УДК 519.714

О сложности линейных операторов в классе схем глубины 2

/ Д. Ю. Черухин

В работе предложены методы получения нижних оценок сложности линейных булевых операторов (и связанных с ними матриц) в двух моделях схем глубины 2. В первой модели допустимы только линейные элементы с произвольным числом входов; во второй — произвольные булевы элементы. Методы применимы к матрицам с достаточно большим расстоянием Хемминга между строками, например, к матрицам Адамара.

Ключевые слова: линейный оператор, булева матрица, матрица Адамара, расстояние Хемминга, схема из функциональных элементов, сложность, глубина.

Keywords: linear operator, Boolean matrix, Hadamard matrix, Hamming distance, combinational circuit, complexity, depth.

О сложности линейных операторов в классе схем глубины 2

Д. Ю. Черухин

Работа относится к области получения нелинейных нижних оценок сложности явно заданных функций или операторов в классе схем из функциональных элементов с ограничениями [1]. Исследуется ограничение на глубину схемы, а именно, рассматриваются схемы глубины 2 в двух разных бесконечных базисах. В качестве класса изучаемых операторов выступает достаточно простой и естественный класс линейных булевых операторов. Каждый оператор соответствует матрице из нулей и единиц, поэтому можно сказать, что в работе изучается сложность булевых матриц.

Первый рассматриваемый базис естественно возникает из выбора реализуемых операторов: для вычисления линейного оператора достаточно линейных базисных элементов. Эта модель в чём-то напоминает теорию вентильных схем [2, 3], в которых роль элементарной операции выполняет не сумма по модулю 2, а дизъюнкция. В то же время рассматриваемая модель сложнее в силу закона приведения подобных слагаемых для суммы по модулю 2: $x \oplus x = 0$. Для дизъюнкции справедлив более мягкий закон $x \vee x = x$, позволяющий сводить оценку сложности матрицы к комбинаторной задаче, подобной задаче на покрытие.

В теории вентильных схем известны нелинейные нижние оценки сложности даже для модели без ограничения на глубину [2]. В рассматриваемом нами базисе подобных оценок не известно; нелинейные нижние оценки сложности получены только при наличии ограничения на глубину [4, 5]. Для схем глубины 2 наибольшие известные оценки имеют вид $\Omega(n \ln n)$. В работе [4] такие оценки получены для матриц Адамара, в работе [5] — например, для полных верхнетреугольных матриц. Работа [4] содержит два достаточно коротких доказательства, опирающихся на известные комбинаторные теоремы. Метод доказательства в [5] основан на теоретико-графовом свойстве схем, подобном наличию в схеме суперконцентратора [6].

В настоящей работе предложен метод получения нижних оценок (лемма 1), отличный от методов работ [4, 5]. Он позволяет получать оценки, чуть более низкие, чем $\Omega(n \ln n)$, для матриц Адамара и более широкого класса кодовых матриц (теорема 1). Отметим, что метод работы [5] применим только к матрицам высокого ранга, тогда как метод данной работы может быть применён к матрицам низкого ранга; например, ранг матрицы Адамара над полем $\mathbb{Z}_2$ может иметь вид $\log_2 n$. Отметим также, что лемма 1 может быть применена к некодовым матрицам, например, к полным верхнетреугольным.

В работе также рассмотрен более сильный базис, состоящий из произвольных булевых функций. Нелинейные нижние оценки сложности в модели схем ограниченной глубины в этом базисе известны [5–10]. В частности, в работе [5] получены оценки сложности вида $\Omega(n \ln n)$ для некоторых матриц высокого ранга (например, полных верхнетреугольных). В настоящей работе доказана нелинейная нижняя оценка сложности для матриц с расстоянием между строками, не меньшим $n/2$ (теорема 2); например, для матриц Адамара. Отметим, что доказательства теорем 1 и 2 (включая леммы) схожи; теорема 2 даёт оценку, столь же высокую по порядку, что и теорема 1, но применима к более узкому классу матриц.

Понятие схемы из функциональных элементов (СФЭ) в данном базисе, вычисляющей данную функцию (оператор), широко известно [1]. Под сложностью схемы мы будем понимать число рёбер в ней, а под глубиной — наибольшую длину ориентированного пути, соединяющего некоторый вход с некоторым выходом схемы. Сложность оператора F в классе СФЭ в базисе B, глубина которых не превосходит 2 (т. е. минимальную сложность схемы из этого класса, вычисляющей оператор F), обозначим через $L^2_B(F)$.

Рассмотрим два базиса: P_2, состоящий из всех булевых функций, и L_0, состоящий из всех линейных однородных булевых функций:

$$P_2 = \{f \mid \exists n \ f\colon \{0,1\}^n \to \{0,1\}\}, \quad L_0 = \{f \mid \exists n \ f = x_1 \oplus \ldots \oplus x_n\}.$$

В целях сокращения записи обозначим:

$$L^2(F) = L^2_{P_2}(F), \quad L^2_{\oplus}(F) = L^2_{L_0}(F).$$

Каждому линейному однородному оператору $F\colon \{0,1\}^n \to \{0,1\}^m$ над полем $\mathbb{Z}_2$ соответствует его матрица M в стандартном базисе, $M = (m_{ij})_{i=1,\dots,n}^{j=1,\dots,m}$. Далее мы не будем различать оператор и соответствующую ему матрицу. В частности, будем оперировать понятиями "матрица, вычисляемая схемой" и "сложность матрицы".

