \otimes b\rangle$ для любых вещественных векторов a, b (через $a \otimes b$ обозначается тензорное произведение векторов a и b), имеем

$$Pr^P_{acc}(\sigma) = \sum_{i=1}^{r} \langle e_i \otimes e_i|U(\sigma) \otimes U(\sigma)|\psi_0 \otimes \psi_0\rangle.$$

При этом справедливо соотношение

$$U(\sigma) \otimes U(\sigma) = \big(U_l(\sigma_{i_l}) \cdots U_1(\sigma_{i_1})\big) \otimes \big(U_l(\sigma_{i_l}) \cdots U_1(\sigma_{i_1})\big) = \big(U_l(\sigma_{i_l}) \otimes U_l(\sigma_{i_l})\big) \cdots \big(U_1(\sigma_{i_1}) \otimes U_1(\sigma_{i_1})\big).$$

Определим линейную бинарную программу LP следующим образом: $LP = \big(|a_0\rangle, T', M'_{acc}\big)$, $|a_0\rangle = |\psi_0 \otimes \psi_0\rangle, T' = \{\langle i_j, W_j(0), W_j(1)\rangle\}^l_{j=1}$, где $W_j(\sigma) = U_j(\sigma) \otimes U_j(\sigma), \sigma = \{0,1\}$, i-я строка $M'_{acc}[i]$ матрицы M'_{acc} равна $\langle e_i \otimes e_i|$. Лемма 2 доказана.

3 *этап.* Построение вероятностной бинарной программы.

На данном этапе в целях простоты изложения удобно предполагать, что линейная бинарная программа имеет единственное принимающее состояние. Следующая лемма показывает, что от произвольной LBP типа I мы может перейти к LBP типа I с данным ограничением.

Лемма 3. *Пусть функция f вычислима (d,l)-*LBP *типа* I *LP. Тогда она вычислима (d,l)-*LBP *типа* I *LP' такой, что*

1) *матрица M_{acc} является булевской матрицей с единственным ненулевым элементом $M_{acc}[1,1] = 1$;*

2) *$Pr^{LP'}_{acc}(\sigma) = Pr^{LP}_{acc}(\sigma)$ для любого $\sigma \in \{0,1\}^n$.*

Доказательство. Пусть (d,l)-LBP типа I $LP = \big(|a_0\rangle, T, M_{acc}\big)$. Здесь

$|a_0\rangle = (a_1, \ldots, a_d)^T$, $T = \{\langle i_j, W_j(0), W_j(1)\rangle\}_{j=1}^{l}$, где $W_j(0), W_j(1)$ $(j = 1, \ldots, l)$ — квадратные матрицы порядка d,

$$M_{acc} = \begin{pmatrix} m_{1,1} & \ldots & m_{1,d} \\ \vdots & \ddots & \vdots \\ m_{d,1} & \ldots & m_{d,d} \end{pmatrix}.$$

Определим (d, l)-LBP типа I LP' следующим образом. $LP' = \big(|a_0\rangle, T', M'_{acc}\big)$, где последовательность преобразований $T' = \{\langle i_j, V_j(0), V_j(1)\rangle\}_{j=1}^{l}$ определена следующим образом: $V_j(\sigma) = W_j(\sigma)$, $j = 1, \ldots, l-1$, $\sigma \in \{0, 1\}$. $V_l(\sigma) = HW_l(\sigma)$, где матрица H порядка d определена следующим образом:

$$H = \begin{pmatrix} \sum\limits_{i=1}^{d} m_{i,1} & \sum\limits_{i=1}^{d} m_{i,2} & \cdots & \sum\limits_{i=1}^{d} m_{i,d} \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \ldots & \cdots & 0 \end{pmatrix}$$

$$M'_{acc} = \begin{pmatrix} 1 & 0 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 0 \end{pmatrix}. \tag{1}$$

Легко проверить, что $Pr_{acc}^{LP'}(\sigma) = Pr_{acc}^{LP}(\sigma) = ||M_{acc}W(\sigma)|a_0\rangle||_1$ для любого входного слова $\sigma \in \{0, 1\}^n$, где $W(\sigma) = W_l(\sigma_{i_l}) \cdots W_1(\sigma_{i_1})$. Лемма 3 доказана.

В следующей лемме говорится о построении вероятностной программы по заданной линейной программе. Для её доказательства используется техника, которая применяется, в частности, при моделировании линейных конечных автоматов вероятностными (см., например, [2]).

