ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Май—июнь 2010. Том 17, № 3. С. 3–18

УДК 519.7, 519.61

О СЛОЖНОСТИ ЛИНЕЙНЫХ БУЛЕВЫХ ОПЕРАТОРОВ С РЕДКИМИ МАТРИЦАМИ *)

С. Б. Гашков, И. С. Сергеев

Аннотация. Рассматривается задача построения квадратной булевой матрицы A порядка n без «прямоугольников» (такой матрицы, что составленная из её элементов, находящихся в каких-либо двух строках и двух столбцах, матрица не состоит из единиц), линейное преобразование по модулю два, определяемое которой, имеет сложность $o(\nu(A) - n)$ над базисом $\{\oplus\}$, где $\nu(A)$ — *вес* матрицы A, т. е. число единиц (такие матрицы без прямоугольников названы *редкими матрицами*). Приведены две конструкции, решающие данную задачу. В первой конструкции $n = p^2$, где p — нечётное простое число. Соответствующая матрица H_p имеет вес p^3 и порождает линейное преобразование сложности $O(p^2 \log p \log\log p)$. Во второй конструкции матрица имеет вес nk, где k — мощность множества Сидона в $\mathbb{Z}_n$. Можно считать, что $k = \Theta(\sqrt{n})$, для некоторых n известны примеры множеств мощности $k \sim \sqrt{n}$. При этом соответствующее линейное преобразование имеет сложность $O(n \log n \log\log n)$. Рассмотрены обобщения указанной задачи.

Ключевые слова: булева схема, сложность, линейный булев оператор, дискретное преобразование Фурье, конечное поле, циркулянтная матрица, множество Сидона.

Введение

В работе Б. С. Митягина и Б. Н. Садовского [13] приведено решение задачи, сформулированной в аннотации, которое, однако, оказалось неверным. В качестве матрицы без прямоугольников в [13] взята описанная ниже циркулянтная матрица, построенная на основе множества Сидона, сконструированного методом Зингера. Доказательство было основано на

*) Исследование выполнено при финансовой поддержке РФФИ (проекты 08–01–00863 и 08–01–00632–а), программы «Ведущие научные школы» (проект НШ–4470.2008.1) и программы фундаментальных исследований Отделения математических наук РАН «Алгебраические методы математической кибернетики и информационные системы нового поколения» (проект «Задачи оптимального синтеза управляющих систем»).

использовании метода Тоома быстрого умножения чисел [16] и теоремы о том, что сложность любого булевского оператора в базисе $\{\oplus, \&, 0, 1\}$ не меньше сложности его «линейной части», причём последняя реализуется в базисе $\{\oplus\}$ (по определению линейная часть не содержит единиц в качестве свободных членов).

Однако доказательство последней теоремы, как заметил Э. И. Нечипорук в [14], содержит, по-видимому, неустранимую ошибку, связанную с тем, что при перемножении многочленов по модулю два (т. е. многочленов Жегалкина) линейные члены в произведении получаются не только при умножении линейных членов одного из сомножителей на свободный член другого (т. е. на константу 1), но и при умножении линейного члена одного из сомножителей на такой же член другого сомножителя. Например, многочлен $(x \oplus y)(x \oplus z)$ имеет линейную часть x, а не 0, так как слагаемое x^2 следует учесть как x. В [14] Э. И. Нечипорук высказал предположение, что эта ошибка вызвана тем, что авторы, крупные специалисты по функциональному анализу, не учли непривычное для классического анализа тождество булевой алгебры $x^2 = x$.

На самом деле, сложность оператора может быть меньше сложности его линейной части, даже если последняя рассматривается в базисе всех двуместных булевых функций, т. е. теорема 1 из [13] неверна. В этом легко убедиться, рассмотрев оператор со следующими компонентами:

$$x \oplus z_1, \qquad x \oplus t_1,$$

$$x \oplus z_1 \oplus z_2, \qquad x \oplus t_1 \oplus t_2,$$

$$x \oplus z_1 \oplus z_2 \oplus y_1, \qquad x \oplus t_1 \oplus t_2 \oplus y_1,$$

$$x \oplus z_1 \oplus z_2 \oplus y_1 \oplus y_2, \qquad x \oplus t_1 \oplus t_2 \oplus y_1 \oplus y_2,$$

$$(x \oplus z_1 \oplus z_2 \oplus y_1 \oplus y_2)(x \oplus t_1 \oplus t_2 \oplus y_1 \oplus y_2).$$

Дальнейшие результаты [13] в той или иной степени опираются на эту теорему и, как отметил Э. И. Нечипорук, не могут считаться доказанными, кроме нескольких лемм и теоремы 2, которая ранее была доказана О. Б. Лупановым [11] в более сильной форме.

Заметим, что лемма 1 (приведённая без доказательства) фактически является леммой о транспозиции (если сложность рассматривать в базисе $\{\oplus\}$), появившейся независимо в статьях ряда авторов (см., например, [20]) несколько позднее, чем [13].

Возможно, что под влиянием [13] Э. И. Нечипорук [15] предложил свой (более элементарный, чем в [13]) пример матрицы без прямоугольников размера $n \times n$ и веса асимптотически $n^{3/2}$ при $n = p^2$, где p —

произвольное простое число, и доказал корректные варианты предложения 2 из [13], а именно, следующие утверждения: сложность реализации такой матрицы вентильными схемами асимптотически равна $n^{3/2}$ и сложность реализации соответствующей этой матрице системы дизъюнкций в монотонном базисе $\{\vee, \&\}$ тоже асимптотически равна $n^{3/2}$. В доказательстве нуждались по существу только нижние оценки, и на тот момент они были рекордными эффективными нижними оценками (т. е. нижними оценками для конкретно заданных индивидуальных булевых функций и операторов) в своём роде.

