

ОРИГИНАЛЬНАЯ СТАТЬЯ

УДК 519.71

doi: 10.26907/2541-7746.2024.4.470-484

КВАНТОВЫЕ И КЛАССИЧЕСКИЕ НЕДЕТЕРМИНИРОВАННЫЕ OBDD

А.Ф. Гайнутдинова

Казанский (Приволжский) федеральный университет, г. Казань, 420008, Россия

Аннотация

Исследована модель недетерминированных упорядоченных ветвящихся диаграмм решений (NOBDD). Дан метод доказательства нижней оценки сложности квантовой NOBDD. Представлены функция, имеющая линейную сложность в квантовой NOBDD и константную сложность в классической NOBDD, а также функция, имеющая одинаковую сложность в квантовой и классической моделях. Описано соотношение сложности классов, определенных для модели OBDD.

Ключевые слова: ветвящаяся программа, упорядоченная ветвящаяся диаграмма решений, OBDD, сложность, квантовый алгоритм, недетерминизм, иерархия классов сложности

Введение

Изучение вычислительных возможностей квантовых моделей в сравнении с их классическими аналогами является актуальным направлением современных исследований. Ветвящиеся программы (BP – Branching Programs) – это известная модель для вычисления булевых функций, имеющая множество приложений в различных областях: в верификации моделей и программ, в базах данных и т. д. [1, с. 5–11]. Упорядоченные ветвящиеся диаграммы решений (OBDD – Ordered Binary Decision Diagrams) – это частный случай модели BP, когда переменные считываются не более одного раза в одном и том же порядке. Естественной мерой сложности для этой модели является ширина. OBDD фиксированной ширины с одинаковыми преобразованиями на каждом шаге (стабильные OBDD) можно рассматривать как конечные автоматы, обрабатывающие слова фиксированной длины. Различные варианты OBDD (детерминированные, недетерминированные, вероятностные, квантовые) исследованы в ряде работ [2–6]: показано, что вероятностные OBDD могут быть экспоненциально более эффективными, чем детерминированные и недетерминированные [4], а квантовые OBDD – экспоненциально более эффективными, чем детерминированные и стабильные вероятностные, и что данная оценка точна [5]. Квантовый и классический недетерминизмы для моделей OBDD рассмотрены в работе [6], где показано превосходство квантового недетерминизма над классическим. В частности, представлена функция, вычисляемая недетерминированными квантовыми OBDD (NQOBDD) константной ширины, в то время как классические недетерминированные OBDD (NOBDD) для этой функции имеют неконстантную ширину.

В настоящей работе исследованы NQOBDD линейной и сублинейной ширины. Представлен метод доказательства нижней оценки ширины NQOBDD для произвольной булевой функции. Рассмотрена булева функция EХАСТ_n^k , зависящая от параметра k и принимающая значение 1 на наборах, в которых число единиц равно k . Показано, что такая функция требует ширины не менее $\max(k+1, n-k+1)$ при вычислении на недетерминированных квантовых OBDD и ширины не менее $\min(k+1, n-k+1) + 1$ при вычислении на классических недетерминированных OBDD. Доказано, что обе нижние оценки точны. При значении параметра $k = n$ ширина NQOBDD для этой функции линейна, в то время как классическая NOBDD имеет ширину 2. Отрицание функции EХАСТ_n^k , напротив, вычислимо квантовой NOBDD ширины 2 для любого значения k , в то время как классическая NOBDD, вычисляющая эту функцию, имеет неконстантную ширину. Рассмотрена также булева функция MOD_n^p , принимающая значение 1 на наборах с числом единиц, кратным p , для которой недетерминированная и квантовая недетерминированная OBDD имеют одинаковую сложность. На основе доказанных утверждений найдено соотношение классов сложности, определённых для моделей недетерминированных и квантовых недетерминированных OBDD.

Предварительная версия части результатов, изложенных в настоящей работе, была представлена в материалах конференции [7]. Здесь мы уточняем некоторые результаты, в частности, доказательство верхней и нижней оценок сложности классической NOBDD для функции EХАСТ_n^k .

Статья организована следующим образом. В разделе 1 представлены определения моделей. Раздел 2 содержит вспомогательные сведения, используемые в доказательствах. Раздел 3 посвящен методу доказательства нижней оценки сложности NQOBDD для произвольной булевой функции. В разделе 4 исследована сложность вычисления функции EХАСТ_n^k , а также её отрицания в квантовых и классических недетерминированных OBDD. Доказаны верхние и нижние оценки сложности для обеих моделей. В разделе 5 рассмотрены функция MOD_n^p и сложность её вычисления в недетерминированных и квантовых недетерминированных OBDD. В разделе 6 приведен результат о соотношении классов сложности, основанных на квантовых и классических недетерминированных OBDD.

1. Определения моделей

Приведем краткие определения моделей ветвящихся программ и OBDD (для более полной информации см., например, [8]). Мы используем верхний индекс для нумерации векторов и наборов, а 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 (назовём их отвергающими и принимающими вершинами соответственно). Внутренние вершины помечены переменными из множества X и имеют по два исходящих ребра, помеченных 0 и 1 соответственно. Входной набор $\sigma \in \{0, 1\}^n$ индуцирует вычислительный путь из выделенной начальной вершины в финальную. BP представляет булеву функцию $f: \{0, 1\}^n \rightarrow \{0, 1\}$, если для любого $\sigma \in \{0, 1\}^n$ значение достигнутой финальной вершины совпадает со значением $f(\sigma)$.

Сложность $\text{Size}(P)$ ветвящейся программы P – это количество её внутренних вершин. Длина $\text{Length}(P)$ ветвящейся программы P – это максимальная длина пути из начальной вершины в конечную. Длина BP очевидным образом оценивает время, требуемое для вычисления функции f в худшем случае. Сложность BP оценивает память, затрачиваемую в процессе вычисления.

Ветвящаяся программа называется *один раз читающей*, если на любом пути из начальной вершины в финальную каждая переменная считывается не более одного раза. Ветвящаяся программа называется *уровневой*, если её вершины могут быть разбиты на уровни $0, 1, \dots$ таким образом, что для каждого i рёбра, исходящие из вершин уровня i , ведут только в вершины уровня $(i + 1)$. Уровневая ВР P называется *забывающей*, если во всех вершинах одного уровня P тестируется одна и та же переменная. *Ширина* $Width(P)$ уровневой ВР P – это максимальное число вершин на уровне. Очевидно, что $Size(P) \leq Length(P) Width(P)$.

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

Так как длина OBDD не превосходит n , естественной мерой сложности для неё является ширина. Модель OBDD константной ширины с естественным порядком считывания переменных и одинаковыми преобразованиями на каждом уровне эквивалентна модели конечных автоматов [9].