Пусть $M = (m_{ij})$ — матрица с n столбцами и m строками. Такую матрицу будем называть (n,m)-матрицей. Введём функции

$$\varphi_m(x) = \min\{x, m-x\}, \quad \psi_m(x) = x(m-x),$$

и следующую характеристику матрицы:

$$\Delta(M) = \sum_{i=1}^{n} \varphi_m\Big(\sum_{j=1}^{m} m_{ij}\Big).$$

Для любого числа $x \geqslant 0$ через $\Delta(M;\, x)$ обозначим минимальное значение величины $\Delta(M')$, взятое по всем подматрицам M' матрицы M, состоящим из некоторых строк матрицы M и содержащих не меньше, чем x строк.

Утверждение 1. $\varphi_m(x) \geqslant \dfrac{1}{m}\psi_m(x), \quad 0 \leqslant x \leqslant m.$

Доказательство. Если $x \in [0,\, 1/2]$, то $\varphi_1(x) = x \geqslant x - x^2 = \psi_1(x)$, поэтому, в силу симметрии функций φ_1 и ψ_1 относительно прямой $x = 1/2$, имеем $\varphi_1(x) \geqslant \psi_1(x)$, $x \in [0,\, 1]$. Тогда

$$\varphi_m(x) = m\varphi_1\Big(\frac{x}{m}\Big) \geqslant m\psi_1\Big(\frac{x}{m}\Big) = \frac{1}{m}\psi_m(x), \quad x \in [0,\, m].$$

Утверждение 1 доказано.

Пусть M — (n,m)-матрица и $\tilde{v}_1,\dots,\tilde{v}_m$ — её строки. Обозначим через $d(\tilde{v},\,\tilde{w})$ расстояние Хемминга между векторами $\tilde{v}=(v_1,\dots,v_n)$ и $\tilde{w}=(w_1,\dots,w_n)$:

$$d(\tilde{v},\,\tilde{w})=\sum_{i=1}^{n}|v_i-w_i|.$$

Матрицу M назовём (n,m,d)-матрицей, если расстояние Хемминга между любыми двумя её различными строками не меньше, чем d.

Утверждение 2. *Для любой (n,m)-матрицы M выполнено*

$$\Delta(M)\geqslant\frac{1}{m}\sum_{1\leqslant i<j\leqslant m}d(\tilde{v}_i,\tilde{w}_i).$$

Доказательство. Применяя утверждение 1, получим

$$\begin{aligned}\sum_{1\leqslant i<j\leqslant m}d(\tilde{v}_i,\,\tilde{v}_j)&=\sum_{1\leqslant i<j\leqslant m}\sum_{k=1}^{n}|m_{ik}-m_{jk}|=\\&=\sum_{k=1}^{n}\sum_{1\leqslant i<j\leqslant m}|m_{ik}-m_{jk}|=\sum_{k=1}^{n}\sum_{i:\,m_{ik}=1}\sum_{j:\,m_{jk}=0}1=\\&=\sum_{k=1}^{n}\Bigl(\sum_{i=1}^{m}m_{ik}\Bigr)\Bigl(m-\sum_{j=1}^{m}m_{jk}\Bigr)=\sum_{k=1}^{n}\psi_m\Bigl(\sum_{i=1}^{m}m_{ik}\Bigr)\leqslant\\&\leqslant m\sum_{k=1}^{n}\varphi_m\Bigl(\sum_{i=1}^{m}m_{ik}\Bigr)=m\Delta(M).\end{aligned}$$

Утверждение 2 доказано.

Пусть M — (n,m)-матрица, $L>0$. Матрице M и числу L поставим в соответствие последовательность чисел $x_0,x_1,\dots,$ определяемую следующим образом:

$$x_0 = \frac{m}{2}, \qquad x_{k+1} = \frac{\Delta(M;\, x_k)}{L}, \quad k = 0,\, 1, \ldots$$

Отметим, что число x_k зависит от двух параметров: M и L, которые явно не указаны для экономии записи.

Лемма 1. *Если в каждой строке матрицы M имеется хотя бы две единицы и $L = L^2_{\oplus}(M)$, то $x_{[2L/m]+1} = 0$.*

Доказательство. Пусть S — минимальная СФЭ глубины 2 в базисе L_0, вычисляющая матрицу M. Перейдём от S к схеме S', обладающей свойством: длина любого ориентированного пути в схеме S', соединяющего произвольный вход с произвольным выходом, равна двум. Вначале заметим, что в силу условия леммы, ни один из входов схемы не совпадает ни с одним из выходов. Рассмотрим все рёбра, соединяющие вход с выходом схемы, и заменим каждое из них цепочкой из двух рёбер, введя промежуточную вершину. Сложность схемы при этом возрастёт, но число рёбер на каждом из ярусов будет не больше, чем L (ребро схемы S' отнесём к первому ярусу, если оно инцидентно некоторому входу схемы, и отнесём ко второму ярусу, если оно инцидентно некоторому выходу).

