Math-Net.Ru

Общероссийский математический портал

А. Ф. Гайнутдинова, О сравнительной сложности квантовых и классических бинарных программ, *Дискрет. матем.*, 2002, том 14, выпуск 3, 109–121

DOI: <https://doi.org/10.4213/dm258>

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

Параметры загрузки:

IP: 54.196.121.252

26 апреля 2023 г., 13:58:27

О сравнительной сложности квантовых и классических бинарных программ

© 2002 г. А. Ф. Гайнутдинова

В работе дается определение квантовой бинарной программы. Рассматривается известная булева функция MOD_p . Доказывается, что любая детерминированная бинарная программа и вероятностная уровневая бинарная программа, $(1/2 + \varepsilon)$ -вычисляющая функцию MOD_p , имеют ширину, не меньшую p . Строится стабильная квантовая бинарная программа ширины $O(\log p)$, которая вычисляет функцию MOD_p с односторонней ошибкой $\varepsilon > 0$.

1. Введение и определения

История квантовых вычислений берет свое начало с 80-х годов. В 1980 году Ю. И. Манин [5] и в 1982 году Ричард Фейнман [11] высказали идею, что, поскольку моделирование квантовых процессов на классических компьютерах является сложной задачей, возможно, использование квантовых эффектов может быть полезным для решения классических задач. В последние годы в области теории квантовых вычислений опубликован ряд книг, в частности, на русском языке вышли книги [4, 2]. Все возрастающий интерес к этой области в немалой степени связан с тем, что были построены эффективные квантовые алгоритмы для некоторых известных задач. В частности, это полиномиальный квантовый алгоритм Шора [16] для факторизации чисел и алгоритм Гровера [12] поиска в неупорядоченной базе данных. Эти примеры подталкивают к исследованию сравнительной сложности квантовых и классических моделей вычислений. В частности, исследуются различные вычислительные модели с ограничениями (например, конечные автоматы [14], схемы с ограничениями [18]). Одной из таких моделей являются бинарные программы, представляющие собой модель для вычисления булевых функций. Напомним основные определения [17, 6].

Бинарная программа (БП) над множеством переменных $X = \{x_1, \dots, x_n\}$ — это ориентированный ациклический граф с двумя конечными вершинами, помеченными 0 и 1 соответственно. Каждая неконечная вершина помечена булевой переменной $x \in X$ и имеет два выходящих ребра, помеченных 0 и 1 соответственно. БП представляет булеву функцию

$$f: \{0, 1\}^n \rightarrow \{0, 1\}$$

следующим образом. Вычисление значения $f(\sigma)$ для входного набора $\sigma \in \{0, 1\}^n$ стартует из выделенной начальной вершины. Для каждой неконечной вершины, помеченной переменной x_j , осуществляется переход из этой вершины либо по 0-ребру, либо по 1-ребру, в соответствии со значением σ_j , которое принимает переменная x_j во входном наборе, до

тех пор, пока не будет достигнута конечная вершина. Значение функции f для входа σ — это значение достигнутой конечной вершины.

В 1995 Ф. М. Аблаев и М. Карпинский дали определение вероятностной бинарной программы [8]. В работе мы будем пользоваться следующим определением. Вероятностная бинарная программа (ВРР) — это бинарная программа, в которой каждая внутренняя вершина имеет выходную степень, не меньшую 2. При этом из каждой внутренней вершины выходит два типа ребер, помеченные 0 и 1. Каждому ребру e приписана вероятность $p(e)$, $0 \leq p(e) \leq 1$, таким образом, что для каждой вершины сумма вероятностей всех ребер, исходящих из этой вершины, помеченных 0 (1), равна 1. Вычисление на входном наборе $\sigma \in \{0, 1\}^n$ осуществляется следующим образом. На каждом шаге, начиная с выделенной начальной вершины, ВРР считывает значение переменной, приписанной вершине, и в зависимости от значения считанной переменной переходит в следующие вершины либо по 0-ребрам, либо по 1-ребрам с вероятностями, приписанными соответствующим ребрам. Вероятность $p_{\text{acc}}(\sigma)$ принятия ВРР входа σ — это вероятность того, что вычисление на входе σ приведет в конечную вершину, помеченную 1.

Определение 1. ВРР P вычисляет функцию f с ограниченной ошибкой, если существует $\varepsilon \in (0, 1/2]$ такое, что для любого $\sigma \in f^{-1}(1)$ вероятность

$$p_{\text{acc}}(\sigma) \geq 1/2 + \varepsilon,$$

и для любого $\sigma' \in f^{-1}(0)$ вероятность

$$p_{\text{acc}}(\sigma') \leq 1/2 - \varepsilon.$$

При этом говорят, что P $(1/2 + \varepsilon)$ -вычисляет функцию f .

Один раз читающая бинарная программа — это бинарная программа с ограничением, что на каждом пути из корня в конечную вершину каждая переменная $x \in X$ встречается не более одного раза.

Сложность $S(P)$ бинарной программы P — это число ее внутренних вершин.