Лемма 4. *Пусть функция f вычислима (d, l)-*LBP *типа* I *LP. Тогда она вычислима такой $(d + 2, l)$-*PBP *P, что для любого $\sigma \in \{0, 1\}^n$*

$$Pr_{acc}^{P}(\sigma) = c^{l+1} Pr_{acc}^{LP}(\sigma) + 1/(d + 2),$$

где константа $c \in (0, 1]$ зависит от программы LP.

Доказательство. Имеем (d, l)-LBP типа I $LP = \big(|a_0\rangle, T, M_{acc}\big)$. Здесь $|a_0\rangle = (a_1, \ldots, a_d)^T$, $T = \{\langle i_j, V_j(0), V_j(1)\rangle\}_{j=1}^{l}$, где $V_j(0), V_j(1)$ $(j = 1, \ldots, l)$ — матрицы порядка d. Для удобства изложения и без ограничения общности согласно лемме 3 полагаем, что LP имеет ровно одно принимающее состояние, т. е. матрица проекции M_{acc} имеет вид (1).

Вектор $|a_0\rangle$ и матрицы $V_j(\sigma)$ ($j = 1, \ldots, l$; $\sigma = \{0, 1\}$) содержат вещественные (не обязательно положительные) значения. Преобразуем вектор $|a_0\rangle$ и матрицы $V_j(\sigma)$ следующим образом. Пусть

$$V'_j(\sigma) = \begin{pmatrix} & & & 0 & \beta_1 \\ & V_j(\sigma) & & 0 & \vdots \\ \alpha_1 & \ldots & \alpha_d & 0 & \beta_{d+1} \\ 0 & \ldots & 0 & 0 & 0 \end{pmatrix},$$

где $\alpha_1, \ldots, \alpha_d, \beta_1, \ldots, \beta_{d+1}$ выбраны таким образом, чтобы сумма чисел в каждой строке и в каждом столбце матрицы $V'_j(\sigma)$ равнялась нулю. По индукции проверяется, что матрица $V'(\sigma) = V'_l(\sigma_{i_l}) \cdots V'_1(\sigma_{i_1})$ имеет аналогичный вид, и сумма чисел в каждом её столбце и в каждой строке равна нулю. Аналогичную процедуру проведем с вектором $|a_0\rangle$. Пусть $|a'\rangle = (a_1, \ldots, a_d, a_{d+1}, 0)^T$, где a_{d+1} таково, что сумма элементов вектора $|a'\rangle$ равна нулю.

Пусть c — положительное число такое, что после умножения на c каждый элемент вектора $|a'\rangle$ и матриц $V'_j(\sigma)$ становится по модулю не больше $1/(d+2)$. Обозначим через B и $|b\rangle$ матрицу порядка $d+2$ и вектор длины $d+2$ соответственно:

$$B = \begin{pmatrix} \frac{1}{d+2} & \cdots & \frac{1}{d+2} \\ \vdots & \ddots & \vdots \\ \frac{1}{d+2} & \cdots & \frac{1}{d+2} \end{pmatrix}, \qquad |b\rangle = (\frac{1}{d+2}, \cdots, \frac{1}{d+2})^T.$$

Матрица B называется унимодулярной. Для неё справедливы следующие (легко проверяемые) равенства: $B^2 = B, B|b\rangle = |b\rangle, V'_j(\sigma)B = BV'_j(\sigma) = 0$ ($j = 1, \ldots, l; \sigma \in \{0, 1\}$).

Будем строить вероятностную бинарную программу P следующим образом. В качестве начального вектора распределения вероятностей возьмём стохастический вектор $|\mu_0\rangle = c|a'\rangle + |b\rangle$. На j-м шаге, $j = 1, \ldots, l$, программа P считывает $x_{i_j} = \sigma_{i_j}$ и получает новый вектор распределения вероятностей $|\mu_j\rangle$ путем умножения дважды стохастической матрицы $A_j(\sigma_{i_j}) = cV'_j(\sigma_{i_j}) + B$ на $|\mu_{j-1}\rangle$. После l-го (последнего) шага матрица проекции M_{acc} умножается на вектор распределения вероятностей $|\mu_l(\sigma)\rangle$. Вероятностная бинарная программа P принимает слово σ с вероятностью $Pr^P_{acc}(\sigma) = ||M_{acc}A_l(\sigma_{i_l}) \cdots A_1(\sigma_{i_1})|\mu_0\rangle||_1 = c^{l+1}||M_{acc}V_l(\sigma_{i_l}) \cdots V_1(\sigma_{i_1})|a_0\rangle||_1 + 1/(d+2) = c^{l+1}Pr^{LP}_{acc}(\sigma) + 1/(d+2)$. Лемма 4 доказана.