Проведём со схемой S' последовательность преобразований, состоящих в удалении некоторых выходов. Удаление выхода схемы соответствует удалению строки матрицы M. Схему, полученную после k-го преобразования, $(k = 0, 1, \ldots)$ обозначим через S_k, а соответствующую матрицу — через M_k. Число строк матрицы M_k обозначим через y_k. Дальнейший план доказательства таков: вначале опишем преобразования схемы, затем индукцией по k докажем неравенство $y_k \geqslant x_k$. Наконец, заметим, что $y_{[2L/m]+1} = 0$, следовательно, $x_{[2L/m]+1} = 0$.

Нулевое преобразование схемы состоит в следующем: удалим те выходы, в которые входит больше, чем $2L/m$ рёбер. Число рёбер второго яруса не больше L, следовательно, число удалённых вершин меньше, чем $m/2$. Тогда число оставшихся выходов не меньше, чем $m/2$, т. е. $y_0 \geqslant m/2 = x_0$. Опишем $(k+1)$-е преобразование ($k = 0, 1, \ldots$). Вершины схемы, отличные от входов и выходов, будем называть вершинами среднего слоя. Выделим в схеме S_k ту вершину среднего слоя v_{k+1}, которая, во-первых, отлична от ранее выделенных вершин $v_1, \ldots, v_l$ ($l \leqslant k$) и, во-вторых, максимальна среди всех невыделенных вершин среднего слоя по числу исходящих из неё рёбер (без учёта входящих). Если вершина v_{k+1} определена, то удалим из S_k все выходы, не соединённые ребром с вершиной v_{k+1}. Если все вершины среднего слоя уже выделены, то удалим из S_k все имеющиеся выходы (для удобства полученный объект тоже будем считать схемой).

Докажем неравенство $y_k \geqslant x_k$. Базис индукции, $y_0 \geqslant x_0$, уже доказан. Проведём индуктивный переход $k \mapsto k+1$. Каждая из ранее выделенных вершин $v_1, \ldots, v_l$ ($l \leqslant k$) соответствует некоторому элементу, на выходе которого реализуется линейная функция от переменных, подаваемых на вход схемы S_k. Пусть Λ_k — сумма по модулю 2 этих функций. По определению 1-го, 2-го и т. д. преобразований каждая из вершин $v_1, \ldots, v_l$ соединена ребром с каждым из выходов схемы S_k. Поэтому элементы $v_1, \ldots, v_l$ дают суммарный вклад Λ_k в каждую из функций, вычисляемых схемой S_k.

Перейдём от схемы S_k к схеме S'_k, удалив вершины $v_1, \ldots, v_l$ и все инцидентные им рёбра. Матрицу, вычисляемую схемой S'_k, обозначим через M'_k. Каждая из функций, вычисляемая схемой S'_k, отличается от соответствующей функции, вычисляемой S_k, на слагаемое Λ_k. На языке матриц это означает следующее: матрица M'_k получена из M_k инвертированием некоторых столбцов, а именно, столбцов, соответствующих переменным, от которых существенно зависит функция Λ_k (инвертирование подматрицы есть замена нулей на единицы и единиц на нули).

Пусть $M'_k = (m'_{ij})$. Оценим число единиц в матрице M'_k. Если сумма элементов в некотором столбце матрицы M'_k равна s, то сумма элементов в соответствующем столбце матрицы M_k равна s или $y_k - s$, т. е. не меньше, чем $\min\{s,\, y_k - s\} = \varphi_{y_k}(s)$. Поэтому, применяя предположение индукции, получим

$$\sum_{i=1}^{n} \sum_{j=1}^{y_k} m'_{ij} \geqslant \sum_{i=1}^{n} \varphi_{y_k}\Bigl(\sum_{j=1}^{y_k} m_{ij}\Bigr) = \Delta(M_k) \geqslant \Delta(M;\, y_k) \geqslant \Delta(M;\, x_k). \qquad (1)$$

Далее, оценим y_{k+1}. Для каждой вершины v среднего слоя схемы S'_k обозначим через p_v число рёбер, входящих в v, а через q_v — число выходящих из v рёбер. Тогда число единиц в матрице M'_k не меньше, чем

$$\sum_{v} p_v q_v. \qquad (2)$$

Действительно, схему S'_k можно превратить в схему глубины 1, удалив каждую вершину v среднего слоя и соединив ребром каждый из p_v инцидентных ей входов с каждым из q_v инцидентных ей выходов. При этом, возможно, какие-то рёбра уничтожатся по правилу $x \oplus x = 0$, но число оставшихся рёбер, равное числу единиц в матрице M'_k, не может быть больше величины (2).

Заметим, что если хотя бы одно число q_v существует (т. е. в S'_k есть хотя бы одна вершина среднего слоя), то y_{k+1} есть максимальное из них. В этом случае имеем (используем, что число рёбер первого яруса не больше L, а также оценку (1))

$$y_{k+1} L \geqslant y_{k+1} \sum_v p_v \geqslant \sum_v p_v q_v \geqslant \sum_{i,j} m'_{ij} \geqslant \Delta(M;\, x_k), \tag{3}$$

поэтому

$$y_{k+1} \geqslant \frac{\Delta(M;\, x_k)}{L} = x_{k+1}. \tag{4}$$

Если же в S'_k нет вершин среднего слоя, то цепочки соотношений (3) и (4) справедливы для любого неотрицательного числа y_{k+1} (считаем, что сумма элементов пустого множества равна нулю). В частности, (4) выполнено для числа $y_{k+1} = 0$.

