КОМПЬЮТЕРНЫЕ НАУКИ И ИНФОРМАТИКА

Научная статья
УДК 519.71
DOI: 10.17072/1993-0550-2024-4-117-131
https://elibrary.ru/tuqhho

Недетерминированные квантовые OBDD большой ширины

Аида Фаритовна Гайнутдинова
Казанский (Приволжский) федеральный университет, г. Казань, Россия
aida.ksu@gmail.com

Аннотация. В статье исследуются упорядоченные ветвящиеся диаграммы решений (OBDD – Ordered Binary Decision Diagrams) – модель для вычисления булевых функций. Целью работы является сравнительный сложностной анализ квантовых и классических недетерминированных OBDD большой ширины. Исследуется сложность вычисления булевой функции "Равенство" в недетерминированных квантовых OBDD для различных порядков считывания переменных в сравнении с классической сложностью. Показывается, что при использовании порядка чтения переменных, при котором ширина классической недетерминированной OBDD константна, ширина квантовой модели линейна, и что доказанная нижняя оценка точна. Определяется булева функция, для которой ширина квантовой недетерминированной OBDD экспоненциальна для любого порядка считывания. Предлагается квантовый алгоритм вычисления этой функции с нулевой ошибкой. Представляется результат о соотношении сложностных классов для квантовых и классических недетерминированных OBDD большой ширины.

Ключевые слова: *ветвящаяся программа; упорядоченная ветвящаяся диаграмма решений; недетерминизм; квантовый алгоритм; сложность; класс сложности; вычислительная модель; иерархия сложностных классов; нижняя оценка; верхняя оценка*

Для цитирования: *Гайнутдинова А.Ф.* Недетерминированные квантовые OBDD большой ширины // Вестник Пермского университета. Математика. Механика. Информатика. 2024. Вып. 4(67). С. 117–131. DOI: 10.17072/1993-0550-2024-4-117-131. https://elibrary.ru/tuqhho.

Благодарности: Работа выполнена за счет средств Программы стратегического академического лидерства Казанского (Приволжского) федерального университета ("ПРИОРИТЕТ-2030").

Статья поступила в редакцию 11.10.2024; одобрена после рецензирования 28.10.2024; принята к публикации 01.12.2024.

COMPUTER SCIENCE

Research article

Large Width Nondeterministic Quantum OBDDs

Aida. F. Gainutdinova
Kazan Federal University, Kazan, Russia
aida.ksu@gmail.com

Abstract. In this paper we investigate ordered binary decision diagrams (OBDD) – a model for computing Boolean functions. The aim of this work is a comparative complexity analysis of quantum and classical nondeterministic OBDDs of large width. We study the complexity of computing the Boolean function "Equality" in nondeterministic quantum OBDDs for different order of reading variables in comparison with the classical complexity. We show that when using the order of reading for which the width of the classical nondeterministic OBDD is constant, the width of the quantum model is linear and the proved lower bound is tight. We define a Boolean function for which the width of nondeterministic quantum OBDD is exponential for any order of reading variables. We construct a quantum algorithm for computing this function with zero error. We present a result on the relationship between complexity classes for quantum and classical nondeterministic OBDDs of large width.

Keywords: *branching program; ordered binary decision diagram; nondeterminism; quantum algorithm; complexity; complexity class; computational model; hierarchy of complexity classes; lower bound; upper bound*

For citation: Gainutdinova, Aida (2024), "Large Width Nondeterministic Quantum OBDDs", *Bulletin of Perm University. Mathematics. Mechanics. Computer Science*, no. 4(67), pp. 117-131. DOI: 10.17072/1993-0550-2024-117-131. https://elibrary.ru/tuqhho.

Acknowledgments: The research has been supported by the Kazan Federal University Strategic Academic Leadership Program ("PRIORITY-2030").

The article was submitted 11.10.2024; approved after reviewing 28.10.2024; accepted for publication 01.12.2024

Введение

Квантовая информатика зародилась в конце прошлого столетия. В 1980-х годах была высказана идея о возможном построении вычислительных моделей с использованием законов квантовой механики [1, 2]. С тех пор эта область стремительно развивается: были определены и активно исследуются квантовые аналоги классических вычислительных моделей: автоматов, схем, ветвящихся программ и т. д., найдены задачи, для которых квантовые алгоритмы оказались значительно эффективнее, чем известные классические. Недетерминированные модели не являются реалистичными, однако позволяют лучше понять возможности моделей реалистичных (детерминированных, вероятностных и т.д.). Недетерминизм играет важную роль в теории компьютерных наук. В частности, вопрос, являются ли недетерминированные модели более эффективными, чем детерминированные, сформулирован как проблема о соотношении классов P и NP, являющихся одной из важнейших на сегодняшний день. Сравнительный анализ квантовых и классических недетерминированных вычислительных моделей, и построение эффективных квантовых алгоритмов для моделей с различными ограничениями является актуальным направлением исследований.

Ветвящиеся программы (BP – Branching Programs) – известная модель для вычисления булевых функций, основанная на применении операций "if", "then", "else" и "goto" и имеющая приложения в различных областях: в области верификации моделей и программ, в базах данных и т.д. [3, с. 5–11]. Известно, что логарифм сложности BP соответствует объему памяти машины Тьюринга, а максимальная длина вычислительного пути – времени вычисления [4, 5]. Модель квантовых BP, как последовательность унитарных эволюций квантовой системы с заключительным измерением для извлечения результата вычислений, была определена в работе [6].

В работах [7, 8] определены несколько иные модели BP, эквивалентные модели работы [6]. Упорядоченные ветвящиеся диаграммы решений (OBDD – Ordered Binary Decision Diagrams) – это модель BP, в которой на каждом вычислительном пути переменные считываются в одном и том же порядке не более одного раза. Естественной мерой сложности для этой модели является ширина. Различные варианты OBDD: детерминированные, недетерминированные, вероятностные, квантовые исследовались разными авторами [9, 7, 10, 8, 11, 12]. В частности, было показано, что вероятностные OBDD могут быть экспоненциально эффективнее детерминированных и недетерминированных [9], а квантовые OBDD – эффективнее детерминированных и стабильных вероятностных [10].

В работе [11] было продемонстрировано превосходство квантового недетерминизма над классическим: была представлена функция, вычислимая недетерминированными квантовыми OBDD (NQOBDD) константной ширины, в то время как ширина классических недетерминированных OBDD (NOBDD) для этой функции неконстантна.

В работе [12] исследовались NQOBDD линейной и сублинейной ширины, для которых, в частности, было показано, что квантовые и классические недетерминированные модели не сравнимы между собой.

Одной из особенностей модели OBDD является возможность выбора порядка считывания переменных. Во всех упомянутых выше работах результаты основывались на симметрических булевых функциях, для которых порядок считывания не важен, поскольку значение функции на конкретном наборе зависит от числа единиц в наборе, а не от их расположения. При этом ширина OBDD для таких функций не более чем линейна. Для получения высоких нижних оценок необходимо исследование несимметрических булевых функций. Для таких функций сложность OBDD может существенным образом зависеть от того, в каком порядке программа считывает переменные. Известны примеры функций, для которых разница в сложности в зависимости от используемого порядка считывания экспоненциальна. При этом задача нахождения наилучшего порядка считывания для заданной функции является NP-полной [13, с. 135].

Целью данной работы является сравнительное исследование NOBDD и NQOBDD линейной и сверхлинейной ширины. Мы исследуем известную булеву функцию "Равенство" и сложность ее вычисления в квантовых недетерминированных OBDD при использовании различных порядков считывания переменных в сравнении с классической недетерминированной сложностью. С использованием метода доказательства нижней оценки сложности NQOBDD, впервые представленного в материалах конференции [12], мы доказываем экспоненциальную нижнюю оценку сложности вычисления функции "Равенство" при "наихудшем" порядке считывания. Мы доказываем линейную нижнюю оценку сложности функции "Равенство" при вычислении в NQOBDD с использованием "наилучшего" порядка, при котором классическая сложность равна 3. Мы показываем, что полученные нижние оценки точны. Мы конструируем функцию, для которой доказываем экспоненциальную нижнюю оценку сложности вычисления в квантовых NOBDD для любого порядка считывания и предлагаем квантовый алгоритм ее вычисления.