Впоследствии результат Э. И. Нечипорука был независимо повторен Ламаньей и Сэвиджем [26]. Теорема о нижней оценке сложности системы дизъюнкций из [15] Мельхорном в [12] была обобщена на более широкий класс матриц (см. также [29]). Это обобщение позволило для матрицы из работы [4] доказать оценку сложности $\Theta(n^{5/3})$ реализации соответствующей системы дизъюнкций в монотонном базисе. Вероятно, если бы Э. И. Нечипорук знал результат [4], он написал бы примерно то же, что и в [12], лет на десять раньше.

Рекордный результат в этом направлении получен в 1985 г. А. Е. Андреевым [1], который для любого t построил пример $(n \times n)$-матрицы веса $O_t(n^{2-1/t})$ без прямоугольников размера $O_t(1) \times O_t(1)$ и получил для этой матрицы нижние оценки вида $\Theta_t(n^{2-1/t})$ для сложности её реализации вентильными схемами (из [12] следуют подобные же оценки и для сложности реализации соответствующей системы дизъюнкций в монотонном базисе). Результат А. Е. Андреева в 1996 г. несколько усилен Роньяи с соавторами в [24].

По-видимому, никому до сих пор не удалось перенести указанные нижние оценки хотя бы в каком-нибудь виде на случай сложности схем, реализующих системы булевых линейных функций (т. е. линейных форм по модулю два) в немонотонном базисе $\{\oplus\}$.

В связи с отмеченными результатами представляет интерес вопрос о том, может ли сложность системы AX линейных форм по модулю два, определяемой по данной булевой матрице A без прямоугольников (далее эта величина $L_\oplus(AX)$ обозначается через $L_\oplus(A)$, так как однозначно определяется матрицей A), быть существенно меньше, чем вес матрицы (и согласно [15] меньше, чем сложность $L_\vee(A) = \nu(A) - m$ определяемой по матрице системы дизъюнкций, где m — число ненулевых строк матрицы A). Это тот самый вопрос, который неудачно попытались решить в [13]. Заметим, что в [13] фактически поставлен вопрос о величине $\lambda(n) = \max_{M_n} L_\vee(M_n)/L_\oplus(M_n)$, где M_n — булева матрица порядка n

(вместо $L_\vee(M_n)$ речь шла о другой мере сложности матрицы, но это несущественно), а также о величине $\lambda^*(n)$, определение которой отличается от $\lambda(n)$ тем, что рассматриваются только матрицы без прямоугольников. В [13] приведено ошибочное доказательство того, что $\lambda^*(n) > n^{1/2-o(1)}$ при достаточно больших n.

На самом деле, не очевидно даже, что $\lambda(n) > 1$ при некотором n. Впрочем, можно проверить, что $\lambda(n) = 1$ для $n \leqslant 4$ и что $\lambda(n) \geqslant \lambda^*(5) = 7/6$ для всех $n \geqslant 5$, предъявив подходящую матрицу порядка 5 [7]. В 1973 г. первый из авторов в курсовой работе показал, что $\lambda^*(n) \geqslant 3/2 - o(1)$, построив конкретный пример матрицы, на которой достигается это неравенство. Фактически было доказано чуть больше, а именно, что $2 \geqslant \lambda_3^*(n) \geqslant 3/2 - o(1)$, где определение функции $\lambda_3^*(n)$ отличается от определения $\lambda^*(n)$ тем, что вместо сложности реализации произвольными схемами в базисе $\{\oplus\}$ рассматриваются схемы глубины 3 (и только матрицы, реализуемые такими схемами). Впоследствии К. А. Зыков [8] усовершенствовал упомянутую конструкцию и доказал, что $\lambda_3^*(n) \geqslant 12/7 - o(1)$. Он же [7] показал, что $\lambda^*(n) \geqslant 2 - o(1)$.

Далее будет показано, что

$$\lambda^*(n) \geqslant \Theta(n^{1/2})/(\log n \log\log n),$$

что даже усиливает гипотетический результат из [13], причём оценка достигается на двух конкретных примерах матриц без прямоугольников — фактически тех самых примерах, которые предлагались в [13] и [15].

Заметим, что из упоминаемой ниже верхней оценки веса матриц без прямоугольников очевидно вытекает верхняя оценка $\lambda^*(n) = O(n^{1/2})$.

Если не ограничиваться матрицами без прямоугольников, то О. Б. Лупанов в 1960-х гг. в неопубликованной работе показал, что для матрицы Сильвестра (о ней см. ниже) отношение сложности вентильной схемы глубины два к сложности вентильной схемы по модулю два* той же глубины по порядку не меньше $n^{1/2}/\log n$.

Далее будет также показано, что

$$\lambda(n) \geqslant \Theta(n/c^{\sqrt{\log n \log\log n}}),$$

причём эта оценка достигается на конкретной матрице, построенной в работе [24]. Более того, используя результат М. И. Гринчука [6], можно

*В отличие от обычных вентильных схем, в случае схем по модулю два элемент $a_{i,j}$ реализуемой такой схемой матрицы равен 1 тогда и только тогда, когда число всех различных путей в схеме, соединяющих (входной и выходной) полюсы i и j, нечётно.