Индукция проведена и неравенство $y_k \geqslant x_k$ доказано. Завершим доказательство леммы. Пусть $t = [2L/m]$. Вспомним, что (по определению нулевого преобразования) в каждый выход схемы S_0 входит не более t рёбер. В то же время, каждый из выходов схемы S_t соединён ребром с каждой из выделенных вершин среднего слоя. Следовательно, при осуществлении t-го преобразования мы не можем выделить ещё одну вершину, а значит, $y_{t+1} = 0$. В силу неравенства $y_{t+1} \geqslant x_{t+1}$ и неотрицательности числа x_{t+1}, имеем $x_{t+1} = 0$.

Лемма 1 доказана.

Теорема 1. *Если M — (n, n, d)-матрица и $d = n^{1-o(1)}$, то*

$$L^2_{\oplus}(M) = \Omega\Big(n \frac{\ln n}{\ln\left(\frac{n}{d}\ln n\right)}\Big).$$

Доказательство. Заметим, что матрица M может содержать нулевую строку или строку с одной единицей, что препятствует применению к ней леммы 1. Условие $d \to \infty$ гарантирует, что при больших n такая строка может быть только одна. Удалим её из матрицы, заметив, что дальшейшие рассуждения легко применимы к (n, m, d)-матрицам, для которых $m \sim n$.

Рассмотрим произвольную матрицу M', полученную из M удалением некоторых строк. Пусть M' содержит m строк, $m \geqslant 2$. Тогда, в силу утверждения 2, имеем:

$$\Delta(M') \geqslant \frac{1}{m} \sum_{1 \leqslant i < j \leqslant m} d(\tilde{v}_i,\, \tilde{v}_j) \geqslant \frac{1}{m} \cdot C_m^2 \cdot d = \frac{(m-1)d}{2} \geqslant \frac{md}{4}$$

Следовательно,

$$\Delta(M;\, x) = \Delta(M;\, \lceil x \rceil) \geqslant \frac{\lceil x \rceil d}{4} \geqslant \frac{xd}{4}, \quad x > 1. \tag{5}$$

Пусть $L = L^2_{\oplus}(M)$. Оценим чи́сла x_k, зависящие от параметров L и M. Из неравенства (5) следует

$$x_0 = \frac{n}{2}; \qquad x_{k+1} = \frac{\Delta(M;\, x_k)}{L} \geqslant \frac{d}{4L} x_k, \quad \text{если } x_k > 1. \tag{6}$$

В силу леммы 1 имеем

$$x_{[2L/n]+1} = 0. \tag{7}$$

Обозначим через t наименьшее число k такое, что $x_k \leqslant 1$. Тогда из (6) следует

$$x_k \geqslant \frac{n}{2}\Big(\frac{d}{4L}\Big)^k > 0, \quad k = 0, \dots, t. \tag{8}$$

Сопоставляя неравенства (7) и (8), получим

$$[2L/n] + 1 \geqslant t + 1. \tag{9}$$

Обозначим $z = 4L/d$. Заметим, что $z > 1$; в противном случае, в силу (6), последовательность чисел $\{x_k\}$ строго положительна, что противоречит равенству (7). Сведём воедино неравенства (8), (9) и $x_t \leqslant 1$, а затем выполним преобразования:

$$\begin{gathered}
1 \geqslant x_t \geqslant \frac{n}{2}\Big(\frac{d}{4L}\Big)^t = \frac{n}{2z^t} \geqslant \frac{n}{2z^{2L/n}} = \frac{n}{2z^{(zd/2n)}},\\
z^{(zd/2n)} \geqslant n/2,\\
z \ln z \geqslant \frac{2n}{d}(\ln n - \ln 2) \asymp \frac{n}{d}\ln n,\\
z = \Omega\Big(\frac{(n/d)\ln n}{\ln((n/d)\ln n)}\Big).
\end{gathered}$$

Раскрывая определение числа z, получим требуемую в теореме оценку.

Теорема 1 доказана.

Следствие 1. *Если M — (n,n,d)-матрица и $d = \dfrac{n}{\ln^{O(1)} n}$, то*

$$L_\oplus^2(M) = \Omega\Big(n\frac{\ln n}{\ln\ln n}\Big).$$

Пусть $n = 2^k$. Индукцией по k определим матрицу Адамара A_n размера $n \times n$:

$$A_1 = (0), \qquad A_{2n} = \begin{pmatrix} A_n & A_n \\ A_n & \overline{A_n} \end{pmatrix},$$

где через $\overline{M}$ обозначена инверсия матрицы M (матрица, полученная из M отрицанием всех элементов). Широко известно, что расстояние Хемминга между любыми двумя строками матрицы A_n равно $n/2$ (это легко можно доказать по индукции), следовательно, A_n является $(n, n, n/2)$-матрицей и к ней применимо следствие 1.

