УДК 519.714

О СЛОЖНОСТИ УНИТАРНЫХ ПРЕОБРАЗОВАНИЙ

Д. Ю. Черухин

В работе предложен метод получения нижних оценок сложности неветвящихся программ, элементарными операциями в которых являются унитарные преобразования над двумя комплексными числами. Метод позволяет получать оценки вида $\Omega(n \log n)$ для унитарных операторов $\mathbb{C}^n \to \mathbb{C}^n$, в частности, для преобразований Фурье и Уолша. При $n = 2^k$ найдены точные значения сложности последних.

Напомним, комплекснозначная матрица M размера $n \times n$ называется *унитарной*, если обратная матрица к ней совпадает с сопряжённой (M^*), полученной из M транспонированием и комплексным сопряжением коэффициентов. Группу унитарных преобразований $\mathbb{C}^n \to \mathbb{C}^n$ обозначим через $\mathcal{U}(\mathbb{C}^n)$, преобразования будем отождествлять с их матрицами в стандартном базисе.

Унитарной неветвящейся программой (*УНП*) назовём последовательность команд $\Pi = (K_1, \dots, K_L)$, имеющих вид

$$K_t = P_t(a_t, b_t), \qquad P_t \in \mathcal{U}(\mathbb{C}^2),\ a_t, b_t \in \mathbb{Z}_+, \quad t = 1, \dots, L. \tag{1}$$

Пусть имеется неограниченное число комплекснозначных *ячеек памяти*, занумерованных числами $0, 1, 2, \dots$ Тогда действие команды K_t состоит в следующем: берутся числа из ячеек с номерами a_t, b_t, с ними производится преобразование P_t и результат записывается в те же ячейки. Действие программы Π состоит в последовательном применении команд $K_1, \dots, K_L$.

Пусть n — натуральное число (размерность исходных данных), m — максимальное из чисел a_t, b_t $(t = 1, \dots, L)$ и числа n. Тогда для описания действия программы можно ограничиться рассмотрением первых m ячеек памяти. Команде K_t поставим в соответствие матрицу $M_t \in \mathcal{U}(\mathbb{C}^m)$, совпадающую с единичной матрицей всюду, кроме подматрицы, образованной строками и столбцами с номерами a_t, b_t (всюду в работе будем считать, что нумерация строк и столбцов матрицы ведётся с нуля); последняя же подматрица совпадает с матрицей преобразования P_t. Действие команды K_t состоит в умножении вектор-столбца значений ячеек памяти слева на матрицу M_t, а действие программы Π — в умножении на матрицу $M_L \cdot \ldots \cdot M_1$.

Пусть $M \in \mathcal{U}(\mathbb{C}^n)$. Скажем, что программа Π *вычисляет* оператор M, если матрица M может быть получена из матрицы $M_L \cdot \ldots \cdot M_1$ удалением всех столбцов, кроме первых n, удалением некоторых $m-n$ строк и перестановкой оставшихся строк. Другими словами, для любого начального состояния памяти, в котором входные данные записаны в первых n ячейках (в остальных ячейках — нули), программа Π, применённая к нему, должна выдавать вектор значений оператора M на данном входном наборе в некоторых n фиксированных ячейках памяти (неважно, в каком порядке). Число L назовём *сложностью программы* Π. *Сложностью оператора* M в классе УНП назовём минимальную сложность УНП, вычисляющей оператор M. Данную сложность обозначим через $L^{\text{УНП}}(M)$.

Теорема. *Для любого $M \in \mathcal{U}(\mathbb{C}^n)$, $M = (m_{i,j})$, выполнено*

$$L^{\text{УНП}}(M) \geqslant -\sum_{i,j} |m_{i,j}|^2 \log_2 |m_{i,j}|,$$

где $|z|$ — модуль комплексного числа z (при $z=0$ полагаем $|z|^2 \log_2 |z| = 0$).