показать, что

$$O(n/\log n) \geqslant \lambda(n) \geqslant \Theta\left(n/\log^{O(1)} n\right),$$

но указать явно матрицу, на которой достигается нижняя оценка, не удаётся.

1. Первый пример — матрица Нечипорука

Пусть p — нечётное простое число. Рассмотрим кольцо

$$K_p = \mathrm{GF}(2)[x]/(x^p + 1).$$

Пусть элементы кольца K_p (классы эквивалентных по модулю $x^p + 1$ многочленов) кодируются коэффициентами (единственного) многочлена из класса степени, меньшей p.

В кольце K_p элемент x (более точно, эквивалентный класс с представителем x; в дальнейшем подобные оговорки будут опускаться) является корнем степени p из единицы. Таким образом, определено одностороннее ДПФ (дискретное преобразование Фурье) порядка p в данном кольце (одностороннее означает, что обратного преобразования не существует).

Пусть $f_0, \ldots, f_{p-1} \in K_p$. Тогда компоненты ДПФ вектора $(f_0, \ldots, f_{p-1})$ задаются формулами

$$f_j^* = \sum_{i=0}^{p-1} f_i x^{ij}, \qquad j = 0, \ldots, p-1.$$

Обозначим через H_p матрицу этого преобразования. Через E_0 обозначим единичную матрицу размера $p \times p$, а через E_i — матрицу, получаемую из E_0 циклическим сдвигом строк на i позиций вниз.

По свойству выбранного представления элементов кольца K_p умножение на x^k выполняется циклическим сдвигом коэффициентов — соответствующее преобразование задаётся матрицей E_k. Следовательно, матрица H_p имеет вид

$$H_p = \begin{bmatrix} E_0 & E_0 & \ldots & E_0 & \ldots & E_0 \\ E_0 & E_1 & \ldots & E_j & \ldots & E_{p-1} \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ E_0 & E_i & \ldots & E_{ij} & \ldots & E_{i(p-1)} \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ E_0 & E_{p-1} & \ldots & E_{(p-1)j} & \ldots & E_{(p-1)^2} \end{bmatrix}.$$

Проверим тот факт, что матрица H_p не содержит прямоугольников. Воспользуемся разбиением указанной матрицы на горизонтальные и вертикальные полосы ширины p, нумеруя их от 0 до $p-1$. Заметим, что на пересечении i-й горизонтальной и j-й вертикальной полосы расположена матрица E_{ij}.

Предположим, что некоторые две строки и некоторые два столбца матрицы H_p в пересечении образуют «единичный» прямоугольник. Пусть эти строки расположены в i_1-й и i_2-й горизонтальных полосах, а столбцы — в j_1-й и j_2-й вертикальных полосах. Очевидно, $i_1 \neq i_2$ и $j_1 \neq j_2$, так как в любой строке и любом столбце матрицы E_k содержится ровно по одной единице.

Легко видеть, что для любой строки i-й горизонтальной полосы расстояние между единицами из l_1-й и l_2-й вертикальных полос, где $l_1 < l_2$, совпадает с $i(l_1 - l_2)$ по модулю p. Согласно предположению имеем совпадение по модулю p расстояний между единицами i_1-й и i_2-й полос на пересечении с j_1-м и j_2-м столбцами. Таким образом,

$$i_1(j_1 - j_2) \equiv i_2(j_1 - j_2) \mod p,$$

откуда следует

$$(i_1 - i_2)(j_1 - j_2) \equiv 0 \mod p,$$

что невозможно в силу того, что $0 < |i_1 - i_2|, |j_1 - j_2| < p$.

Матрица H_p является матрицей Нечипорука [15] (ранее эта матрица была построена в [25]), в которой строки и столбцы нумеруются двойными индексами (a, b) и (x, y) соответственно, а единица стоит на пересечении строки (a, b) и столбца (x, y) в том и только том случае, когда $y \equiv ax + b \mod p$. Для столбцов следует принять лексикографический порядок нумерации:

$$(x, y) = (0,0), (0,1), \ldots, (0, p-1), (1,0), \ldots, (1, p-1), \ldots\ldots, (p-1, p-1),$$

а для строк несколько видоизменённый:

$$(a, b) = (0,0), (0,1), \ldots, (0, p-1), (p-1, 0), (p-1, 1), \ldots, (p-1, p-1),$$

$$(p-2, 0), (p-2, 1) \ldots, (p-2, p-1), \ldots\ldots, (1,0), (1,1), \ldots, (1, p-1).$$

Проверим: i-ю горизонтальную полосу такой матрицы определяет соотношение $a = -i \bmod p$, а j-ю вертикальную — соотношение $x = j$. Тогда позиции единиц матрицы в пересечении полос определяются из

соотношения $y \equiv -ij + b \mod p$, где b и y нумеруют строки и соответственно столбцы данной подматрицы. Это в точности матрица E_{ij}, что и требовалось доказать.

Очевидно, $\nu(H_p) = p^3$. Покажем, что сложность линейного преобразования с матрицей H_p, т. е. ДПФ порядка p в кольце K_p, составляет $O(p^2 \log p \log\log p)$. Для этого воспользуемся известным приёмом — сведéнием ДПФ порядка p к циклической свёртке двух векторов длины p над K_p. Эта свёртка сводится к умножению двоичных многочленов степени не выше $2p^2 - 1$.