Глубина бинарной программы P — это длина ее самого длинного пути из корня в финальную вершину.

Бинарная программа называется уровневой, если ее вершины могут быть разбиты на уровни $0, 1, \dots$ таким образом, что для каждого i ребра из вершин уровня i ведут только в вершины уровня $i + 1$. Каждая бинарная программа P может быть преобразована в уровневую бинарную программу P' , вычисляющую ту же самую функцию. При этом полученная программа P' будет иметь ту же глубину, что и исходная программа, и $S(P') \leq S^2(P)$ [10].

Ширина $w(P)$ уровневой бинарной программы P — это максимум числа вершин на уровне, взятый по всем уровням программы P .

Уровневая бинарная программа P называется забывающей, если на любом уровне P тестируется только одна переменная.

Определение 2. Забывающая бинарная программа P называется стабильной, если преобразования, применяемые при значении переменной, равном 0 (1), не зависят от номера уровня, на котором они применяются.

Модель квантовой бинарной программы, которая рассматривается в работе, была впервые описана в [7]. Без ограничения общности мы рассматриваем уровневые бинарные

программы. Встает естественный вопрос о сравнительной сложности квантовых и классических бинарных программ. В работе рассматриваются один раз читающие бинарные программы. Поскольку для таких бинарных программ глубина всегда ограничена величиной n , естественной мерой сложности в этом случае является ширина бинарной программы. В статье показывается, что квантовые бинарные программы могут быть экспоненциально более экономные, чем классические. Для этого мы рассматриваем известную булеву функцию MOD_p . Мы доказываем, что любая детерминированная бинарная программа и вероятностная стабильная бинарная программа, $(1/2 + \varepsilon)$ -вычисляющая функцию MOD_p , имеют ширину, не меньшую p . В то же время мы строим стабильную квантовую бинарную программу ширины $O(\log p)$, которая вычисляет функцию MOD_p с односторонней ошибкой $\varepsilon > 0$. Отметим, что при построении квантовой бинарной программы для функции MOD_p использованы подходы, предложенные в [9].

1.1. Определение квантовой бинарной программы

Пусть $\mathcal{H}^d$ — d -мерное гильбертово пространство с нормой $\|\cdot\|_2$, то есть, для $z \in \mathcal{H}^d$, $z = \{z_1, \dots, z_d\}$,

$$\|z\|_2 = \sqrt{\sum_{i=1}^d |z_i|^2}.$$

Обозначим через QS квантовую систему с d устойчивыми состояниями $\{1, \dots, d\}$. Чистое квантовое состояние квантовой системы QS задается сопоставлением каждому состоянию i квантовой системы QS амплитуды z_i , где z_i — комплексные числа.

В квантовой механике для описания квантовой системы и ее эволюции приняты следующие обозначения. Рассмотрим квантовые базисные состояния

$$\{|1\rangle, \dots, |d\rangle\},$$

где $\{|i\rangle\}$ — множество d -мерных ортогональных базисных векторов (назовем его стандартным базисом). Здесь $|i\rangle$ (обозначение Дирака) — это единичный вектор-столбец со значением 1 в i -й позиции и значением 0 во всех остальных. Тогда чистое квантовое состояние $|\psi\rangle$ может быть представлено как

$$|\psi\rangle = \sum_{i=1}^d z_i |i\rangle$$

или коротко

$$|\psi\rangle = (z_1, \dots, z_d)^T,$$

где

$$\sum_{i=1}^d |z_i|^2 = 1.$$

Всюду далее в работе будем называть $|\psi\rangle$ конфигурацией. Элемент z_i называется амплитудой базисного состояния $|i\rangle$ квантовой системы QS, при этом $|z_i|^2$ дает вероятность обнаружения QS в состоянии $|i\rangle$. Эволюция квантовой системы 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 $U — d \times d$ унитарная матрица. Пусть X — множество булевых переменных. Определим квантовое преобразование (d -мерное квантовое преобразование) конфигурации $|\psi\rangle$ как тройку

$$\langle j, U(0), U(1) \rangle,$$

где j — индекс переменной $x_j \in X$, $U(0), U(1)$ — обратимые преобразования, действующие в $\mathcal{H}^d$, представленные унитарными $d \times d$ матрицами. Квантовое преобразование $\langle j, U(0), U(1) \rangle$ действует следующим образом. Для конфигурации $|\psi\rangle$

$$U|\psi\rangle = |\psi'\rangle,$$

где $U = U(1)$, если $x_j = 1$, и $U = U(0)$, если $x_j = 0$.

