ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Сентябрь—октябрь 2011. Том 18, № 5. С. 38–53

УДК 519.7

РЕДКИЕ ЦИРКУЛЯНТНЫЕ МАТРИЦЫ И НИЖНИЕ ОЦЕНКИ СЛОЖНОСТИ НЕКОТОРЫХ БУЛЕВЫХ ОПЕРАТОРОВ *)

М. И. Гринчук, И. С. Сергеев

Аннотация. Доказана нижняя оценка $\Omega\big(\frac{k+l}{k^2l^2}N^{2-\frac{k+l+2}{kl}}\big)$ максимально возможного веса (k,l)-редкой (т. е. не содержащей единичных подматриц размера $k\times l$) циркулянтной матрицы порядка N. Эта оценка близка к известной оценке для класса всех (k,l)-редких матриц. В качестве следствия получены новые нижние оценки для нескольких мер сложности систем булевых сумм и нижняя оценка $\Omega(N^2\log^{-6}N)$ монотонной сложности булевой свёртки порядка N.

Ключевые слова: сложность, циркулянтная матрица, редкая матрица, проблема Заранкевича, монотонная схема, вентильная схема, булева сумма, булева свёртка.

Введение

Булева матрица, не содержащая единичных подматриц размера $k\times l$, называется (k,l)-*редкой матрицей* (под единичными матрицами здесь и далее понимаются матрицы, все элементы которых равны 1). При $k=l$ используется термин k-*редкая матрица*. Далее полагаем $2\leqslant k\leqslant l$.

Матрица $(c_{i,j})$ порядка N называется *циркулянтной* (или циклической), если либо $c_{i,j}=c_{0,(i+j)\bmod N}$ при любых i,j, либо $c_{i,j}=c_{0,(i-j)\bmod N}$ при любых i,j.

В [1] первый автор доказал существование k-редких циркулянтных $N\times N$-матриц веса[1)] $\Omega(k^{-4}N^{2-\sqrt{3/k}})$ и получил следствия для слож-

*) Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований (проекты 08–01–00863 и 08–01–00632) и программы фундаментальных исследований Отделения математических наук РАН «Алгебраические и комбинаторные методы математической кибернетики и информационные системы нового поколения» (проект «Задачи оптимального синтеза управляющих систем»).

1) *Вес* матрицы — число ненулевых элементов в ней.

ности[2)] систем булевых сумм[3)], соответствующих циркулянтным матрицам, при реализации вентильными схемами и вентильными схемами глубины (ранга) 2. Более конкретно, для первой задачи получена оценка $\Omega(N^2 \log^{-12} N)$, а для второй — $\Omega(N^2 \log^{-10} N)$.

На самом деле, в методе заложена возможность для уточнения оценок, что представляет интерес, например, в связи с проблемой Заранкевича (подробно о ней рассказано, например, в [7]). Эта возможность состоит в применении более точной оценки мощности суммы двух множеств в евклидовом пространстве, следующей из работ [9, 10].

Ниже показано, что существуют (k, l)-редкие циркулянтные матрицы порядка N с весом $\Omega\bigl(\frac{k+l}{k^2 l^2} N^{2-\frac{k+l+2}{kl}}\bigr)$. Для сравнения классический результат Эрдеша — Спенсера [7] даёт лишь чуть лучшую оценку $\Omega_{k,l}(N^{2-\frac{k+l-2}{kl-1}})$ в классе всех (k, l)-редких матриц.

Как следствие устанавливается существование циркулянтной матрицы такой, что для сложности соответствующей ей системы булевых сумм справедливы оценки: $\Omega(N^2 \log^{-6} N)$ при реализации схемами из функциональных элементов[4)] над базисом $\{\vee, \wedge\}$, $\Omega(N^2 \log^{-5} N)$ — схемами над базисом $\{\vee\}$ или вентильными схемами, $\Omega(N^2 \log^{-4} N)$ — вентильными схемами глубины 2.

В [1] рассматривается величина $\lambda(N) = \max\limits_A \frac{L_\vee(A)}{L_\oplus(A)}$, где $L_\vee(A)$ — сложность системы булевых сумм с матрицей A при реализации схемами над базисом $\{\vee\}$, а $L_\oplus(A)$ — сложность линейного оператора с матрицей A при реализации схемами над базисом $\{\oplus\}$ и максимум берётся по матрицам порядка N. Результат настоящей работы позволяет указать оценку $\lambda(N) = \Omega\bigl(\frac{N}{(\log N)^6 \log\log N}\bigr)$, в определённом смысле близкую к верхней оценке $\lambda(N) = O(N/\log N)$.