Сведéние ДПФ к свёртке можно выполнить, например, методом Блюстейна или методом Райдера (см., например, [3]). Изложим первый из них как более простой. Положим $\beta = x^{(p-1)/2} \in K_p$. Заметим, что $\beta^{-2} = x$. Тогда

$$f_j^* = \sum_{i=0}^{p-1} f_i x^{ij} = \beta^{-j^2} \sum_{i=0}^{p-1} \beta^{(j-i)^2} \beta^{-i^2} f_i = \beta^{-j^2} \sum_{i+k \equiv j \bmod p} U_k V_i = \beta^{-j^2} C_j,$$

где $U_k = \beta^{k^2}$, $V_i = \beta^{-i^2} f_i$. Поскольку умножение на степени β выполняется с нулевой сложностью, сложность ДПФ порядка p совпадает со сложностью вычисления компонент $C_0, \ldots, C_{p-1}$ циклической свёртки векторов $(U_0, \ldots, U_{p-1})$ и $(V_0, \ldots, V_{p-1})$. Определим многочлены $u(y) = \sum U_i y^i$, $v(y) = \sum V_i y^i$, $c(y) = \sum C_i y^i$. По построению

$$c(y) = u(y)v(y) \bmod (y^p + 1).$$

Это умножение можно интерпретировать как умножение в кольце

$$K_{p,2} = (\mathrm{GF}(2)[x]/(x^p + 1))[y]/(y^p + 1) \cong \mathrm{GF}(2)[x, y]/(x^p + 1,\, y^p + 1).$$

Оно стандартным образом (при помощи подстановки Кронекера) сводится к умножению двоичных многочленов степени $2p^2 - 1$. Справедлива более общая, чем требуется в данном случае,

Лемма 1. *Умножение в кольце*

$$K_{p,t} = \mathrm{GF}(2)[x_1, x_2, \ldots, x_t]/\left(x_1^p + 1,\, x_2^p + 1, \ldots,\, x_t^p + 1\right)$$

выполняется билинейной схемой сложности $O((2p)^t t \log p \log(t \log p))$ *и глубины* $O(t \log p)$.

Доказательство. Элементы кольца $K_{p,t}$ представляются многочленами переменных $x_1, \ldots, x_t$ степени не выше $p-1$ по каждой переменной.

В результате умножения таких многочленов (без приведения по модулям) получается многочлен степени не выше $2p-2$ по каждой переменной. Рассмотрим замену переменных

$$x_1 = x, \quad x_2 = x^{2p}, \quad \ldots, \quad x_t = x^{(2p)^{t-1}},$$

которая элементы $K_{p,t}$ переводит в двоичные многочлены переменной x степени меньше $(2p)^t/2$. Обратная замена выполняется по правилу

$$x^{[m_t,\ldots,m_1]_{2p}} = x_t^{m_t} \cdot \ldots \cdot x_1^{m_1},$$

где $[m_t, \ldots, m_1]_{2p}$ — запись числа в системе счисления с основанием $2p$.

Указанная замена сохраняет произведение многочленов t переменных, если оно имеет степень не выше $2p-1$ по каждой из переменных. Это легко проверить, так как в силу линейности проверку можно ограничить мономами.

Замена переменных в обе стороны выполняется с нулевой сложностью. Умножение двоичных многочленов степени m можно выполнить билинейным алгоритмом А. Шёнхаге [28] сложности $O(m \log m \log\log m)$ и глубины $O(\log m)$. Приведение произведения по модулям $x_i^p + 1$ по сути есть приведение подобных слагаемых и выполняется со сложностью $(2p)^t$: независимых слагаемых — p^t, подобных слагаемых в каждой группе — не более 2^t. Лемма 1 доказана.

Билинейность означает, что в случае, когда один из множителей является постоянным, схема умножения вырождается в схему над базисом $\{\oplus, 0\}$.

В рассматриваемом случае постоянным является множитель $u(y)$. Таким образом, сложность ДПФ порядка p над K_p и, как следствие, $L_\oplus(H_p)$, составляют $O(p^2 \log p \log\log p)$, откуда вытекает оценка

$$\frac{L_\vee(H_p)}{L_\oplus(H_p)} \geqslant \Theta(p)/(\log p \log\log p).$$

2. Второй пример — циркулянтная матрица

Циркулянтной называется квадратная матрица, каждая строка которой получается циклическим сдвигом предыдущей строки на одну позицию. Таким образом, циркулянтная $(n \times n)$-матрица имеет вид

$$\begin{bmatrix} a_0 & a_1 & \ldots & a_j & \ldots & a_{n-1} \\ a_{n-1} & a_0 & \ldots & a_{j+1} & \ldots & a_{n-2} \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ a_1 & a_2 & \ldots & a_{j-1} & \ldots & a_0 \end{bmatrix}.$$

Как известно (см., например, [21]), линейное преобразование с циркулянтной матрицей есть циклическая свёртка с вектором, образованным коэффициентами первой строки матрицы. Используя метод Шёнхаге умножения многочленов с коэффициентами из поля GF(2), умножение булевского вектора на булевскую циркулянтную матрицу по модулю два можно реализовать со сложностью $O(n \log n \log\log n)$.

Для построения циркулянтной матрицы без прямоугольников рассмотрим множество $S = \{s_1, \ldots, s_k\} \subset \mathbb{Z}_n$, в котором все разности $s_i - s_j$, где $i \neq j$, различны (эта конструкция имеется в [13], но была известна и ранее). Такое множество называется *множеством Сидона* [27]. Для всех $i = 1, \ldots, k$ положим $a_{s_i} = 1$, а остальные a_j положим равными нулю.