Лемма 4 показывает, что, имея (d,l)-LBP типа I, вычисляющую функцию f с точкой сечения $1/2$, можно построить $(d+2,l)$-PBP, вычисляющую функцию f с точкой сечения $\lambda = c^{l+1}1/2 + 1/(d+2)$, где константа c зависит от исходной программы.

Следующий этап позволяет перейти от точки сечения λ к точке сечения $1/2$. При этом используется техника из теории линейных автоматов [2].

4 *этап*. Увеличение вероятности правильного результата.

Лемма 5. *Пусть* (d,l)-PBP P *вычисляет функцию* f *с точкой сечения* $\lambda \in [0,1)$. *Тогда для любого* $\lambda' \in (\lambda,1)$ *существует* $(d+1,l)$-PBP P', *которая вычисляет* f *с точкой сечения* λ'.

Доказательство. Пусть (d,l)-PBP $P = \big(|\mu_0\rangle, T, M_{acc}\big)$, где $T = \{\langle i_j, U_j(0), U_j(1)\rangle\}_{j=1}^{l}$. Определим вероятностную бинарную программу P' следующим образом: $(d+1,l)$-PBP $P' = \big(|\mu_0'\rangle, T', M_{acc}'\big)$. Здесь $|\mu_0'\rangle = (\beta, (1-\beta)\mu_0)^T$, где β мы определим позднее. Последовательность преобразований $T' = \{\langle i_j, U_j'(0), U_j'(1)\rangle\}_{j=1}^{l}$. Матрицы $U_j'(\sigma)$ $(j = 1,\ldots,l;$ $\sigma \in \{0,1\})$ переходных вероятностей и матрица проекции M_{acc}' определены следующим образом:

$$U_j'(\sigma) = \begin{pmatrix} 1 & 0 & \ldots & 0 \\ 0 & & & \\ \vdots & & U_j(\sigma) & \\ 0 & & & \end{pmatrix}, \quad M_{acc}' = \begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0} & M_{acc} \end{pmatrix}.$$

Пусть вероятность $Pr_{acc}^{P}(\sigma)$ принятия входного слова σ программой P равна λ. Тогда бинарная программа P' принимает σ с вероятностью $Pr_{acc}^{P'} = ||M_{acc}'U_l'(\sigma_{i_l})\cdots U_1'(\sigma_{i_1})|\mu_0'\rangle||_1 = \beta + (1-\beta)\lambda$. Для того чтобы выполнялось неравенство $Pr_{acc}^{P'} > \lambda'$, достаточно взять $\beta > 1 - (1-\lambda')/(1-\lambda)$. При этом ширина $\mathrm{Width}(P')$ построенной PBP P' равна $d+1$. Лемма 5 доказана.

Таким образом, имея квантовую бинарную программу, в соответствие с четырьмя этапами, описанными выше, строим вероятностную бинарную программу. При этом вероятность принятия входного слова σ изменяется только на этапах 3, 4 (леммы 4, 5). Учитывая изменения ширины бинарной программы на этапах 1–4, имеем: ширина $\mathrm{Width}(P')$ построенной вероятностной бинарной программы равна $4\mathrm{Width}(P)^2 + 3$. Теорема 2 доказана.

Комментарий. Из теоремы 2 линейного моделирования квантовых бинарных программ следует, что если имеется квантовая BP P, вычис-

ляющая функцию f с ε-изолированной точкой сечения $1/2$, то можно построить вероятностную программу Q, вычисляющую ту же функцию f с точкой сечения $1/2$. При этом длина Q не изменится, ширина программы Q увеличится квадратично: $\mathrm{Width}(Q)=4\mathrm{Width}^2(P)+3$, т. е. сложность возрастет полиномиально. Однако за это приходится «платить» потерей ε-изолированности точки сечения (что следует из леммы 4). В построенной ВР вероятность ошибки может быть сколь угодно близкой к $1/2$, тогда как в исходной ВР вероятность ошибки была мала.