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 σ может существовать несколько вычислительных путей. NOBDD P принимает входной набор σ , если существует вычислительный путь, соответствующий данному набору, который завершается в принимающей вершине. В противном случае P отвергает набор σ .

Для определения квантовой OBDD нам понадобятся некоторые сведения из теории квантовых вычислений (для большей информации см., например, [10]).

Квантовая система (QS) с d устойчивыми 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 $|\psi\rangle = (z_0, \dots, z_{d-1})$ с единичной нормой (унитарный вектор): $\| |\psi\rangle \| = \sqrt{\langle \psi | \psi \rangle} = 1$ ($\langle \psi |$ – сопряженная к $|\psi\rangle$ вектор-строка).

Комплексное число z_i ($i = 0, \dots, d - 1$) называется амплитудой устойчивого состояния $|i\rangle$, где $|i\rangle$ обозначает унитарный вектор со значением 1 в позиции i (нумерация элементов вектора осуществляется с 0).

Унитарная эволюция – это изменение состояния квантовой системы за определённый период времени, она описывается d -мерной унитарной матрицей U .

Матрица U называется унитарной, если выполняется $UU^\dagger = I$, где $U^\dagger$ – транспонированная комплексносопряжённая к U матрица, I – единичная матрица.

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

- а) $p_k = \|P_k |\psi\rangle\|^2$ – вероятность того, что исходом измерения является значение k ;
- б) $|\psi'\rangle = \frac{P_k |\psi\rangle}{\|P_k |\psi\rangle\|}$ – состояние квантовой системы после измерения, результатом которого является значение k .

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

$$Q = (|\psi^0\rangle, R, \mathcal{O}_{final}),$$

где $|\psi^0\rangle$ – начальная суперпозиция; R – последовательность (длины l) инструкций, содержащих d -мерные унитарные преобразования квантовой системы QS

с d устойчивыми 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; $\mathcal{O}_{final} = \{P_{accept}, P_{reject}\}$ – система операторов, задающих финальное измерение с исходами *accept* и *reject* соответственно.

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

$$Pr_{accept}^Q(\sigma) = \|P_{accept}|\psi_{final}\rangle\|^2.$$

Q недетерминированно вычисляет функцию f , если Q принимает вход σ с вероятностью больше 0 тогда и только тогда, когда $f(\sigma) = 1$. Такую OBDD будем называть недетерминированной квантовой OBDD (NQOBDD).

Q вычисляет функцию f без ошибки, если Q принимает с вероятностью 1 входы σ , для которых $f(\sigma) = 1$, и принимает с вероятностью 0 входы σ , для которых $f(\sigma) = 0$.

2. Сведения из линейной алгебры

Ниже приведены необходимые сведения из линейной алгебры (см., например, [11]).

Пусть V – векторное пространство над полем комплексных чисел с нормой $\|\cdot\|_2$. Через $\mathbf{0}$ обозначим нулевой элемент V . Система векторов $\psi_1, \psi_2, \dots, \psi_d \in V$ называется линейно зависимой, если существуют такие числа $\alpha_1, \alpha_2, \dots, \alpha_d \in \mathbb{C}$, одновременно не равные нулю, что $\alpha_1\psi_1 + \dots + \alpha_d\psi_d = \mathbf{0}$. Если это равенство выполняется только при $\alpha_1 = \alpha_2 = \dots = \alpha_d = 0$, то система векторов называется линейно независимой.

Два вектора ψ_1 и ψ_2 линейно зависимы тогда и только тогда, когда $\psi_1 = \alpha\psi_2$ или $\psi_2 = \beta\psi_1$ при некоторых α, β , т. е. когда векторы ψ_1 и ψ_2 коллинеарны.

Лемма 1. Пусть $\psi_1, \psi_2, \dots, \psi_d \in V$ – линейно независимая система векторов, U – унитарное преобразование в пространстве V . Тогда векторы $U\psi_1, U\psi_2, \dots, U\psi_d$ линейно независимы.

Доказательство. Унитарное преобразование является взаимнооднозначным, его можно рассматривать как переход к другому базису. Взаимнооднозначное линейное преобразование сохраняет свойство линейной независимости преобразуемых векторов. $\square$

Свойства нормы:

- а) $\|\psi\| = 0 \Rightarrow \psi = \mathbf{0}$;
- б) $\forall \psi, \phi \in V \quad \|\psi + \phi\| \leq \|\psi\| + \|\phi\|$ (неравенство треугольника);
- в) $\forall \alpha \in \mathbb{C}, \forall \psi \in V \quad \|\alpha\psi\| = |\alpha| \cdot \|\psi\|$.

Лемма 2. Пусть векторы $\psi_1, \dots, \psi_m, \psi \in V$, $\psi_1, \dots, \psi_m$ – линейно независимы. Пусть U – такое линейное преобразование пространства V , что

$$\|U\psi_i\| = 0, \quad i = 1, \dots, m, \quad \|U\psi\| \neq 0.$$

Тогда система векторов $\{\psi_1, \dots, \psi_m, \psi\}$ линейно независима.

Доказательство. Докажем утверждение от противного. Предположим, что вектор ψ линейно зависим с системой $\psi_1, \dots, \psi_m$. Тогда существуют $\alpha_1, \alpha_2, \dots, \alpha_m \in \mathbb{C}$, одновременно не равные нулю и такие, что $\psi = \alpha_1\psi_1 + \dots + \alpha_m\psi_m$.

В силу линейности имеем $U\psi = U(\alpha_1\psi_1 + \dots + \alpha_m\psi_m) = \alpha_1U\psi_1 + \dots + \alpha_mU\psi_m$. По свойству нормы $\|U\psi\| \leq |\alpha_1|\|U\psi_1\| + \dots + |\alpha_m|\|U\psi_m\|$. По условию леммы $\|U\psi_1\| = \dots = \|U\psi_m\| = 0$. Значит, $\|U\psi\| = 0$. Получили противоречие. $\square$

3. Нижняя оценка ширины недетерминированной QOBDD

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

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

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

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

Теорема 1. Для любой QOBDD Q , недетерминированно вычисляющей функцию $f : \{0, 1\}^n \rightarrow \{0, 1\}$ и использующей порядок $\pi = (i_1, \dots, i_n)$ считывания переменных,

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

Доказательство. Пусть $d = \max_k |S_k^\pi|$, где $S_k^\pi = \{(\sigma^1, \gamma^1), \dots, (\sigma^d, \gamma^d)\}$ – строгое 1-полное множество для функции f . Предположим, что существует NQOBDD Q , вычисляющая функцию f с использованием порядка π считывания переменных, ширина которой меньше d . Рассмотрим уровень k . Пусть $\Psi = \{|\psi(\sigma^j)\rangle \mid j = 1, \dots, d\}$ – множество квантовых состояний, в которых находится программа после обработки входов $\sigma^1, \dots, \sigma^d$, т.е. $|\psi(\sigma^j)\rangle = U(\sigma^j)|\psi^0\rangle$.