Определённая таким способом циркулянтная матрица состоит из k циклических единичных диагоналей, проходящих через s_i-е позиции первой строки. Величины $s_i - s_j$ имеют смысл расстояния между соответствующими диагоналями. Единицы, стоящие на одинаковых позициях в некоторых двух строках, относятся к разным циклическим диагоналям. Следовательно, если бы по две единицы в некоторых двух строках были расположены на одних и тех же позициях, то для каждой из строк эти единицы относились бы к различным (упорядоченным) парам циклических диагоналей, но это противоречит построению: расстояния между диагоналями не повторяются. Поэтому построенная матрица не содержит прямоугольников.

Известно, что $k = \Theta(\sqrt{n})$, в частности, $k < \sqrt{n} + 1/2$ (см., например, [27]). Следуя [27], приведём несколько примеров, в которых достигается асимптотическая оценка $k \sim \sqrt{n}$.

(i) Множество Ружи. Пусть $n = p(p-1)$, где p — простое число, а ζ — порождающий элемент мультипликативной группы поля GF(p). Положим $k = p - 1$, а s_i определим из соотношений

$$s_i \equiv i \mod (p-1), \qquad s_i \equiv \zeta^i \mod p.$$

(ii) Множество Боуза. Пусть $n = q^2 - 1$, где q — степень простого числа, $k = q$. Пусть θ — примитивный элемент в поле GF(q^2). Положим $S = \{s_i \in [0,\, q^2 - 1] \mid \theta^{s_i} = \theta + \alpha_i,\ \mathrm{GF}(q) = \{\alpha_1, \ldots, \alpha_q\}\}$.

(iii) Множество Зингера (см. также [17]). Пусть $n = q^2 + q + 1$, q — степень простого числа, $k = q + 1$. Пусть θ — примитивный элемент в поле GF(q^3). Положим

$$S = \{0\} \cup \{s_i \in [1,\, q^2+q+1] \mid \theta^{s_i}/(\theta+\alpha_i) \in \mathrm{GF}(q),\ \mathrm{GF}(q) = \{\alpha_1, \ldots, \alpha_q\}\}.$$

Для построения описанной выше циркулянтной матрицы без прямоугольников вместо множества Сидона можно с тем же успехом использовать близкое к нему $(n, k, 1)$-разностное множество (k-элементное подмножество $\mathbb{Z}_n$, разности элементов которого различны и образуют $\mathbb{Z}_n$). Зингер [17, 27] построил семейство разностных множеств, одно из которых совпадает с указанным выше множеством Сидона. (Подробнее о разностных множествах и примере Зингера см. [17].)

Известно, что матрица, построенная на основе множества Зингера, фактически совпадает с матрицей, строки которой представляют собой характеристические функции прямых конечной проективной плоскости порядка q. Тот факт, что матрица не содержит прямоугольников, вытекает из того, что любые две прямые проективной плоскости пересекаются ровно в одной точке. С этой точки зрения матрица Нечипорука представляет собой матрицу характеристических функций прямых конечной аффинной плоскости порядка p. Разумеется, в последней можно взять вместо p степень любого простого числа, если в качестве аффинной плоскости использовать координатную плоскость над конечным полем $\mathrm{GF}(q)$ (подобные вопросы рассматриваются, например, в [10]).

Во всех приведённых примерах матрицы относятся к числу наиболее плотных в классе матриц без прямоугольников: несложно убедиться в том, что $(n \times n)$-матрица без прямоугольников не может иметь вес более $n^{1,5}+n/2$. Примечательно, что при этом циркулянтная матрица, основанная на множестве Зингера, имеет в точности максимально возможный вес для $n = q^2 + q + 1$ (доказательство этого факта можно найти в [10] или [18]).

М. И. Гринчук доказал в [6] существование циркулянтных булевских $(n \times n)$-матриц Z_n таких, что $L_{\vee,\&}(Z_n) \geqslant \Theta(n^2/\log^{O(1)} n)$ (на самом деле, он конкретно указал константу в знаке $O(1)$ и получил аналогичный результат для сложности реализации таких матриц вентильными схемами как глубины два, так и произвольной глубины). Отсюда и из указанной выше оценки сложности умножения циркулянтной матрицы на вектор по модулю два следует, что $\lambda(n) \geqslant \Theta(n/\log^{O(1)} n)$. Однако эта оценка неэффективна, так как матрица, на которой она достигается, не указана явно. Из упоминавшейся выше принадлежащей О. Б. Лупанову [11] верхней оценки $L_\vee(M_n) = O(n^2/\log n)$ вытекает, что $\lambda(n) = O(n/\log n)$.

3. Обобщения первого примера

Рассмотрим умножение на константу

$$a = \sum_{\{0 \leqslant k_1 < p,\, \ldots,\, 0 \leqslant k_t < p\}} a_{(k_1, \ldots, k_t)} x_1^{k_1} \cdot \ldots \cdot x_t^{k_t}.$$

в кольце $K_{p,t}$ (см. лемму 1). Для коэффициентов $A_{(i_1,\ldots,i_t),(j_1,\ldots,j_t)}$ матрицы умножения на a имеет место свойство цикличности

$$A_{(i_1,\ldots,i_t),(j_1,\ldots,j_t)} = a_{(\,(i_1-j_1) \bmod p,\ldots,(i_t-j_t) \bmod p\,)}. \tag{1}$$

Действительно, коэффициент $c_{(i_1,\ldots,i_t)}$ при мономе $x_1^{i_1}\cdot\ldots\cdot x_t^{i_t}$ произведения $ab \in K_{p,t}$, где $b = \sum b_{(j_1,\ldots,j_t)} x_1^{j_1}\cdot\ldots\cdot x_t^{j_t}$, вычисляется по формуле

$$c_{(i_1,\ldots,i_t)} = \sum_{\{(j_1+k_1) \bmod p = i_1,\ \ldots,\ (j_t+k_t) \bmod p = i_t\}} a_{(k_1,\ldots,k_t)} b_{(j_1,\ldots,j_t)}.$$

Ясно, что циклическая в смысле (1) матрица есть матрица умножения на некоторую константу кольца $K_{p,t}$. Соответствующее линейное преобразование можно реализовать способом леммы 1.