На основе полученных результатов мы представляем результат об иерархии классов сложности, основанных на модели недетерминированных OBDD сверхлинейной ширины.

1. Предварительные сведения

1.1. Определения моделей

В работе мы используем верхний индекс для нумерации векторов и наборов, нижний индекс – для нумерации элементов векторов и наборов.

Детерминированная ветвящаяся программа (BP – Branching Program) над множеством переменных $X = \{x_1, \dots, x_n\}$ – это ориентированный ациклический граф с финальными вершинами, помеченными 0 и 1 (будем называть их отвергающими и принимающими вершинами, соответственно). Каждая внутренняя вершина помечена булевской переменной $x \in X$, и имеет два исходящих ребра, помеченных 0 и 1, соответственно. BP обрабатывает входной набор $\boldsymbol{\sigma} \in \{0,1\}^n$, стартуя из выделенной начальной вершины. Для каждой внутренней вершины, помеченной переменной x_j, BP осуществляет 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. BP представляет булеву функцию $f: \{0,1\}^n \to \{0,1\}$, если для любого $\boldsymbol{\sigma} \in \{0,1\}^n$ она завершает работу в финальной вершине, помеченной $f(\boldsymbol{\sigma})$.

Сложность $Size(P)$ BP P – это количество ее внутренних вершин. *Длина* $Length(P)$ BP P – это максимальная длина пути из начальной вершины в конечную. Длина BP оценивает время, требуемое для вычисления функции f в худшем случае, сложность BP оценивает память, затрачиваемую в процессе вычисления.

BP называется *один раз читающей*, если на любом вычислительном пути каждая переменная считывается не более одного раза. BP называется *уровневой*, если ее вершины могут быть разбиты на уровни $0,1, \dots$ таким образом, что для каждого i ребра, исходящие из вершин уровня i, ведут только в вершины уровня $i+1$.

Ширина $Width(P)$ уровневой BP P – это максимальное число вершин на уровне.

Очевидно, что $Size(P) \leq Length(P) \cdot Width(P)$.

Уровневая BP P называется *забывающей*, если во всех вершинах одного уровня P тестируется одна и та же переменная.

OBDD (Ordered Binary Decision Diagram) – это уровневая забывающая один раз читающая ветвящаяся программа.

Поскольку длина OBDD не превосходит n, естественной мерой сложности является ее ширина. Модель OBDD константной ширины с естественным порядком считывания и одинаковыми преобразованиями на всех уровнях эквивалентна модели конечных автоматов [14].

Недетерминированная OBDD (NOBDD) допускает переходы из вершины текущего уровня в более чем одну вершину последующего уровня при считывании одной и той же переменной. В этом случае для входного набора $\boldsymbol{\sigma}$ могут существовать несколько вычислительных путей. NOBDD P принимает входной набор $\boldsymbol{\sigma}$, если существует вычислительный путь, соответствующий данному набору, завершающийся в принимающей вершине. В противном случае P отвергает набор $\boldsymbol{\sigma}$.

Для определения квантовой OBDD нам понадобятся некоторые сведения из теории квантовых вычислений. Для большей информации см., например [15]. Квантовая система (QS) с d базисными состояниями (использующая $\log d$ квантовых битов) может быть описана при помощи d-мерного комплекснозначного Гильбертова пространства $\mathcal{H}^d$.

Чистое состояние QS – это элемент пространства $\mathcal{H}^d$, вектор-столбец $|\boldsymbol{\psi}\rangle = (z_0, \dots, z_{d-1})$ с единичной нормой (унитарный вектор): $\||\boldsymbol{\psi}\rangle\| = \sqrt{\langle\boldsymbol{\psi}|\boldsymbol{\psi}\rangle} = 1$ ($\langle\boldsymbol{\psi}|$ – сопряженный к $|\boldsymbol{\psi}\rangle$ вектор-строка). Комплексное число z_i ($i = 0, \dots, d-1$) называется амплитудой базисного состояния $|\boldsymbol{i}\rangle$, где $|\boldsymbol{i}\rangle$ обозначает унитарный вектор со значением 1 в позиции i (нумерация элементов вектора осуществляется с 0).

Таким образом, чистое состояние – это суперпозиция базисных состояний QS с комплекснозначными амплитудами. Унитарная эволюция – это изменение состояния квантовой системы за определенный период времени, описывается d-мерной унитарной матрицей U. Матрица U называется унитарной, если выполняется $UU^\dagger = I$, где $U^\dagger$ – транспонированная комплексносопряженная к U матрица, I – единичная матрица.

Квантовое измерение – это процедура извлечения классической информации из квантового состояния. Ортогональное измерение QS описывается системой операторов $O = \{P_1, \dots, P_t\}$, действующих в $\mathcal{H}^d$ таких, что $P_i = P_i^\dagger$, $P_i^2 = P_i$, $P_iP_j = \mathbf{0}$, $\sum_{i=1}^t P_i = I$ ($i, j = 1, \dots, t$, $i \neq j$, $t \leq d$). Если $|\psi\rangle$ – состояние QS до измерения, то результатом измерения является одно из значений из множества $\{1, \dots, t\}$. При этом:

1. $p_k = \|P_k\,|\boldsymbol{\psi}\rangle\|^2$– вероятность того, что исход измерения – значение k;
2. $|\psi'\rangle = P_k|\boldsymbol{\psi}\rangle / \|P_k\,|\boldsymbol{\psi}\rangle\|$– состояние квантовой системы после измерения, результатом которого является значение k.

Квантовая OBDD Q ширины d и длины l ((d, l)-QOBDD) определяется как

$$Q = (\,|\boldsymbol{\psi^0}\rangle, R, O_{final}\,)\,,$$

где $|\boldsymbol{\psi}^0\rangle$ – начальная суперпозиция; R – последовательность (длины l) инструкций, содержащих d-мерные унитарные преобразования квантовой системы QS с d базисными состояниями, определенная следующим образом:

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

где $U_i(0)$ и $U_i(1)$ – унитарные $(d \times d)$-матрицы, описывающие преобразования, применяемые на i-ом шаге, $O_{final} = \{P_{accept}, P_{reject}\}$ – система операторов, задающих финальное измерение с исходами $accept$ и $reject$, соответственно.

QOBDD Q обрабатывает вход $\boldsymbol{\sigma} = \sigma_1 \dots \sigma_n \in \{0,1\}^n$, начиная работу в суперпозиции $|\boldsymbol{\psi}^0\rangle$. Если после текущего шага Q находится в состоянии $|\boldsymbol{\psi}\rangle$, то на следующем i-ом шаге ($i = 1, \dots, n$) Q считывает очередной символ σ_{j_i} входного слова $\boldsymbol{\sigma} \in \Sigma^n$, определяемый последовательностью R инструкций программы, и преобразует текущую суперпозицию $|\boldsymbol{\psi}\rangle$ в суперпозицию $|\boldsymbol{\psi}'\rangle = U_i(\sigma_{j_i})|\boldsymbol{\psi}\rangle$. После считывания входного набора производится измерение финальной суперпозиции $|\boldsymbol{\psi}_{final}\rangle = U_n(\sigma_{i_n}) \cdots U_1(\sigma_{i_1})|\boldsymbol{\psi}^0\rangle$. Если исход измерения $accept$, вход принимается, в противном случае – отвергается. Вероятность принятия слова $\boldsymbol{\sigma}$ определяется как

$$Pr_{accept}^{Q}(\boldsymbol{\sigma}) = \|P_{accept}|\boldsymbol{\psi}_{final}\rangle\|^2\,.$$

Q недетерминированно вычисляет функцию f, если Q принимает вход $\boldsymbol{\sigma}$ с вероятностью > 0 тогда и только тогда, когда $f(\boldsymbol{\sigma}) = 1$. Такую OBDD будем называть недетерминированной квантовой OBDD (NQOBDD). Q вычисляет функцию f без ошибки, если Q принимает с вероятностью 1 входы $\boldsymbol{\sigma}$, для которых $f(\boldsymbol{\sigma}) = 1$ и принимает с вероятностью 0 входы $\boldsymbol{\sigma}$, для которых $f(\boldsymbol{\sigma}) = 0$.