В качестве ещё одного следствия получаем, что сложность булевой свёртки порядка N при реализации схемами над базисом $\{\vee, \wedge\}$ равна $\Omega(N^2 \log^{-6} N)$, более конкретно, эта оценка справедлива для числа дизъюнкторов в любой вычисляющей свёртку монотонной схеме. В литературе даже последних лет (например, [3, 8]) в качестве рекордной фигурирует оценка $\Omega(N^{3/2})$, хотя более сильный результат вытекает из [2]

[2)] Используемые далее понятия *сложности*, *глубины*, *вентильной схемы*, *схемы из функциональных элементов* определяются, например, в [4, 5].

[3)] *Булева сумма* — это функция вида $x_1 \vee \ldots \vee x_n$. Система булевых сумм с матрицей $(c_{i,j})$ порядка N есть вектор-функция с компонентами $\bigvee\limits_{j=1}^{N} c_{i,j} x_j$, $1 \leqslant i \leqslant N$.

[4)] Далее схемы из функциональных элементов называются просто схемами.

автоматически[5)]. Полученная нижняя оценка близка к очевидной верхней оценке $O(N^2)$.

1. Свойства «прямоугольников»

Изложим основной результат, следуя схеме доказательства из [2]. Пусть $k, l \in \mathbb{N}$, $2 \leqslant k \leqslant l$. Обозначим $\mathbb{Z}_+ = \mathbb{N} \cup \{0\}$. Элементы множества

$$R_{k,l} = \left\{(x_1, \ldots, x_k, y_1, \ldots, y_l) \in \mathbb{Z}_+^{k+l} \mid \forall_{i \neq j}(x_i \neq x_j),\ \forall_{i \neq j}(y_i \neq y_j)\right\}$$

будем называть *прямоугольниками*.

Пусть $E = (a_1, \ldots, a_k, b_1, \ldots, b_l)$ — прямоугольник. Обозначим число точек прямоугольника через $m(E) = |\{a_i + b_j \mid 1 \leqslant i \leqslant k,\ 1 \leqslant j \leqslant l\}|$.

Рассмотрим систему $S(E)$ линейных уравнений

$$\{x_r + y_s = x_u + y_v \mid a_r + b_s = a_u + b_v,\ 1 \leqslant r, u \leqslant k,\ 1 \leqslant s, v \leqslant l\}$$

над полем $\mathbb{R}$. Множество решений системы образует линейное подпространство T_E в $\mathbb{R}^{k+l}$, его размерность обозначим через $n(E)$. Через $C(E)$ обозначим множество прямоугольников $\{(x_1, \ldots, x_k, y_1, \ldots, y_l)\}$, удовлетворяющих системе уравнений $S(E)$ и не удовлетворяющих никаким другим уравнениям вида $x_r + y_s = x_u + y_v$ (класс эквивалентности в терминологии [2]).

Для вывода основных результатов удобно иметь оценку числа прямоугольников с ограниченными (некоторым числом N) координатами и заданным числом точек. Эта зависимость (между числом прямоугольников и числом точек) будет установлена в неявной форме посредством промежуточного параметра $n(E)$, а именно, оценено число прямоугольников E, характеризующихся заданным значением параметра $n(E)$, и затем получены соотношения между $n(E)$ и $m(E)$.

Число прямоугольников с координатами $0 \leqslant x_1, \ldots, y_l < N$ в классе $C(E)$ можно грубо оценить при помощи следующей леммы.

Лемма 1. *Пусть $N \in \mathbb{N}$. Тогда $|C(E) \cap \{0, \ldots, N-1\}^{k+l}| \leqslant N^{n(E)}$.*

Доказательство. Координаты $x_1, \ldots, x_k, y_1, \ldots, y_l$ вектора из T_E определяются значениями $n(E)$ свободных переменных-координат, которые в случае, если вектор принадлежит $C(E) \cap \{0, \ldots, N-1\}^{k+l}$, можно задать не более чем $N^{n(E)}$ способами. Лемма 1 доказана.