Лемма 3. Множество Ψ линейно независимо.

Доказательство. Проведем доказательство от противного. Предположим, что множество векторов Ψ является линейно зависимым. Тогда существует состояние $|\psi\rangle = |\psi(\sigma^i)\rangle \in \Psi$, которое может быть представлено в виде линейной комбинации остальных векторов из множества Ψ :

$$|\psi(\sigma^i)\rangle = \sum_{\substack{j=1 \\ j \neq i}}^d \alpha_j |\psi(\sigma^j)\rangle,$$

при этом неверно, что $\alpha_j = 0$ для всех j .

Пусть γ^i такое, что $(\sigma^i, \gamma^i) \in S_k^\pi$. Согласно определению строгого 1-полного множества, для всех входов σ^j ($j \neq i$) выполняется $f_{\pi,k}^{\sigma^j}(\gamma^i) = 0$, следовательно, программа Q принимает входы $\sigma^j \gamma^i$ с нулевой вероятностью:

$$Pr_{accept}^Q(\sigma^j \gamma^i) = \|P_{accept} U(\gamma^i) |\psi(\sigma^j)\rangle\|^2 = 0.$$

После обработки входа $\sigma^i \gamma^i$ финальное состояние программы

$$|\psi(\sigma^i \gamma^i)\rangle = U(\gamma^i) |\psi(\sigma^i)\rangle = U(\gamma^i) \sum_{\substack{j=1 \\ j \neq i}}^d \alpha_j |\psi(\sigma^j)\rangle,$$

и по свойству линейности преобразований

$$|\psi(\sigma^i \gamma^i)\rangle = \sum_{\substack{j=1 \\ j \neq i}}^d \alpha_j U(\gamma^i) |\psi(\sigma^j)\rangle = \sum_{\substack{j=1 \\ j \neq i}}^d \alpha_j |\psi(\sigma^j \gamma^i)\rangle.$$

Тогда

$$\begin{aligned} Pr_{accept}^Q(\sigma^i \gamma^i) &= \|P_{accept} |\psi(\sigma^i \gamma^i)\rangle\|^2 = \left\| \sum_{\substack{j=1 \\ j \neq i}}^d \alpha_j P_{accept} |\psi(\sigma^j \gamma^i)\rangle \right\|^2 \leq \\ &\leq \left(\sum_{\substack{j=1 \\ j \neq i}}^d |\alpha_j| \|P_{accept} |\psi(\sigma^j \gamma^i)\rangle\| \right)^2 = 0. \end{aligned}$$

Следовательно, программа Q неверно вычисляет функцию f , поскольку принимает набор $\sigma^i \gamma^i$, для которого $f_{\pi,k}^{\sigma^i}(\gamma^i) > 0$, с нулевой вероятностью. Получили противоречие. Следовательно, наше предположение о том, что множество Ψ линейно зависимо, неверно. $\square$

Так как множество Ψ состояний программы, достижимых на уровне k , линейно независимо, размерность пространства состояний программы Q не может быть меньше d . Следовательно, $Width(Q) \geq d$. $\square$

4. Функция Exact

Определим функцию $EXACT_n^k : \{0, 1\}^n \rightarrow \{0, 1\}$:

$$EXACT_n^k(\sigma) = \begin{cases} 1, & \text{если } \#_1(\sigma) = k, \\ 0, & \text{иначе,} \end{cases}$$

где $\#_1(\sigma)$ обозначает число единиц в наборе σ . При $k = n$ имеем $EXACT_n^k \equiv AND_n$, где функция $AND_n : \{0, 1\}^n \rightarrow \{0, 1\}$ принимает значение 1 на единственном наборе, где все переменные равны 1.

Теорема 2. *Ширина любой QOBDD, недетерминированно вычисляющей функцию $EXACT_n^k$, не менее чем $\max\{k + 1, n - k + 1\}$.*

Доказательство. Пусть Q – NQOBDD, вычисляющая функцию $EXACT_n^k$ и считающая переменные в порядке $\pi = (i_1, \dots, i_n)$. Покажем, что ширина Q не может быть меньше $\max\{k + 1, n - k + 1\}$.

Вычисление на входе $\sigma = \sigma_1 \cdots \sigma_n$ начинается из начальной суперпозиции $|\psi^0\rangle$. На шаге l программа считывает переменную $x_{i_l} = \sigma_{i_l}$ и преобразует суперпозицию $|\psi(\sigma_{i_1} \cdots \sigma_{i_{l-1}})\rangle$ в суперпозицию $|\psi(\sigma_{i_1} \cdots \sigma_{i_l})\rangle$ (положим $|\psi^0\rangle = |\psi(\epsilon)\rangle$, где ϵ – пустое слово). После считывания входного слова Q производит измерение финальной суперпозиции $|\psi(\sigma_{i_1} \cdots \sigma_{i_n})\rangle$ и принимает входной набор с вероятностью $Pr_{accept}^Q(\sigma) = \|P_{accept}|\psi(\sigma_{i_1} \cdots \sigma_{i_n})\rangle\|^2$.

Оценим размерность пространства состояний программы Q . Для этого для каждого уровня l ($l = 0, \dots, n$) рассмотрим множество квантовых состояний, достижимых программой на этом уровне, и оценим количество линейно независимых векторов из этого множества.

Обозначим $\Psi_l = \{|\psi(\sigma)\rangle \mid \sigma \in \{0, 1\}^l\}$ множество состояний, достижимых программой Q после шага l , т.е. $|\psi(\sigma)\rangle = U_l(\sigma_{i_l}) \cdots U_1(\sigma_{i_1})|\psi^0\rangle$.