1.2. Сведения из линейной алгебры

Приведем некоторые сведения из линейной алгебры, которые понадобятся нам в дальнейшем (см. напр. [16]).

Пусть V – векторное пространство над полем комплексных чисел с нормой $\|\cdot\|_2$. Система векторов $\boldsymbol{\psi}^1, \boldsymbol{\psi}^2, \ldots, \boldsymbol{\psi}^d \in V$ является линейно зависимой, если существуют числа $\alpha_1, \alpha_2, \ldots, \alpha_d \in \mathbb{C}$, одновременно не равные нулю такие, что $\alpha_1 \boldsymbol{\psi}^1 + \cdots + \alpha_d \boldsymbol{\psi}^d = \mathbf{0}$ ($\mathbf{0}$ обозначает нулевой элемент пространства V). Если это равенство выполняется только при $\alpha_1 = \alpha_2 = \cdots = \alpha_d = 0$, то система векторов является линейно независимой.

Лемма 1. Пусть $\boldsymbol{\psi}^1, \boldsymbol{\psi}^2, \ldots, \boldsymbol{\psi}^d \in V$ – линейно независимая система векторов, U – унитарное преобразование в пространстве V. Тогда вектора $U\boldsymbol{\psi}^1, U\boldsymbol{\psi}^2, \ldots, U\boldsymbol{\psi}^d$ линейно независимы.

Доказательство. Унитарное преобразование является взаимно-однозначным преобразованием, которое можно рассматривать как переход к другому базису. Взаимно-однозначное линейное преобразование сохраняет свойство линейной независимости преобразуемых векторов.

Лемма 2. Пусть вектора $\boldsymbol{\psi}^1, \ldots, \boldsymbol{\psi}^m, \boldsymbol{\psi} \in V$, $\boldsymbol{\psi}^1, \ldots, \boldsymbol{\psi}^m$, – линейно независимы, U – линейное преобразование пространства V такое, что $\|U\boldsymbol{\psi}^i\| = 0, i = 1, \ldots, m$, $\|U\boldsymbol{\psi}\| \neq 0$. Тогда система векторов $\{\boldsymbol{\psi}^1, \ldots, \boldsymbol{\psi}^m, \boldsymbol{\psi}\}$ линейно независима.

Доказательство. Докажем от противного. Предположим, вектор $\boldsymbol{\psi}$ линейно зависим с системой $\boldsymbol{\psi}^1, \ldots, \boldsymbol{\psi}^m$. Тогда существуют $\alpha_1, \alpha_2, \ldots, \alpha_m \in \mathbb{C}$, одновременно не равные нулю такие, что $\boldsymbol{\psi} = \alpha_1 \boldsymbol{\psi}^1 + \cdots + \alpha_m \boldsymbol{\psi}^m$.

В силу линейности имеем $U\boldsymbol{\psi} = U(\alpha_1 \boldsymbol{\psi}^1 + \cdots + \alpha_m \boldsymbol{\psi}^m) = \alpha_1 U\boldsymbol{\psi}^1 + \cdots + \alpha_m U\boldsymbol{\psi}^m$.

По свойству нормы имеем

$$\|U\boldsymbol{\psi}\| \leq |\alpha_1| \cdot \|U\boldsymbol{\psi}^1\| + \cdots + |\alpha_m| \cdot \|U\boldsymbol{\psi}^m\|.$$

По условию леммы $\|U\boldsymbol{\psi}^1\| = \cdots = \|U\boldsymbol{\psi}^m\| = 0$. Значит $\|U\boldsymbol{\psi}\| = 0$. Получили противоречие.

1.3. Нижняя оценка ширины NQOBDD

Пусть $f: \{0,1\}^n \to \{0,1\}$ – произвольная булева функция, $\pi = (i_1, \ldots, i_n)$ – произвольная перестановка индексов $\{1, \ldots, n\}$. Для $X = \{x_1, \ldots, x_n\}$, целого k ($0 < k < n$) обозначим $X_k^\pi = \{x_{i_1}, \ldots, x_{i_k}\}$. Набор значений $\boldsymbol{\sigma} \in \{0,1\}^k$, сопоставленный переменным из множества X_k^π определяет подфункцию $f_{\pi,k}^{\boldsymbol{\sigma}}: \{0,1\}^{n-k} \to \{0,1\}$.

Множество пар $S_k^\pi = \{(\boldsymbol{\sigma}, \boldsymbol{\gamma}): \boldsymbol{\sigma} \in \{0,1\}^k, \boldsymbol{\gamma} \in \{0,1\}^{n-k}\}$ назовем строгим 1-полным множеством (*strong 1-fooling set*) для функции f, если выполняются следующие условия:

1. $f_{\pi,k}^{\boldsymbol{\sigma}}(\boldsymbol{\gamma}) = 1$ для любой пары $(\boldsymbol{\sigma}, \boldsymbol{\gamma}) \in S_k^\pi$,
2. для любых двух пар $(\boldsymbol{\sigma}, \boldsymbol{\gamma}), (\boldsymbol{\sigma}', \boldsymbol{\gamma}') \in S_k^\pi$ выполняется $f_{\pi,k}^{\boldsymbol{\sigma}}(\boldsymbol{\gamma}') = 0$ и $f_{\pi,k}^{\boldsymbol{\sigma}'}(\boldsymbol{\gamma}) = 0$.

Для двух наборов $\boldsymbol{\sigma}, \boldsymbol{\sigma}' \in \{0,1\}^k$ будем говорить, что набор $\boldsymbol{\gamma} \in \{0,1\}^{n-k}$ отличает набор $\boldsymbol{\sigma}$ от набора $\boldsymbol{\sigma}'$, если выполняется $f_{\pi,k}^{\boldsymbol{\sigma}}(\boldsymbol{\gamma}) > 0$ и $f_{\pi,k}^{\boldsymbol{\sigma}'}(\boldsymbol{\gamma}) = 0$. Отметим, что данное свойство не является симметричным.

Теорема 1. [12] Для любой QOBDD Q, недетерминированно вычисляющей функцию $f: \{0,1\}^n \to \{0,1\}$ и использующей порядок $\pi = (i_1, \ldots, i_n)$ считывания переменных, выполняется

$$Width(Q) \geq max_k |S_k^\pi|.$$

2. Основные результаты

2.1. Квантовая сложность вычисления функции "Равенство"

Функция "Равенство" EQ_{2n}: $\{0,1\}^{2n} \to \{0,1\}$ определяется следующим образом:

$$EQ_{2n}(\boldsymbol{\sigma}) = \begin{cases} 1, \text{если } \sigma_1 \dots \sigma_n = \sigma_{n+1} \dots \sigma_{2n}, \\ 0, \text{иначе}. \end{cases}$$

Известно, что сложность вычисления данной функции критическим образом зависит от порядка считывания переменных. Так, ширина классической OBDD (детерминированной и недетерминированной), вычисляющей EQ_{2n}, равна 3, если переменные считываются в порядке $x_1,\ x_{n+1}, x_2, x_{n+2}, \dots, x_n, x_{2n}$ (назовем этот порядок "наилучшим") и равна $\Omega(2^n)$, если сначала считываются переменные первой половины набора и только потом – переменные второй половины набора (назовем такой порядок "наихудшим").