1. Матрица Брауна [4]. Пусть p — простое число. Если выбрать в качестве первой строки «циклической» (p^3,p^3)-матрицы булевский вектор, изображающий характеристическую функцию p-ичной трёхмерной сферы $x^2+y^2+z^2=\alpha$, то остальные строки матрицы со свойством цикличности (1) будут изображать характеристические функции сфер $(x-a)^2+(y-b)^2+(z-c)^2=\alpha$, полученных из исходной сферы произвольным сдвигом, $a,b,c \in \mathrm{GF}(p)$. Параметр $\alpha \in \mathrm{GF}(p)$ выбирается так, что любые три такие сферы пересекаются не более чем в двух точках, поэтому матрица не содержит прямоугольников размера 3×3. Мощность каждой сферы равна p^2-p, поэтому вес матрицы равен p^5-p^4. Следовательно, согласно [12] нижняя оценка сложности реализации монотонными схемами системы дизъюнкций, определяемой такой матрицей C_n, где $n=p^3$, имеет вид $L_{\vee,\&}(C_n) \geqslant (1/4-o(1))n^{5/3}$, а очевидная верхняя оценка равна $L_\vee(C_n)=O(n^{5/3})$. Согласно лемме 1 верхняя оценка сложности реализации линейного преобразования по модулю два, определяемого матрицей C_n, есть $L_\oplus(C_n) = O(n\log n\log\log n)$. Поэтому имеем эффективный пример булевской $(n\times n)$-матрицы C_n такой, что

$$\frac{L_{\vee,\&}(C_n)}{L_\oplus(C_n)} \geqslant \Theta(n^{2/3})/(\log n\log\log n).$$

2. Матрица Коллара — Роньяи — Жабо [24]. Пусть p — простое число, $t\in\mathbb{N}$. В качестве первой строки (p^t,p^t)-матрицы выберем вектор, изображающий характеристическую функцию множества $x^{(p^t-1)/(p-1)}=1$ в поле $\mathrm{GF}(p^t)$ (это множество элементов нормы 1). В матрице, достроенной по правилу (1), любая строка изображает характеристическую функ-

цию множества $(x-\alpha)^{(p^t-1)/(p-1)} = 1$ при некотором $\alpha \in \mathrm{GF}(p^t)$. Элементы поля $\mathrm{GF}(p^t)$ кодируются p-ичными векторами длины t — коэффициентами разложения в некотором базисе над $\mathrm{GF}(p)$. В [24] показано, что данная матрица не содержит прямоугольников размера $t \times (t!+1)$ (и, в силу симметрии, размера $(t!+1) \times t$). Мощность множества единичной нормы в $\mathrm{GF}(p^t)$ равна $(p^t-1)/(p-1)$. Поэтому из [12] для этой матрицы R_n, $n = p^t$, имеем оценки

$$L_{\vee}(R_n) \gtrsim \frac{n^{2-1/t}}{t \cdot t!}, \qquad L_{\vee,\&}(R_n) \gtrsim \frac{n^{2-1/t}}{t^2 t!}.$$

С другой стороны, $L_{\oplus}(R_n) = O(2^t n \log n \log\log n)$ согласно лемме 1. При $t \asymp \log p / \log\log p$ получаем

$$\frac{L_{\vee,\&}(R_n)}{L_{\oplus}(R_n)} \geqslant \Theta(n/c^{\sqrt{\log n \log\log n}}),$$

где c — постоянная.

4. Замечания

Упомянутые верхние оценки можно также распространить на случай матриц над произвольным коммутативным кольцом K — в базис при этом надо включить линейные арифметические операции: сложение, вычитание и умножение на константы из K (первый пример годится не для всех колец). Оценки сложности в обоих примерах зависят от алгоритма умножения над K и могут быть записаны в виде $O(M(n))$ (в первом примере $n = p^2$), где $M(k)$ — сложность алгоритма умножения многочленов степени k. Оценка $M(k) = O(k \log k \log\log k)$ справедлива при любом K [22]. В некоторых случаях она может быть улучшена: например, для $K = \mathbb{C}$ имеет место $M(k) = O(k \log k)$, что влечёт оценку сложности матриц из обоих примеров $O(n \log n)$.

Во время написания [13] не был известен метод Шёнхаге быстрого умножения, понятия ДПФ и циклической свёртки были малоизвестны, иначе бы то, что написано здесь, давно было бы кем-нибудь опубликовано. Тем не менее заметим, что, например, для зингеровой матрицы без прямоугольников результат $\lambda(n) > n^{O(1)}$ можно было получить, используя вместо метода Шёнхаге простейший «троичный» вариант метода Тоома для умножения двоичных многочленов с оценкой сложности $O(n^{\log_3 5})$ (для этого достаточно рассмотреть умножение многочленов с коэффициентами не в поле $\mathrm{GF}(2)$, а в поле $\mathrm{GF}(2^3)$, или даже $\mathrm{GF}(2^2)$, если применить один известый трюк). «Двоичный» вариант метода Тоома,

т. е. метод Карацубы, для этого недостаточен. Любопытно, однако, что, тем не менее, в случае матрицы Нечипорука при $p = 7$, используя для вычисления ДПФ 7-го порядка метод Райдера сведения его к циклической свёртке 6-го порядка и вычисляя последнюю методом Карацубы в сочетании с обычным методом умножения квадратных трехчленов, получаем неравенство $\lambda(49) \geqslant 42/41$.