Следующая лемма оценивает число классов, характеризующихся заданным значением $n(E)$.

[5)] При этом в [3] допущена неточность: оценка $\Omega(N^{3/2})$ должна быть отнесена к числу дизъюнкторов, а не конъюнкторов в монотонной схеме. Впрочем, в [8] такая же оценка заявлена (доказательство не приводится) и для числа конъюнкторов.

Лемма 2. *Пусть* $n \in \mathbb{N}$. *Тогда* $|\{C(E) \mid n(E) = n\}| \leqslant C_{k^2l^2}^{k+l-n}$.

Доказательство. Класс $C(E)$ однозначно определён системой уравнений $S(E)$, которая однозначно определяется линейно независимой подсистемой из $k + l - n$ уравнений. Число таких подсистем можно сверху оценить числом способов выбрать из k^2l^2 уравнений $k+l-n$ штук. Лемма 2 доказана.

Перейдём к выводу соотношений между $n(E)$ и $m(E)$. Этот фрагмент доказательства отличается от [2].

Обозначим единичный координатный вектор пространства $\mathbb{R}^{k+l}$ с i-й координатой, равной единице (и нулевыми остальными координатами), через ξ_i .

Пусть $n = n(E)$. Для единообразия введём обозначение $x_{i+k} = y_i$, $1 \leqslant i \leqslant l$. Положим

$$\bar{x} = (\underbrace{1, \ldots, 1}_{k}, \underbrace{0, \ldots, 0}_{l}), \quad \bar{y} = (\underbrace{0, \ldots, 0}_{k}, \underbrace{1, \ldots, 1}_{l}).$$

Заметим, что $\bar{x}, \bar{y} \in T_E$ (независимо от E). Пусть T'_E — подпространство решений системы уравнений

$$S'(E) = S(E) \cup \{x_1 = y_1 = 0\}.$$

Тогда $\dim T'_E = n-2$ и $T_E = T'_E + \{\alpha\bar{x} + \beta\bar{y} \mid \alpha, \beta \in \mathbb{R}\}$ (через $A+B$ здесь и далее обозначается поэлементная сумма (сумма Минковского) множеств A и B). Пусть

$$T'_E = \left\{ (x_1, \ldots, x_{k+l}) \mid x_i = \sum_{j=1}^{n-2} \alpha_{i,j} x_{i_j},\ 1 \leqslant i \leqslant k+l \right\},$$

где $x_{i_1}, \ldots, x_{i_{n-2}}$ — набор свободных переменных системы $S'(E)$, а $\alpha_{i,j}$ — действительные константы. Тогда, полагая $i_{n-1} = 1$ и $i_n = k + 1$, получаем набор $x_{i_1}, \ldots, x_{i_n}$ свободных переменных системы $S(E)$ и

$$T_E = \left\{ (x_1, \ldots, x_{k+l}) \mid x_i = \sum_{j=1}^{n} \alpha_{i,j} x_{i_j},\ 1 \leqslant i \leqslant k+l \right\},$$

где $\alpha_{i,n-1} = \alpha_{k+j,n} = 1$ и $\alpha_{i,n} = \alpha_{k+j,n-1} = 0$ при $1 \leqslant i \leqslant k$, $1 \leqslant j \leqslant l$.

Рассмотрим линейное отображение ψ_E пространства $\mathbb{R}^{k+l}$ в пространство $\mathbb{R}^{n-2}$ с евклидовой метрикой и ортонормированным базисом $\{e_1, \ldots,$

$e_{n-2}\}$ такое, что $\psi_E : \xi_i \to \sum\limits_{j=1}^{n-2} \alpha_{i,j} e_j$ при любом i. В частности, $\psi_E(\xi_1) = \psi_E(\xi_{k+1}) = 0$ (через 0 здесь и далее обозначается нулевой вектор пространства, если это не влечёт недоразумений).

Обозначим $A_E = \psi_E(\{\xi_1, \ldots, \xi_k\})$, $B_E = \psi_E(\{\xi_{k+1}, \ldots, \xi_{k+l}\})$.

Под размерностью $\dim A$ множества A в евклидовом пространстве далее, как обычно, будет пониматься минимум размерностей аффинных подпространств, в которых содержится данное множество.

