УЧЕНЫЕ ЗАПИСКИ КАЗАНСКОГО ГОСУДАРСТВЕННОГО УНИВЕРСИТЕТА
Том 151, кн. 2 Физико-математические науки *2009*

УДК 519.71

К ВОПРОСУ О СЛОЖНОСТИ КЛАССИЧЕСКОГО МОДЕЛИРОВАНИЯ КВАНТОВЫХ ВЕТВЯЩИХСЯ ПРОГРАММ

Ф.М. Аблаев

Аннотация

В статье рассматриваются синтаксические квантовые ветвящиеся программы (СКВП), вычисляющие булевы функции с большой надежностью. Представляется техника классического детерминированного моделирования СКВП, дается оценка сложности такого моделирования. На примере функции MOD_m показывается, что оценка сложности детерминированного моделирования близка к оптимальной. Предлагаемая техника классического моделирования СКВП дает другое (конструктивное) доказательство включения класса функций, вычислимых СКВП константной ширины в класс сложности NC^1.

Ключевые слова: квантовые алгоритмы, сложность вычислений, ветвящаяся программа.

Введение

Основы теории квантовых вычислений заложены в 80-х годах двадцатого столетия в работах Ю. Манина и Р. Фейнмана [1, 2]. Хорошим введением в проблематику квантовых алгоритмов и квантовых моделей вычислений являются книги [3–6].

Исследования сравнительных возможностей классических и квантовых математических моделей вычислений активно развиваются с начала возникновения теории квантовых вычислений. Ветвящиеся программы – известная модель вычислений. В книге [7] представлен современный взгляд на эту модель вычислений и изложены результаты последних десятилетий по теории и практике ветвящихся программ.

В настоящей работе рассматриваются синтаксические квантовые ветвящиеся программы (СКВП), вычисляющие булевы функции с ограниченной ошибкой. В работе [8] доказано, что класс функций, вычислимых СКВП константной ширины, совпадает с классом сложности NC^1. В обзоре [9] приводятся все необходимые определения и обсуждаются результаты работы [8] и ее расширенного изложения [10].

В статье представляется техника построения классической детерминированной ветвящейся программы (ДВП), вычисляющей ту же функцию, что и исходная СКВП. Предлагаемая техника по СКВП $\mathcal{Q}$ ширины $w(\mathcal{Q})$ (ширина ветвящейся программы – это сложностная характеристика рассматриваемой математической модели) строит ДВП P ширины $w(P) \leq (1+1/\varepsilon)^{2w(\mathcal{Q})}$, где $\varepsilon \in (0, 1/2)$ – показатель надежности вычисления функции программой Q. Эта верхняя оценка на ширину $w(P)$ дает нижнюю оценку $w(\mathcal{Q}) \geq c(\varepsilon)\log w(P)$ на ширину $w(\mathcal{Q})$ СКВП $\mathcal{Q}$, представляющую функцию f. На примере функции MOD_m показывается, что полученная нижняя оценка точна с точностью до мультипликативной константы.

Предлагаемая техника классического моделирования СКВП дает другое (конструктивное) доказательство включения класса функций, вычислимых СКВП константной ширины, в класс сложности NC^1. Неконструктивное доказательство такого включения представлено в [8].

1. Определения и результаты

Приведем необходимые в дальнейшем определения (см. [9]).

1.1. Детерминированная ветвящаяся программа (ДВП) над множеством переменных $X = \{x_1, \ldots, x_n\}$ – это ориентированный ациклический граф, вершины которой делятся на множество внутренних и множество финальных вершин. Финальные вершины не имеют исходящих ребер и помечены нулем или единицей соответственно. Каждой внутренней вершине соответствует переменная $x \in X$, каждая внутренняя вершина имеет два исходящих ребра, помеченные 0 $(x = 0)$ и 1 $(x = 1)$ соответственно. Вычисление ДВП P на двоичном наборе $\sigma = \sigma_1 \ldots \sigma_n$ начинается из выделенной начальной вершины. Если текущей внутренней вершине a соответствует переменная x_j, то осуществляется переход из этой вершины по σ_j-ребру. ДВП P вычисляет булеву функцию $f(X)$, если на каждом входе σ программа P достигает финальной вершины $f(\sigma)$.

Такое задание ДВП будем называть «графовым» заданием ДВП.