Основные результаты статьи относительно функции $\lambda(n)$ остаются, очевидно, справедливыми, если в её определении заменить $L_\vee(M_n)$ сложностью реализации этой матрицы вентильными схемами и вентильными схемами глубины два, а также просто весом матрицы. В последнем случае пример матрицы, для которой соответствующее отношение не меньше $n/2 + 1/(2n-2)$, строится тривиально — это матрица Q_n, всюду заполненная единицами, кроме соседней с главной диагонали, так как для неё $L_\oplus(Q_n) \leqslant 2n-2$. Очевидно также, что $L_\vee(Q_n) \leqslant 3n-6$. В то же время сложность реализации этой матрицы вентильными схемами глубины два по порядку равна $n \log n$ согласно известному результату Анселя и Р. Е. Кричевского [2, 10], а сложность реализации произвольными вентильными схемами по порядку равна n согласно результату, полученному независимо Чандра, Форчуном и Липтоном [23] и М. И. Гринчуком [5]. На самом деле, М. И. Гринчук получил и нижнюю, точную по порядку, оценку. А именно, он показал, что сложность реализации вентильными схемами глубины h матрицы P_n, в которой единицы стоят ниже главной диагонали, а на ней и выше — нули, равна по порядку $nF_h(n)$, где $F_1(n) = n$, $F_2(n) = \lceil \log_2 n \rceil$, $F_2(n) = 0$ при $n \leqslant 1$, $F_3(n) = 1 + \lceil \log_2 \log_2 n \rceil$, $F_3(n) = 0$ при $n \leqslant 1$, $F_h(n) = G(F_{h-2}(n), n)$, где оператор $G(f(n), n)$ для произвольной функции $f(n)$ такой, что $f(0) = 0$, $f(n) < n$ при $n > 0$, определяется как минимальное натуральное m такое, что $f^{(m)}(n) \leqslant 1$, где $f^{(0)}(n) = n$, $f^{(m)}(n) = f(f^{(m-1)}(n))$. В [23] вместо функции $F_h(n)$ использовалась другая функция, определение которой основывалось на обращении рекурсивной функции Аккермана.

Вопрос о получении нетривиальных эффективных нижних оценок $L_\oplus(M_n)$ для конкретных матриц представляется трудным. Очевидно, что в классе всех циркулянтных матриц такой оценки нет, так как для матрицы J_n, получаемой из упомянутой выше матрицы Q_n удалением одной единицы, справедлива оценка $L_\oplus(J_n) \leqslant 2n-1$. Алон, Карчмер и Вигдерсон [19] получили для сложности реализации вентильными схемами по модулю два глубины два произвольной булевой матрицы Адамара A_n (т. е. (n, n)-матрицы (в булевом случае), расстояние Хэмминга между любыми двумя строками которой равно $n/2$) нижнюю оценку $\Theta(n \log n)$.

Для одной из таких матриц, а именно, для матрицы Сильвестра* S_n, они получили верхнюю оценку $O(n)$ сложности реализации произвольными вентильными схемами по модулю два (а в случае её реализации вентильными схемами по модулю два глубины два — оценку $\Theta(n \log n)$). Их методом, используя представление $S_n = D_n \times D_n^T$, где D_n — матрица, образованная всеми n различными булевыми строками длины $\log_2 n$, можно показать, что $L_\oplus(S_n) \leqslant 3n$, причём одновременно глубина схемы равна $O(\log n)$.

Представляет интерес также вопрос об оценке величины

$$\Lambda(n) = \max_{A_n} \frac{L_\oplus(A_n)}{L_\vee(A_n)},$$

в какой-то мере обратной к $\lambda(n)$. Из верхней оценки О. Б. Лупанова [11] для $L_\oplus(A_n)$ следует, что $\Lambda(n) = O(n/\log n)$. Можно предположить, что $\Lambda(n) \to \infty$. Если $\Lambda(n) > 3+\varepsilon$, то получится контрпример к теореме 1 [13].

Рассмотрим матрицу B_n порядка $n = 2^k$, составленную из трёх подматриц $B_{n/2}$ и одной подматрицы того же размера, состоящей только из единиц. По аналогии с матрицей Сильвестра можно представить B_n как произведение матриц D_n и D_n^T, при этом в определении операции умножения матриц вместо сложения по модулю два используется дизъюнкция. Тогда аналогично оценке $L_\oplus(S_n) \leqslant 3n$ можно доказать, что $L_\vee(B_n) \leqslant 3n$. Легко доказать, что $L_\oplus(B_n) = O(n \log n)$. Можно предположить, что $L_\oplus(B_n)/n \to \infty$. Если удастся доказать, что $L_\oplus(B_n) = o(n \log n)$, то получится, что преобразование Мёбиуса, переводящее многочлен Жегалкина в совершенную д.н.ф., имеет тоже сложность $o(n \log n)$, так как она равна $L_\oplus(B_n) + O(n)$.