Покажем, что сложность недетерминированной QOBDD для этой функции при использовании "наилучшего" порядка считывания линейна.

Теорема 2. Любая QOBDD, недетерминированно вычисляющая функцию EQ_{2n} и использующая порядок считывания переменных $\pi = (1, n+1, 2, n+2, \dots, n, 2n)$, имеет ширину не менее $n+1$.

Доказательство. Пусть Q – NQOBDD, вычисляющая EQ_{2n} и считывающая переменные в порядке $\pi = (1, n+1, 2, n+2, \dots, n, 2n)$.

Вычисление на входе $\boldsymbol{\sigma} = \sigma_1 \dots \sigma_{2n}$ начинается из начальной суперпозиции $|\boldsymbol{\psi}^0\rangle$. На шаге l программа считывает переменную $x_{i_l} = \sigma_{i_l}$ и преобразует суперпозицию $|\boldsymbol{\psi}(\sigma_{i_1} \dots \sigma_{i_{l-1}})\rangle$ в суперпозицию $|\boldsymbol{\psi}(\sigma_{i_1} \dots \sigma_{i_l})\rangle$. После считывания входного слова Q производит финальное измерение финальной суперпозиции $|\boldsymbol{\psi}(\sigma_{i_1} \dots \sigma_{i_{2n}})\rangle$ и принимает входной набор с вероятностью $Pr^Q_{accept}(\boldsymbol{\sigma}) = \|P_{accept}\ |\boldsymbol{\psi}(\sigma_{i_1} \dots \sigma_{i_{2n}})\|^2$.

На каждом уровне l программы Q будем рассматривать множество Ψ_l квантовых состояний, достижимых программой на этом уровне, а также подмножество $\Phi_l \subseteq \Psi_l$ состояний, которые являются линейно независимыми векторами.

Лемма 4. Пусть $|\boldsymbol{\psi}^1\rangle, \dots, |\boldsymbol{\psi}^m\rangle, |\boldsymbol{\psi}\rangle \in \Psi_l$ $(m \geq 1)$ и $|\boldsymbol{\psi}^1\rangle, \dots, |\boldsymbol{\psi}^m\rangle$ – линейно независимы, где $|\boldsymbol{\psi}^i\rangle = |\boldsymbol{\psi}(\boldsymbol{\sigma}^i)\rangle$ для $i = 1, \dots, m$ и $|\boldsymbol{\psi}\rangle = |\psi(\boldsymbol{\sigma})\rangle$. Если существует строка $\boldsymbol{\gamma} \in \{0,1\}^{n-l}$, отличающая строку $\boldsymbol{\sigma}$ от каждой из строк $\boldsymbol{\sigma}^1, \dots, \boldsymbol{\sigma}^m$, то множество $\{|\boldsymbol{\psi}^1\rangle, \dots, |\boldsymbol{\psi}^m\rangle, |\boldsymbol{\psi}\rangle\}$ линейно независимо.

Доказательство. Пусть $U = U_n(\gamma_{n-l}) \cdots U_{l+1}(\gamma_1)$. Тогда выполняется $\|P_{accept}\ U\ |\boldsymbol{\psi}^i\ \rangle\| = 0$ для всех $i = 1, \dots, m$, и $\|P_{accept} U|\ \boldsymbol{\psi}\rangle\| > 0$. Согласно Лемме 2, множество $\{\ |\boldsymbol{\psi}^1\rangle, \dots, |\boldsymbol{\psi}^m\rangle, |\boldsymbol{\psi}\rangle\}$ является линейно независимым.

Индукцией по i $(i = 1, \dots, n)$ покажем, что после считывания i-й пары: значений переменных x_i и x_{n+i} (на уровне $l = 2i$) выполняется $|\Phi_{2i}| \geq\ i+1$.

База индукции. $\Phi_0 = \{|\boldsymbol{\psi}^0\rangle\}$. На первом шаге после считывания $x_1 = \sigma_1$ $(\sigma_1 \in \{0,1\})$, согласно Лемме 4, множество $\Phi_1 = \{|\boldsymbol{\psi}(0)\rangle, |\boldsymbol{\psi}(1)\rangle\}$ является линейно независимым множеством, так как строка 1^{2n-1} отличает строку 1 от строки 0. После считывания $x_{n+1} = \sigma_{n+1}(\sigma_{n+1} \in\ \{0,1\})$, множество состояний $\Phi_2 = \{|00\rangle, |10\rangle\}$ является линейно независимым по Лемме 1. Следовательно, $|\Phi_2| \geq\ 2$.

Индукционный шаг (для $i = 2, \dots, n$). По предположению индукции $\Psi_{2(i-1)}$ содержит не менее i векторов. Обозначим их $\left|\boldsymbol{\psi}^{j_0}\right\rangle, \dots, \left|\boldsymbol{\psi}^{j_{i-1}}\right\rangle$, а соответствующие им частичные входы $\boldsymbol{\sigma}^{j_0}, \dots, \boldsymbol{\sigma}^{j_{i-1}}$. После считывания $x_i = \sigma_i$, по Лемме 1 множество $\Phi^0_{2(i-1)} = \left\{U(0)\left|\boldsymbol{\psi}^{j_0}\right\rangle, \dots, U(0)\left|\boldsymbol{\psi}^{j_{i-1}}\right\rangle\right\}$ является линейно независимым, вектор $\left|\boldsymbol{\psi}\left(1^{2i-1}\right)\right\rangle =$

$U_{2i-1}(1)\cdots U_1(1)|\boldsymbol{\psi}^0\rangle$ не входит в $\Phi^0_{2(i-1)}$, при этом строка $1^{2n-2i+1}$ отличает строку 1^{2i-1} от любой из строк $\boldsymbol{\sigma}^{j_0}0,\dots,\boldsymbol{\sigma}^{j_{i-1}}0$. Значит, множество $\Phi_{2i-1}=\Phi^0_{2(i-1)}\cup\{|\boldsymbol{\psi}(1^{2i-1})\rangle\}$ является линейно независимым. После считывания $x_{n+i}=\sigma_{n+i}$, по Лемме 1 множество $\Psi_{2i}=\Phi^0_{2i-1}=\{U(0)|\boldsymbol{\psi}\rangle : |\boldsymbol{\psi}\rangle\in\Phi_{2i-1}\}$ является линейно независимым. Следовательно, $|\Phi_{2i}|\geq i+1$.

После считывания n-ой пары $x_n,\ x_{2n}$ на уровне $l=2n$ получаем $|\Phi_{2n}|\geq n+1$. Таким образом, размерность пространства состояний программы Q не менее $n+1$, что завершает доказательство теоремы.

Покажем, что доказанная нижняя оценка точна.

Теорема 3. Существует QOBDD Q ширины $n+1$, вычисляющая функцию EQ_{2n} без ошибки и использующая порядок считывания переменных $\pi=(1,n+1,2,n+2,\dots,n,2n)$.

Доказательство. Программа Q использует регистр из $n+1$ состояния $s_0,s_1,\dots,s_n$, где s_0 – начальное и принимающее состояние. При считывании пары значений переменных $x_i,\ x_{n+i}$ $(i=1,\dots,n)$ программа применяет преобразования:

- $|s_0\rangle\to|s_i\rangle,\ |s_i\rangle\to|s_0\rangle$, если считанное значение 1;
- $|s_0\rangle\to|s_0\rangle,\ |s_i\rangle\to|s_i\rangle$, если считанное значение 0;
- $|s_j\rangle\to|s_j\rangle$, для всех $j=1,\dots,n, j\neq i$.

Докажем корректность работы программы.

Пусть вход $\boldsymbol{\sigma}$ такой, что $EQ_{2n}(\boldsymbol{\sigma})=1$. Это означает, что $\sigma_i=\sigma_{n+i}\ \forall\, i=1,\dots,n$. В этом случае программа будет завершать обработку каждой пары в состоянии $|s_0\rangle$ и примет такой вход с вероятностью 1.