Извлечение информации о QS из конфигурации $|\psi\rangle$ называется измерением и определяется следующим образом (см., например, главу 1.6 в [13]). Пусть $E_{\text{acc}}, E_{\text{rej}}$ — такие ортогональные подпространства $\mathcal{H}^d$ размерности r и $d - r$ соответственно, $r \leq d$, что

$$\mathcal{H}^d = E_{\text{acc}} \oplus E_{\text{rej}}$$

— ортогональная сумма. Назовем E_{acc} подпространством принимающих состояний, E_{rej} подпространством отвергающих состояний. Конфигурация $|\psi\rangle$ может быть однозначно представлена как линейная суперпозиция проекций $|\psi\rangle$ на E_{acc} и E_{rej} , то есть

$$|\psi\rangle = |\psi_{E_{\text{acc}}}\rangle + |\psi_{E_{\text{rej}}}\rangle,$$

где

$$|\psi_{E_{\text{acc}}}\rangle \in E_{\text{acc}}, \quad |\psi_{E_{\text{rej}}}\rangle \in E_{\text{rej}}.$$

Обозначим через $|\psi_{E_{\text{acc}}}^n\rangle, (|\psi_{E_{\text{rej}}}^n\rangle)$ нормализованную проекцию на подпространство E_{acc} (E_{rej}), то есть

$$\| |\psi_{E_{\text{acc}}}^n\rangle \| = 1, \quad (\| |\psi_{E_{\text{rej}}}^n\rangle \| = 1).$$

Тогда

$$|\psi\rangle = \alpha_{\text{acc}} |\psi_{E_{\text{acc}}}^n\rangle + \alpha_{\text{rej}} |\psi_{E_{\text{rej}}}^n\rangle.$$

Здесь $\alpha_{\text{acc}} (\alpha_{\text{rej}})$ — это амплитуда проекции на подпространство принимающих (отвергающих) состояний.

Вероятность выбора подпространства принимающих состояний

$$p_{\text{acc}} = |\alpha_{\text{acc}}|^2.$$

Вероятность выбора подпространства отвергающих состояний

$$p_{\text{rej}} = |\alpha_{\text{rej}}|^2.$$

Очевидно, что $p_{\text{acc}} + p_{\text{rej}} = 1$.

Формально измерение удобно описывать следующим образом. Пусть $|\psi\rangle$ — конфигурация, и пусть подпространство $E_{\text{acc}} \subseteq \mathcal{H}^d$ принимающих состояний задается системой $\{|e_i\rangle\}_{i=1}^r$ ортонормированных векторов. Измерение (считывание результата квантового вычисления) представляется $r \times d$ матрицей проекции M_{acc} на подпространство принимающих состояний. Здесь i -я строка $M_{\text{acc}}[i], i \in \{1, \dots, r\}$, определяется следующим образом:

$$M_{\text{acc}}[i] = (\alpha_1, \dots, \alpha_d),$$

где

$$|e_i\rangle = \alpha_1|1\rangle + \dots + \alpha_d|d\rangle,$$

то есть i -я строка матрицы M_{acc} — это представление базисного вектора $|e_i\rangle$ в стандартном базисе $\{|1\rangle, \dots, |d\rangle\}$.

Для конфигурации $|\psi\rangle$ вероятность выбора подпространства принимающих состояний

$$p_{\text{acc}} = \|M_{\text{acc}}|\psi\rangle\|^2.$$

Квантовая бинарная программа P ширины d и длины l ((d, l) -QBP), основанная на QS, определяется как

$$P = \langle T, |\psi_0\rangle, M_{\text{acc}} \rangle,$$

где T — последовательность (длины l) d -мерных квантовых преобразований квантовой системы QS с d состояниями:

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

где $|\psi_0\rangle$ — начальная конфигурация P , M_{acc} — матрица проекции.

Определим вычисление P на входном наборе

$$\sigma = (\sigma_1, \dots, \sigma_n) \in \{0, 1\}^n$$

следующим образом.

- (1) Вычисление P начинается из конфигурации $|\psi_0\rangle$. На i -м шаге вычисления, $1 \leq i \leq l$, программа P преобразует конфигурацию $|\psi\rangle$ в конфигурацию

$$|\psi'\rangle = U_i(\sigma_{j_i})|\psi\rangle.$$

- (2) После l -го (последнего) шага квантовых преобразований производится измерение (считывание результата вычисления) полученной конфигурации $|\psi_\sigma\rangle$, где

$$|\psi_\sigma\rangle = U_l(\sigma_{i_l})U_{l-1}(\sigma_{i_{l-1}}) \dots U_1(\sigma_{i_1})|\psi_0\rangle,$$

которое задается матрицей M_{acc} . Если результирующее состояние принадлежит подпространству принимающих состояний, то вход σ принимается. Если результирующее состояние принадлежит подпространству отвергающих состояний, то вход σ отвергается.

Вероятность $p_{\text{acc}}(\sigma)$ принятия программой P входа σ определяется как

$$p_{\text{acc}}(\sigma) = \|M_{\text{acc}}|\psi_\sigma\rangle\|^2.$$

Определенная нами QBP является забывающей.

Определение 3. QBP P вычисляет функцию f с ограниченной ошибкой, если существует $\varepsilon > 0$ такое, что для любого $\sigma \in f^{-1}(1)$ вероятность принятия программой P входа σ не меньше $1/2 + \varepsilon$ и для любого $\sigma' \in f^{-1}(0)$ вероятность принятия программой P входа σ' не больше $1/2 - \varepsilon$. При этом говорят, что программа P $(1/2 + \varepsilon)$ -вычисляет функцию f .