Лемма 3. $|A_E + B_E| = m(E)$, $\dim(A_E + B_E) = n - 2$.

Доказательство. Первое утверждение верно в силу следующей цепочки эквивалентных переходов:

$$a_r + b_s = a_u + b_v \Longleftrightarrow ((x_1, \ldots, x_k, y_1, \ldots, y_l) \in T_E \Longrightarrow x_r + y_s = x_u + y_v)$$

$$\Longleftrightarrow \Bigg((x_1, \ldots, x_k, y_1, \ldots, y_l) \in T_E \Longrightarrow \sum_{j=1}^{n} (\alpha_{r,j} + \alpha_{k+s,j}) x_{i_j} = \sum_{j=1}^{n} (\alpha_{u,j} + \alpha_{k+v,j}) x_{i_j} \Bigg)$$

$$\Longleftrightarrow \forall\, j,\ 1 \leqslant j \leqslant n\, (\alpha_{r,j} + \alpha_{k+s,j} = \alpha_{u,j} + \alpha_{k+v,j})$$

$$\Longleftrightarrow \forall\, j,\ 1 \leqslant j \leqslant n-2\, (\alpha_{r,j} + \alpha_{k+s,j} = \alpha_{u,j} + \alpha_{k+v,j})$$

$$\Longleftrightarrow \psi_E(\xi_r + \xi_{k+s}) = \sum_{j=1}^{n-2} (\alpha_{r,j} + \alpha_{k+s,j}) e_j = \sum_{j=1}^{n-2} (\alpha_{u,j} + \alpha_{k+v,j}) e_j = \psi_E(\xi_u + \xi_{k+v}).$$

Второе утверждение очевидно в силу того, что $0 \in A_E \cap B_E$ и

$$\{e_1, \ldots, e_{n-2}\} \subset A_E \cup B_E.$$

Лемма 3 доказана.

Целям оценки $m(E)$ служит следующий раздел.

2. Мощность суммы двух множеств в евклидовом пространстве

В [10] Ружа установил следующий результат.

Теорема 1. *Пусть A и B — конечные множества в евклидовом пространстве $\mathbb{R}^n$, причём $|A| \leqslant |B|$ и $\dim(A+B) = n$. Тогда*

$$|A+B| \geqslant n|A| + |B| - \frac{n(n+1)}{2}.$$

Ружа также указал более точную оценку

$$|A+B| \geqslant |B| + \sum_{i=1}^{|A|-1} \min\{n,\, |B|-i\}.$$

Можно без ограничения общности считать, что $0 \in A \cap B$.

Уже этих оценок достаточно для вывода результатов, принципиально совпадающих с заявленными во введении. Но при больших n данные оценки не являются асимптотически точными. Наоборот, оценка $|A+B| \geqslant \lfloor n^2/4 \rfloor$, использованная в [2], неточна при малых n (впрочем, её достоинством является простота доказательства). Точные оценки позволяет получить метод из [9].

Пусть $\{e_1, \ldots, e_n\}$ — ортонормированный базис пространства $\mathbb{E}^n$. Следуя [9], будем называть *длинным симплексом* множество F вида

$$\{me_1 \mid m = 0, \ldots, |F| - k\} \cup \{e_{i_1}, \ldots, e_{i_{k-1}}\}, \tag{1}$$

где числа $1, i_1, \ldots, i_{k-1}$ попарно различны, $k \geqslant 0$.

Следующая лемма является переформулировкой следствия 3.8 из [9].

Лемма 4. *Минимум величины $|A+B|$ в условиях теоремы 1 либо равен $|A||B|$ (в этом случае $\dim A + \dim B = n$), либо достигается на паре длинных симплексов.*

Подчеркнём, что множества A и B из леммы удовлетворяют определению (1) с одним и тем же базисом и, в частности, с одним и тем же вектором e_1.