Пусть вход $\boldsymbol{\sigma}$ такой, что $Q_{2n}(\boldsymbol{\sigma})=0$. Это означает, что $\exists\, i\in\{1,\dots,n\}$, для которого $\sigma_i\neq\sigma_{n+i}$. После обработки этой пары программа останется в состоянии s_i и, таким образом, амплитуда состояния s_0 до конца обработки будет равна 0. Вероятность принятия такого набора равна 0.

Рассмотрим сложность NQOBDD для "наихудшего" порядка считывания.

Теорема 4. Любая QOBDD, недетерминированно вычисляющая функцию EQ_{2n} и считывающая переменные одной из половин набора после считывания всех переменных второй половины набора, имеет ширину не менее 2^n.

Доказательство. Пусть Q – QOBDD, недетерминированно вычисляющая EQ_{2n}, использующая порядок считывания $\pi=(i_1,\dots,i_{2n}\}$, при котором любая переменная одной из половин набора считывается после того, как считаны все переменные другой половины набора. Множество $S^\pi_n=\{(\boldsymbol{\sigma},\boldsymbol{\sigma}) : \boldsymbol{\sigma}\in\{0,1\}^n\}$ является строгим 1-полным множеством для функции EQ_{2n}. Согласно Теореме 1, $Width(Q)\geq|S^\pi_n|$. Заметим, что $|S^\pi_n|=2^n$, что завершает доказательство теоремы.

Покажем, что оценка теоремы 4 точна.

Теорема 5. Пусть $\pi=(i_1,\dots,i_{2n})$ – произвольная перестановка индексов $\{1,\dots,2n\}$ такая, что выполняется одно из двух условий: либо $\pi(i)\leq n\ \forall\, i\leq n$ и $\pi(i)>n\ \forall\, i>n$, либо $\pi(i)>n\ \forall\, i\leq n$ и $\pi(i)\leq n\ \forall\, i>n$. Существует QOBDD ширины 2^n, недетерминированно вычисляющая функцию EQ_{2n} и считывающая переменные в порядке π.

Доказательство. Пусть Q – NQOBDD, вычисляющая EQ_{2n}, использующая порядок $\pi=(i_1,\dots,i_{2n})$ считывания переменных, удовлетворяющий условию теоремы. Для определенности считаем, что Q сначала считывает переменные первой половины набора, потом – переменные второй половины набора (противоположный случай доказывается аналогично). Q имеет 2^n состояний $s_0,\dots,s_{2^n-1}$, где s_0 – начальное и принимающее состояние. При считывании переменной $x_i=\sigma_i$ $(i=1,\dots\ 2n,\sigma_i\in\{0,1\})$ Q применяет преобразования:

- $|s_j\rangle \to |s_{(j+2^{i-1}\sigma_i) mod\ 2^n}\rangle$, $j = 0, \dots, 2^n - 1$, если $i \in \{1, \dots, n\}$,
- $|s_j\rangle \to |s_{(j-2^{i-n-1}\sigma_i+2^n) mod\ 2^n}\rangle$, $j = 0, \dots , 2^n - 1$, если $i \in \{n + 1, \dots, 2n\}$.

После считывания первой половины входа состояние программы будет равно $|s_{m(\sigma_1 \dots \sigma_n)}\rangle$, где $m(\sigma_1 \dots \sigma_n)$ – целое число, двоичное представление которого равно $\sigma_1 \dots \sigma_n$. После считывания второй половины набора состояние программы равно $|s_{(m(\sigma_1 \dots \sigma_n)+ 2^n - m(\sigma_{n+1} \dots \sigma_{2n})) mod 2^n}\rangle$.

Если $\sigma_1 \dots \sigma_n = \sigma_{n+1} \dots \sigma_{2n}$, финальное состояние программы будет $|s_0\rangle$ и программа примет такой набор с вероятностью 1.

В противном случае программа завершит обработку входа в состоянии, отличном от $|s_0\rangle$ и примет такой набор с вероятностью 0.

2.2. Функция "XOR-перемешанное равенство"

Как было показано в предыдущем разделе, сложность вычисления функции EQ_n зависит от того, в каком порядке считываются переменные. Для устранения зависимости сложности вычисления от используемого порядка считывания, используют различные приемы для определения функций, при которых порядок следования битов входа определятся самим входным набором (или его частью). Для таких функций не удается подобрать оптимальный порядок считывания битов входа. В частности, в работе [17] рассматривалась функция "Перемешанное равенство", определенная на основе функции "Равенство" и сложность ее вычисления в классических детерминированных и недетерминированных OBDD.

В данной работе мы определим и исследуем функцию $EQXS_{2n}$ (Equality-Xor-Shuffled), которая задается на основе функции EQ_{2n} с использованием приема, аналогичного описанному в работе [18]. Формально, функция $EQXS_{2n}$ определяется следующим образом.

Пусть $x_1, x_2, x_3, \dots, x_n, y_1, y_2, y_3, \dots, y_n$ – последовательность переменных, от которых зависит функция (n кратно 2). Назовем переменные $x_1, \dots, x_n$ – "переменными принадлежности", переменные $y_1, \dots, y_n$ – "переменными значения". Переменную значения y_i назовем соответствующей переменной принадлежности x_i.

По входной последовательности $\boldsymbol{\sigma\gamma} \in \{0,1\}^n \times \{0,1\}^n$ формируются новые битовые последовательности $\boldsymbol{\tau}, \boldsymbol{\alpha}, \boldsymbol{\beta}$:

- последовательность $\boldsymbol{\tau}$ имеет длину n и формируется по значениям $\sigma_1, \dots, \sigma_n$ переменных принадлежности $x_1, \dots, x_n$ следующим образом: $\tau_1 = \sigma_1, \tau_i = \tau_{i-1} \oplus \sigma_i$ $(i = 2, \dots, n)$;
- последовательности $\boldsymbol{\alpha}, \boldsymbol{\beta}$ формируются по переменным значения, начиная с пустых последовательностей: для $i = 1, \dots, n$ бит значения γ_i дописывается к последовательности $\boldsymbol{\alpha}$, если $\tau_i = 0$, в противном случае γ_i дописывается к последовательности $\boldsymbol{\beta}$;

Например, для набора $\boldsymbol{\sigma} = 1011001101$ получим последовательности $\boldsymbol{\tau} = 10011$, $\boldsymbol{\alpha} = 10, \boldsymbol{\beta} = 011$.

Функция $EQXS_{2n} = 1$ тогда и только тогда, когда $\boldsymbol{\alpha} = \boldsymbol{\beta}$.

Теорема 6. Существует квантовая OBDD, вычисляющая функцию $EQXS_{2n}$ с нулевой ошибкой, и имеющая ширину $2^{n/2}(2n + 4)$.

Доказательство. Программа Q считывает переменные в порядке $x_1, y_1, x_2, y_2, \dots, x_n, y_n$. Состояние программы хранится в регистрах: $|\boldsymbol{num}_\alpha\rangle, |\boldsymbol{num}_\beta\rangle, |\boldsymbol{\phi}\rangle, |\boldsymbol{b}\rangle$:

- однокубитный "регистр активности" $|\boldsymbol{b}\rangle$ хранит значение бита τ_i, соответствующего последнему считанному биту принадлежности;
- регистр $|\boldsymbol{num}\rangle$ является ортогональной суммой двух регистров $|\boldsymbol{num}_\alpha\rangle$ и $|\boldsymbol{num}_\beta\rangle$, которые устроены одинаково и хранят номер последнего считанного бита последовательности $\boldsymbol{\alpha}$ и $\boldsymbol{\beta}$, соответственно;
- регистр $|\boldsymbol{\phi}\rangle$ хранит информацию о значении $(m(\boldsymbol{\alpha}) - m(\boldsymbol{\beta}))\ mod\ 2^{n/2}$, где $m(\boldsymbol{\alpha})$ и $m(\boldsymbol{\beta})$ – целые числа, двоичными представлениями которых являются последовательности $\boldsymbol{\alpha}$ и $\boldsymbol{\beta}$, соответственно.

