УДК 519.7

МЕТОД ОТПЕЧАТКОВ В КВАНТОВЫХ ВЫЧИСЛЕНИЯХ

Машимов Наурызбай Кенесариевич
nauzik@mail.ru
Докторант кафедры математического и компьютерного моделирования ЕНУ им. Л.Н.Гумилева, Нур-Султан, Казахстан
Научный руководитель – Сергибаев Р.А.

Задача физической реализации полномасштабного квантового вычислителя — открытаяпроблема для современной технологии. Дальнейшее уменьшение масштабов при производстве электронных схем приведет к тому, что функционирование их компонент будет происходить по законам квантовой механики. Поэтому по мере развития квантовых нанотехнологий в классические компьютеры будут включаться квантовые компоненты и отдельные модули.

При преодолении современных технологических трудностей построенияквантовых вычислительных систем квантовые технологии откроют возможности реализации массивного распараллеливания вычислений, известного как квантовый параллелизм.Один из первых эффективных квантовых алгоритмов (полиномиальный квантовый алгоритм факторизации числа [1]) продемонстрировал потенциальные преимущества квантовых моделей вычислений для ряда задач по сравнению с классическими.

Помимо физических проблем в области исследований и разработок квантовых моделей вычислений требуют своего разрешения серьезные математические вопросы. Важнойоткрытой математической проблемой является описание класса задач, решаемых на квантовых моделях вычислений более эффективно, чем на классических.

Метод отпечатков позволяет представлять объекты их образами (отпечатками), значительно более компактными, чем оригиналы. Кроме того, они позволяют достаточно достоверно извлекать информацию о входной информации. Техника отпечатков [1] дает

возможность строить оптимальный коммуникационный протокол в некоторой трехсторонней модели SMP для определения тождества двух двоичных наборов.

В данной работе мы применим технику отпечатков, адаптированную для квантовых ветвящихся программ. Она представлена в работе [2], тем самым обобщая построения в данной работе. Разработанный метод применяется для построения оптимальной КВП (квантовой ветвящейся программы), вычисляющей булеву функцию MOD_m. Показано, что этот подход для проблемы равенства в модели SMP приводит к результату, аналогичному результату из [1].

Метод отпечатков обладает следующими свойствами.

– Он ориентирован на модели с классическим управлением, а значит, и на КВП.

– Образы входных слов легко построить, используются только контролируемые вращения вокруг оси $\hat{y}$ сферы Блоха на различные углы и преобразования Адамара[3].

– Гарантирует существование хорошего множества параметров, этопозволяет ограничить вероятность ошибки сверху некоторой константой $0 < \varepsilon < 1$.

Техника отпечатков. Для решаемой задачи выбираются целое $m \geq 2$ и допустимаявероятность ошибки $\varepsilon > 0$. Затем фиксируется

$$t_\varepsilon = \left[\frac{2}{\varepsilon} \ln 2m \right],$$

где $[A]$ есть целая часть числа A, затем строится отображение

$$g : \{0, 1\}^n \to Z,$$

описывающее некоторое свойство входного набора.

Рассмотрим некоторое применение техники отпечатков. Для произвольного двоичного набора $\sigma = \sigma_1 ... \sigma_n$ порождается ее отпечаток $|h_\sigma\rangle$,объединяющий в себе t_ε однокубитных отпечатков $\left|h_\sigma^i\right\rangle$:

$$\left|h_\sigma^i\right\rangle = \cos\frac{2\pi k_i g(\sigma)}{m}|0\rangle + \sin\frac{2\pi k_i g(\sigma)}{m}|1\rangle,$$

$$|h_\sigma\rangle = \frac{1}{\sqrt{t_\varepsilon}} \sum_{i=1}^{t_\varepsilon} |i\rangle \left|h_\sigma^i\right\rangle,$$

т.е. последний кубит в квантовом регистре поворачивается на t_ε, различных углов (вокруг оси $\hat{y}$ сферы Блоха), определяемых параметрами $k_i \in \{1, ..., m-1\}$.

Метод отпечатков направлен на достоверное распознавание равенства нулю значения $g(\sigma)$. Для этой цели параметры $k_i \in \{1, ..., m-1\}$ для всех $i = 1, ..., t_\varepsilon$ выбираются специальным образом, исходя из следующего определения.

Определение. Множество $K = \{k_1, ..., k_t\}$ называется хорошим для целого числа $b \neq 0 \bmod m$, если

$$\frac{1}{t_\varepsilon^2} \left(\sum_{i=1}^{t_\varepsilon} \cos\frac{2\pi k_i b}{m} \right)^2 < \varepsilon.$$

Левая часть неравенства соответствует квадрату амплитуды базисного состояния $|0\rangle^{\otimes \log t}|0\rangle$ после применения оператора $H^{\otimes \log t} \otimes I$ к отпечатку $|h_\sigma\rangle$. Применительно к нашим алгоритмам такое множество гарантирует, что вероятность ошибки будет ограничена константой, меньшей 1.

Следующая лемма утверждает существование хорошего множества и развивает идеи соответствующего утверждения из [2].

Лемма. Существует множество K, где $|K| = t = \lceil (2/\varepsilon) \ln 2m \rceil$ ($|A|$ означает мощность множества A), которое является хорошим для всех целых $b \neq 0 \bmod m$.

Вычисление функции MOD_m методом отпечатков. Рассмотрим булеву функцию MOD_m: на входном наборе информации $\sigma = \sigma_1 ... \sigma_n \in \{0, 1\}^n$ она равна единице тогда и только тогда, когда число единиц в наборе σ кратно m, где $m > 2$ — целое число.

Теорема. Для любого $\varepsilon \in (0, 1)$ существует $O(\log\log m)$ - кубитная QOBDD P (один раз читающая $O(\log\log m)$-кубитная КВП), вычисляющая функцию MOD_m с односторонней ошибкой ε.

В данном алгоритме полагается, что

$$g(x) = \sum_{i=1}^{n} x_i ,$$

а параметр m равен модулю в определении MOD_m. Заметим, что число кубит, используемых данной конструкцией, равно

$$q = \log t + 1 = O(\log\log m),$$

а ширина программы есть $2^q = (\log m)$.Этот результат асимптотически оптимален в силу того, что любая детерминированная OBDD для MOD_m требует ширины $\Omega(m)$.

Список использованных источников

1. Buhrman H., Cleve R., Watrous J., Wolf R., Quantum fingerprinting. Phys. Rev. Lett. (2001) 87 (16), 167902.

2. Ambainis A., Nahimovs N., Improved constructions of quantum automata.Lect. Notes Comput. Sci.(2008) 5106, 47–56.

3. Nielsen M. A., Chuang I. L., Quantum computation and quantum information. Cambridge University Press, Cambridge, 2000.