Точные (при любых значениях параметров) оценки в [9] не выводились, однако их несложно получить, опираясь на эту лемму. Справедлива

Теорема 2. *Пусть $A, B \subset \mathbb{R}^n$, $K = |A| \leqslant |B| = L$ и $\dim(A+B) = n$. Тогда*

(i) *если $n = K + L - 2$, то $|A+B| = KL$;*

(ii) *если* $n \leqslant L - K$, *то* $|A + B| \geqslant L + n(K - 1)$;
(iii) *если* $L - K \leqslant n \leqslant L$, *то*

$$|A + B| \geqslant (n + 1)K - \frac{(n - L + K)(n - L + K + 1)}{2};$$

(iv) *если* $L \leqslant n \leqslant K + L - 3$, *то*

$$|A + B| \geqslant KL - \frac{(K + L - n)(K + L - n - 1)}{2}.$$

Доказательство. Если $\dim A + \dim B = n$, то множество $A + B$ имеет максимально возможную мощность KL, откуда, в частности, следует (i). При $n < K + L - 2$ мы, таким образом, можем считать, что $\dim A + \dim B > n$.

Поэтому согласно лемме 4 достаточно рассмотреть случай, когда множества A и B являются длинными симплексами (1). Пусть без ограничения общности $A = C_A \cup D \cup D_A$, $B = C_B \cup D \cup D_B$, где

$$C_A = \{me_1 \mid m = 0, \dots, K - s - s_A - 1\},$$

$$C_B = \{me_1 \mid m = 0, \dots, L - s - s_B - 1\},$$

$D = \{e_2, \dots, e_{s+1}\}$, $D_A = \{e_{s+2}, \dots, e_{s+s_A+1}\}$, $D_B = \{e_{s+s_A+2}, \dots, e_n\}$, $s = |D|$, $s_A = |D_A|$, $s_B = |D_B|$, $s + s_A + s_B = n - 1$. Тогда

$$\begin{aligned}|A + B| = |C_A + C_B| + |(C_A \cup C_B) + D| + |C_A + D_B| \\ + |C_B + D_A| + |D + D| + |D + (D_A \cup D_B)| + |D_A + D_B|.\end{aligned}$$

Непосредственно проверяется, что

$$|C_A + C_B| = K + L - s - n, \quad |(C_A \cup C_B) + D| = s(\max\{L - s_B, K - s_A\} - s),$$

$$|C_A + D_B| = (K - s - s_A)s_B, \quad |C_B + D_A| = (L - s - s_B)s_A,$$

$$|D + D| = \frac{s(s + 1)}{2}, \quad |D + (D_A \cup D_B)| = s(s_A + s_B), \quad |D_A + D_B| = s_A s_B.$$

Суммируя, получаем

$$\begin{aligned}|A + B| = (s_A + 1)K + (s_B + 1)L + s \cdot \max\{L - s_B, K - s_A\} \\ - n - \frac{s(s + 1)}{2} - s_A s_B. \quad (2)\end{aligned}$$

Задача сводится к тому, чтобы найти минимум выражения (2). Обозначим через s^*, s_A^*, s_B^* значения параметров s, s_A, s_B, доставляющих этот минимум. Перечислим ограничения, накладываемые на параметры:

$$s + s_A + s_B = n - 1, \quad s + s_A \leqslant K - 1, \quad s + s_B \leqslant L - 1. \qquad (*)$$

Докажем (ii). Пусть $n \leqslant L - K$. В этом случае

$$L - s_B \geqslant K + (n - s_B) \geqslant K \geqslant K - s_A.$$

Поэтому минимизация (2) (если отбросить постоянные члены) равносильна максимизации выражения

$$s_B(n + L - K - 1 - s_B) + \frac{s(s+1)}{2}. \qquad (3)$$

При фиксированном s значение (3) возрастает при уменьшении s_A (и соответствующем увеличении s_B) ввиду того, что $2s_B < n + L - K - 1$ и функция $x(a - x)$ монотонно возрастает на отрезке $[0, a/2]$. При этом условия $(*)$ не нарушаются. Следовательно, $s_A^* = 0$.

Положим $s_B = n - 1 - s$. Тогда выражение (3) при отбрасывании постоянных членов принимает вид

$$-\frac{s(s+1)}{2} - ((L - K) - n)s,$$

откуда находим $s^* = 0$. Подставляя $s_B = n - 1$ и $s = s_A = 0$ в (2), получаем неравенство (ii).

Докажем (iii). Пусть $L - K \leqslant n \leqslant L$. Рассмотрим два случая.

