Теорема. *При любом $a \geqslant 2$ и ограничении на кратность $k \leqslant \frac{2^n}{n^a}$ верно:*

$$2^n(a-1)\log(n) - O(2^n) \leqslant A_R(\overrightarrow{Q}_n, \frac{2^n}{n^a}) \leqslant 2^n a \log(n) + O(2^n)$$

Список литературы

1. Кравцов С. С. О реализации функций алгебры логики в одном классе схем из функциональных и коммутационных элементов // Проблемы кибернетики. М.: Наука. — 1967. — Т. 19 — С. 285—292.

2. Альбрехт А. О схемах из клеточных элементов // Проблемы кибернетики. М.: Наука. — 1975. — Т. 33 —С. 209—214.

3. Thompson C. D. A complexity theory for VLSI. —1980.

4. Bilardi G., Pracchi M., Preparata F. A critique of network speed in VLSI models of computation // Solid-State Circuits, IEEE Journal of. — 1982. — Т. 17. — С. 696–702..

5. Ложкин С. А., Зизов В. С. Уточненные оценки сложности дешифратора в модели клеточных схем из функциональных и коммутационных элементов // Учен. зап. Казан. ун-та. Сер. Физ.-матем. науки. —2020. — Т. 162, №3. — С. 322–334..

6. Ложкин С. А. Оценки высокой степени точности для сложности управляющих систем из некоторых классов // Математическиевопросы кибернетики. — М.: Наука, Физматлит. — 2005. — Т. 6.

DOI: 10.20948/dms-2022-12

НИЖНЯЯ ОЦЕНКА КВАНТОВОЙ ЗАПРОСНОЙ СЛОЖНОСТИ ПОРАЗРЯДНОЙ СОРТИРОВКИ

М. Т. Зиятдинов (Казань)

Развитие квантовых технологий делает возможным использование квантовых алгоритмов, которые до этого имели только теоретический интерес. В то же время, в теории квантовых вычислений остаётся много нерешённых вопросов, в частности, нижние оценки сложности квантовых решений различных задач. Одной из мер сложности квантовых алгоритмов является запросная сложность. Она измеряет, сколько нужно сделать запросов к оракулу входных данных для решения задачи.

Как известно [1], в классическом случае для сортировки n элементов массива требуется $\Theta(n \log n)$ попарных сравнений. Этот же результат справедлив и в квантовом случае [2]: для сортировки требуется $\Omega(n \log n)$ попарных сравнений. Если же доступны не только попарные сравнения, возможно, например, использовать поразрядную сортировку, которая выполняется за $\Theta(nl)$ шагов для сортировки n последовательностей из l цифр. Данная работа посвящена нижней оценке квантовой запросной сложности поразрядной сортировки, которая оказывается равной $\Omega(n\sqrt{l/\log n})$. Таким образом, в отличие от общего случая, при поразрядной сортировке квантовые вычисления могут дать преимущество по сравнению с классическими. В работе [3] это преимущество достигается: показано, что поразрядная сортировка возможна за $O(n\sqrt{l}\log l)$, поэтому верхняя и нижняя оценки сложности поразрядной сортировки совпадают с точностью до логарифмических множителей.

Определение. Пусть $n, l \in \mathbb{Z}^+$ являются натуральными числами. Определим функцию $\mathrm{RADIX}_{n,l} : \{0,1\}^{nl} \to \mathbb{S}_n$ следующим образом. Пусть $\sigma_1, \ldots, \sigma_n \in \{0,1\}^l$ являются входными словами. Тогда

$$\mathrm{RADIX}_{n,l}(\sigma_1, \ldots, \sigma_n) = (j_1, \ldots, j_n),$$

где $(j_1, \ldots, j_n) \in \mathbb{S}_n$ является перестановкой, и для каждого $i \in \{1, \ldots, n-1\}$ соответствующие входные слова расположены в порядке возрастания: $\sigma_{j_i} \leq \sigma_{j_{i+1}}$. Если два входных слова равны, то мы сортируем их на основе их положения во входной последовательности: если $\sigma_{j_i} = \sigma_{j_{i+1}}$, то $j_i < j_{i+1}$.

Каждая перестановка $\sigma \in \mathbb{S}_n$ может быть представлена в виде произведения m транспозиций. Определим знак перестановки $\mathrm{sgn}(\sigma)$ как 0, если m чётное, и 1, если m нечётное.

Будем использовать обозначение $\|M\|$ для спектральной нормы M, и обозначение $A \circ B$ для поэлементного произведения матриц A и B: $(A \circ B)(\sigma, \tau) = A(\sigma, \tau)B(\sigma, \tau)$.

Доказательство нижней оценки для RADIX использует Adversary-метод [4]:

Теорема (Adversary-метод)**.** *Пусть $f : \{0,1\}^n \to \Sigma_O$ является произвольной функцией.*

Пусть A является произвольной матрицей, строки и столбцы которой индексируются входными последовательностями, такой, что $A(\sigma, \tau) = 0$ если $f(\sigma) = f(\tau)$.

Пусть D_i является матрицей такой, что $D_i(\sigma, \tau) = 1$ при $\sigma_i \neq \tau_i$, и $D_i(\sigma, \tau) = 0$ иначе.