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

Доказательство. По условию леммы строка $\gamma \in \{0, 1\}^{n-l}$ отличает строку σ от каждой из строк $\sigma^1, \dots, \sigma^m$. Это означает, что на наборе, где переменные принимают значения $x_{\pi(1)} = \sigma_1, \dots, x_{\pi(l)} = \sigma_l, x_{\pi(l+1)} = \gamma_1, \dots, x_{\pi(n)} = \gamma_{n-l}$, функция ЕХАСТ_n^k равна 1, а на наборах, в которых переменные принимают значения $x_{\pi(1)} = \sigma_1^i, \dots, x_{\pi(l)} = \sigma_l^i, x_{\pi(l+1)} = \gamma_1, \dots, x_{\pi(n)} = \gamma_{n-l}$ ($i = 1, \dots, m$), функция ЕХАСТ_n^k равна 0. Пусть $U = U_n(\gamma_{n-l}) \cdots U_{l+1}(\gamma_1)$. Так как программа Q недетерминированно вычисляет ЕХАСТ_n^k , то выполняется $\|P_{accept}U|\psi^i\rangle\| = 0$ для всех $i = 1, \dots, m$, и $\|P_{accept}U|\psi\rangle\| > 0$. Согласно лемме 2 множество $\{|\psi^1\rangle, \dots, |\psi^m\rangle, |\psi\rangle\}$ является линейно независимым. $\square$

Пусть Φ_l ($\Phi_l \subseteq \Psi_l$) – максимальное число линейно независимых векторов. Обозначим $d = \max\{k, n-k\}$. По индукции покажем, что $|\Phi_l| \geq l+1$ для $l = 0, \dots, d$. Рассмотрим отдельно два случая: $k \geq n/2$ и $k < n/2$.

Случай 1. Пусть $k \geq n/2$, т.е. $d = k$.

База индукции: на уровне $l = 0$ множество Ψ_0 состоит из единственного вектора $|\psi^0\rangle$, т.е. $|\Phi_0| = 1$. На уровне $l = 1$ множество Ψ_1 состоит из двух векторов $|\psi(0)\rangle, |\psi(1)\rangle$. Векторы $|\psi(0)\rangle$ и $|\psi(1)\rangle$ линейно независимы, так как набор $\gamma = 1^{k-1}0^{n-k}$ отличает строку 1 от строки 0, то есть $|\Phi_1| = 2$.

Индукционный шаг (для $l = 2, \dots, d$): по предположению индукции, на уровне $(l-1)$ множество $\Phi_{l-1} \subseteq \Psi_{l-1}$ содержит не менее l векторов. Обозначим их $|\psi^{j_0}\rangle, \dots, |\psi^{j_{l-1}}\rangle$, а соответствующие им входы – $\sigma^{j_0}, \dots, \sigma^{j_{l-1}} \in \{0, 1\}^{l-1}$.

На шаге l программа Q считывает значение переменной $x_{i_l} = \sigma_{i_l}$. Согласно лемме 1 множество $\Phi_l^0 = \{U_l(0)|\psi^{j_0}\rangle, \dots, U_l(0)|\psi^{j_{l-1}}\rangle\}$ является линейно независимым. Очевидно, что вектор $|\psi(1^l)\rangle = U_l(1)U_{l-1}(1) \cdots U_1(1)|\psi^0\rangle$ не входит в множество Φ_l^0 . При этом строка $1^{k-l}0^{n-k}$ отличает строку 1^l от каждой из строк $\sigma^{j_0}0, \dots, \sigma^{j_{l-1}}0$. Согласно лемме 4 множество $\Phi_l^0 \cup \{|\psi(1^l)\rangle\}$ линейно независимо. Получили, что множество Φ_l содержит по крайней мере $(l+1)$ векторов $U_l(0)|\psi^{j_0}\rangle, \dots, U_l(0)|\psi^{j_{l-1}}\rangle$ и $|\psi(1^l)\rangle$.

Поскольку множество Φ_d содержит не менее $d+1$ элементов, размерность пространства состояний программы Q не менее $d+1$.

Случай 2. Пусть $k < n/2$ и, следовательно, $d = n-k$. Очевидно, что $\text{ЕХАСТ}_n^k(\sigma) = 1$ тогда и только тогда, когда $\#_0(\sigma) = n-k$, где $\#_0(\sigma)$ обозначает число нулей в наборе σ , при этом $n-k > n/2$. Доказательство проведем по той же схеме, что и для случая 1.

Для $l = 0, \dots, d$ множество Φ_l содержит векторы $|\psi^{j_0}\rangle, \dots, |\psi^{j_l}\rangle$ такие, что для соответствующих им входов выполняется $\#_0(\sigma^{j_i}) = i$ ($i = 0, \dots, l$). Опишем индукционный шаг для $l = 1, \dots, d$.

Пусть $\Phi_{l-1} = \{|\psi^{j_0}\rangle, \dots, |\psi^{j_{l-1}}\rangle\}$, где $|\psi^{j_i}\rangle = |\psi(\sigma^{j_i})\rangle$, $\sigma^{j_i} \in \{0, 1\}^{l-1}$. Тогда множество $\Phi_l^1 = \{U_l(1)|\psi^{j_0}\rangle, \dots, U_l(1)|\psi^{j_{l-1}}\rangle\}$ линейно независимо по лемме 1. Строка $\gamma = 0^{n-k-l}1^k$ отличает строку 0^l от каждой их строк $\sigma^{j_0}1, \dots, \sigma^{j_{l-1}}1$, при этом $|\psi(0^l)\rangle \notin \Phi_l^1$. Согласно лемме 4 множество $\Phi_l = \Phi_l^1 \cup \{|\psi(0^l)\rangle\}$ является линейно независимым и при этом содержит $l+1$ вектор. На уровне $l = d$ имеем $|\Phi_d| \geq d+1$.

Поскольку в обоих случаях $|\Phi_d| \geq d+1$, получим, что размерность пространства состояний программы Q не менее $d+1$, где $d = \max\{k, n-k\}$. $\square$

Следующая теорема показывает, что доказанная нижняя оценка точна.

Теорема 3. *Существует QOBDD Q ширины $d = \max\{k+1, n-k+1\}$, вычисляющая функцию EXACT $_n^k$ без ошибки.*

Доказательство. Рассмотрим случай $k \geq n/2$. QOBDD Q считывает переменные в естественном порядке. Состояние программы хранится в регистре из $k+1$ состояния $q_0, \dots, q_{k-1}, q_k$, где q_0 – начальное состояние, а q_k – принимающее состояние. При считывании значения 0 программа Q применяет тождественное преобразование, при считывании единицы Q – преобразование $|q_j\rangle \rightarrow |q_{j+1 \bmod (k+1)}\rangle$ для $0 \leq j \leq k$. Очевидно, что при обработке входного набора, содержащего ровно k единиц, программа закончит работу в состоянии $|q_k\rangle$ и примет такой набор с вероятностью 1. Если входной набор содержит число единиц, не равное k , то свойство $k \geq n/2$ гарантирует, что программа завершит обработку такого набора в состоянии, отличном от k , следовательно, примет такой набор с вероятностью 0.