Опишем подробнее каждый из регистров.

Регистр $|\boldsymbol{b}\rangle$ имеет два состояния $|0\rangle$ и $|1\rangle$, изменяет свое состояние при считывании бита принадлежности $\sigma \in \{0,1\}$ и не меняется при считывании бита значения. Преобразования:

$$U(\sigma) = \begin{cases} NOT, \text{если } \sigma = 1, \\ I \quad\ \ , \text{если } \sigma = 0. \end{cases}$$

где NOT – однокубитное преобразование инвертирования квантового бита, I – тождественное преобразование.

Состояние данного регистра хранит значение текущего бита последовательности $\boldsymbol{\tau}$ и управляет преобразованиями на следующем шаге. Зона активности регистра $|\boldsymbol{num}\rangle$ ($|\boldsymbol{num}_\alpha\rangle$ или $|\boldsymbol{num}_\beta\rangle$) меняется, если считанный бит принадлежности равен 1, и сохраняется, если считанный бит принадлежности равен 0. Таким образом, на следующем шаге при считывании бита значения преобразования будут производиться в регистре $|\boldsymbol{num}_\alpha\rangle$, если очередной бит значения принадлежит последовательности $\boldsymbol{\alpha}$ и в регистре $|\boldsymbol{num}_\beta\rangle$, если бит значения принадлежит $\boldsymbol{\beta}$.

Каждый из регистров $|\boldsymbol{num}_\alpha\rangle$ и $|\boldsymbol{num}_\beta\rangle$ имеет $n/2\ +\ 1$ состояние

$$s_0, s_1, \dots, s_{n/2}$$

(состоит из $log\ (n/2 + 1)$ кубитов). Начальное состояние $|s_0\rangle$. При считывании очередного бита принадлежности происходит преобразование $|s_i\rangle \to\ |s_{(i+1) mod\ \left(\frac{n}{2}+1\right)}\rangle$ в регистре $|\boldsymbol{num}_\alpha\rangle$, если значение регистра активности $|\boldsymbol{b}\rangle = |0\rangle$, и в регистре $|\boldsymbol{num}_\beta\rangle$, если $|\boldsymbol{b}\rangle = |1\rangle$.

$2^{n/2}$ -кубитный регистр $|\boldsymbol{\phi}\rangle$ хранит неотрицательное значение $c = (m(\boldsymbol{\alpha}) - m(\boldsymbol{\beta}))\ mod\ 2^{n/2}$. Базисные состояния регистра соответствуют значениям $0, 1, \dots, 2^{\frac{n}{2}} - 1$. При считывании бита из последовательности $\boldsymbol{\alpha}$ ($\boldsymbol{\beta}$) выполняется преобразование $|c\rangle \to |(c\ +\ \alpha_j 2^{j-1}) mod\ 2^{\frac{n}{2}}\rangle$ (соответственно, $|c\rangle \to\ |(c - \beta_j 2^{j-1}\ +\ 2^{\frac{n}{2}}) mod\ 2^{\frac{n}{2}}\rangle$), если последний считанный бит значения является j-ым битом последовательности $\boldsymbol{\alpha}$ ($\boldsymbol{\beta}$). Управляют изменением регистра $|\boldsymbol{\phi}\rangle$ регистры $|\boldsymbol{num}\rangle$ и $|\boldsymbol{b}\rangle$.

Состояние программы Q описывается в виде

$$|\boldsymbol{\psi}\rangle = |\boldsymbol{b}\rangle \otimes 1/\sqrt{2}\ (|\boldsymbol{num}_\alpha\rangle \oplus\ |\boldsymbol{num}_\beta\rangle) \otimes |\boldsymbol{\phi}\rangle.$$

Начальное состояние

$$|\boldsymbol{\psi}^0\rangle = |\boldsymbol{0}\rangle \otimes 1\sqrt{2}(|\boldsymbol{s}_0\rangle \oplus |\boldsymbol{s}_0\rangle) \otimes |\boldsymbol{0}\rangle.$$

Подпространство принимающих состояний – это подпространство, в котором состояние регистров $|\boldsymbol{num}\rangle \otimes |\boldsymbol{\phi}\rangle\ = 1\sqrt{2}(|\boldsymbol{s}_{\frac{n}{2}}\rangle \oplus\ |\boldsymbol{s}_{\frac{n}{2}}\rangle) \otimes |\boldsymbol{0}\rangle$.

Опишем работу программы. Q попеременно считывает биты принадлежности и соответствующие им биты значения. На очередном шаге при считывании бита принадлежности σ_i $(i = 1, \dots, n)$ программа применяет преобразование $U(\sigma_i)$ к регистру $|\boldsymbol{b}\rangle$. К регистрам $|\boldsymbol{num}\rangle$ и $|\boldsymbol{\phi}\rangle$ применяется тождественное преобразование.

При считывании бита значения γ_i $(i = 1, \dots, n)$ программа применяет преобразование U_ϕ, управляемое регистрами $|\boldsymbol{num}\rangle$ и $|\boldsymbol{b}\rangle$ и воздействующее на регистр $|\boldsymbol{\phi}\rangle$. Затем применяет преобразование U_{num}, управляемое регистром $|\boldsymbol{b}\rangle$ и воздействующее на регистр $|\boldsymbol{num}\rangle$. При этом к регистру $|\boldsymbol{\phi}\rangle$ применяется тождественное преобразование. Матрицы данных преобразований описываются следующим образом:

$$U_\phi(0) = I,\ U_\phi(1) = \begin{pmatrix} U_\phi^\alpha & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & I & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & I & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & U_\phi^\beta \end{pmatrix},$$

где

$$U_\phi^\alpha = \begin{pmatrix} M_0^\alpha & \mathbf{0} & \cdots & \mathbf{0} \\ \mathbf{0} & M_1^\alpha & & \mathbf{0} \\ \vdots & & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \cdots & M_{\frac{n}{2}-1}^\alpha \end{pmatrix},$$

$$U_\phi^\beta = \begin{pmatrix} M_0^\beta & \mathbf{0} & \cdots & \mathbf{0} \\ \mathbf{0} & M_1^\beta & & \mathbf{0} \\ \vdots & & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \cdots & M_{\frac{n}{2}-1}^\beta \end{pmatrix}.$$

Здесь M_j^α $(j = 0, \dots, n/2 - 1)$ – унитарные (перестановочные) матрицы, реализующие преобразования:

$$|c\rangle \to |(c + 2^j) mod\ 2^{\frac{n}{2}}\rangle.$$

Соответственно, M_j^β $(j = 0, \dots, \frac{n}{2} - 1)$ – унитарные матрицы, реализующие преобразования:

$$|c\rangle \to \left|\left(c - 2^j\ + 2^{\frac{n}{2}}\right) mod\ 2^{\frac{n}{2}}\right\rangle,\ c \in \{0, \dots, 2^{\frac{n}{2}} - 1\}.$$

$$U_{num} = \begin{pmatrix} S & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & I & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & I & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & S \end{pmatrix} \otimes I,$$

где $S = \begin{pmatrix} 0 & 0 & & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & & 0 & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}$ – матрица циклического сдвига, применяемая к регистру $|\boldsymbol{num}_\alpha\rangle$ и регистру $|\boldsymbol{num}_\beta\rangle$.

Докажем корректность работы программы. После обработки входа финальные состояния регистров $|\boldsymbol{num}\rangle$ и $|\boldsymbol{\phi}\rangle$ следующие:

$\left|\boldsymbol{num}_{final}\right\rangle = 1/\sqrt{2}(|l_\alpha\ mod(\frac{n}{2} + 1)\rangle \oplus\ |l_\beta\ mod(\frac{n}{2} + 1)\rangle)$, где $l_\alpha = |\boldsymbol{\alpha}|$, $l_\beta = |\boldsymbol{\beta}|$,

$\left|\boldsymbol{\phi}_{final}\right\rangle = |c\rangle$, где $c = (m(\boldsymbol{\alpha}) - m(\boldsymbol{\beta}) + 2^{n/2}) mod\ 2^{n/2}$.