Обозначим

$$\mathrm{ADV}(f) = \max_{A \geq 0} \frac{\|A\|}{\max_i \|A \circ D_i\|},$$

где максимум взят по всем ненулевым матрицам A.

Через $\mathrm{Q}_\epsilon(f)$ обозначим двустороннюю квантовую запросную сложность функции f, т.е. наименьшее число запросов, производящихся алгоритмом, вычисляющим f с вероятностью, не меньшей $1-\epsilon$.

Тогда верно неравенство $\mathrm{Q}_\epsilon(f) \geq \mathrm{ADV}(f)(1 - 2\sqrt{\epsilon(1-\epsilon)})/2$.

Оценки, полученные при помощи Adversary-метода, можно объединять [4]:

Утверждение. *Если $h = f \circ (g_1, \ldots, g_k)$, подфункции g_k действуют на непересекающихся подмножествах входных переменных, и $g_k = g$, то* $\mathrm{ADV}(h) = \mathrm{ADV}(f)\mathrm{ADV}(g)$.

Для доказательства нижней оценки заметим, что сортировка не проще, чем вычисление знака перестановки, являющейся результатом сортировки.

Определение. Пусть $n, l \in \mathbb{Z}^+$ являются натуральными числами. Определим функцию $\mathrm{SGN}_{n,l} : \{0,1\}^{nl} \to \{0,1\}$ следующим образом. Пусть $\sigma_1, \ldots, \sigma_n \in \{0,1\}^l$ являются входными словами. Тогда

$$\mathrm{SGN}_{n,l}(\sigma_1, \ldots, \sigma_n) = \mathrm{sgn}(\mathrm{RADIX}_{n,l}(\sigma_1, \ldots, \sigma_n)),$$

Лемма. *Вычисление $\mathrm{RADIX}_{n,l}$ не проще вычисления $\mathrm{SGN}_{n,l}$:* $\mathrm{Q}_\epsilon(\mathrm{RADIX}_{n,l}) \geq \mathrm{Q}_\epsilon(\mathrm{SGN}_{n,l})$.

Далее мы ограничиваем входные данные для SGN следующим образом. Будем рассматривать входную матрицу из $n \times l$ нулей и единиц как набор из $l/\log n$ полос нулей и единиц, каждая из которых имеет размер $n \times \log n$. Мы интерпретируем каждую полосу как список из n чисел от 0 до $n-1$.

Назовём полосу *правильной*, если она либо содержит перестановку (т.е. каждое число от 0 до $n-1$ встречается ровно один раз), либо она содержит только нули.

Будем рассматривать только такие входные данные для SGN, которые составлены из правильных полос.

Определение. Функция $\mathrm{SG}_n : \{0,1\}^{n \log n} \to \{0,1,\perp\}$ принимает на вход правильную полосу из n слов из $\log n$ символов и возвращает либо знак перестановки, либо символ $\perp$, если все слова равны.

Определение. Функция $\mathrm{FST}_m : \{0,1,\perp\}^m \to \{0,1\}$ принимает на вход m символов и возвращает первый из них, отличный от $\perp$. Если все символы равны $\perp$, функция FST_m возвращает 0.

Справедлива следующая

Лемма. *Функция* SGN *может быть представлена в виде следующей композиции функций:* $\mathrm{SGN}_{n,l} = \mathrm{FST}_{l/\log n} \circ \left(\mathrm{SG}_n, \ldots, \mathrm{SG}_n\right)$, *где каждая функция* SG_n *действует на отдельной полосе.*

Для доказательства нижней оценки функции RADIX осталось построить нижние оценки квантовой запросной сложности функций FST и SG, используя Adversary-метод.

Лемма. *Нижние оценки сложности равны, соответственно:*

$$\mathrm{ADV}(\mathrm{FST}_m) = \Omega(\sqrt{m})$$

$$\mathrm{ADV}(\mathrm{SG}_n) = \Omega(n)$$

Объединяя оценки, полученные Adversary-методом, получаем, что верна

Теорема.

$$\mathrm{Q}_\epsilon(\mathrm{RADIX}_{n,l}) = \Omega(n\sqrt{l/\log n})(1 - 2\sqrt{\epsilon(1-\epsilon)})/2.$$

Список литературы

1. Кормен Т. Х., Лейзерсон Ч. И., Ривест Р. Л., Штайн К. Алгоритмы: построение и анализ. — М.: Вильямс, 2005.

2. Høyer P., Neerbek J., Shi Y. Quantum complexities of ordered searching, sorting, and element distinctness // International Colloquium on Automata, Languages, and Programming. — Berlin: Springer, 2001. — С. 346–357.

3. Khadiev K., Ilikaev A., Vihrovs J. Quantum Algorithms for Some Strings Problems Based on Quantum String Comparator // Mathematics. — 2022. — Т. 10, вып. 3. — С. 377.

4. Hoyer P., Lee T., Spalek R. Negative weights make adversaries stronger. // Proceedings of the thirty-ninth annual ACM symposium on Theory of computing. — New-York: ACM, 2007. — С. 526–535.

DOI: 10.20948/dms-2022-13