О СЛОЖНОСТИ КВАНТОВОГО АЛГОРИТМА САЙМОНА

К.В. Антонов

Алгоритм Саймона решает задачу нахождения периода периодической булевой функции. Сама функция представлена в виде «чёрного ящика», обращение к которому меняет состояния кубитов. Под сложностью понимается число обращений к «чёрному ящику», которое равно числу шагов алгоритма до нахождения периода. Алгоритм Саймона является вероятностным, поэтому для определения сложности считается математическое ожидание числа шагов.

Булева функция $f(x)\colon\{0,1\}^n \to \{0,1\}$ называется периодической с периодом $p \in \{0,1\}^n$, $p \neq \mathbf{0}$, если $\forall x \in \{0,1\}^n\ f(x) = f(x \oplus p)$. Символом $\oplus$ обозначается побитовое сложение по модулю 2.

Подробно алгоритм Саймона описан в [1]. Далее будем считать, что все рассматриваемые векторы лежат в векторном пространстве $\mathbb{Z}_2^n$. С помощью квантовой схемы на -м шаге алгоритм находит случайный вектор $y^i \in \{0,1\}^n$, ортогональный периоду p, в соответствии с равномерным распределением. Это значит, что для найденного вектора и периода верно равенство

$$p_1 y_1^i \oplus \ldots \oplus p_n y_n^i = 0.$$

Все такие равенства составляют СЛАУ над $\mathbb{Z}_2$. Алгоритм считается завершённым, когда на очередном шаге система имеет единственное ненулевое решение.

Все векторы $y \perp p$ составляют ортогональное дополнение к линейной оболочке $\langle p\rangle$, их количество равно 2^{n-1}, так как $\dim\langle p\rangle^\perp = n-1$. В процессе выполнения алгоритма составляем линейную оболочку всех полученных векторов $Y_i = \langle y^1, \ldots, y^i\rangle$. Изначально $Y_0 = \{\mathbf{0}\}$. Ясно, что $p \in Y_i^\perp$, т. к. $p \in \langle y^j\rangle^\perp\ \forall j$. На -м шаге либо $\dim Y_i = \dim Y_{i-1}$, если был получен вектор $y^i \in Y_{i-1}$, либо $\dim Y_i = \dim Y_{i-1} + 1$, если был найден «новый» вектор $y^i \in \langle p\rangle^\perp \setminus Y_{i-1}$.

Пусть $\dim Y_i = k$. Тогда «новых» векторов остаётся ровно $|\langle p\rangle^\perp \setminus Y_i| = 2^{n-1} - 2^k$. Вероятность получения «нового» вектора равна

$$p_k = \frac{2^{n-1} - 2^k}{2^{n-1}} = 1 - 2^{k+1-n}.$$

Таким образом, алгоритм завершает работу, когда $\dim Y_i = n-1$ и $Y_i^\perp = \{\mathbf{0}, p\}$.

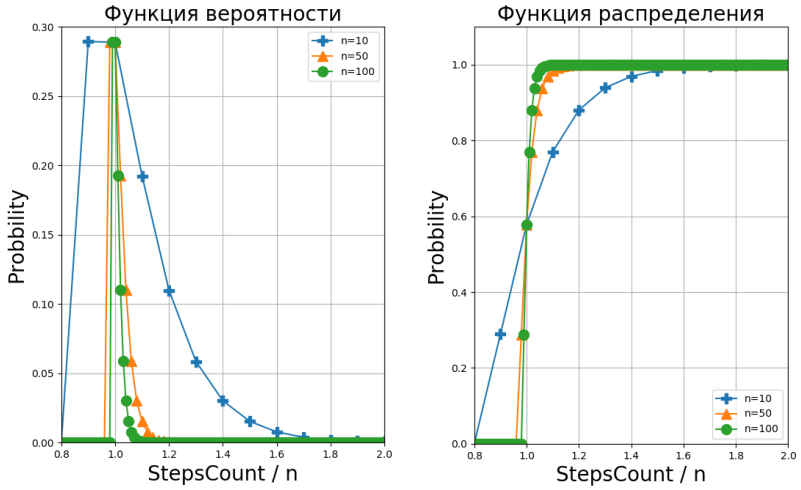
Рассмотрим все шаги алгоритма, перед началом которых $\dim Y_i = k$. На каждом таком шаге проводится испытание Бернулли с вероятностью успеха p_k и вероятностью неудачи $q_k = 1 - p_k$. Успех означает переход к такому Y_j на следующем шаге, что $\dim Y_j = k+1$. Введём случайную величину m_k, равную числу испытаний до первого успеха. $r_{k,s} = q_k^{s-1} p_k$ – вероятность того, что $m_k = s$ $(s \in \mathbb{N})$, $\mathrm{E}[m_k] = 1/p_k$ – матожидание m_k, $m = m_0 + \cdots + m_{n-2}$ – общее число шагов алгоритма. Определим формальные ряды

$$R_k(x) = \sum_{s=1}^{\infty} r_{k,s} x^s,$$

$$R(x) = \prod_{k=0}^{n-2} R_k(x) = \sum_{s=1}^{\infty} r_s x^s.$$

Лемма. Вероятность того, что общее число шагов алгоритма составит s, равна коэффициенту при x^s в ряде $R(x)$. Т. е. $\Pr(m = s) = r_s$.

Для вычисления коэффициентов ряда $R(x)$ при различных значениях n использован компьютер. Результаты вычислений представлены на графиках.



Литература

1. Simon, D.R. (1994) On the power of quantum computation // Foundations of Computer Science 1994 Proceedings, 35th Annual Symposium, P. 116–123.