Случай 1. Пусть $L - s_B \geqslant K - s_A$. Тогда, как и выше, задача сводится к максимизации (3). Заметим, что при фиксированном s_B значение (3) возрастает с уменьшением s_A (и соответствующим увеличением s), и при этом условия $(*)$ не нарушаются. Тогда либо

(1.1) $s_B^* \leqslant L - K$ и $s_A^* = 0$,

либо

(1.2) $s_B^* = L - K + s_A^*$.

Если выполнено (1.1), то полагаем $s = n - 1 - s_B$, после чего при отбрасывании постоянных членов выражение (3) принимает вид

$$s_B(2(L - K) - 1 - s_B),$$

откуда находим $s_B^* \in \{L - K - 1, L - K\}$.

Если выполнено (1.2), то полагаем $s_B = L - K + s_A$ и $s = n - 1 - L + K - 2s_A$. Подставляя эти выражения в (3) и отбрасывая постоянные члены, получаем

$$s_A(s_A + L - K - n).$$

Второй сомножитель равен $s_B - n$ и поэтому отрицателен, откуда получаем $s_A^* = 0$ и, как следствие, $s_B^* = L - K$ — то же, что и в (1.1).

Случай 2. Пусть $L - s_B \leqslant K - s_A$. Тогда

$$s + s_A = n - 1 - s_B \leqslant L - 1 - s_B \leqslant K - 1 - s_A \leqslant K - 1,$$

значит, из условий $(*)$ существенно только первое. В этом случае минимизация (2) равносильна максимизации выражения

$$s_A(n - L + K - 1 - s_A) + \frac{s(s+1)}{2}. \tag{4}$$

При фиксированном s_A значение выражения (4) возрастает с ростом s и соответствующим уменьшением s_B, поэтому $s_B^* = L - K + s_A^*$. Эта ситуация рассмотрена в рамках (1.2) случая 1.

Подставляя $s_A = 0$, $s_B = L - K$, $s = n - 1 - L + K$ в (2), приходим к неравенству (iii) (в смысле получаемого значения подстановка корректна и при $L - K = n$).

Докажем (iv). Пусть $L \leqslant n \leqslant K + L - 3$. Опять рассмотрим два случая.

Случай 1. Пусть $L - s_B \geqslant K - s_A$. Тогда последнее из условий $(*)$ следует из второго:

$$s + s_B \leqslant s + s_A + L - K \leqslant L - 1.$$

Снова задача состоит в максимизации выражения (3). Заметим, что при фиксированном s_B значение (3) возрастает с уменьшением s_A (и соответствующим увеличением s), при этом условия $(*)$ не нарушаются, поэтому $s_A^* = s_B^* - L + K$ (исходя из минимально возможного значения s_A при фиксированном s_B).

При подстановке $s = n + L - K - 1 - 2s_B$ и отбрасывании постоянных членов выражение (3) преобразуется к виду

$$s_B(s_B - n - L + K).$$

Ввиду того, что $2s_B < (L - K + s_A) + (n - s_A) = n + L - K$, второй сомножитель отрицателен и по абсолютной величине превосходит первый, значит, максимум достигается на минимальном из удовлетворяющих условиям $(*)$ значении s_B, откуда заключаем, что $s_B^* = n - K$.

Случай 2. Пусть $L - s_B \leqslant K - s_A$. Тогда несущественным является второе из условий $(*)$:

$$s + s_A \leqslant s + s_B - L + K \leqslant K - 1$$

и максимизируется выражение (4). Заметим, что оно возрастает при фиксированном s_A с ростом s и уменьшением s_B, при этом условия $(*)$ не нарушаются. Поэтому $s_B^* = L - K + s_A^*$. Таким образом, мы оказываемся в рамках уже рассмотренного случая 1.

Подставляя $s_A = n - L$, $s_B = n - K$, $s = L + K - 1 - n$ в (2), получаем неравенство (iv). Теорема 2 доказана.

Как следует из доказательства, оценки теоремы достижимы.

В условиях теоремы 2 определим величину

$$\rho(K, L) = \max_{1 \leqslant n \leqslant K+L-2} \frac{n+2}{|A+B|}. \tag{5}$$

Лемма 5. *Имеет место равенство* $\rho(2, L) = \frac{L+2}{2L}$. *Если* $K \geqslant 3$, *то*

$$\rho(K, L) = \max\left\{ \frac{K+L}{KL},\ \frac{K+L-1}{KL-3},\ \frac{2(L+2)}{K(2L-K+1)} \right\} < \frac{K+L+2}{KL}.$$

В частности, $\rho(K, K) = \frac{2(K+2)}{K(K+1)}$.