В случае $k < n/2$ программа устроена аналогичным образом, только производит подсчет нулей, а не единиц. $\square$

Теорема 4. *Существует NOBDD N , вычисляющая функцию EXACT $_n^k$ и такая, что*

$$\text{Width}(N) = \min(k+1, n-k+1) + 1, \text{ если } k \neq n/2, \text{ } n \text{ нечётно,}$$

$$\text{Width}(N) = k+1, \text{ если } k = n/2, \text{ } n \text{ чётно.}$$

Доказательство. Пусть $k < n/2$, n нечётно. Программа N считывает переменные в естественном порядке $\pi = (1, \dots, n)$ и использует состояния $q_0, \dots, q_k, q_{k+1}$. Начальное состояние программы q_0 , принимающее состояние q_k . Программа N детерминированно считает количество единиц во входном наборе, выполняя преобразование $q_i \rightarrow q_{i+1}$ ($i = 0, \dots, k$) при считывании единицы и тождественное преобразование при считывании нуля. При достижении состояния q_{k+1} программа остаётся в этом состоянии до конца обработки входа. Таким образом, программа закончит работу в состоянии q_k тогда и только тогда, когда в наборе ровно k единиц.

Пусть $k > n/2$, n нечётно ($n-k < n/2$). В этом случае программа устроена аналогичным образом, за исключением того, что она считает количество нулей, а не количество единиц.

Рассмотрим случай $k = n/2$, n чётно. В этом случае программа N использует состояния $q_0, \dots, q_k$, где состояние q_0 – начальное, а состояние q_k – принимающее. При считывании единицы программа применяет преобразование $q_i \rightarrow q_{i+1 \bmod (k+1)}$ ($i = 0, \dots, k$), при считывании нуля выполняет тождественное преобразование. Условие $k = n/2$ гарантирует, что если число единиц в наборе больше k , программа не успеет достигнуть состояния q_k до конца обработки входа. $\square$

Теорема 5. Для любой NOBDD, вычисляющей функцию EXACT_n^k ,

$$\text{Width}(N) \geq \min(k+1, n-k+1) + 1, \text{ если } k \neq n/2, \text{ } n \text{ нечётно,}$$

$$\text{Width}(N) \geq k+1, \text{ если } k = n/2, \text{ } n \text{ чётно.}$$

Доказательство. Рассмотрим случай $k < n/2$, n нечётно. Предположим, что существует NOBDD N , которая вычисляет EXACT_n^k и имеет ширину меньше $k+2$. Рассмотрим множество вершин V_{k+1} уровня $k+1$ программы N и подмножество строк длины $k+1$, содержащих разное количество единиц: $S^{k+1} = \{\sigma^j \in \{0,1\}^{k+1} : \sigma^j = \underbrace{0 \cdots 0}_{k+1-j} \underbrace{1 \cdots 1}_j, j = 0, \dots, k\}$. Принимающие пути, соответствующие

частичным наборам из множества S^{k+1} , должны проходить через разные вершины множества V_{k+1} . Предположим, что это не так, и два принимающих пути, соответствующих разным частичным наборам $\sigma, \sigma' \in S^{k+1}$, проходят через одну и ту же вершину $v \in V_{k+1}$, и пусть $\sigma\gamma$ и $\sigma'\gamma'$ – наборы, соответствующие этим принимающим путям. Обозначим $a = \#_1(\sigma)$, $a' = \#_1(\sigma')$ ($a \neq a'$, $a, a' \leq k$). Поскольку путь, соответствующий набору $\sigma\gamma$, ведет в принимающую вершину, значит, $\#_1(\gamma) = k-a$. Так как пути, соответствующие наборам $\sigma\gamma$ и $\sigma'\gamma'$, пересекаются в вершине v , то путь, соответствующий $\sigma'\gamma$, также ведет в принимающую вершину. Но поскольку $\#_1(\sigma') \neq a$, следовательно, $\#_1(\sigma'\gamma) \neq k$, и функция на данном наборе равна нулю. Значит, программа неверно вычисляет функцию EXACT_n^k .

Теперь рассмотрим частичный набор $\sigma \in \{0,1\}^{k+1}$, $\#_1(\sigma) = k+1$. Очевидно, этот набор не принадлежит S^{k+1} . Вычислительный путь, соответствующий σ , не может проходить ни через одну из вершин уровня V_{k+1} , через которые проходят принимающие пути, соответствующие наборам из множества S^{k+1} . В противном случае программа будет принимать вход, содержащий более k единиц. Следовательно, уровень $k+1$ содержит по крайней мере $k+2$ вершины и $\text{Width}(N) \geq k+2$.

Если $k > n/2$ (n нечётно), то $n-k < n/2$. В этом случае мы применим те же аргументы, что и для случая, рассмотренного выше, с заменой нулей на единицы и единиц на нули.

Рассмотрим случай $k = n/2$, n чётно. Уровень k не может содержать менее $k+1$ вершины, через которые проходят принимающие пути, соответствующие частичным входам из множества $S^k = \{\sigma^j \in \{0,1\}^k : \sigma^j = \underbrace{0 \cdots 0}_{k-j} \underbrace{1 \cdots 1}_j, j = 0, \dots, k\}$.

Следовательно, в этом случае ширина программы $\geq k+1$. $\square$

Следствие 1. Функция AND_n вычислима NOBDD N ширины 2. Функция AND_n вычислима NQOBDD Q ширины $n+1$. При этом не существует QOBDD, недетерминированно вычисляющей функцию AND_n и имеющей ширину, меньшую $n+1$.

Определим функцию $\text{notEXACT}_n^k : \{0,1\}^n \rightarrow \{0,1\}$:

$$\text{notEXACT}_n^k(\sigma) = \begin{cases} 0, & \text{если } \#_1(\sigma) = k, \\ 1, & \text{иначе.} \end{cases}$$

Теорема 6. Для любого k ($k \leq n$) функция notEXACT_n^k вычислима недетерминированной QOBDD ширины 2.

Доказательство. QOBDD Q , недетерминированно вычисляющая функцию notEXACT_n^k , имеет два состояния q_1, q_2 , состояние q_2 является принимающим, а начальное состояние программы $|\psi^0\rangle = \cos(-k\alpha)|q_1\rangle + \sin(-k\alpha)|q_2\rangle$, где $\alpha = \frac{\pi}{2n}$. При обработке входа программа Q применяет преобразование, осуществляющее

поворот вектора состояния на угол α против хода часовой стрелки, если считанное значение равно 1, и тождественное преобразование, если считанное значение равно 0. Очевидно, что если входной набор σ содержит ровно k единиц, финальное состояние программы $|\psi_{final}\rangle = |q_1\rangle$, и программа примет такой набор с вероятностью 0. Если число единиц во входном наборе не равно k , амплитуда у состояния q_2 в состоянии $|\psi_{final}\rangle$ не равна нулю, и такой набор принимается программой с ненулевой вероятностью. $\square$

Теорема 7. Для любого k ($k \leq n$) для любой детерминированной OBDD P , вычисляющей функцию notEXACT_n^k ,

$$\text{Width}(P) \geq \min(k+1, n-k+1) + 1, \text{ если } k \neq n/2, \text{ } n \text{ нечётно};$$

$$\text{Width}(P) \geq k+1, \text{ если } k = n/2, \text{ } n \text{ чётно}.$$

Доказательство. Идея доказательства аналогична доказательству теоремы 5 с той разницей, что в детерминированной OBDD каждому $\sigma \in \{0, 1\}^n$ соответствует единственный вычислительный путь и вместо принимающих путей мы анализируем отвергающие пути.