Перейдём к рассмотрению базиса P_2. Вначале выясним связь между вычислением функции в этом базисе и вычислением её линейной части с помощью теоретико-множественных операций. Пусть f — произвольная булева функция. Разложим f в полином Жегалкина и выделим линейную часть:

$$f = \alpha_0 \oplus \alpha_1 x_1 \oplus \ldots \oplus \alpha_n x_n \oplus f', \tag{10}$$

где f' — нелинейная часть. Обозначим через $\mathrm{Lin}\,(f)$ множество переменных, входящих в линейную часть функции f с коэффициентом 1, т. е.

$$\mathrm{Lin}\,(f) = \{x_i \mid \alpha_i = 1\}.$$

Утверждение 3. *Если функция f представлена в виде суперпозиции булевых функций:*

$$f = g(f_1, \ldots, f_s),$$

то множество $\mathrm{Lin}\,(f)$ выражается через $\mathrm{Lin}\,(f_1), \ldots, \mathrm{Lin}\,(f_s)$ с помощью теоретико-множественных операций объединения, пересечения и *разности.*

Доказательство. Любую булеву функцию, в том числе g, можно выразить в базисе $\{xy,\ \bar{x}\}$, поэтому утверждение достаточно доказать только в случаях $g = \overline{x}$ и $g = xy$. В первом случае имеем $f = \overline{f}_1 = f_1 \oplus 1$, следовательно, $\mathrm{Lin}\,(f) = \mathrm{Lin}\,(f_1)$.

Рассмотрим случай $g = f_1 f_2$. Пусть

$$f_j = \alpha_0^j \oplus \alpha_1^j x_1 \oplus \ldots \oplus \alpha_n^j x_n \oplus f_j', \quad j = 1, 2.$$

Тогда

$$f = f_1 f_2 = \alpha_0^1 \alpha_0^2 \oplus \bigoplus_{i=1}^{n} (\alpha_0^1 \alpha_i^2 \oplus \alpha_0^2 \alpha_i^1 \oplus \alpha_i^1 \alpha_i^2) x_i \oplus f'. \tag{11}$$

В силу единственности полинома Жегалкина, можно приравнять коэффициенты при переменных из (10) и (11).

Если $\alpha_0^1 = \alpha_0^2 = 0$, то имеем $\alpha_i = \alpha_i^1 \alpha_i^2$, поэтому $\mathrm{Lin}\,(f) = \mathrm{Lin}\,(f_1) \cap \mathrm{Lin}\,(f_2)$. Если $\alpha_0^1 = 0,\ \alpha_0^2 = 1$, то $\alpha_i = \alpha_i^1 \oplus \alpha_i^1 \alpha_i^2 = \alpha_i^1 \overline{\alpha_i^2}$, следовательно, $\mathrm{Lin}\,(f) = \mathrm{Lin}\,(f_1) \setminus \mathrm{Lin}\,(f_2)$; случай $\alpha_0^1 = 1,\ \alpha_0^2 = 0$ аналогичен. Наконец, если $\alpha_i^1 = \alpha_i^2 = 1$, то имеем $\alpha_i = \alpha_i^1 \oplus \alpha_i^2 \oplus \alpha_i^1 \alpha_i^2 = \alpha_i^1 \vee \alpha_i^2$, а значит, $\mathrm{Lin}\,(f) = \mathrm{Lin}\,(f_1) \cup \mathrm{Lin}\,(f_2)$.

Утверждение 3 доказано.

Пусть M — (n, m)-матрица, $M_1, \ldots, M_s$ — матрицы с m строками; число столбцов матрицы M_i может равняться нулю. Через $[M_1 \ldots M_s]$ обозначим матрицу, составленную из блоков $M_1, \ldots, M_s$, расположенных по горизонтали в указанном порядке. Введём обозначение:

$$\Delta'_s(M) = \min_{M_1,\ldots,M_s\colon [M_1\ldots M_s]=M} \sum_{i=1}^{s} \Delta(M_i^T), \tag{12}$$

где M_i^T — транспонированная матрица M_i. Пусть $\Delta'_s(M;\, x)$ — минимальное значение величины $\Delta_s(M')$ среди всех матриц M', полученных из M удалением некоторых строк и содержащих не менее x строк.

Утверждение 4. *Если M — $(n, m, n/2)$-матрица и M' — матрица с n' столбцами, полученная из M удалением некоторых столбцов, то*

$$\Delta(M') \geqslant \frac{1}{4}(n'm - n).$$

Доказательство. Назовём 0–1-парой два различных элемента матрицы M (нуль и единицу), стоящие в одном и том же её столбце; 0–1-пару считаем неупорядоченной. Пусть R — число 0–1-пар в матрице M, R_i — число таких пар, находящихся в i-м столбце. Через $\tilde{v}_1, \ldots, \tilde{v}_m$ обозначим строки матрицы M. Будем также считать, что матрица M' состоит из первых n' столбцов матрицы M. Подсчитывая 0–1-пары по столбцам и строкам, получим

$$\sum_{i=1}^{n} R_i = R = \sum_{1\leqslant i<j\leqslant m} d(\tilde{v}_i, \tilde{v}_j) \geqslant C_m^2 \cdot \frac{n}{2}.$$

Пусть h_i — число единиц в i-м столбце матрицы M. Тогда

$$R_i = h_i(m - h_i) = \left(\sqrt{h_i(m-h_i)}\right)^2 \leqslant \left(\frac{h_i + m - h_i}{2}\right)^2 = \frac{m^2}{4},$$