Обозначим 1QBP квантовую бинарную программу с ограничением, состоящим в том, что каждая переменная $x \in X$ присутствует в последовательности T квантовых преобразований P не более одного раза.

Шириной $w(P)$ квантовой программы P называется размерность d пространства $\mathcal{H}^d$ конфигураций.

1.2. Основные результаты

Рассмотрим булеву функцию MOD_p . На наборе $\sigma = (\sigma_1, \dots, \sigma_n) \in \{0, 1\}^n$

$$\text{MOD}_p(\sigma) = 1$$

тогда и только тогда, когда число единиц в наборе кратно p , где p — простое число, $p \leq n/2$.

Предложение 1. *Любая детерминированная OBDD, вычисляющая MOD_p , имеет ширину, не меньшую p .*

Доказательство. Действительно, предположим, что существует детерминированная OBDD, вычисляющая функцию MOD_p , которая имеет ширину, строго меньшую p . Тогда в соответствии с принципом Дирихле, найдутся два подслова

$$\sigma_1, \dots, \sigma_{n-p}, \quad \sigma'_1, \dots, \sigma'_{n-p}$$

с разным по модулю p числом единиц, которые ведут в одну вершину. Возьмем подслово

$$\sigma_{n-p+1}, \dots, \sigma_n$$

такое, что

$$\text{MOD}_p(\sigma_1, \dots, \sigma_{n-p}, \sigma_{n-p+1}, \dots, \sigma_n) = 1,$$

а

$$\text{MOD}_p(\sigma'_1, \dots, \sigma'_{n-p}, \sigma_{n-p+1}, \dots, \sigma_n) = 0.$$

При этом пути

$$\sigma_1, \dots, \sigma_{n-p}, \sigma_{n-p+1}, \dots, \sigma_n, \quad \sigma'_1, \dots, \sigma'_{n-p}, \sigma_{n-p+1}, \dots, \sigma_n$$

ведут в одну финальную вершину, что противоречит тому, что данная бинарная программа правильно вычисляет функцию MOD_p .

Теорема 1. *Существует стабильная $(O(\log p), n)$ -1QBP, с односторонней ошибкой $\varepsilon \geq 0$ вычисляющая функцию MOD_p , где p , $p < n/2$, — простое число.*

Теорема 2. *Любая стабильная один раз считывающая вероятностная бинарная программа, вычисляющая функцию MOD_p , где p , $p < n/2$, — простое число с вероятностью $1/2 + \varepsilon$ для фиксированного $\varepsilon \in (0, 1/2]$, имеет ширину, не меньшую p .*

Доказательства теорем 1, 2 приводятся в следующих разделах.

2. Доказательство теоремы 1

Сначала построим QBP P , принимающую входы $\sigma \in \text{MOD}_p^{-1}(1)$ с вероятностью 1 и отвергающие входы $\sigma \in \text{MOD}_p^{-1}(0)$ с вероятностью, не меньшей $1/8$. Рассмотрим $(2, n)$ -1QBP P^k для $k \in \{1, \dots, p-1\}$. Квантовая бинарная программа

$$P^k = \langle T^k, |\psi_0\rangle, M_{\text{acc}} \rangle$$

основана на квантовой системе из двух состояний. Здесь

$$T^k = (\langle j, U(0), U^k(1) \rangle)_{j=1}^n,$$

где

$$j = 1, \dots, n, \quad U(0) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad U^k(1) = \begin{pmatrix} e^{2\pi i k/p} & 0 \\ 0 & e^{-2\pi i k/p} \end{pmatrix},$$

$$M_{\text{acc}} = \left(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}} \right), \quad |\psi_0\rangle = \left(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}} \right)^T.$$

Отметим, что матрицы преобразований $U(0), U^k(1)$ не зависят от j , то есть P^k — стабильная бинарная программа. Обозначим через $l(\sigma)$ число единиц в наборе σ ,

$$l(\sigma) = \sum_{i=1}^n \sigma_i.$$

Лемма 1. Квантовая бинарная программа P^k , $k \in \{1, \dots, p-1\}$, принимает входной набор $\sigma = (\sigma_1, \dots, \sigma_n)$ с вероятностью

$$p_{\text{acc}}(\sigma) = \cos^2 \left(\frac{2\pi l(\sigma)k}{p} \right).$$

Доказательство. Из описания программы P^k следует, что после считывания входного набора σ результирующая конфигурация $|\psi(\sigma)\rangle$ имеет вид

$$|\psi(\sigma)\rangle = \frac{1}{\sqrt{2}} e^{2\pi i l(\sigma)k/p} |1\rangle + \frac{1}{\sqrt{2}} e^{-2\pi i l(\sigma)k/p} |2\rangle.$$

После умножения матрицы M_{acc} на $|\psi(\sigma)\rangle$ получаем, что

$$M_{\text{acc}}|\psi(\sigma)\rangle = \frac{1}{2} \left(e^{2\pi i l(\sigma)k/p} + e^{-2\pi i l(\sigma)k/p} \right),$$