Ветвящаяся программа называется *уровневой*, если ее вершины могут быть разбиты на уровни $0, 1, \ldots$ таким образом, что для $i \geq 0$ рёбра из вершин уровня i ведут только в вершины уровня $(i + 1)$.

Ширина $w(P)$ уровневой ветвящейся программы P – это максимум количества вершин на уровне, взятый по всем уровням программы P.

Длина $l(P)$ уровневой ветвящейся программы P – это число уровней программы P.

Уровневая ветвящаяся программа P называется *забывающей*, если на любом уровне P тестируется только одна переменная. Каждая ветвящаяся программа P может быть преобразована (с полиномиальным усложнением) в забывающую ветвящуюся программу P', вычисляющую ту же самую функцию [7].

Определяемая в следующем разделе линейная ветвящаяся программа [8] обобщает понятие забывающей детерминированной программы и является обобщением определяемой далее в статье квантовой ветвящейся программы.

1.2. Линейная ветвящаяся программа (ЛВП) $\mathcal{P}$ над множеством переменных $X = \{x_1, \ldots, x_n\}$ и над d-мерным векторным пространством $\mathbf{V}^d$ есть тройка

$$\mathcal{P} = \langle T, |\mu_0\rangle, F\rangle \ .$$

- Множество $B^d = \{|1\rangle = (1, 0, \ldots, 0),\ \ldots,\ |d\rangle = (0, \ldots, 0, 1)\}$ базисных векторов будем называть базисными состояниями ЛВП.

- Вектора $|\mu\rangle = \sum_{i=1}^{d} z_i |i\rangle$ пространства $\mathbf{V}^d$ будем называть состояниями.

- Преобразования состояний $\mathcal{P}$ определяются последовательностью $T = (T_1, \ldots, T_\ell)$ (длины ℓ) инструкций. Каждая инструкция T_i – это тройка $T_i = \{j_i, M_{j_i}(0), M_{j_i}(1)\}$, где j_i определяет переменную x_{j_i}, считываемую на шаге i, $M_{j_i}(0)$ и $M_{j_i}(1)$ – это $(d \times d)$-матрицы – линейные преобразования векторного пространства $\mathbf{V}^d$.

- $|\mu_0\rangle$ – начальное состояние программы $\mathcal{P}$.
- $F \subseteq B^d$ – подмножество базисных состояний, элементы которого будем называть принимающими состояниями. Элементы множества $\bar{F} = B^d \backslash F$ будем называть отвергающими состояниями. Через Accept и Reject будем обозначать множества индексов принимающих и отвергающих состояний соответственно: $\text{Accept} = \{i : |i\rangle \in F\}$ и $\text{Reject} = \{i : |i\rangle \in \bar{F}\}$.

Вычисление программы $\mathcal{P}$ на входе $\sigma = \sigma_1 \dots \sigma_n \in \{0,1\}^n$ определяется следующим образом:

1) вычисление $\mathcal{P}$ начинается из начального состояния $|\mu_0\rangle$;

2) на i-м шаге вычисления $\mathcal{P}$ применяется инструкция T_i: если $x_{j_i} = \sigma_{j_i}$, то к текущему состоянию μ применяется преобразование $M_{j_i}(\sigma_{j_i})$ и программа $\mathcal{P}$ переходит в состояние $|\mu'\rangle = M_{j_i}(\sigma_{j_i})|\mu\rangle$ (состояния программы представляются в виде вектор-столбцов);

3) финальным состоянием (состоянием после последнего шага ℓ) будет состояние

$$|\mu(\sigma)\rangle = \prod_{i=\ell}^{1} M_{j_i}(\sigma_{j_i})|\mu_0\rangle \ .$$

Определенная выше линейная программа является забывающей и имеет $\ell + 1$ уровень. Нумерация уровней начинается с нуля, последний (финальный) уровень имеет номер ℓ.

Шириной $w(\mathcal{P})$ ЛВП $\mathcal{P}$ будем называть размерность d пространства $\mathbf{V}^d$ состояний $\mathcal{P}$, а число ℓ – длиной $l(\mathcal{P})$ программы $\mathcal{P}$.

Теперь забывающую ДВП можно определить следующим образом.

1.3. Линейное представление забывающей ДВП. Забывающая ДВП – это ЛВП над векторным пространством $\mathbb{F}^d$, где $\mathbb{F}$ – подходящее конечное поле. Множеством состояний такой ЛВП является множество B^d базисных состояний. Матрицы преобразований M задают преобразования множества B^d.