поэтому

$$\sum_{i=n'+1}^{n} R_i \leqslant (n-n')\frac{m^2}{4},$$

а значит,

$$\sum_{i=1}^{n'} R_i = R - \sum_{i=n'+1}^{n} R_i \geqslant C_m^2 \cdot \frac{n}{2} - (n-n')\frac{m^2}{4} =$$
$$= \frac{m}{4}\left((m-1)n - nm + n'm\right) = \frac{m}{4}(n'm - n). \quad (13)$$

Заметим, что $R_i = \psi_m(h_i)$. Поэтому, в силу утверждения 1, имеем

$$\sum_{i=1}^{n'} R_i = \sum_{i=1}^{n'} \psi_m(h_i) \leqslant m \sum_{i=1}^{n'} \varphi_m(h_i) = m\Delta(M'). \quad (14)$$

Из (13) и (14) следует доказываемое утверждение 4.

Утверждение 5. *Пусть M — $(n, m, n/2)$-матрица. Тогда*

$$\Delta'_s(M) \geqslant \frac{n}{4}(m - 2s).$$

Доказательство. Пусть $M_1, \dots, M_s$ — такие матрицы, на которых достигается минимум в определении (12). Далее, пусть n_i — число столбцов в M_i, $\tilde{v}_i^j$ — j-я строка матрицы M_i, h_{ij} — сумма элементов в $\tilde{v}_i^j$.

Разобъём матрицу M_i на две подматрицы, M_i' и M_i'', отнеся каждую строку матрицы M_i либо к M_i', либо к M_i''. А именно, если $h_{ij} \leqslant n_i/2$, то строку $\tilde{v}_i^j$ отнесём к M_i', обозначив это через $\tilde{v}_i^j \in M_i'$; в противном случае, строку $\tilde{v}_i^j$ отнесём к M_i'', $\tilde{v}_i^j \in M_i''$.

Имеем

$$\Delta(M_i^T) = \sum_{j=1}^{m} \varphi_{n_i}(h_{ij}) = \sum_{j=1}^{m} \min\{h_{ij},\, n_i - h_{ij}\}. \quad (15)$$

Если $\tilde{v}_i^j \in M_i'$, то минимум в j-м слагаемом суммы (15) равен h_{ij}; в противном случае, он равен $n_i - h_{ij}$. Следовательно,

$$\Delta(M_i^T) = \sum_{j:\,\tilde{v}_i^j \in M_i'} h_{ij} + \sum_{j:\,\tilde{v}_i^j \in M_i''} (n_i - h_{ij}) = |M_i'| + |\overline{M_i''}|, \tag{16}$$

где через $|A|$ обозначено число единиц в матрице A.

Заметим, что для любой матрицы A выполнено

$$\Delta(A) \leqslant |A| \quad \text{и} \quad \Delta(A) \leqslant |\overline{A}|. \tag{17}$$

Пусть m_i' и m_i'' — число строк, соответственно, в матрицах M_i' и M_i''. Заметим, что M_i' является подматрицей некоторой $(n, m_i', n/2)$-матрицы (которая, в свою очередь, является подматрицей матрицы M). Аналогично, M_i'' является подматрицей некоторой $(n, m_i'', n/2)$-матрицы. Применим к этим матрицам утверждение 4 и просуммируем результаты. С учётом (16) и (17), получим

$$\Delta_s'(M) = \sum_{i=1}^{s} \Delta(M_i^T) = \sum_{i=1}^{s} \big(|M_i'| + |\overline{M_i''}|\big) \geqslant$$
$$\geqslant \sum_{i=1}^{s} \big(\Delta(M_i') + \Delta(M_i'')\big) \geqslant \frac{1}{4} \sum_{i=1}^{s} (n_i m_i' - n + n_i m_i'' - n) =$$
$$= \frac{1}{4} \sum_{i=1}^{s} (n_i m - 2n) = \frac{1}{4}(nm - 2ns) = \frac{n}{4}(m - 2s).$$

Утверждение 5 доказано.

Следствие 2. *Если M — $(n, m, n/2)$-матрица, то*

а) для любого $x > 0$

$$\Delta_s'(M;\, x) \geqslant \frac{n}{4}(x - 2s);$$

б) если $x \geqslant 4s$, то

$$\Delta'_s(M;\, x) \geqslant \frac{nx}{8}.$$

Пусть M — (n,m)-матрица. Поставим в соответствие матрице M и числу $L > 0$ последовательность чисел $x'_0, x'_1, \ldots$:

$$x'_0 = \frac{m}{2}, \qquad x'_{k+1} = \frac{\Delta'_{2^k}(M;\, x'_k)}{L}, \quad k = 0, 1, \ldots \tag{18}$$

Лемма 2. *Если в каждой строке матрицы M имеется хотя бы две единицы и $L = L^2(M)$, то $x'_{[2L/m]+1} = 0$.*

Доказательство. Будем следовать доказательству леммы 1: по минимальной схеме S построим схему S', а затем последовательность схем $S_0, S_1, \ldots$, полученных в результате преобразований, определяемых также, как в доказательстве леммы 1. Пусть схема S_k соответствует матрице M_k, имеющей y'_k строк. По индукции докажем неравенство $y'_k \geqslant x'_k$. Базис индукции, $y'_0 \geqslant x'_0$, следует из определения нулевого преобразования и (18). Докажем индуктивный переход $k \mapsto k+1$.