и используя равенство $e^{ix} = \cos x + i \sin x$, находим, что

$$M_{\text{acc}}|\psi(\sigma)\rangle = \cos \left(\frac{2\pi l(\sigma)k}{p} \right),$$

$$p_{\text{acc}} = \|M_{\text{acc}}|\psi(\sigma)\rangle\|^2 = \cos^2 \left(\frac{2\pi l(\sigma)k}{p} \right).$$

Если число $l(\sigma)$ единиц во входном наборе σ кратно p , то $2\pi l(\sigma)k/p$ кратно 2π и $\cos(2\pi l(\sigma)k/p) = 1$. Поэтому все QBP P^k принимают вход $\sigma \in \text{MOD}_p^{-1}(1)$ с вероятностью 1.

Мы будем называть программу P^k хорошей для входного набора $\sigma \in \text{MOD}_p^{-1}(0)$, если P^k отвергает σ с вероятностью, не меньшей $1/2$.

Лемма 2. Для любого $\sigma \in \text{MOD}_p^{-1}(0)$ не менее $(p-1)/2$ всех P^k являются хорошими.

Доказательство. Согласно лемме 1 вероятность принятия набора $\sigma = (\sigma_1, \dots, \sigma_n)$ программой P^k равна

$$p_{\text{асс}} = \cos^2(2\pi l(\sigma)k/p).$$

Ясно, что

$$\cos^2(2\pi l(\sigma)k/p) \leq 1/2$$

тогда, когда

$$|\cos(2\pi l(\sigma)k/p)| \leq 1/\sqrt{2}.$$

Это произойдет в том случае, если $(2\pi l(\sigma)k/p)$ находится в секторе

$$[\pi/4 + 2\pi j, 3\pi/4 + 2\pi j]$$

или

$$[5\pi/4 + 2\pi j, 7\pi/4 + 2\pi j]$$

для некоторого $j \in N$. Но

$$(2\pi l(\sigma)k/p) \in [\pi/4 + 2\pi j, 3\pi/4 + 2\pi j] \quad ([5\pi/4 + 2\pi j, 7\pi/4 + 2\pi j]),$$

если

$$(2\pi (l(\sigma)k \bmod p)/p) \in [\pi/4, 3\pi/4] \quad ([5\pi/4, 7\pi/4]).$$

Число p простое, $l(\sigma)$ относительно просто с p . Поэтому

$$l(\sigma) \bmod p, 2l(\sigma) \bmod p, \dots, (p-1)l(\sigma) \bmod p$$

— это числа $1, 2, \dots, p-1$, расположенные в некотором порядке. Поэтому достаточно подсчитать мощность множества

$$I = \{i_1, \dots, i_l\} \subset \{1, \dots, p-1\}$$

такого, что

$$2\pi i_j / p \in [\pi/4, 3\pi/4]$$

или

$$2\pi i_j / p \in [5\pi/4, 7\pi/4]$$

для всех $i_j \in I$. Так как p точек

$$2\pi/p, \dots, 2\pi(p-1)/p, 2\pi$$

равномерно распределены на окружности от 0 до 2π , а секторы

$$[\pi/4, 3\pi/4], \quad [5\pi/4, 7\pi/4]$$

составляют ровно половину окружности, то не менее $\lfloor p/2 \rfloor$ точек попадут в указанные секторы. Следовательно,

$$|I| \geq \lfloor p/2 \rfloor \geq (p-1)/2.$$

Назовем подмножество квантовых бинарных программ

$$S = \{P^{i_1}, \dots, P^{i_l}\} \subset \{P^1, \dots, P^{p-1}\}$$

подходящим для входного набора $\sigma \in \text{MOD}_p^{-1}(0)$, если не менее $1/4$ его элементов являются хорошими для этого σ .

Лемма 3. Существует подмножество $S \subset \{P^1, \dots, P^{p-1}\}$ один раз считывающих квантовых бинарных программ, $|S| = t = \lceil 16 \ln p \rceil$, которое является подходящим для всех входных наборов $\sigma \in \text{MOD}_p^{-1}(0)$.

Доказательство. Рассмотрим следующую процедуру $\mathcal{A}$ для построения подходящего подмножества S квантовых бинарных программ:

для фиксированного входа $\sigma \in \text{MOD}_p^{-1}(0)$ с $l(\sigma) \leq p-1$ процедура $\mathcal{A}$ равновероятно выбирает программы из множества $\{P^1, \dots, P^{p-1}\}$.