Входной набор σ принимается, если $|\mu(\sigma)\rangle \in F$.

1.4. Квантовая ветвящаяся программа (КВП) – это ЛВП над комплекснозначным гильбертовым d-мерным пространством $\mathcal{H}^d$. Состояниями КВП $\mathcal{Q}$ являются вектора $|\psi\rangle = \sum_{i=1}^{d} z_i|i\rangle$ с единичной нормой

$$\| \, |\psi\rangle \, \| = \sqrt{\sum_{i=1}^{d} |z_i|^2} = 1.$$

Они называются чистыми состояниями или просто состояниями КВП. Преобразования КВП задаются комплекснозначными унитарными $d \times d$ матрицами.

Если $|\psi(\sigma)\rangle = \sum_{i=1}^{d} z_i|i\rangle$ – финальное состояние КВП после считывания входа σ, то вероятность $p_{acc}(\sigma)$ принятия входа σ программой P определяется как

$$p_{\text{acc}}(\sigma) = \sum_{i \in \text{Accept}} |z_i|^2.$$

Определение 1. Пусть $\varepsilon > 0$. Говорят, что КВП $\mathcal{Q}$ вычисляет функцию f с надежностью $1/2 + \varepsilon$, если для $\sigma \in f^{-1}(1)$ выполняется неравенство $p_{\text{acc}}(\sigma) \geq 1/2 + \varepsilon$, а для $\sigma' \in f^{-1}(0)$ – неравенство $p_{\text{acc}}(\sigma) \leq 1/2 - \varepsilon$.

1.5. Синтаксические вероятностные и квантовые ветвящиеся программы. Из определения КВП, представляющей функцию с надежностью $1/2+\varepsilon$, следует, что финальные состояния (состояния ℓ-ого уровня) программы, достижимые на входных наборах σ из $\{0,1\}^n$ разбиваются на два множества

$$\mathcal{A} = \{|\psi(\sigma)\rangle : p_{\text{acc}}(\sigma) \geq 1/2+\varepsilon\} \quad \text{и} \quad \mathcal{R} = \{|\psi(\sigma)\rangle : p_{\text{acc}}(\sigma) \leq 1/2-\varepsilon\}.$$

Из этого следует, что расстояние $\rho(\mathcal{A},\mathcal{R})$ между множествами $\mathcal{A}$ и $\mathcal{R}$ оценивается снизу некоторой константой $\theta(\varepsilon)$. (Расстояние между множествами определяется стандартно на основе метрики $\rho(|\psi\rangle,|\psi'\rangle) = \| \, |\psi\rangle - |\psi'\rangle \, \|$).

В этом случае будем говорить, что множества $\mathcal{A}$ и $\mathcal{R}$ *изолированы*. В случае много раз читающих ветвящихся программ могут возникать *фиктивные состояния* (состояния, не достижимые при вычислениях на входных наборах). При этом фиктивные финальные состояния могут «разрушить» свойство изолированности множеств $\mathcal{A}$ и $\mathcal{R}$.

Определение 2. СКВП – это программы, множество всех финальных состояний (достижимых и фиктивных) которых разбивается на два изолированных множества.

Непосредственно из определения 2 следует, что все финальные состояния $|\psi\rangle = (z_1,\ldots,z_d)$ (достижимые и фиктивные) СКВП $\mathcal{Q}$ разбиваются на два множества

$$[\mathcal{A}] = \left\{ |\psi\rangle : \sum_{i\in \text{Accept}} |z_i|^2 \geq 1/2+\varepsilon \right\} \quad \text{и} \quad [\mathcal{R}] = \left\{ |\psi\rangle : \sum_{i\in \text{Accept}} |z_i|^2 \leq 1/2-\varepsilon \right\}.$$

Отметим, что квантовая модель один раз читающей ветвящейся программы (каждая переменная на каждом пути вычисления может читаться только один раз), вычисляющая функцию f с надежностью $1/2+\varepsilon$, является синтаксической.

Теорема 1. *Пусть функция f вычислима СКВП $\mathcal{Q}$ с надежностью $1/2+\varepsilon$. Тогда f вычислима ДВП P, для которой выполняется равенство*

$$l(P) = l(\mathcal{Q}) = \ell$$

и

$$w(P) \leq \left(1+\frac{1}{\varepsilon}\right)^{2w(\mathcal{Q})}.$$

Доказательство теоремы 1 приводится в следующем разделе.