Будем считать, что входам схемы S_k соответствуют переменные $u_1, \ldots, u_n$. На предыдущих шагах индукции были выделены вершины среднего слоя $v_1, \ldots, v_l$ $(l \leqslant k)$. Пусть f_i $(1 \leqslant i \leqslant y'_k)$ — функция, вычисляемая на i-м выходе схемы S_k (переменными функции f_i являются $u_1, \ldots, u_n$), g_r $(1 \leqslant r \leqslant l)$ — функция, вычисляемая в вершине v_r. Обозначим через V_i множество таких переменных $u_{i'}$, что существует ориентированный путь от i'-го входа к i-му выходу схемы S_k, не проходящий через вершины $v_1, \ldots, v_l$. Наша цель — оценить сумму мощностей множеств $|V_i|$.

Введём отношение эквивалентности на множестве $\{u_1, \ldots, u_n\}$: переменные u_a и u_b эквивалентны, если для любого из множеств $\mathrm{Lin}\,(g_r)$ переменные u_a и u_b либо обе входят в это множество, либо обе не входят, т. е.

$$u_a \sim u_b \iff \forall r\ (u_a \in \mathrm{Lin}\,(g_r) \iff u_b \in \mathrm{Lin}\,(g_r)).$$

Пусть $K^1, \ldots, K^s$ — классы эквивалентности данного отношения. Их число не превосходит 2^l. Действительно, если $l = 1$, то существует не более двух классов эквивалентности: один соответствует множеству $\mathrm{Lin}\,(g_1)$, а другой — его дополнению $\{u_1, \ldots, u_n\} \setminus \mathrm{Lin}\,(g_1)$. При добавлении каждого следующего множества $\mathrm{Lin}\,(g_r)$ число классов увеличивается не более, чем в два раза, а именно, каждый имеющийся класс может разделиться не более, чем на две части: одна из них соответствует множеству $\mathrm{Lin}\,(g_r)$, а другая — его дополнению. Таким образом, $s \leqslant 2^l \leqslant 2^k$.

Представим матрицу M_k в виде $M = [M_k^1 \ldots M_k^s]$, где M_k^j $(1 \leqslant j \leqslant s)$ состоит из всех столбцов, соответствующих переменным из класса K^j. Пусть S_k^j — схема, полученная из S_k подстановкой нулей вместо всех переменных, не входящих в K^j. Очевидно, схема S_k^j вычисляет матрицу M_k^j. Далее, через f_i^j и g_r^j обозначим функции, полученные, соответственно, из функций f_i и g_r в результате этой подстановки. Наконец, пусть $V_i^j = V_i \cap K^j$. Заметим, что $\mathrm{Lin}\,(g_r^j) = \mathrm{Lin}\,(g_r) \cap K^j$, так как при подстановке нулей вместо переменных ни одно слагаемое из нелинейной части полинома Жегалкина не может перейти в линейную часть.

Функция f_i^j вычислима через функции $g_1^j, \dots, g_l^j$ и переменные из множества V_i^j, т. е. представима в виде

$$f_i^j = h(g_1^j, \dots, g_l^j, u_1', \dots, u_t'),$$

где h — булева функция и $V_i^j = \{u_1', \dots, u_t'\}$. Действительно, множество V_i содержит все переменные, используемые при вычислении функции f_i, если функции $g_1, \dots, g_l$ уже вычислены. Свойство вычислимости, очевидно, сохраняется при подстановке констант вместо некоторых переменных. Тогда, в силу утверждения 3, множество $\mathrm{Lin}\,(f_i^j)$ выражается через множества $\mathrm{Lin}\,(g_1^j), \dots, \mathrm{Lin}\,(g_l^j)$, $\{u_1'\}, \dots, \{u_t'\}$ с помощью операций $\cup$, $\cap$, $\setminus$.

Для любого r, по определению эквивалентности переменных, либо все переменные из класса K^j входят в множество $\mathrm{Lin}\,(g_r)$, либо ни одна из них не входит в $\mathrm{Lin}\,(g_r)$. Так как $\mathrm{Lin}\,(g_r^j) = \mathrm{Lin}\,(g_r) \cap K^j$, то либо $\mathrm{Lin}\,(g_r^j) = K^j$, либо $\mathrm{Lin}\,(g_r^j) = \varnothing$. Таким образом, множество $\mathrm{Lin}\,(f_i^j)$ выражается через множества K^j, $\{u_1'\}, \dots, \{u_t'\}$ с помощью операций $\cup$, $\cap$, $\setminus$. Несложно понять, что для любого множества X, выразимого через указанные множества, выполнено либо $X \subseteq V_i^j$, либо $K^j \setminus V_i^j \subseteq X \subseteq K^j$. Следовательно, либо $V_i^j \supseteq X$, либо $V_i^j \supseteq K^j \setminus X$. Окончательно,

$$|V_i^j| \geqslant \min\{|X|,\ |K^j \setminus X|\} = \varphi_{|K^j|}(|X|). \tag{19}$$

Заметим, что $|\,\mathrm{Lin}\,(f_i^j)|$ — число единиц в i-й строке матрицы M_k^j. Применим неравенство (19) к множеству $X = \mathrm{Lin}\,(f_i^j)$ и просуммируем