Прежде, чем приступить к доказательству теоремы, приведём некоторые её следствия. Обозначим через φ_n корень n-й степени из единицы, $\varphi_n = \exp\{2\pi i/n\}$. *Преобразование Фурье* [1] задаётся матрицей $\Phi_n = \frac{1}{\sqrt{n}}(\varphi_n^{ij})$, $(i,j = 0,\ldots,n-1)$. Пусть $n = 2^k$, $0 \leqslant i,j \leqslant n-1$. Представим числа i,j в двоичной системе счисления: $i = \sum_{i=0}^{k-1} i_l 2^l$, $j = \sum_{i=0}^{k-1} j_l 2^l$ и положим $\langle i,j\rangle = \sum_{i=0}^{k-1} i_l j_l$. *Преобразование Уолша* имеет матрицу $W_n = \frac{1}{\sqrt{n}} A_n$, где A_n — *матрица Адамара*, $A_n = ((-1)^{\langle i,j\rangle})$, $(i,j = 0,\ldots,n-1)$. Все коэффициенты матриц Φ_n и W_n по модулю равны $\frac{1}{\sqrt{n}}$ (этот множитель введён для того, чтобы преобразование стало унитарным).

Следствие 1. *Для любого n из области определения*

$$L^{\text{УНП}}(\Phi_n) \geqslant \frac{1}{2} n \log_2 n, \quad L^{\text{УНП}}(W_n) \geqslant \frac{1}{2} n \log_2 n.$$

Известные алгоритмы быстрого преобразования Фурье и Уолша легко моделируются унитарными преобразованиями, что мы и покажем для случая $n = 2^k$. Пусть w — комплексное число, по модулю равное единице. Введём оператор $U_w = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ w & -w \end{pmatrix}$. Обозначим $D_n = \mathrm{diag}(1, \varphi_{2n}, \varphi_{2n}^2, \ldots, \varphi_{2n}^{n-1})$ — диагональная матрица размера $n \times n$ с соответствующими элементами на диагонали; через E_n будем обозначать единичную матрицу размера $n \times n$, а через O_n — нулевую (состоящую из нулей) того же размера.

Легко видеть, что $\Phi_2 = U_1$, поэтому $L^{\text{УНП}}(\Phi_2) \leqslant 1$. Далее, пусть Φ'_n — матрица, полученная из Φ_n следующей перестановкой строк: вначале в Φ'_n идут строки, имеющие в Φ_n чётные номера: $0, 2, \ldots, n-2$ (с сохранением их порядка), затем — нечётные: $1, 2, \ldots, n-1$ (также с сохранением порядка). Справедливо представление

$$\Phi'_{2n} = \frac{1}{\sqrt{2}}\begin{pmatrix} \Phi_n & \Phi_n \\ \Phi_n D_n & -\Phi_n D_n \end{pmatrix} = \begin{pmatrix} \Phi_n & O_n \\ O_n & \Phi_n \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} E_n & E_n \\ D_n & -D_n \end{pmatrix},$$

в силу которого для вычисления Φ_{2n} достаточно применить последовательность команд

$$U_1(0,n),\ U_{\varphi_{2n}}(1, n+1),\ U_{\varphi_{2n}^2}(2, n+2),\ \ldots,\ U_{\varphi_{2n}^{n-1}}(n-1, 2n-1),$$

а затем вычислить Φ_n для двух наборов ячеек памяти (перестановка строк соответствует изменению номеров ячеек, в которых будет храниться результат, и не влияет на сложность). Таким образом, мы имеем $L^{\text{УНП}}(\Phi_{2n}) \leqslant 2L^{\text{УНП}}(\Phi_n) + n$, откуда по индукции находим $L^{\text{УНП}}(\Phi_n) \leqslant \frac{1}{2} n \log_2 n$.