Положим $w(f) = \min\{w(P)\}$, где минимум берется по всем ДВП P, вычисляющих функцию f. Непосредственно из теоремы 1 следует нижняя оценка на $w(\mathcal{Q})$.

Свойство 1. Если функция f вычислима СКВП $\mathcal{Q}$ с надежностью $1/2+\varepsilon$, тогда

$$w(\mathcal{Q}) \geq c(\varepsilon)\log w(f)^{1}.$$

Реализация функции MOD_m в один раз читающих моделях ДВП и СКВП (в этом случае СКВП есть в точности КВП) показывает, что нижняя оценка свойства 1 точна с точностью до мультипликативной константы. ($\text{MOD}_m(\sigma) = 1$ тогда и только тогда, когда число единиц в наборе σ кратно m.)

[1] Все логарифмы в данной работе берутся по основанию 2.

Легко проверяется [10], что для произвольной один раз читающей ДВП P, вычисляющей MOD_m, выполняется неравенство $w(P) \geq m$.

С другой стороны, для простых чисел p в [10] приводится один раз читающая КВП $\mathcal{Q}$, вычисляющая MOD_p с надежностью $1/2 + \varepsilon$, для которой выполняется равенство $w(\mathcal{Q}) = O(\log p)$.

2. Доказательство теоремы 1

Доказательство теоремы состоит из двух этапов. На первом этапе по СКВП $\mathcal{Q}$ строится ДВП DP экспоненциальной (от ℓ) ширины, вычисляющая ту же функцию f. На втором этапе по ДВП DP строится искомая ДВП P.

2.1. Первый этап (построение ДВП DP). Вычисление программы $\mathcal{Q}$ на наборах $\sigma \in \{0,1\}^n$ – это ℓ-шаговые линейные преобразования состояний, начинающиеся с начального состояния $|\psi_0\rangle$. Все возможные вычисления программы $\mathcal{Q}$ на входных наборах из $\{0,1\}^n$ представляются $(\ell+1)$-уровневой забывающей ДВП DP, задаваемой в виде полного $(\ell+1)$-уровневого бинарного дерева. Вершины программы DP помечаются состояниями $|\psi\rangle$ программы $\mathcal{Q}$. Уровень 0 содержит начальную вершину DP, помеченную начальным состоянием $|\psi_0\rangle$ программы $\mathcal{Q}$. Уровень $i \in \{0,\ldots,\ell\}$ представляет из себя i-й шаг вычисления. Из каждой вершины $|\psi\rangle$ уровня i, $i \in \{0,\ldots,\ell-1\}$, исходят два ребра, помеченные $x_{j_i} = 0$ и $x_{j_i} = 1$, где x_{j_i} – переменная, считываемая на шаге i. Ребро $x_{j_i} = \gamma$ ведет из вершины $|\psi\rangle$ уровня i в вершину $|\psi'\rangle$ уровня $i+1$, если СКВП $\mathcal{Q}$, находясь на шаге i в состоянии $|\psi\rangle$, переходит в состояние $|\psi'\rangle$ при считывании $x_{j_i} = \gamma$.

Вершины ℓ-го уровня являются финальными. Финальные вершины $|\psi\rangle \in [\mathcal{A}]$ дополнительно помечаются единицей (принимающие вершины программы DP), а вершины $|\psi\rangle \in [\mathcal{R}]$ дополнительно помечаются нулем (отвергающие вершины программы DP).

Непосредственно из описания программы DP следует

Свойство 2. ДВП DP вычисляет ту же функцию f, что и СКВП $\mathcal{Q}$, и имеет следующие характеристики: $l(DP) = \ell$ и $w(DP) = 2^\ell$.

2.2. Метрические свойства ДВП DP. Следующие понятия и факты теории метрических пространств приведены в книге [11]. Пусть $\mathcal{M}$ – это метрическое пространство с метрикой ρ. Говорят, что точки μ, μ' из $\mathcal{M}$ связаны θ-цепью, если существует конечное множество $\mu_1, \mu_2, \ldots, \mu_m$ точек из $\mathcal{M}$ таких, что $\mu_1 = \mu, \mu_m = \mu'$ и $\rho(\mu_i, \mu_{i+1}) < \theta$ для $i \in \{1,\ldots,m-1\}$. Подмножество $\mathcal{C} \subseteq \mathcal{M}$ называется θ-компонентой, если произвольные две точки $\mu, \mu' \in \mathcal{C}$ связаны θ-цепью.