4. Определение много раз измеряемой квантовой бинарной программы

Введем понятие *много раз измеряемой квантовой бинарной программы* (ММ–QBP). Отличие этой модели от MO–QBP (см. определение) состоит в следующем. Для входного набора $\sigma \in \{0,1\}^n$ один раз измеряемая (d,l)-MO–QBP P начинает вычисление из начальной конфигурации $|\psi_0\rangle$. На шаге i $(i=1,\ldots,l)$ P считывает значение переменной $x_{j_i}=\sigma_{j_i}$ и преобразует текущую конфигурацию $|\psi\rangle$ в конфигурацию $|\psi'\rangle = U_i(\sigma_{j_i})|\psi\rangle$. После l-го (последнего) шага программа P производит финальное измерение результирующей конфигурации, т. е. измерение производится один раз по окончании вычисления. Преобразования $U_i(\sigma)$, применяемые на каждом шаге вычисления, являются унитарными, а следовательно, обратимыми.

В ММ–QBP после каждого вычислительного шага i $(i=1,\ldots,l)$ производится измерение текущей конфигурации, и выбор дальнейшего преобразования зависит от исхода измерения. Применение операции измерения в ходе вычисления нарушает обратимость процесса вычисления.

Пусть $\mathcal{H}^d = W_1 \oplus \cdots \oplus W_k$, $k \leqslant d$, — ортогональная декомпозиция пространства $\mathcal{H}^d$ на подпространства $W_1,\ldots,W_k$. Определим (d,l)-ММ–QBP P ширины d и длины l как $P=\big(|\psi_0\rangle, R, M_{acc}\big)$, где $|\psi_0\rangle$ — начальная конфигурация, R — последовательность (длины l) d-мерных квантовых преобразований квантовой системы QS с d устойчивыми состояниями, определенная следующим образом

$$R=\{\langle j_i, U_i^1(0),\ldots,U_i^k(0),U_i^1(1),\ldots,U_i^k(1)\rangle\}_{i=1}^{l},$$

где $U_i^j(0)$ и $U_i^j(1)$ $(i=1,\ldots,l;j=1,\ldots,k)$ — унитарные матрицы порядка d, M_{acc} — матрица проекции на пространство принимающих состояний.

Определим вычисление на входном наборе $\sigma=(\sigma_1,\ldots,\sigma_n)\in\{0,1\}^n$ программой P следующим образом:

1) Вычисление начинается из начальной конфигурации $|\psi_0\rangle$;

2) Каждый шаг j ($j = 1, \ldots, l$) работы программы P состоит из двух этапов:

2.1) *Измерение*: Производится промежуточное измерение $\mathcal{O} = \{W_1, \ldots, W_k\}$ текущей конфигурации $|\psi\rangle$ относительно подпространств $W_1, \ldots, W_k$. Результат измерения — вероятностный. Вероятность выбора подпространства W_i равна $||P_{W_i}(|\psi\rangle)||_2^2$. В качестве исхода измерения на j-м шаге программа P выдает значение $\mu_j \in \{1, \ldots, k\}$. Конфигурацией после измерения становится $|\psi'\rangle = \dfrac{P_{W_{\mu_j}}(|\psi\rangle)}{||P_{W_{\mu_j}}(|\psi\rangle)||_2}$.

2.2) *Преобразование*: P применяет к текущей конфигурации $|\psi'\rangle$ унитарное преобразование $U_j^{\mu_j}(\sigma_{i_j})$, определяемое исходом измерения μ_j на j-м шаге и входным символом $x_{i_j} = \sigma_{i_j}$.

3) После l-го (последнего) шага P производит финальное измерение текущей конфигурации, задаваемое матрицей проекции M_{acc}.

Замечание 1. Отметим, что на каждом шаге после промежуточного измерения состояние квантовой бинарной программы — это система $\{p_r, |\psi_r\rangle\}_{r=1}^k$, где p_r — вероятность нахождения квантовой системы в чистом состоянии $|\psi_r\rangle$. В квантовой механике состояние $\{p_r, |\psi_r\rangle\}_{r=1}^k$ называется *смешанным состоянием*. Традиционно в теории квантовых вычислений смешанное состояние описывается при помощи матрицы плотности ρ (см., например, [3]). В статье по техническим соображениям конструктивного описания квантовой бинарной программы фактически не используется представление смешанного состояния при помощи матрицы плотности.

Обозначим через BQP–BP$_{MM}$, PrQP–BP$_{MM}$ — классы функций, вычислимых с изолированной и неизолированной ошибкой соответственно на много раз измеряемых квантовых бинарных программах полиномиальной сложности.