Пусть $k < n/2$. Предположим, что существует детерминированная OBDD, имеющая ширину $d < k+2$ и вычисляющая функцию notEXACT_n^k . Рассмотрим множество частичных входов $S^{k+1} = \{\sigma^j \in \{0, 1\}^{k+1} : \sigma^j = \underbrace{0 \dots 0}_{k+1-j} \underbrace{1 \dots 1}_j, j = 0, \dots, k\}$.

Покажем, что вычислительные пути, соответствующие частичным входам из множества S^{k+1} , проходят через разные вершины уровня $k+1$.

Предположим, что это не так, и существуют такие $\sigma^i, \sigma^j \in S^{k+1}$ ($\sigma^i \neq \sigma^j$), что вычислительные пути, соответствующие этим частичным входам, проходят через одну и ту же вершину v . Рассмотрим такой набор $\gamma \in \{0, 1\}^{n-k-1}$, что $\#_1(\gamma) = k-j$. Поскольку $\#_1(\sigma^j) + \#_1(\gamma) = k$, вычислительный путь, соответствующий набору $\sigma^j\gamma$, ведёт в отвергающую вершину. Но тогда и путь, соответствующий $\sigma^i\gamma$, также ведёт в отвергающую вершину, что противоречит тому, что программа верно вычисляет функцию. Кроме того, частичный набор $\sigma \in \{0, 1\}^{k+1}$ такой, что $\#_1(\sigma) = k+1$, не может проходить ни через одну из $k+1$ вершин, соответствующих наборам из множества S^{k+1} , так как все пути, соответствующие σ , должны вести в принимающую финальную вершину.

Случай $k > n/2$, а также $k = n/2$ при чётном n могут быть обоснованы аналогично теореме 5. $\square$

Теорема 8. Для любого k ($k \leq n$) ширина NOBDD, вычисляющей функцию notEXACT_n^k , имеет ширину не менее $\log(m+1)$, где $m = \min(k+1, n-k+1)$, если $k \neq n/2$, n нечётно, и $m = k$, если $k = n/2$ и n чётно.

Доказательство. Доказательство основано на хорошо известном соотношении между детерминированной и недетерминированной сложностями. Если функция f вычислима детерминированной OBDD ширины d , то ширина любой недетерминированной OBDD, вычисляющей f и использующей тот же порядок считывания переменных, не может быть меньше $\log d$. В предыдущей теореме показано, что для любого порядка считывания переменных ширина детерминированной OBDD, вычисляющей функцию notEXACT_n^k , не может быть меньше $m+1$, где $m = \min(k+1, n-k+1)$, если $k \neq n/2$, n нечётно, и $m = k$, если $k = n/2$ и n чётно. Следовательно, ширина NOBDD, вычисляющей notEXACT_n^k , не может быть меньше $\log(m+1)$. $\square$

5. Функция MOD

Представим функцию, для которой квантовая и классическая недетерминированные OBDD имеют одинаковую сложность.

Функция $\text{MOD}_n^p : \{0, 1\}^n \rightarrow \{0, 1\}$ определена следующим образом:

$$\text{MOD}_n^p(\sigma) = \begin{cases} 1, & \text{если } \#_1(\sigma) \equiv 0 \pmod{p}, \\ 0, & \text{иначе,} \end{cases}$$

где $\#_1(\sigma)$ – число единиц в наборе σ .

Лемма 5 ([6]). *Функция MOD_n^p вычислима NOBDD ширины p .*

Доказательство. NOBDD N , вычисляющая функцию MOD_n^p , имеет p состояний $s_0, \dots, s_{p-1}$, где состояние s_0 – начальное и принимающее. При обработке входа N детерминированным образом считает количество единиц по модулю p во входном наборе, применяя преобразование $q_i \rightarrow q_{i+1 \pmod{p}}$ при считывании единицы и тождественное преобразование при считывании нуля. Очевидно, что программа завершит работу в состоянии q_0 тогда и только тогда, когда число единиц во входном наборе кратно p . $\square$

Следствие 2. *Функция MOD_n^p вычислима NQOBDD ширины p .*

Доказательство. Программа, построенная в доказательстве леммы 5, применяет на каждом шаге обратимые преобразования, которые являются унитарными. Следовательно, эта программа является квантовой. $\square$

Далее покажем, что построенные выше недетерминированная и квантовая недетерминированная программы являются оптимальными.

Теорема 9 ([6]). *Для любого $p \leq n/2$ ширина NOBDD, вычисляющей функцию MOD_n^p , не меньше p .*

Теорема 10. *Для любого $p \leq n$ ширина NQOBDD, вычисляющей функцию MOD_n^p , не меньше p .*

Доказательство. Пусть $p \leq n/2$. Для любого порядка π считывания переменных можно построить строгое 1-полное множество для функции MOD_n^p :

$$S_{n-p+1}^\pi = \{(\sigma^i, \gamma^i) : i = 0, \dots, p-1, \sigma^i = \underbrace{0 \dots 0}_{n-p+1-i} \underbrace{1 \dots 1}_i, \gamma^i = \underbrace{0 \dots 0}_{i-1} \underbrace{1 \dots 1}_{p-i}\}.$$

Согласно теореме 1 ширина программы не может быть меньше, чем $|S_{n-p+1}^\pi| = p$.

Рассмотрим случай $p > n/2$. Используя те же аргументы, что и при доказательстве теоремы 2, можно показать, что на $(p-1)$ -м уровне программы множество линейно независимых векторов, являющихся квантовыми состояниями, достижимыми программой на этом уровне, содержит не менее p элементов. Это множество состоит из векторов $|\psi(\sigma^0)\rangle, \dots, |\psi(\sigma^{p-1})\rangle$, где $\sigma^j = 1^j 0^{p-j-1}$, $j = 0, \dots, p-1$. $\square$

6. Иерархия для NQOBDD

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

В работах [6, 12] построена следующая иерархия классов для OBDD и NOBDD: для любого целого $n > 3$ и $1 < d \leq \frac{n}{2}$

$$\text{OBDD}_n^{d-1} \subsetneq \text{OBDD}_n^d \quad \text{и} \quad \text{NOBDD}_n^{d-1} \subsetneq \text{NOBDD}_n^d.$$

Для любых целых n и $d = d(n)$, удовлетворяющих условию $16 \leq d \leq 2^{n/4}$,

$$\text{OBDD}^{\lfloor d/8 \rfloor - 1} \subsetneq \text{OBDD}^d \quad \text{и} \quad \text{NOBDD}^{\lfloor d/8 \rfloor - 1} \subsetneq \text{NOBDD}^d.$$

На основе изложенных результатов представим результат о соотношении классов сложности для недетерминированных и квантовых недетерминированных OBDD линейной и сублинейной ширины.