Обозначим через Ψ_i, $i \in \{0,\ldots,\ell\}$, множество всех состояний (вершин) программы DP уровня i. На множестве Ψ_i определим метрику ρ по формуле $\rho(|\psi\rangle, |\psi'\rangle) = \| \, |\psi\rangle - |\psi'\rangle \, \|$. Для $\theta > 0$ число θ-компонент множества Ψ_i, $i \in \{0,\ldots,l\}$, зависит от строения множества Ψ_i (может оказаться, что все множество Ψ_i представляет собой одну θ-компоненту). Следующее свойство дает верхнюю оценку числа возможных θ-компонент множества Ψ_i.

Свойство 3. Для $i \in \{0,\ldots,\ell\}$, $\theta > 0$ число t_i θ-компонент множества Ψ_i оценивается сверху величиной

$$t_i \leq \left(1 + \frac{2}{\theta}\right)^{2w(\mathcal{Q})}.$$

Доказательство. Обозначим через $\mathcal{C}_i$ множество всех θ-компонент множества Ψ_i. В каждой θ-компоненте $C \in \mathcal{C}_i$ выберем одну точку $|\alpha\rangle \in C$. Если

рассмотреть сферы радиуса $\theta/2$ с центрами в таких точках $|\alpha\rangle \in C$, тогда все эти сферы попарно не пересекаются и могут иметь общие точки лишь на границах. Все эти сферы находятся в большей сфере радиуса $1+\theta/2$ с центром в $|(0,0,\ldots,0)\rangle$. Объем сферы радиуса r в комплексном пространстве $\mathcal{H}^d$ is равен cr^{2d} (в комплекснозначном пространстве $\mathcal{H}^d$ каждая точка $|\alpha\rangle$ имеет размерность $2d$). Константа c зависит от используемой метрики пространства $\mathcal{H}^d$. Таким образом, имеем

$$t_i \le \frac{c\left(1+\dfrac{\theta}{2}\right)^{2d}}{c\left(\dfrac{\theta}{2}\right)^{2d}} = \left(1+\frac{2}{\theta}\right)^{2w(\mathcal{Q})}.$$

□

На каждом уровне $i \in \{0,\ldots,\ell-1\}$ преобразования состояний $|\psi\rangle$ программы DP задаются унитарной $(d\times d)$-матрицей, которая определяется значением γ считываемой переменной x_{j_i}. Для подмножества $D \subseteq \Psi_i$ и унитарной $(d\times d)$-матрицы M положим $D' = \{|\psi'\rangle : |\psi'\rangle = M|\psi\rangle, |\psi\rangle \in D\}$ (множество $D' = M(D)$ – образ D для преобразования M). Следующее утверждение показывает, что программа DP сохраняет свойство принадлежности состояний одной θ-компоненте при унитарных преобразованиях.

Свойство 4. Для ДВП DP, для $i \in \{0,\ldots,\ell-1\}$, $\theta > 0$, для произвольной θ-компоненты C множества Ψ_i и произвольной унитарной $(d\times d)$-матрицы M множество $M(C)$ является подмножеством некоторой θ-компоненты C' множества Ψ_{i+1}.

Доказательство. Унитарное преобразование сохраняет расстояние ρ между векторами. Следовательно, если состояния $|\psi\rangle$ и $|\mu\rangle$ входят в одну θ-компоненту $C \in \mathcal{C}_i$, то их образы $|\psi'\rangle = M|\psi\rangle$ и $|\mu'\rangle = M|\mu\rangle$ входят в одну θ-компоненту $C' \in \mathcal{C}_{i+1}$. □

Следующее утверждение показывает, что для $\theta = 2\varepsilon$ множество $[\mathcal{A}]$ принимающих вершин и множество $[\mathcal{R}]$ отвергающих вершин программы DP являются объединениями θ-компонент множества Ψ_ℓ состояний уровня ℓ.

Свойство 5. Пусть $\mathcal{C}_\ell = \{C_1,\ldots,C_t\}$ – это множество θ-компонент Ψ_ℓ для $\theta = 2\varepsilon$. Тогда

$$[\mathcal{A}] = \bigcup_{i\in I} C_i \quad \text{и} \quad [\mathcal{R}] = \bigcup_{i\in J} C_i,$$

где $I \cup J = \{1,\ldots,t\}$ и $I \cap J = \emptyset$.