Утверждение. *Справедливы включения*:

$$\text{PrQP-BP}_{MO} \subseteq \text{PrQP-BP}_{MM}, \quad \text{BQP-BP}_{MO} \subseteq \text{BQP-BP}_{MM}.$$

Это утверждение следует из того факта, что MO–QBP можно рассматривать как частный случай MM–QBP, когда на каждом шаге производится тривиальное промежуточное измерение $\mathcal{O} = \{\mathcal{H}^d\}$.

Теорема 3. *Справедливы включения*:

$$\text{PP-BP} \subseteq \text{PrQP-BP}_{MM}, \quad \text{BPP-BP} \subseteq \text{BQP-BP}_{MM}.$$

Справедливость теоремы следует из теоремы 4, которая доказывается в следующем разделе.

5. Квантовое моделирование вероятностной бинарной программы

Теорема 4. *Пусть функция f вычислима (d,l)-РВР P. Тогда она вычислима (d,l)-ММ–QBP Q такой, что*

$$Pr^{Q}_{acc}(\sigma) = Pr^{P}_{acc}(\sigma) \text{ для всех } \sigma \in \{0,1\}^n.$$

Доказательство. Пусть (d,l)-РВР $P = \big(|\mu_0\rangle, T, M_{acc}\big)$, $T = \{\langle i_j, W_j(0), W_j(1)\rangle\}_{j=1}^{l}$,

$$W_j(\sigma) = \begin{pmatrix} w_{1,1}(\sigma) & \dots & w_{1,d}(\sigma) \\ \vdots & \ddots & \vdots \\ w_{d,1}(\sigma) & \dots & w_{d,d}(\sigma) \end{pmatrix}, \qquad j = 1,\dots,l, \quad \sigma \in \{0,1\}.$$

(d,l)-ММ–QBP Q определяется следующим образом: $Q = \big(|\mu_0\rangle, R, M_{acc}\big)$, где $R = \{\langle i_j, U_j^1(0),\dots,U_j^d(0), U_j^1(1),\dots,U_j^d(1)\rangle\}_{j=1}^{l}$.

Матрицы $U_j^i(\sigma)$ $(j = 1,\dots,l; i = 1,\dots,d; \sigma \in \{0,1\})$ устроены следующим образом: i-м столбцом матрицы $U_j^i(\sigma)$ является столбец $U_j^i(\sigma)[i] = (\sqrt{w_{1,i}(\sigma)},\dots,\sqrt{w_{d,i}(\sigma)})$. Значения остальных столбцов матрицы $U_j^i(\sigma)$ доопределяются произвольно с соблюдением условия унитарности матрицы.

Измерение, которое производится на каждом шаге работы программы Q, является так называемым «максимальным» измерением. В этом случае d-мерный вектор конфигурации проецируется на одно из d одномерных подпространств, каждое из которых образовано одним из d базисных векторов стандартного базиса. При этом результат измерения $\mu \in \{1,\dots,d\}$. После промежуточного измерения на каждом шаге работы программы Q в текущей конфигурации ровно одно состояние представлено с амплитудой, равной 1; остальные амплитуды равны нулю. Преобразования, применяемые на каждом шаге вычисления, зависят от значения считанной входной переменной и от результата измерения.

Построенная квантовая бинарная программа Q принимает входной набор $\sigma \in \{0,1\}^n$ с той же вероятностью, что и вероятностная бинарная программа P. Действительно, на каждом шаге работы программы Q после этапа измерения состояние ММ–QBP Q может быть описано

стохастическим вектором $|p\rangle = (p_1, \ldots, p_d)$, где p_i — вероятность нахождения Q в базисном состоянии $|i\rangle, i = 1, \ldots, d$. Тогда в соответствии с определением Q последующее унитарное преобразование и измерение на следующем шаге преобразуют вектор $|p\rangle$ в вектор $|p'\rangle = (p'_1, \ldots, p'_d)$ такой, что $p'_k = \sum\limits_{i=1}^{d} p_i w_{k,i},\ k = 1, \ldots, d$.

Вероятностная бинарная программа P на каждом шаге работы преобразует текущий стохастический вектор $|\mu\rangle = (\mu_1, \ldots \mu_d)$ в вектор $|\mu'\rangle = (\mu'_1, \ldots, \mu'_d)$ такой, что $\mu'_k = \sum\limits_{i=1}^{d} \mu_i w_{k,i},\ k = 1, \ldots, d$.