Вероятность выбора хорошей программы на каждом шаге согласно лемме 2 не менее $1/2$. Согласно оценке Чернова, вероятность того, что в множестве мощности $16 \ln p$ менее чем $1/4$ часть его элементов окажутся хорошими, не больше, чем

$$\exp\left(-\frac{16 \ln p}{2} \frac{1}{2^2} \frac{1}{2}\right) = \frac{1}{p}.$$

Следовательно, вероятность того, что построенное подмножество окажется неподходящим хотя бы для одного $\sigma \in \text{MOD}_p^{-1}(0)$ с $l(\sigma) \in \{1, \dots, p-1\}$, меньше или равна $(p-1)/p$. Поэтому существует подмножество, которое является подходящим для всех $\sigma \in \text{MOD}_p^{-1}(0)$ с $l(\sigma) \leq p-1$. Это же подмножество программ будет подходящим и для всех $\sigma \in \text{MOD}_p^{-1}(0)$ с $l(\sigma) > p$, поскольку каждая программа P^k переводит текущую конфигурацию в начальную после считывания каждых p единиц и поэтому работает одинаково на всех словах с одинаковым по модулю p значением $l(\sigma)$.

1QBP P , которая принимает входы $\sigma \in \text{MOD}_p^{-1}(1)$ с вероятностью 1 и отвергает входы $\sigma \in \text{MOD}_p^{-1}(0)$ с вероятностью, не меньшей $1/8$, устроена следующим образом.

$(2t, n)$ -1QBP $P = \langle T, |\Psi_0\rangle, \mathcal{M}_{\text{acc}} \rangle$ основана на квантовой системе из $2t$ состояний. Здесь

$$T = ((j, \mathcal{U}(0), \mathcal{U}(1)))_{j=1}^n,$$

$$|\Psi_0\rangle = \left(\frac{1}{\sqrt{2t}}, \frac{1}{\sqrt{2t}}, \dots, \frac{1}{\sqrt{2t}} \right)^T.$$

Матрица $\mathcal{U}(0)$ — единичная $2t \times 2t$ матрица, $\mathcal{U}(1)$ и $\mathcal{M}_{\text{acc}}$ — матрицы размерностей $2t \times 2t$ и $t \times 2t$, соответственно, определенные следующим образом:

$$\mathcal{U}(1) = \begin{pmatrix} U^{i_1} & \mathbf{0} & \dots & \mathbf{0} \\ \mathbf{0} & U^{i_2} & \dots & \mathbf{0} \\ & & \dots & \\ \mathbf{0} & \mathbf{0} & \dots & U^{i_t} \end{pmatrix},$$

$$\mathcal{M}_{\text{acc}} = \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1/\sqrt{2} & 1/\sqrt{2} & \dots & 0 & 0 \\ & & & & \dots & & \\ 0 & 0 & 0 & 0 & \dots & 1/\sqrt{2} & 1/\sqrt{2} \end{pmatrix}.$$

Построенную квантовую бинарную программу P удобно рассматривать как программу, состоящую из подходящего подмножества S квантовых бинарных программ $\{P^{i_1}, \dots, P^{i_t}\}$, которые работают квантово параллельно. В начальной конфигурации программы P эти программы представлены с равными амплитудами. Матрицы $\mathcal{U}(0)$, $\mathcal{U}(1)$,

M_{acc} — это блочно диагональные матрицы, где на диагонали стоят матрицы $U(0)$, $U(1)$ преобразований и матрицы M_{acc} проекции, соответственно, $(2, n)$ -IQBP бинарных программ $\{P^{i_1}, \dots, P^{i_t}\}$. При этом каждый блок воздействует только на соответствующую пару состояний.

Программа P принимает входы $\sigma \in \text{MOD}_p^{-1}(1)$ с вероятностью 1, так как все P^k принимают их. Для любого $\sigma \in \text{MOD}_p^{-1}(0)$ не менее $1/4$ программ $P^k \in S$ отвергают его с вероятностью, не меньшей $1/2$, поэтому общая вероятность отвергнуть любой $\sigma \in \text{MOD}_p^{-1}(0)$ не менее $1/8$.

Используя стандартную технику для вычислений с односторонней ошибкой, можно увеличить вероятность правильного ответа до $1 - \varepsilon$ для произвольного $\varepsilon \geq 0$. Для этого возьмем $d = d(\varepsilon)$ копий квантовых бинарных программ P и запустим их детерминированно параллельно. Вход принимается, если все бинарные программы принимают его. В противном случае вход отвергается. В этом случае ширина IQBP будет $O(\log p)$.

Теорема 1 доказана.

3. Доказательство теоремы 2

Предположим, что существует стабильная вероятностная бинарная программа P ширины $q < p$, вычисляющая MOD_p с вероятностью $1/2 + \varepsilon$ для фиксированного $\varepsilon \in (0, 1/2]$. Без ограничения общности предполагаем, что каждый уровень P содержит ровно q вершин. В противном случае мы можем достроить бинарную программу так, чтобы это условие выполнялось.

Каждому уровню j программы P сопоставим вектор распределения вероятностей

$$\mu^j = (\mu_1^j, \dots, \mu_q^j),$$

где μ_i^j — вероятность нахождения в i -й вершине j -го уровня. Мы можем описать процесс вычисления функции f программой P для входа $\tilde{\sigma} = (\sigma_1, \dots, \sigma_n)$ следующим образом.

Вычисление начинается с начального вектора распределения вероятностей μ^0 .