Доказательство. В силу определения ДВП DP имеем, что множество Ψ_ℓ состояний уровня ℓ разбивается на множество $[\mathcal{A}]$ принимающих вершин и множество $[\mathcal{R}]$ отвергающих вершин программы DP. Покажем, что для произвольной θ-компоненты $C \in \mathcal{C}_\ell$ выполняется одно из двух включений $C \subseteq [\mathcal{A}]$ или $C \subseteq [\mathcal{R}]$. Для этого достаточно показать отсутствие θ-цепей между точками множеств $[\mathcal{A}]$ и $[\mathcal{R}]$, то есть что для произвольных $|\psi\rangle \in [\mathcal{A}]$ и $|\psi'\rangle \in [\mathcal{R}]$ справедливо соотношение

$$\rho(|\psi\rangle, |\psi'\rangle) \ge \theta = 2\varepsilon. \tag{1}$$

Пусть $|\psi\rangle = (z_1,\ldots,z_d)$ и $|\psi'\rangle = (z'_1,\ldots,z'_d)$. Тогда имеем

$$2\varepsilon \le \sum_{i\in \mathrm{Accept}} (|z_i|^2 - |z'_i|^2) = \sum_{i\in \mathrm{Accept}} (|z_i| - |z'_i|)(|z_i| + |z'_i|) \le \sum_{i\in \mathrm{Accept}} (|z_i - z'_i|)(|z_i| + |z'_i|).$$

Аналогично предыдущему имеем

$$2\varepsilon \le \sum_{i\in\mathrm{Reject}} (|z_i'|^2 - |z_i|^2) = \sum_{i\in\mathrm{Reject}} (|z_i'| - |z_i|)(|z_i| + |z_i'|) \le \sum_{i\in\mathrm{Reject}} (|z_i - z_i'|)(|z_i| + |z_i'|).$$

Объединяя два этих неравенства, получаем

$$4\varepsilon \le \sum_{i=1}^{d} (|z_i - z_i'|)(|z_i| + |z_i'|). \tag{2}$$

Применяя неравенство Коши–Буняковского $\left(\sum_{i=1}^{d} a_i b_i \le \sqrt{\sum_{i=1}^{d} a_i^2}\sqrt{\sum_{i=1}^{d} b_i^2}\right)$, из (2) получаем

$$4\varepsilon \le \| \, |\psi\rangle - |\psi'\rangle \, \| \sqrt{\sum_{i=1}^{d} (|z_i| + |z_i'|)^2}.$$

Из неравенства Коши–Буняковского также непосредственно следует, что

$$\sqrt{\sum_{i=1}^{d} (|z_i| + |z_i'|)^2} \le \| \, |\psi\rangle \, \| + \| \, |\psi'\rangle \, \| = 2$$

Два последних неравенства доказывают (1). □

2.3. Второй этап (построение ДВП P). Построение искомой ДВП P основывается на свойствах предыдущего раздела. Положим $\theta = 2\varepsilon$. Программа P – это $(\ell+1)$-уровневая забывающая ветвящаяся программа. На уровне j считывается переменная x_{i_j} (как в программе DP). Вершинам уровня j соответствуют θ-компоненты из $\mathcal{C}_j$. Из вершины $C \in \mathcal{C}_j$ ребро, помеченное $x_{i_j} = \gamma$, ведет в вершину $C' \in \mathcal{C}_{j+1}$, если $M_j(\gamma)(C) \subseteq C'$. Вершина $C \in \mathcal{C}_\ell$ последнего уровня ℓ дополнительно помечается единицей (нулем), если $C \subseteq [\mathcal{A}]$ $(C \subseteq [\mathcal{R}])$.

Из описания ДВП P следует, что P вычисляет ту же функцию f, что и ДВП DP, и ее ширина $w(P)$ оценивается сверху:

$$w(P) \le \max_{0\le i\le \ell} |\mathcal{C}_i| \le \left(1 + \frac{1}{\varepsilon}\right)^{2w(\mathcal{Q})}.$$

Теорема 1 доказана.