Теорема 11. Для любых $n > 1$ и $1 < d \leq n$ имеем $\text{NQOBDD}_n^{d-1} \subsetneq \text{NQOBDD}_n^d$.

Доказательство. Включение $\text{NQOBDD}_n^{d-1} \subseteq \text{NQOBDD}_n^d$ очевидно. При $d \leq n/2$, согласно следствию 2 и теореме 10, функция $\text{MOD}_n^d \in \text{NQOBDD}_n^d$ и $\text{MOD}_n^d \notin \text{NQOBDD}_n^{d-1}$. При $d > n/2$, согласно теоремам 3 и 2, функция $\text{EXACT}_n^{d-1} \in \text{NQOBDD}_n^d$ и $\text{EXACT}_n^{d-1} \notin \text{NQOBDD}_n^{d-1}$. $\square$

Теорема 12. Для любых $n > 1$ и $2 \leq d \leq \log n - 2$ NOBDD_n^d и NQOBDD_n^d несравнимы.

Доказательство. На основе функции AND_n для положительного целого $k \leq n$ определим функцию AND_n^k следующим образом: AND_n^k зависит от первых k переменных и $\text{AND}_n^k \equiv \text{AND}_k$. Согласно следствию 1 $\text{AND}_n^d \in \text{NOBDD}_n^d$ и $\text{AND}_n^d \notin \text{NQOBDD}_n^d$ для любых d таких, что $2 \leq d \leq n$.

Согласно теоремам 6 и 8 функция $\text{notEXACT}_n^{2^d} \notin \text{NOBDD}^d$ и $\text{notEXACT}_n^{2^d} \in \text{NQOBDD}^d$ для любых d таких, что $2 \leq d \leq \log n - 2$. $\square$

Заключение

Исследованы классические и квантовые недетерминированные OBDD линейной и сублинейной ширины, вычисляющие симметрические булевы функции. Значение таких функций зависит от числа единиц во входном наборе и не зависит от порядка их следования. Известно, что квантовые NOBDD для таких функций могут превосходить по эффективности классические недетерминированные программы. С использованием предложенного метода доказательства нижней оценки сложности квантовых NOBDD показано, что классические NOBDD также могут превосходить по эффективности квантовые аналоги. Этот факт является следствием свойства обратимости квантовых преобразований.

В качестве направлений дальнейших работ предполагается исследовать модель квантовых OBDD сверхлинейной ширины, вычисляющих несимметрические булевы функции, для которых порядок считывания переменных может существенным образом влиять на сложность. Также интересным представляется применение разработанных техник доказательства нижних оценок для других вычислительных моделей.

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

Конфликт интересов. Авторы заявляют об отсутствии конфликта интересов.

Литература

1. Wegener I. Branching Programs and Binary Decision Diagrams: Theory and Applications. Ser.: Discrete Mathematics and Applications / Hammer P.L. (Ed.). Philadelphia, PA: Soc. Ind. Appl. Math., 2000. 396 p. <https://doi.org/10.1137/1.9780898719789>.
2. 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 (COCOON 2000): Proc. 6th Annu. Int. Conf. / Du D.-Z., Eades P., Estivill-Castro V., Lin X., Sharma A. (Eds.). Ser.: Lecture Notes in Computer Science. V. 1858. Berlin, Heidelberg: Springer, 2000. P. 467–476. https://doi.org/10.1007/3-540-44968-X_46.
3. Sauerhoff M., Sieling D. Quantum branching programs and space-bounded nonuniform quantum complexity // Theor. Comput. Sci. 2005. V. 334, Nos 1–3. P. 177–225. <https://doi.org/10.1016/j.tcs.2004.12.031>.
4. Ablayev F.M., Karpinski M. On the power of randomized branching programs // Automata, Languages and Programming (ICALP' 96): Proc. 23rd Int. Colloq. / Meyer F., Monien B. (Eds.). Ser.: Lecture Notes in Computer Science. V. 1099. Berlin, Heidelberg: Springer, 1996. P. 348–356. https://doi.org/10.1007/3-540-61440-0_141.
5. Ablayev F., Gainutdinova A., Karpinski M., Moore C., Pollette C. On the computational power of probabilistic and quantum branching program // Inf. Comput. 2005. V. 203, No 2. P. 145–162. <https://doi.org/10.1016/j.ic.2005.04.003>.
6. Ablayev F., Gainutdinova A., Khadiev K., Yakaryilmaz A. Very narrow quantum OBDDs and width hierarchies for classical OBDDs // Lobachevskii J. Math. 2016. V. 37, No 6. P. 670–682. <https://doi.org/10.1134/S199508021606007X>.
7. Gainutdinova A., Yakaryilmaz A. Nondeterministic unitary OBDDs // Computer Science – Theory and Applications (CSR 2017): Proc. 12th Int. Comput. Sci. Symp. in Russia / Weil P. (Ed.). Ser.: Lecture Notes in Computer Science. V. 10304. Cham: Springer, 2017. P. 126–140. https://doi.org/10.1007/978-3-319-58747-9_13.
8. Гайнутдинова А.Ф. Сравнительная сложность квантовых и классических OBDD для всюду определенных и частичных функций // Изв. вузов. Матем. 2015. № 11. С. 32–43.
9. Ablayev F., Gainutdinova A. Complexity of quantum uniform and nonuniform automata // Developments in Language Theory (DLT 2005): Proc. 9th Int. Conf. / De Felice C., Restivo A. (Eds.). Ser.: Lecture Notes in Computer Science. V. 3572. Berlin, Heidelberg: Springer, 2005. P. 78–87. https://doi.org/10.1007/11505877_7.
10. Nielsen M.A., Chuang I. Quantum Computation and Quantum Information. Ser.: Cambridge Series on Information and the Natural Sciences. V. 2. Cambridge, Cambridge Univ. Press, 2000. 676 p.
11. Кострикин А.И. Введение в алгебру. В 3-х ч. Ч. 2: Линейная алгебра. М.: МЦНМО, 2020. 368 с.
12. Ablayev F., Gainutdinova A., Khadiev K., Yakaryilmaz A. Very narrow quantum OBDDs and width hierarchies for classical OBDDs // Descriptive Complexity of Formal Systems (DCFS 2014): Proc. 16th Int. Workshop / Jürgensen H., Karhumäki J., Okhotin A. (Eds.). Ser.: Lecture Notes in Computer Science. V. 8614. Cham: Springer, 2014. P. 53–64. https://doi.org/10.1007/978-3-319-09704-6_6.