Для вычисления преобразования Уолша воспользуемся представлением матрицы Адамара $A_{2n} = \begin{pmatrix} A_n & A_n \\ A_n & -A_n \end{pmatrix}$:

$$W_{2n} = \frac{1}{\sqrt{2}}\begin{pmatrix} W_n & W_n \\ W_n & -W_n \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} E_n & E_n \\ E_n & -E_n \end{pmatrix}\begin{pmatrix} W_n & O_n \\ O_n & W_n \end{pmatrix}.$$

Мы видим, что для вычисления W_{2n} нужно два раза вычислить W_n и применить команды $U_1(0,n), \ldots, U_1(n-1, 2n-1)$. Отсюда, с учётом тождества $W_2 = U_1$ имеем $L^{\text{УНП}}(W_n) \leqslant \frac{1}{2} n \log_2 n$.

Следствие 2. *Если $n = 2^k$, то*

$$L^{\text{УНП}}(\Phi_n) = L^{\text{УНП}}(W_n) = \frac{1}{2} n \log_2 n.$$

Перейдём к доказательству теоремы. Введём обозначения: $\psi(x) = x \log_2 x$, $x \geqslant 0$ ($\psi(0) = 0$); $\mathcal{E}(z) = -\frac{1}{2}\psi(|z|^2)$, $z \in \mathbb{C}$. Заметим, что $\mathcal{E}(z) = -|z|^2 \log_2 |z|$. Для произвольной комплекснозначной матрицы M (в том числе для вектора) обозначим через $\mathcal{E}(M)$ сумму величин $\mathcal{E}(m_{i,j})$ по всем элементам $m_{i,j}$ матрицы M.

Утверждение. *Пусть неотрицательные числа x, y, x', y' связаны равенством $x + y = x' + y'$. Тогда*

$$|\psi(x) + \psi(y) - \psi(x') - \psi(y')| \leqslant x + y. \tag{2}$$

Доказательство. В силу возрастания функции $\log_2 x$ имеем

$$\psi(x) + \psi(y) \leqslant x \log_2(x + y) + y \log_2(x + y) = \psi(x + y). \tag{3}$$

С другой стороны, функция $\psi(x)$ выпукла (так как $\psi''(x) = (\log_2 x + \frac{1}{\ln 2})' = \frac{1}{x \ln 2} > 0$), поэтому

$$\psi(x + y) = \psi\Big(\frac{2x + 2y}{2}\Big) \leqslant \frac{1}{2}(\psi(2x) + \psi(2y)) = \\ = x \log_2(2x) + y \log_2(2y) = \psi(x) + \psi(y) + x + y. \tag{4}$$

Из (3), (4) и равенства $x + y = x' + y'$ следует

$$\psi(x) + \psi(y) - \psi(x') - \psi(y') = (\psi(x) + \psi(y) - \psi(x + y)) + \\ + (\psi(x' + y') - \psi(x') - \psi(y')) \leqslant 0 + (x' + y') = x + y, \tag{5}$$

и аналогично,

$$\psi(x') + \psi(y') - \psi(x) - \psi(y) \leqslant x + y. \tag{6}$$

Неравенства (5) и (6) дают в совокупности оценку (2).

Утверждение доказано.

Следствие 3. *Если комплексные числа z, w, z', w' связаны соотношением $|z|^2 + |w|^2 = |z'|^2 + |w'|^2$, то*

$$|\mathcal{E}(z, w) - \mathcal{E}(z', w')| \leqslant \frac{1}{2}(|z|^2 + |w|^2).$$

Лемма. *Пусть $M = (m_{i,j}) \in \mathcal{U}(\mathbb{C}^m)$, M_t — матрица, соответствующая команде P_t вида (1). Тогда*

$$|\mathcal{E}(M_t M) - \mathcal{E}(M)| \leqslant 1.$$

Доказательство. Умножение на матрицу M_t состоит в преобразовании a_t-й и b_t-й строк исходной матрицы; остальные строки остаются неизменными.