Доказательство. Дополнительно обозначим

$$\rho(K, L, n) = \frac{n+2}{\min\limits_{A,B} |A+B|}.$$

Таким образом, $\rho(K, L) = \max\limits_n \rho(K, L, n)$.

Проверим сначала, что на каждом из интервалов значений n, определяемых пп. (ii)–(iv) теоремы 2, максимум величины $\rho(K, L, n)$ достигается на концах интервалов.

В случае $1 \leqslant n \leqslant L - K$ функция

$$\rho^{-1}(K, L, n) = \frac{L + n(K-1)}{n+2} = K - 1 + \frac{L - 2K + 2}{n+2}$$

очевидно является монотонной (здесь и далее $\rho(K, L, n)$ рассматривается как функция переменной n).

В случае $L - K \leqslant n \leqslant L$ обозначим $n' = n - (L - K)$. Тогда

$$\rho^{-1}(K, L, n) = K - \frac{n'(n'+1) + 2K}{2(n' + L - K + 2)}.$$

Вычитаемая функция является выпуклой вниз при $n' \geqslant 0$, поскольку имеет вид $c\frac{n'(n'+1)+a}{n'+1+b}$, где $a, b, c \geqslant 0$, поэтому принимает максимальное на интересующем нас отрезке $[0,\, K]$ значение на концах отрезка (при $K \geqslant 3$; при $K = 2$ — на отрезке $[0,\, 1]$). Следовательно, там же принимает максимальное значение функция $\rho(K, L, n)$.

В случае $L \leqslant n \leqslant K + L - 3$ обозначим $n' = n - L$. Тогда

$$\rho^{-1}(K, L, n) = K - \frac{2(n'+2)K + (K-n')(K-n'-1)}{2(n'+L+2)} = K - \frac{n'(n'+1) + K(K+3)}{2(n'+L+2)}.$$

В этом случае справедлива та же аргументация, что и в предыдущем. Следовательно, при $K \geqslant 3$ имеем

$$\arg \max_{1 \leqslant n \leqslant K+L-2} \rho(K, L, n) \in \{1,\, L-K,\, L,\, K+L-3,\, K+L-2\},$$

$$\arg \max_{1 \leqslant n \leqslant K+L-2} \rho(2, L, n) \in \{1,\, L-2,\, L-1,\, L\}.$$

Проверим, что $\rho(K, L, 1) \leqslant \rho(K, L, K+L-2)$. Действительно,

$$\rho(K, L, 1) = \frac{3}{K+L-1} \leqslant \frac{4}{K+L} \leqslant \frac{1}{K} + \frac{1}{L} = \frac{K+L}{KL} = \rho(K, L, K+L-2)$$

в силу известного неравенства $\frac{a^2}{b} + \frac{c^2}{d} \geqslant \frac{(a+c)^2}{b+d}$, где $b, d > 0$.

Далее, заметим, что

$$\rho(K, L, L-K) = \frac{1}{K}\left(1 + \frac{1}{L-(K-1)}\right) \leqslant \frac{1}{K}\left(1 + \frac{K}{L}\right) = \rho(K, L, K+L-2).$$

Кроме того,

$$\rho(2, L, L-1) = \frac{L+1}{2L-1} \leqslant \frac{L+2}{2L} = \rho(2, L, L).$$

Таким образом, доказано, что $\rho(2, L) = \rho(2, L, L) = \frac{L+2}{2L}$ и

$$\rho(K, L) = \max\{\rho(K, L, K+L-2),\, \rho(K, L, K+L-3),\, \rho(K, L, L)\} = \max\left\{\frac{K+L}{KL},\, \frac{K+L-1}{KL-3},\, \frac{2(L+2)}{K(2L-K+1)}\right\}.$$

В силу выкладки

$$\frac{2(L+2)}{K(2L-K+1)} = \frac{L+(K+3)\frac{L}{2L-K+1}}{KL} \leqslant \frac{L+(K+3)\frac{K}{K+1}}{KL} < \frac{K+L+2}{KL}$$

неравенство $\rho(K,L) < \frac{K+L+2}{KL}$ становится очевидным. Несложно проверяется последнее утверждение леммы в отношении $\rho(K,K)$. Лемма 5 доказана.