Начальный вектор $|p_0\rangle = |\mu_0\rangle$. Следовательно, на j-м шаге $(j = 1, \ldots, l)$ имеем $|p_l\rangle = |\mu_l\rangle$. Теорема 4 доказана.

ЛИТЕРАТУРА

1. **Баррингтон Д.** Ветвящиеся программы ограниченной ширины, имеющие полиномиальную сложность, распознают в точности языки из NC^1 // Кибернетический сборник. Вып. 28. М.: Мир. 1991. С. 94–113.
2. **Бухараев Р. Г.** Основы теории вероятностных автоматов. М.: Наука. 1985.
3. **Валиев В. А., Кокин А. А.** Квантовые компьютеры: надежды и реальность. Ижевск: НИС "Регулярная и хаотическая динамика 2001.
4. **Гайнутдинова А. Ф.** О сравнительной сложности квантовых и классических бинарных программ // Дискретная математика. 2002. Т. 14, вып. 3. С. 109–121.
5. **Гайнутдинова А. Ф.** Сравнительная сложность квантовых и вероятностных бинарных программ // Тезисы VIII Международного семинара «Дискретная математика и её приложения». (МГУ, Москва, февраль, 2004 г.). М: Изд-во механико-математического факультета МГУ, 2004. С. 58–61.
6. **Китаев А., Шень А., Вялый М.** Классические и квантовые вычисления. М.: МЦНМО, ЧеРО, 1999.
7. **Кострикин А. И., Манин Ю. И.** Линейная алгебра и геометрия. М.: Изд-во Моск. ун-та, 1980.
8. **Манин Ю. И.** Вычислимое и невычислимое. М.: Сов. радио, 1980.
9. **Ablayev F. M., Gainutdinova A., Karpinski M.** On computational power of quantum branching programs // Fundamentals of computation theory. 13th international symposium, FCT 2001. Proc. Berlin: Springer, 2001. P. 59–70. (Lecture Notes in Comput. Sci.; V.2138).
10. **Ablayev F. M., Karpinski M.** On the power of randomized branching programs // Automata, languages and programming. 23th international colloqium, ICALP 1996. Proc. Berlin, Springer, 1996. P. 348–356. (Lecture Notes in Comput. Sci.; V.1099).

11. Borodin A., Fischer M., Kirkpatrick D., Lynch N., Tompa M. A time-space tradeoff for sorting on non-oblivious machines // 20th annual symposium on foundations of computer science. New York: IEEE, 1979. P. 319–327.

12. Brodsky A., Pippenger N. Characterization of 1-way quantum finite automata // http://xxx.lanl.gov/archive/quant-ph. quant-ph/9903014.

13. Feynman R. Simulating physics with computers // Internat. J. Theoret. Phys. 1982. V. 21, N 6,7. P. 467–488.

14. Grover L. A fast quantum mechanical algorithm for database search // Proc. of the 28th annual ACM symposium on the theory of computing. New York: ACM Press, 1996. P. 212–219.

15. Gruska J. Quantum computing. New York: McGraw-Hill Publishing Company, 1999.

16. Kondacs A., Watrous J. On the power of quantum finite state automata // 38th annual symposium on foundations of computer Science. Los Alamitos, CA: IEEE Comput. Soc. Press, 1997. P. 66–75.

17. Moore C., Nilson M. Some notes on parallel quantum computing // http://xxx.lanl.gov/archive/quant-ph. quant-ph/9804034.

18. Nakanishi M., Hamaguchi K., Kashiwabara T. Ordered quantum branching programs are more powerful than ordered probabilistic branching programs under a bounded-width restriction // Computing and Combinatorics. 6th annual international conference, COCOON'2000. Proc. Berlin, Springer, 2000. P. 467–476. (Lecture Notes in Comput. Sci.; V. 1858).

19. Sauerhoff M., Sieling D. Quantum branching programs and space-bounded nonuniform quantum complexity // Theoret. Comput. Sci. 2005. V. 334, N 1–3. P. 177–225.

20. Shor P. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer // SIAM J. on Computing, 1997. V. 26, N 5. P. 1484–1509.

21. Yao A. C-C. Quantum circuit complexity // 34th annual symposium on foundation of computer science. Los Alamitos, CA: IEEE Comput. Soc. Press, 1993. P. 352–361.

Адрес автора:

Научно-исследовательский
институт математики и механики
им. Н. Г. Чеботарёва,
ул. Университетская, 17,
420008 Казань,
Россия.
E-mail: aida@ksu.ru

Статья поступила
24 мая 2005 г.