Заключение

Класс сложности NC^1 (см., например, [12]) содержит в себе все булевы функции $f(x_1, \ldots, x_n)$, вычислимые схемами из функциональных элементов полиномиальной сложности глубины $O(\log n)$. Класс NC^1 входит в класс P. Вопрос о собственном включении $NC^1 \subsetneqq P$ является открытой проблемой.

Обозначим через BP_w множество булевых функций, вычислимых ветвящимися программами полиномиальной (от числа переменных функции) сложности и ширины w. Положим $BP_{\mathrm{const}} = \cup_{w\ge 1} BP_w$. Обозначим через $SQBP_w$ класс сложности, содержащий булевы функции, вычислимые синтаксическими квантовыми ветвящимися программами полиномиальной сложности и ширины w.

В работе [8] показано, что уже в случае ширины 2 квантовые ветвящиеся программы обладают большими вычислительными возможностями: $SQBP_2 = NC^1$.

Доказательство этого факта основано на соотношении $BP_{\text{const}} = BP_5 = NC^1$, установленного в [12], а именно: в [8] доказываются два включения

$$BP_5 \subseteq SQBP_2 \quad \text{и} \quad SQBP_w \subseteq BP_{\text{const}}.$$

Доказательство Теоремы 1 дает конструктивный метод доказательства второго включения $SQBP_w \subseteq BP_{\text{const}}$, то есть по СКВП $\mathcal{Q}$ ширины const, вычисляющей булеву функцию f с надежностью $1/2+\varepsilon$, мы строим ДВП P ширины $\text{const}' \leq (1+ + 1/\varepsilon)^{2\text{const}}$, вычисляющую ту же функцию f.

Summary

F.M. Ablayev. On Complexity of Classical Simulation of Quantum Branching Programs.

The paper considers syntactical quantum branching programs that compute Boolean functions with bounded error. Classical simulation technique is presented for such quantum programs and complexity of such simulation is estimated. The estimation of simulation complexity is shown to be close to optimal on the example of MOD_m function.

Classical simulation technique for quantum programs presents constructive approach for proving inclusion of class of functions, computed with bounded error by syntactical quantum branching programs, into the complexity class NC^1.

Key words: quantum algorithms, simulation complexity, branching program.

Литература

1. *Манин Ю.И.* Вычислимое и невычислимое. – М.: Сов. радио, 1980. – 128 с.
2. *Feynman R.* Simulating physics with computers // Int. J. Theor. Phys. – 1982. – V. 21, No 6, 7. – P. 467–488.
3. *Валиев К.А., Кокин А.А.* Квантовые компьютеры: надежды и реальность. – Ижевск: НИЦ «Регулярная и хаотическая динамика», 2001. – 352 с.
4. *Китаев А., Шень А., Вялый М.* Классические и квантовые вычисления. – М.: МЦНМО, ЧеРО, 1999. – 192 с.
5. *Ожигов Ю.И.* Квантовые вычисления. – М.: Изд-во фак. ВМиК Моск. ун-та, 2003. – 104 с.
6. *Nielsen M.A., Chuang I.L.* Quantum Computation and Quantum Information. – Cambridge: Cambridge Univ. Press, 2000. – 676 p.
7. *Wegener I.* Branching Programs and Binary Decision Diagrams. – Philadelphia: Society for Industrial and Applied Mathematics, 2000. – 408 p.
8. *Ablayev F., Moore C., Pollett C.* Quantum and Stochastic Branching Programs of Bounded Width // Proc. of the Intern. Colloquium on Automata, Languages and Programming (ICALP'2002). Lecture Notes in Computer Science. – Berlin: Springer-Verlag, 2002. – P. 343–354.
9. *Аблаев Ф.М.* О сложности классических и квантовых моделей вычислений // Матем. вопр. кибернетики. – 2004. – № 13. – С. 137–146.
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. – V. 203. – P. 145–162.
11. *Александров П.С.* Введение в теорию множеств и общую топологию. – М.: Наука, 1977. – 368 с.

12. *Баррингтон Д.* Ветвящиеся программы ограниченной ширины, имеющие полиномальную сложность, распознают в точности языки из NC^1 // Киберн. сб. – 1991. – Вып. 28.– С. 94–113.

Поступила в редакцию
30.03.09

Аблаев Фарид Мансурович – доктор физико-математических наук, профессор, заведующий кафедрой теоретической кибернетики Казанского государственного университета.

E-mail: *fablayev@gmail.com*