Обозначим через $(z_0, \dots, z_{m-1})$ и $(w_0, \dots, w_{m-1})$, соответственно, a_t-ю и b_t-ю строки матрицы M, а через $(z'_0, \dots, z'_{m-1})$ и $(w'_0, \dots, w'_{m-1})$ — соответствующие строки матрицы M_tM. Тогда

$$\mathcal{E}(M_tM) - \mathcal{E}(M) = \sum_{j=0}^{m-1} \big(\mathcal{E}(z_j, w_j) - \mathcal{E}(z'_j, w'_j)\big). \tag{7}$$

Матрицы M и M_t унитарны, поэтому M_tM унитарна. Сумма квадратов модулей чисел в любой строке и любом столбце унитарной матрицы равна единице (действительно, из равенства $MM^* = E_m$ следует $1 = \sum\limits_l m_{i,l}\overline{m_{i,l}} = \sum\limits_l |m_{i,l}|^2$, а из равенства $M^*M = E_m$ — аналогичное утверждение для столбцов). В частности,

$$\sum_{j=0}^{m-1} |z_j|^2 = \sum_{j=0}^{m-1} |w_j|^2 = 1. \tag{8}$$

Кроме того, в силу совпадения j-х столбцов матриц M и M_tM всюду, кроме a_t-й и b_t-й позиции, имеем

$$|z_j|^2 + |w_j|^2 = |z'_j|^2 + |w'_j|^2, \qquad j = 0, \dots, m-1. \tag{9}$$

Наконец, из (7–9) и следствия 3 получаем

$$|\mathcal{E}(M_tM) - \mathcal{E}(M)| \leqslant \sum_{j=0}^{m-1} \big|\mathcal{E}(z_j, w_j) - \mathcal{E}(z'_j, w'_j)\big| \leqslant \\ \leqslant \frac{1}{2}\sum_{j=0}^{m-1} (|z_j|^2 + |w_j|^2) = \frac{1}{2}(1+1) = 1.$$

Лемма доказана.

Доказательство теоремы. Рассмотрим программу Π вида (1), вычисляющую оператор M и имеющую при этом минимальную сложность. Обозначим $M_{\leqslant t} = M_tM_{t-1} \cdot \ldots \cdot M_1E_m$, $t = 0, 1, \dots, L$. Заметим, что для любой унитарной матрицы M выполнено $\mathcal{E}(M) \geqslant 0$, причём $\mathcal{E}(E_m) = 0$ (действительно, все элементы унитарной матрицы по модулю не превосходят единицы, а $\psi(x) \leqslant 0$ при $x \in [0, 1]$; кроме того, $\psi(0) = \psi(1) = 0$). Применим лемму L раз:

$$\mathcal{E}(M_{\leqslant L}) = |\mathcal{E}(M_{\leqslant L}) - \mathcal{E}(M_{\leqslant 0})| \leqslant \sum_{t=1}^{L} |\mathcal{E}(M_tM_{\leqslant t-1}) - \mathcal{E}(M_{\leqslant t-1})| \leqslant L.$$

Матрица M получена из некоторой подматрицы матрицы $M_{\leqslant L}$ перестановкой строк, следовательно, $\mathcal{E}(M) \leqslant \mathcal{E}(M_{\leqslant L})$. Окончательно имеем

$$L^{\text{УНП}}(M) = L \geqslant \mathcal{E}(M_{\leqslant L}) \geqslant \mathcal{E}(M).$$

Теорема доказана.

Заметим, что в основе квантовых вычислений [2] (более сильных, чем булевы), лежат унитарные преобразования, однако доказанная теорема дословно не переносится на квантовый случай из-за параллелизма последнего (на каждом шаге вычисления изменяются значения всех коэффициентов).

Автор выражает благодарность академику РАН О. Б. Лупанову за внимание к работе.

Работа выполнена при финансовой поддержке Программы поддержки ведущих научных школ РФФИ (проект 00-15-96103).

Литература

1. Сэвидж Дж. Э. Сложность вычислений. — М.: Изд-во "Факториал", 1998.

2. Стин Э. Квантовые вычисления. — Ижевск: НИЦ "Регулярная и хаотическая динамика", 2000.

МГУ, мех.-мат. факультет, Воробьевы горы, 119992 Москва, Россия