Поступила в редакцию 5.07.2024

Принята к публикации 10.10.2024

Гайнутдинова Аида Фаритовна, кандидат физико-математических наук, доцент кафедры теоретической кибернетики Института вычислительной математики и информационных технологий

Казанский (Приволжский) федеральный университет
ул. Кремлевская, д. 18, г. Казань, 420008, Россия
E-mail: aida.ksu@gmail.com

ISSN 2541–7746 (Print)
ISSN 2500–2198 (Online)

UCHENYE ZAPISKI KAZANSKOGO UNIVERSITETA.
SERIYA FIZIKO-MATEMATICHESKIE NAUKI
(Proceedings of Kazan University. Physics and Mathematics Series)

2024, vol. 166, no. 4, pp. 470–484

ORIGINAL ARTICLE

doi: 10.26907/2541-7746.2024.4.470-484

Quantum and Classical Nondeterministic OBDDs

A.F. Gainutdinova

Kazan Federal University, Kazan, 420008 Russia
E-mail: aida.ksu@gmail.com

Received July 5, 2024; Accepted October 10, 2024

Abstract

A model of nondeterministic ordered binary decision diagrams (NOBDDs) was analyzed. A method for proving a lower bound on the complexity of quantum NOBDDs was developed. Two functions were introduced: one function has linear complexity in the quantum NOBDD but constant complexity in the classical NOBDD, while the other function demonstrates the same complexity in both quantum and classical NOBDD models. The relationships among the complexity classes specific to the OBDD model were described.

Keywords: branching program, ordered binary decision diagram, OBDD, complexity, quantum algorithm, nondeterminism, hierarchy of complexity classes

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

Conflicts of Interest. The authors declare no conflicts of interest.

References

1. Wegener I. *Branching Programs and Binary Decision Diagrams: Theory and Applications*. Ser.: Discrete Mathematics and Applications. Hammer P.L. (Ed.). Philadelphia, PA, Soc. Ind. Appl. Math., 2000. 396 p. <https://doi.org/10.1137/1.9780898719789>.
2. 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 (COCOON 2000): Proc. 6th Annu. Int. Conf. Du D.-Z., Eades P., Estivill-Castro V., Lin X., Sharma A. (Eds.). Ser.: Lecture Notes in Computer Science. Vol. 1858. Berlin, Heidelberg, Springer, 2000, pp. 467–476.* https://doi.org/10.1007/3-540-44968-X_46.

3. Sauerhoff M., Sieling D. Quantum branching programs and space-bounded nonuniform quantum complexity. *Theor. Comput. Sci.*, 2005, vol. 334. nos. 1–3, pp. 177–225. <https://doi.org/10.1016/j.tcs.2004.12.031>.
4. Ablayev F.M., Karpinski M. On the power of randomized branching programs. *Automata, Languages and Programming (ICALP' 96): Proc. 23rd Int. Colloq.* Meyer F., Monien B. (Eds.). Ser.: Lecture Notes in Computer Science. Vol. 1099. Berlin, Heidelberg, Springer, 1996, pp. 348–356. https://doi.org/10.1007/3-540-61440-0_141.
5. Ablayev F., Gainutdinova A., Karpinski M., Moore C., Pollette C. On the computational power of probabilistic and quantum branching program. *Inf. Comput.*, 2005, vol. 203, no. 2, pp. 145–162. <https://doi.org/10.1016/j.ic.2005.04.003>.
6. Ablayev F., Gainutdinova A., Khadiev K., Yakaryılmaz A. Very narrow quantum OBDDs and width hierarchies for classical OBDDs. *Lobachevskii J. Math.*, 2016, vol. 37, no. 6, pp. 670–682. <https://doi.org/10.1134/S199508021606007X>.
7. Gainutdinova A., Yakaryılmaz A. Nondeterministic unitary OBDDs. *Computer Science – Theory and Applications (CSR 2017): Proc. 12th Int. Comput. Sci. Symp. in Russia*. Weil P. (Ed.). Ser.: Lecture Notes in Computer Science. Vol. 10304. Cham, Springer, 2017, pp. 126–140. https://doi.org/10.1007/978-3-319-58747-9_13.
8. Gainutdinova A.F. Comparative complexity of quantum and classical OBDDs for total and partial functions. *Russ. Math.*, 2015, vol. 59, no. 11, pp. 26–35. <https://doi.org/10.3103/S1066369X15110031>.
9. Ablayev F., Gainutdinova A. Complexity of quantum uniform and nonuniform automata. *Developments in Language Theory (DLT 2005): Proc. 9th Int. Conf.* De Felice C., Restivo A. (Eds.). Ser.: Lecture Notes in Computer Science. Vol. 3572. Berlin, Heidelberg, Springer, 2005, pp. 78–87. https://doi.org/10.1007/11505877_7.
10. Nielsen M.A., Chuang I.L. *Quantum Computation and Quantum Information*. Ser.: Cambridge Series on Information and the Natural Sciences. Vol. 2. Cambridge, Cambridge Univ. Press, 2000. 676 p.
11. Kostrikin A.I. *Vvedenie v algebru* [Introduction to Algebra]. Pt. 2: Linear algebra. Moscow, MtsNMO, 2020. 368 p. (In Russian)
12. Ablayev F., Gainutdinova A., Khadiev K., Yakaryılmaz A. Very narrow quantum OBDDs and width hierarchies for classical OBDDs. *Descriptive Complexity of Formal Systems (DCFS 2014): Proc. 16th Int. Workshop*. Jürgensen H., Karhumäki J., Okhotin A. (Eds.). Ser.: Lecture Notes in Computer Science. Vol. 8614. Cham, Springer, 2014, pp. 53–64. https://doi.org/10.1007/978-3-319-09704-6_6.

⟨ **Для цитирования:** Гайнутдинова А.Ф. Квантовые и классические недетерминированные OBDD // Учен. зап. Казан. ун-та. Сер. Физ.-матем. науки. 2024. Т. 166, кн. 4. С. 470–484. <https://doi.org/10.26907/2541-7746.2024.4.470-484>. ⟩

⟨ **For citation:** Gainutdinova A.F. Quantum and classical nondeterministic OBDDs. *Uchenye Zapiski Kazanskogo Universiteta. Seriya Fiziko-Matematicheskie Nauki*, 2024, vol. 166, no. 4, pp. 470–484. <https://doi.org/10.26907/2541-7746.2024.4.470-484>. (In Russian) ⟩