Пусть вход $\boldsymbol{\sigma\gamma}$ такой, что $EQXS_n(\boldsymbol{\sigma\gamma}) = 1$. Это означает одновременное выполнение двух условий:

1) $|\boldsymbol{\alpha}| = |\boldsymbol{\beta}|$,
2) $\forall\, i: \alpha_i\ = \beta_i$.

Выполнение условия 1) означает, что $|\boldsymbol{\alpha}| = |\boldsymbol{\beta}| = n/2$ и после обработки входа состояние регистров $|\boldsymbol{num}_\alpha\rangle$ и $|\boldsymbol{num}_\beta\rangle$ равно $|\boldsymbol{s}_{n/2}\rangle$. Выполнение условия 2) означает, что числа, двоичными представлениями которых являются последовательности $\boldsymbol{\alpha}$ и $\boldsymbol{\beta}$, равны, откуда следует, что финальное состояние регистра $|\boldsymbol{\phi}\rangle$ равно $|\boldsymbol{0}\rangle$. Поэтому после обработки входа финальное состояние программы является одним из двух:

$$|\boldsymbol{\psi}_{final}\rangle = |\boldsymbol{0}\rangle \otimes 1/\sqrt{2}(|\boldsymbol{s}_{\frac{n}{2}}\rangle \oplus |\boldsymbol{s}_{\frac{n}{2}}\rangle) \otimes |\boldsymbol{0}\rangle,$$
$$|\boldsymbol{\psi}_{final}\rangle = |\boldsymbol{1}\rangle \otimes 1/\sqrt{2}(|\boldsymbol{s}_{\frac{n}{2}}\rangle \oplus |\boldsymbol{s}_{\frac{n}{2}}\rangle) \otimes |\boldsymbol{0}\rangle.$$

Вероятность принятия такого набора равна 1.

Пусть вход $\boldsymbol{\sigma\gamma}$ такой, что $EQXS_n(\boldsymbol{\sigma\gamma}) = 0.$ В этом случае выполняется по крайней мере одно из двух условий:

3) $|\boldsymbol{\alpha}| \neq |\boldsymbol{\beta}|$,
4) $\exists\, i: \alpha_i \neq \beta_i$.

Если произошел случай 3), то $|\boldsymbol{\alpha}| \neq n/2$ и $|\boldsymbol{\beta}| \neq n/2$, следовательно, после завершения работы и в регистре $|\boldsymbol{num}_\alpha\rangle$ и в регистре $|\boldsymbol{num}_\beta\rangle$ амплитуда состояния $|\boldsymbol{s}_{\frac{n}{2}}\rangle$ равна 0. Следовательно, вероятность принятия таких наборов равна 0.

Если $|\boldsymbol{\alpha}| = |\boldsymbol{\beta}|$, это означает, что произошел случай 4) и $\boldsymbol{\alpha} \neq \boldsymbol{\beta}$. Покажем, что в этом случае состояние регистра $|\boldsymbol{\phi}\rangle$ не равно $|\boldsymbol{0}\rangle$.

Действительно, предположим, это не так, и $c = m(\boldsymbol{\alpha}) - m(\boldsymbol{\beta}) + 2^{\frac{n}{2}} = 0 \; mod \; 2^{n/2}$. Это означает, что $m(\boldsymbol{\alpha}) = m(\boldsymbol{\beta}) \; mod \; 2^{n/2}$, но так как $m(\boldsymbol{\alpha}) < 2^{n/2}$ и $m(\boldsymbol{\beta}) < 2^{n/2}$, последнее равенство возможно только если $\boldsymbol{\alpha} = \boldsymbol{\beta}$. Следовательно, вероятность принятия в данном случае также равна 0.

Ширина итоговой программы равна $2 \cdot 2 \cdot \left(\frac{n}{2} + 1\right) \cdot 2^{\frac{n}{2}} = 2^{\frac{n}{2}}(2n + 4)$.

Следствие. Функция $EQXS_{2n}$ вычислима NQOBDD ширины $2^{n/2}(2n + 4)$.

Доказательство. Квантовая OBDD, построенная в доказательстве Теоремы 6, вычисляет функцию $EQXS_{2n}$ с нулевой ошибкой, а следовательно недетерминированно.

Теорема 7. Для любого порядка считывания переменных QOBDD, недетерминированно вычисляющая функцию $EQXS_{2n}$, имеет ширину $\Omega(2^{n/2})$.

Доказательство. Пусть Q – произвольная NQOBDD, вычисляющая функцию $EQXS_{2n}$ и использующая порядок π считывания переменных. Зафиксируем значения переменных принадлежности таким образом, чтобы в соответствии с порядком π ровно $n/2$ первых считанных переменных значения принадлежали последовательности $\boldsymbol{\alpha}$, $n/2$ последних считанных переменных значения принадлежали последовательности $\boldsymbol{\beta}$. Работу программы Q на получившихся наборах можно рассматривать как вычисление функции EQ_n, при использовании порядка, когда одна половина набора считывается строго после другой половины. Согласно Теореме 4, ширина программы в этом случае $\Omega(2^{n/2})$.

2.3. Иерархия для NQOBDD

Обозначим через $NOBDD_n^d$, и $NQOBDD_n^d$ классы булевых функций, зависящих от n переменных, вычислимых недетерминированными и квантовыми недетерминированными OBDD шириной не более d, соответственно.

В работе [12] представлена иерархия классов сложности для квантовых и классических недетерминированных OBDD линейной и сублинейной ширины.

В частности, было показано следующее:

Для любых $n > 1$ и $1 < d \leq n$ выполняется:

- $NQOBDD_n^{d-1} \subsetneq NQOBDD_n^d$.
- $NQOBDD_n^{d_1}$ и $NOBDD_n^{d_2}$ несравнимы для любых пар (d_1, d_2), удовлетворяющих условию $1 < d_1, d_2 \leq n/2$.

В данной работе мы представляем иерархию для квантовых недетерминированных OBDD сверхлинейной ширины.

Теорема 8. Для любых $n > 3$, $2 \leq d \leq 2^{n/4}$ выполняется

$$NQOBDD_n^{d-1} \subsetneq NQOBDD_n^{4d\,(log\,d\,+\,1)}.$$

Доказательство. Включение $NQOBDD_n^{d-1} \subseteq NQOBDD_n^{4d(log\,d\,+\,1)}$ очевидно. Покажем, что эти классы не совпадают. На основе функции $EQXS_n$ определим функцию $EQXS_n^k$, где $k \leq n$, k кратно 4, при этом $EQXS_n^k$ существенным образом зависит от первых k переменных и $EQXS_n^k \equiv EQXS_k$. Согласно Теореме 6, $EQXS_n^{4log\,d} \in NQOBDD_n^{4d(log\,d\,+\,1)}$. Согласно Теореме 7, $EQXS_n^{4log\,d} \notin NQOBDD_n^{d-1}$.

Заключение

В статье исследуется модель недетерминированных квантовых упорядоченных диаграмм решений (NQOBDD) большой ширины. Рассматривается функция "Равенство", для которой сложность вычисления в классических OBDD существенно зависит от порядка считывания переменных: ширина программы равна 3 для наилучшего порядка и экспоненциальна для наихудшего порядка. В работе доказываются нижние оценки сложности вычисления этой функции в модели NQOBDD: линейная нижняя оценка для наилучшего порядка считывания и экспоненциальная нижняя оценка для наихудшего порядка. Показывается, что полученные нижние оценки точны. Конструируется функция, для которой доказывается экспоненциальная нижняя оценка для квантовой модели для любого порядка считывания переменных. Строится квантовый алгоритм для вычисления данной функции в модели NQOBDD. Доказывается результат о соотношении классов сложности, основанных на квантовых и классических недетерминированных OBDD большой ширины.