по всем i:
$$\sum_{i=1}^{y'_k}|V_i^j| \geqslant \sum_{i=1}^{y'_k}\varphi_{|K^j|}\big(|\operatorname{Lin}(f_i^j)|\big) = \Delta\big((M_k^j)^T\big).$$
Следовательно (учитывая предположение индукции),
$$\sum_{i=1}^{y'_k}|V_i| = \sum_{i,j}|V_i^j| \geqslant \sum_{j=1}^{s}\Delta\big((M_k^j)^T\big) \geqslant \Delta'_s(M_k) \geqslant$$
$$\geqslant \Delta'_{2^k}(M_k) \geqslant \Delta'_{2^k}(M;\, y'_k) \geqslant \Delta'_{2^k}(M;\, x'_k). \quad (20)$$

Далее мы в основном следуем доказательству леммы 1. Удалив из схемы S_k вершины $v_1, \ldots, v_l$ (не заботясь о функциональности), получим схему S'_k. Через p_v и q_v обозначим число рёбер, соответственно, входящих и выходящих из вершины v среднего слоя схемы S'_k. Тогда число ориентированных путей, соединяющих некоторый вход с некоторым выходом схемы S'_k, не больше величины (2). С другой стороны, это число не меньше суммы $|V_1| + \ldots + |V_{y'_k}|$. Отсюда и из (20) следуют соотношения, аналогичные (3) и (4):
$$y'_{k+1}L \geqslant y'_{k+1}\sum_v p_v \geqslant \sum_v p_v q_v \geqslant \sum_{i=1}^{y'_k}|V_i| \geqslant \Delta'_{2^k}(M;\, x'_k),$$
$$y'_{k+1} \geqslant \frac{\Delta'_{2^k}(M;\, x'_k)}{L} = x'_{k+1}.$$
Далее доказательство леммы 1 повторяется почти дословно.

Лемма 2 доказана.

Теорема 2. *Если M — $(n, n, n/2)$-матрица, то*
$$L^2(M) = \Omega\Big(n\frac{\ln n}{\ln\ln n}\Big).$$

Доказательство. Теорема 2 доказывается аналогично теореме 1. Пусть $L = L^2(M)$, t — наименьшее число k такое, что $x'_k \leqslant 4 \cdot 2^k$. Тогда в силу (18) и следствия 2 б) имеем

$$x'_k \geqslant \frac{n}{2}\Big(\frac{n}{8L}\Big)^k, \quad k = 0, \dots, t.$$

Согласно лемме 2, $x'_{[2L/n]+1} = 0$, поэтому $2L/n \geqslant t$. Обозначим $z = 16L/n$ и проведём преобразования:

$$4 \cdot 2^t \geqslant x'_t \geqslant \frac{n}{2}\Big(\frac{n}{8L}\Big)^t,$$
$$1 \geqslant \frac{n}{8}\Big(\frac{n}{16L}\Big)^t = \frac{n}{8z^t} \geqslant \frac{n}{8z^{2L/n}} = \frac{n}{8z^{z/8}},$$
$$z^{z/8} \geqslant n/8,$$
$$z \ln z \geqslant 8(\ln n - \ln 8) \asymp \ln n,$$
$$z = \Omega\Big(\frac{\ln n}{\ln\ln n}\Big).$$

Теорема 2 доказана.

Работа выполнена при финансовой поддержке РФФИ (проект 05–01–00994), программы "Университеты России" (проект УР.04.02.528) и программы поддержки ведущих научных школ РФ (проект НШ–1807.2003.01).

Литература

1. Нигматуллин Р. Г. *Сложность булевых функций.* Наука, Москва, 1991.

2. Нечипорук Э. И. Об одной булевской матрице. В кн.: *Пробл. кибернетики, вып. 21.* Наука, Москва, 1969. с. 237–240.

3. Гринчук М. И. О сложности реализации последовательности треугольных булевых матриц вентильными схемами различной глубины. В кн.: *Методы дискретного анализа в синтезе управляющих систем, вып. 44.* ИМ СО АН СССР, Новосибирск, 1986. с. 3–23.

4. Alon N., Karchmer M., Wigderson A. Linear circuits over GF(2). *SIAM J. Comput.* (1990) **19**, 1064–1067.

5. Pudlak P. Communication in bounded depth circuits. *Combinatorica* (1994) **14**, No 2, 203–216.

6. Radhakrishnan J., Ta-Shma A. Bounds for dispersers, extractors, and depth-two superconcentrators. *SIAM J. of Discrete Mathematics* (2000) **13**, No 1, 2–24.

7. Pudlak P., Savicky P. On shifting networks. *Theoretical Comput. Sci.* (1993) **116**, 415–419.

8. Pudlak P., Rödl V., Sgall J. Boolean circuits, tensor ranks and communication complexity. *SIAM J. Comput.* (1997) **26**, No 3, 605–633.

9. Raz R., Shpilka A. Lower bounds for matrix product, in bounded depth circuits with arbitrary gates. *SIAM J. Comput.* (2003) **32**, No 2, 488–513.

10. Черухин Д. Ю. Нижняя оценка сложности в классе схем глубины 2 без ограничений на базис. *Вестник Московского университета. Серия 1. Математика. Механика.* (2005), No 4, 54–56.