На j -м шаге, $1 \leq j \leq n$, программа P считывает входной символ σ_{ij} и преобразует вектор распределения вероятностей μ^{j-1} в

$$\mu^j = \mu^{j-1} A,$$

где A — стохастическая матрица размера $q \times q$, $A = A(0)$, если $\sigma_{ij} = 0$, и $A = A(1)$, если $\sigma_{ij} = 1$.

После последнего n -го шага вычисления P принимает вход $\tilde{\sigma}$ с вероятностью

$$P_{\text{acc}}(\tilde{\sigma}) = \sum_{i \in F} \mu_i^n.$$

Здесь F — множество конечных вершин, помеченных 1. Если $f(\tilde{\sigma}) = 1$, то

$$P_{\text{acc}}(\tilde{\sigma}) \geq 1/2 + \varepsilon,$$

в противном случае

$$P_{\text{acc}}(\tilde{\sigma}) \leq 1/2 - \varepsilon.$$

Без ограничения общности полагаем, что P считывает переменные в естественном порядке $x_1, \dots, x_n$. В противном случае мы можем просто переупорядочить входной набор. Через Σ^n обозначим всевозможные n входных наборов $\tilde{\sigma}_n, \dots, \tilde{\sigma}_1$, в которых сначала идут все нули, а затем все единицы. При $i \in \{1, \dots, n\}$ набор $\tilde{\sigma}_i$ имеет вид

$$\tilde{\sigma}_i = \tilde{\sigma}_i^0 \tilde{\sigma}_i^1,$$

где

$$\tilde{\sigma}_i^0 = 0 \dots 0, \quad \tilde{\sigma}_i^1 = 1 \dots 1,$$

причем число нулей равно $n - i$, а число единиц i .

Будем подавать на вход P только входные наборы из Σ^n . Пусть μ^i — вектор распределения вероятностей после считывания $\tilde{\sigma}_i^0$, то есть

$$\mu^i = \mu^0 A(0) \dots A(0) = \mu^0 A^{n-i}(0).$$

Часть $\tilde{\sigma}_i^1$ содержит только единицы, следовательно, вычисление после считывания $\tilde{\sigma}_i^0$ может быть описано цепью Маркова. В этом случае μ^i — начальное распределение вероятностей, $A(1)$ — матрица переходных вероятностей. Состояния марковской цепи разделяются на эргодические и невозвратные (см., например, [3]). Эргодическое множество состояний — это множество, которое процесс никогда не сможет покинуть, если в него однажды попадет. Невозвратное множество — это множество, в которое процесс не может вернуться, если его покидает. Эргодическое состояние — это элемент эргодического множества. Невозвратное состояние — это элемент невозвратного множества.

Любая цепь Маркова обязательно содержит хотя бы одно эргодическое множество. Наличие невозвратных множеств необязательно. Если цепь Маркова содержит более чем одно эргодическое множество, то между этими множествами нет взаимодействия. Следовательно, мы имеем две или более изолированные цепи Маркова, объединенные вместе, которые мы можем изучать по отдельности. Если цепь Маркова состоит из единственного эргодического множества, она называется эргодической цепью. Каждая эргодическая цепь либо регулярна, либо циклична.

Если эргодическая цепь регулярна, то достаточно высокая степень матрицы переходных вероятностей содержит только положительные элементы. Это значит, что из какого бы состояния процесс ни начался, по прошествии достаточно большого числа шагов он может оказаться в любом состоянии. Кроме того, существует предельный вектор вероятностей состояний, не зависящий от выбора вектора начального распределения вероятностей (см., например, теорему 4.1.6. [3]).

Если цепь Маркова циклична, то она имеет период t и все ее состояния подразделяются на t циклических множеств, $t > 1$. При выбранном начальном состоянии процесс движется по циклическим множествам в определенном порядке, возвращаясь в множество, содержащее начальное состояние, через каждые t шагов. По прошествии достаточного времени процесс может находиться в любом состоянии циклического множества, соответствующего данному моменту. Следовательно, для каждого из циклических множеств t -я степень матрицы переходных вероятностей описывает регулярную цепь Маркова. К тому же, если эргодическая цепь циклична с периодом t , она имеет не менее t состояний.

Мы предположили, что число состояний $q < p$, то есть для каждой циклической цепи число $t < p$. Через D обозначим наименьшее общее кратное всех таких t . Так как p — простое число и $t < p$, t относительно просто с p . Следовательно, D относительно просто с p , и любая положительная степень D^m также относительно проста с p .