Справедливость ряда утверждений из работы [13], по всей видимости, до сих пор остаётся под вопросом. Например, верно ли, что сложность линейного булева оператора в базисе Жегалкина $\{\oplus, \&, 0, 1\}$ совпадает с его сложностью в линейном базисе $\{\oplus, 0\}$ (предложение 1 из [13])? Известно, что ответ на аналогичный вопрос с операцией дизъюнкции вместо $\oplus$ — отрицательный [29].

ЛИТЕРАТУРА

1. **Андреев А. Е.** Об одном семействе булевых матриц // Вестн. МГУ. Математика. Механика. — 1986. — Вып. 2. — С. 97–100.

*Матрица Сильвестра S_n строится индуктивно из трёх матриц $S_{n/2}$ и одной матрицы $\overline{S_{n/2}}$ (черта сверху означает поэлементное отрицание матрицы).

2. **Ансель Ж.** Минимальное число замыкающих контактов, достаточное для реализации симметрической булевой функции n переменных // Кибернетический сб. Вып. 5. — М.: Мир, 1968. — С. 47–52.
3. **Блейхут Р.** Быстрые алгоритмы цифровой обработки сигналов. — М.: Мир, 1989. — 448 с.
4. **Браун У. Г.** Графы, не содержащие графа Томсена // Кибернетический сб. Вып. 18. — М.: Мир, 1981. — С. 34–38.
5. **Гринчук М. И.** О сложности реализации последовательности булевых матриц вентильными схемами различной глубины // Методы дискретного анализа в синтезе управляющих систем. Вып. 44. — 1986. — С. 3–23.
6. **Гринчук М. И.** О сложности реализации циклических булевых матриц вентильными схемами // Изв. вузов. Математика. — 1988. — № 7. — С. 39–44.
7. **Зыков К. А.** О сравнении сложности двух способов реализации некоторых линейных булевых преобразований // Дискрет. математика. — 1996. — Т. 8, вып. 2. — С. 151–159.
8. **Зыков К. А.** О сложности реализации линейных булевых преобразований схемами глубины три // Вест. МГУ. Математика. Механика. — 1998. — № 2. — С. 68–70.
9. **Картеси Ф.** Введение в конечные геометрии. — М.: Мир, 1980. — 320 с.
10. **Кричевский Р. Е.** О сложности параллельно-последовательных схем, реализующих одну последовательность булевых функций // Проблемы кибернетики. Вып. 12. — М.: Наука, 1964. — С. 45–55.
11. **Лупанов О. Б.** О вентильных и контактно-вентильных схемах // Докл. АН СССР. — 1956. — Т. 111, № 6. — С. 1171–1174.
12. **Мельхорн К.** Некоторые замечания, касающиеся булевых сумм // Кибернетический сб. Вып. 18. — М.: Мир, 1981. — С. 39–45.
13. **Митягин Б. С., Садовский Б. Н.** О линейных булевских операторах // Докл. АН СССР. — 1965 — Т. 165, № 4. — С. 773–776.
14. **Нечипорук Э. И.** Реферат 1.В.206. // РЖМат. №1. — 1967.
15. **Нечипорук Э. И.** Об одной булевской матрице // Проблемы кибернетики. Вып. 21. — М.: Наука, 1969. — С. 237–240.
16. **Тоом А. Л.** О сложности схемы из функциональных элементов, реализующей умножение целых чисел // Докл. АН СССР. — 1963. — Т. 150, № 3. — С. 496–498.
17. **Холл М.** Комбинаторика. — М.: Мир, 1970. — 424 с.
18. **Эрдёш П., Спенсер Дж.** Вероятностные методы в комбинаторике. — М.: Мир, 1976. — 130 с.
19. **Alon N., Karchmer M., Wigderson A.** Linear circuits over GF(2) // SIAM J. Comput. — 1990 — Vol. 19, N 6. — C. 1064–1067.
20. **Bernstein D. J.** The transposition principle // http://cr.yp.to/transposition.html

21. Bini D., Pan V. Polynomial and matrix computations. Vol. 1. — Boston: Birkhäuser, 1994. — 415 p.

22. Cantor D., Kaltofen E. On fast multiplication of polynomials over arbitrary algebras // Acta Inf. — 1991. — Vol. 28, N 7. — С. 693–701.

23. Chandra A. K., Fortune S., Lipton R. Unbounded fan-in circuits and associative functions // Proc. 15th ACM Symp. Theory Comput. — New-York: ACM, 1983. — С. 52–60.

24. Kóllar J., Rónyai L., Szabó T. Norm-graphs and bipartite Turán numbers // Combinatorica. — 1996. — Vol. 16, N 3. — С. 399–406.

25. Kövari T., Sós V. T., Turán P. On a problem of K. Zarankiewicz // Coll. Math. — 1954. — Vol. 3. — С. 50–57.

26. Lamagna E. A., Savage J. E. Computational complexity of some monotone functions // Proc. 15th SWAT Conference. — Long Beach: IEEE Comput. Soc. Press, 1974. — С. 140–144.

27. O'Bryant K. A complete annotated bibliography of work related to Sidon sequences // Elect. J. Comb. — 2004. (Dynamic survey, Vol. 11).

28. Schönhage A. Schnelle multiplikation von polynomen über körpern der charakteristik 2. — Acta Inf. — 1977. — Vol. 7. — С. 395–398.

29. Wegener I. The complexity of boolean functions. — Stuttgart: Wiley, 1987. — 470 p.

Гашков Сергей Борисович,
e-mail: sbgashkov@gmail.com

Сергеев Игорь Сергеевич,
e-mail: isserg@gmail.com

Статья поступила
22 октября 2009 г.