Список источников

1. *Манин Ю.И.* Вычислимое и невычислимое. М.: Сов. Радио. 1980. 128 с.

2. *Feynman R.* Simulating physics with computers // International Journal of Theoretical Physics. 1982. Vol. 21, № 6, 7. С. 467−488.

3. *Wegener I.* Branching programs and binary decision diagrams: theory and applications. Society for Industrial and Applied Mathematics. 2000. 408 p.

4. *Cobham A.* The recognition problem for the set of perfect squares // Proc. of the 7th Symposium on Switching an Automata Theory (SWAT). 1996. P. 78−87.

5. *Pudlak P., Zak S.* Space complexity of computations. Technical report, Univ. Prague. 1983.

6. *Ablayev F., Gainutdinova A., Karpinski M.* On Computational Power of Quantum Branching Programs // Proc. of the 13th Intern. Symposium, Fundamentals of Computation Theory, FCT2001. 2001. Vol. 2138. P. 59−70.

7. *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 Intern. Conference, COCOON 2000, Proc. 2000. Vol. 2138. P. 467−476.

8. *Sauerhoff M., Sieling D.* Quantum branching programs and space-bounded nonuniform quantum complexity // Theoretical Computer Science. 2005. Vol. 334. № 1–3. P. 177–225.
9. *Ablayev F., Karpinski M.* On the power of randomized branching programs // Proc. ICALP96. 1996. Vol. 1099. P. 348–356.
10. *Ablayev F., Gainutdinova A., Karpinski M., Moore C., Pollette C.* On the computational power of probabilistic and quantum branching program // Information and Computation. 2005. Vol. 203, № 2. P. 145–162.
11. *Ablayev F., Gainutdinova A., Khadiev K., Yakaryılmaz A.* Very narrow quantum OBDDs and width hierarchies for classical OBDDs // Lobachevskii Journal of Mathematics. 2016. Vol. 37. P. 670–682.
12. *Gainutdinova A., Yakaryılmaz A.* Nondeterministic unitary OBDDs // Computer Science – Theory and Applications: 12th Intern. Computer Science Symposium in Russia, CSR2017, Proceedings. 2017. P. 126–140.
13. *Meinel C., Theobald T.* Algorithms and Data Structures in VLSI Design: OBDD-foundations and applications. Springer Science & Business Media, 1998. 279 p.
14. *Ablayev F., Gainutdinova A.* Complexity of quantum uniform and nonuniform automata // Developments in Language Theory: 9th Intern. Conference, DLT2005, Proceedings. 2005. P. 78–87.
15. *Nielsen M. A., Chuang I. L.* Quantum computation and quantum information. Cambridge university press, 2010. 710 p.
16. *Кострикин А.И.* Введение в алгебру: учебник: в 3 частях. Часть II: Линейная алгебра. М.: МЦНМО, 2020. 367 с.
17. *Ablayev F., Gainutdinova A., Khadiev K., Yakaryılmaz A.* Very narrow quantum OBDDs and width hierarchies for classical OBDDs // Descriptional Complexity of Formal Systems: 16th Intern. Workshop DCFS2014, Proceedings. 2014. P. 53–64.
18. *Khadiev K., Khadieva A.* Reordering method and hierarchies for quantum and classical ordered binary decision diagrams // International computer science symposium in Russia, Springer International Publishing, 2017. P. 162–175.

References

1. Manin, Yu. I. (1980), *Computable and non-computable*, Sov. Radio, Moscow, Russia.
2. Feynman, R. (1982), "Simulating physics with computers", *International Journal of Theoretical Physics*, vol. 21, no. 6–7, pp. 467-488.
3. Wegener, I. (2000), *Branching programs and binary decision diagrams: theory and applications*, Society for Industrial and Applied Mathematics. USA.
4. Cobham, A. (1996), "The recognition problem for the set of perfect squares", *Proc. of the 7th Symposium on Switching an Automata Theory (SWAT)*, pp. 78-87.
5. Pudlak, P., Zak, S. (1983), *Space complexity of computations*, *Technical report*, Univ. Prague, Prague, Czech Republic.
6. Ablayev, F., Gainutdinova, A. and Karpinski, M. (2001), "On Computational Power of Quantum Branching Programs", *Proc. of the 13th Intern. Symposium, Fundamentals of Computation Theory FCT 2001*, vol. 2138, pp. 59-70.
7. Nakanishi, M., Hamaguchi, K. and Kashiwabara, T. (2000), "Ordered quantum branching programs are more powerful than ordered probabilistic branching programs under a bounded-width restriction", *Computing and Combinatorics: 6th Annual Intern. Conference, COCOON 2000, Proc.*, vol. 2138, pp. 467-476.

8. Sauerhoff, M., Sieling, D. (2005), "Quantum branching programs and space-bounded nonuniform quantum complexity", *Theoretical Computer Science*, vol. 334, no.1-3, pp. 177-225.
9. Ablayev, F., Karpinski, M. (1996), "On the power of randomized branching programs", *Proceeding of the conference. ICALP*, vol. 1099, pp. 348-356.
10. Ablayev, F., Gainutdinova, A., Karpinski, M., Moore, C. and Pollette, C. (2005), "On the computational power of probabilistic and quantum branching program", *Information and Computation*, vol. 203, no. 2, pp. 145-162.
11. Ablayev, F., Gainutdinova, A., Khadiev, K. and Yakaryılmaz, A. (2016), "Very narrow quantum OBDDs and width hierarchies for classical OBDDs", *Lobachevskii Journal of Mathematics*, no. 37, pp. 670-682.
12. Gainutdinova, A., Yakaryılmaz, A. (2017), "Nondeterministic unitary OBDDs", *Computer Science – Theory and Applications: 12th Intern. Computer Science Symposium in Russia, Proc*., vol. 10304, pp. 126-140.
13. Meinel, T., Theobald, T. (1998), *Algorithms and Data Structures in VLSI Design: OBDD – foundations and applications*, Springer Science & Business Media, Berlin/Heidelberg, Germany.
14. Ablayev, F., Gainutdinova, A. (2005), "Complexity of quantum uniform and nonuniform automata", *Developments in Language Theory*, vol. 3572, pp. 78-87.
15. Nielsen, M., Chuang, I. (2000), *Quantum Computation and Quantum Information*, Cambridge University Press, Cambridge, UK.
16. Kostrikin, A. I. (2020), *Introduction to Algebra: textbook: in 3 parts. Part II: Linear Algebra*, MCNO, Moscow, Russia.
17. Ablayev, F., Gainutdinova, A., Khadiev, K. and Yakaryılmaz, A. (2014), "Very narrow quantum OBDDs and width hierarchies for classical OBDDs", *Proc. of the Intern. conference DCFS 2014*, vol. 8614, pp. 53-64.
18. Khadiev, K., Khadieva, A. (2017), "Reordering method and hierarchies for quantum and classical ordered binary decision diagrams", *Computer Science – Theory and Applications: 12th Intern. Computer Science Symposium in Russia*, vol. 10304, pp. 162-175.

Информация об авторе:

А. Ф. Гайнутдинова – кандидат физико-математических наук, доцент, доцент кафедры теоретической кибернетики института вычислительной математики и информационных технологий Казанского (Приволжского) федерального университета (420008, Россия, г. Казань, ул. Кремлевская, 18), AuthorID: 122490.

Information about the author:

A. F. Gainutdinova – Candidate of Physical and Mathematical Sciences, Associate Professor, Associate Professor of the Department of Theoretical Cybernetics of the Institute of Computational Mathematics and Information Technology of the Kazan (Volga Region) Federal University (18, Kremlevskaya St., Kazan, Russia, 420008), AuthorID: 122490.