Пусть α^k — распределение вероятностей после считывания части $\tilde{\sigma}_k^1$ слова $\tilde{\sigma}_k$. Без ограничения общности мы можем считать, что у нас одно принимающее состояние. Пусть α_{acc}^k — вероятность нахождения в принимающем состоянии после считывания $\tilde{\sigma}_k^1$. Так как после каждых D шагов процесс может быть в любом состоянии множества, содержащего принимающее состояние, D -я степень матрицы $A(1)$ описывает регулярную марковскую цепь для этого множества. Из теории марковских цепей известно, что существует α_{acc} такое, что

$$\lim_{k \rightarrow \infty} \alpha_{\text{acc}}^{kD} = \alpha_{\text{acc}}.$$

Следовательно, для любого $\varepsilon > 0$ верно неравенство

$$|\alpha_{\text{acc}}^{D^m} - \alpha_{\text{acc}}^{D^m P}| < 2\varepsilon$$

для достаточно большого m . Но так как по предположению P $(1/2 + \varepsilon)$ -вычисляет функцию MOD_p , справедливы неравенства

$$\alpha_{\text{acc}}^{D^m P} \geq 1/2 + \varepsilon, \quad \alpha_{\text{acc}}^{D^m} \leq 1/2 - \varepsilon.$$

Получаем противоречие с неравенством, полученным выше.

Теорема 2 доказана.

4. Заключение

Описанная в работе модель квантовых бинарных программ является достаточно мощной, она способна вычислять любую булеву функцию [7]. Отметим, что данная модель является забывающей. Известная модель перестановочных бинарных программ является частным случаем описанной модели. В [1] показано, что перестановочные бинарные программы ограниченной ширины (а именно, ширины 5) полиномиальной сложности в точности совпадают с известным классом NC^1 схем из функциональных элементов логарифмической глубины.

В [15] введена модель квантовой бинарной программы как непосредственного обобщения вероятностной модели. В отличие от нашей модели, язык описания этой бинарной программы графовый. Квантовая бинарная программа из [15] не обязательно уровневая и забывающая. Иначе определяются понятия ширины и конфигурации квантовой бинарной программы. Под конфигурацией в модели, описанной в [15], понимается суперпозиция множества всех вершин бинарной программы. В нашей модели конфигурация — это суперпозиция множества вершин на уровне. С этой точки зрения преимуществом квантовой бинарной программы, описанной в работе, является то, что в данной модели задействовано гораздо меньше кубитов, чем в модели из [15], что может оказаться важным для практической реализации. Напомним, что число кубитов равно логарифму от числа устойчивых состояний квантовой системы.

Автор выражает благодарность своему научному руководителю Ф. М. Аблаеву за оказанную помощь и полезные замечания при подготовке статьи.

Список литературы

1. Баррингтон Д., Ветвящиеся программы ограниченной ширины, имеющие полиномиальную сложность, распознают в точности языки из NC^1 . *Киберн. сб.* (1991) **28**, 94–113.
2. Валиев В. А., Кокин А. А., *Квантовые компьютеры: надежды и реальность*. НИС, Ижевск, 2001.
3. Кемени Д., Снелл Д., *Конечные цепи Маркова*. Наука, Москва, 1970.
4. Китаев А., Шень А., Вялый М., *Классические и квантовые вычисления*. МЦНМО, Москва, 1999.
5. Манин Ю. И., *Вычислимое и невычислимое*. Сов. радио, Москва, 1980.
6. Окольнішнікова Е. А., Нижние оценки сложности реализации характеристических функций двоичных кодов бинарными программами. *Методы дискретного анализа в синтезе реализаций булевых функций* (1991) **51**, 61–83.
7. Ablayev F., Gainutdinova A., Karpinski M., On computational power of quantum branching programs. *Lect. Notes Computer Sci.* (2001) **2138**, 59–70.
8. Ablayev F., Karpinski M., On the power of randomized branching programs. *Lect. Notes Computer Sci.* (1996) **1099**, 348–356.
9. Ambainis A., Freivalds R., 1-way quantum finite automata: strengths, weaknesses and generalization. *Proc. 39th Annual Symp. Found. Computer Sci.* (1998), 332–342.
10. Borodin A., Fischer M., Kirkpatrick D., Lynch N., Tompa M., A time-space tradeoff for sorting on non-oblivious machines. *Proc. 20th Annual Symp. Found. Computer Sci.* (1979), 319–327.
11. Feynman R., Simulation physics with computers. *Intern. J. Theoretical Physics* (1982) **21**, 467.
12. Grover L., A fast quantum mechanical algorithm for database search. In: *Proc. 28th STOC*, 1996, pp. 212–219.
13. Gruska J. *Quantum computing*. McGraw–Hill, New York, 1999.
14. Kondacs A., Watrous J., On the power of quantum finite state automata. In: *Proc. 38th Annual Symp. Found. Computer Sci.*, 1997, pp. 66–75.
15. Nakanishi M., Hamaguchi K., Kashiwabara T., Ordered quantum branching programs are more powerful than ordered probabilistic branching programs under a bounded-width restriction. *Lect. Notes Computer Sci.* (2000) **1858**, 467–476.
16. Shor P., Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.* (1997) **26**, 1484–1509.
17. Wegener I., *Branching programs and binary decision diagrams. Theory and applications*. SIAM, Philadelphia, 2000.
18. Yao A., Quantum circuit complexity. In: *Proc. 34th Annual Symp. Found. Computer Sci.*, 1993, pp. 352–361.

Статья поступила 22.02.2002.

Переработанный вариант поступил 18.07.2002.