3. Вес редкой циркулянтной матрицы

Циркулянтная матрица $(c_{i,j})$ определяется одной строкой, например, первой. Обозначим элементы строки через $c_j = c_{0,j}$, $0 \leqslant j \leqslant N-1$, где N — порядок матрицы. Для удобства будем считать, что для остальных элементов матрицы выполнено $c_{i,j} = c_{(i+j) \bmod N}$ (т. е. «единичные» диагонали матрицы параллельны побочной диагонали).

Тогда условие, что матрица $(c_{i,j})$ содержит единичную подматрицу, образованную строками с номерами $a_1, \ldots, a_k$ и столбцами с номерами $b_1, \ldots, b_l$, можно записать так:

$$c_{(a_i+b_j) \bmod N} = 1, \quad 1 \leqslant i \leqslant k,\ 1 \leqslant j \leqslant l.$$

Пусть $\gamma_0, \ldots, \gamma_{N-1}$ — независимые случайные величины, принимающие значение 1 с вероятностью p, а 0 — с вероятностью $1-p$, и пусть $\gamma = \sum \gamma_i$. Вероятность события Q будем обозначать через $\mathbf{P}(Q)$, математическое ожидание и дисперсию случайной величины ξ — через $\mathbf{M}\xi$ и $\mathbf{D}\xi$ соответственно.

Лемма 6. $\mathbf{P}(\gamma \geqslant pN - 2\sqrt{pN}) \geqslant 3/4$.

Доказательство. Доказываемое неравенство вытекает из неравенства Чебышёва

$$\mathbf{P}\left(|\gamma - \mathbf{M}\gamma| > \varepsilon\right) < \frac{\mathbf{D}\gamma}{\varepsilon^2}$$

при подстановке $\mathbf{M}\gamma = pN$, $\mathbf{D}\gamma = p(1-p)N$ и $\varepsilon = 2\sqrt{pN}$. Лемма 6 доказана.

Считаем, что $\gamma_i = 0$ при $i \geqslant N$. Обозначим через $Q(E, \gamma_0, \ldots, \gamma_{N-1})$, где $E = (a_1, \ldots, a_k, b_1, \ldots, b_l) \in R_{k,l} \cap \{0, \ldots, N-1\}^{k+l}$, событие

$$\forall_{i,\,j}(\gamma_{a_i+b_j} = 1).$$

Содержательно оно означает, что случайная циркулянтная матрица Γ порядка $2N$ с первой строкой $(\gamma_0, \ldots, \gamma_{N-1}, 0, \ldots, 0)$ содержит единичную

подматрицу размера $k \times l$ на пересечении строк с номерами $a_1, \ldots, a_k$ и столбцов с номерами $b_1, \ldots, b_l$.

Заметим, что любую единичную подматрицу матрицы Γ можно циклическим сдвигом (номеров строк и столбцов) перевести в единичную подматрицу, целиком расположенную в верхней левой угловой подматрице порядка N (т. е. образованной строками и столбцами с номерами от 0 до $N-1$) матрицы Γ. Порождение единичных подматриц циклическими сдвигами иллюстрируется рис. 1: единичные подматрицы C_i изображаются прямоугольниками, подматрица C_0 — искомая.

Таким образом, матрица Γ является (k,l)-редкой в том и только том случае, если (k,l)-редкой является её верхняя левая угловая подматрица порядка N.

Теорема 3. *Существует (k,l)-редкая циркулянтная матрица порядка N и веса $\Omega\bigl(\frac{k+l}{k^2l^2}N^{2-\rho(k,l)}\bigr)$.*

Доказательство. Непосредственно из определения следует, что вероятность события $Q(E,\gamma_0,\ldots,\gamma_{N-1})$ не превосходит $p^{m(E)}$. Тогда

$$\begin{aligned}
&\mathbf{P}(\exists_{E\in R_{k,l}}(Q(E,\gamma_0,\ldots,\gamma_{N-1}))\,) \\
&\qquad\leqslant \sum_{E\in R_{k,l}\cap\{0,\ldots,N-1\}^{k+l}} \mathbf{P}\,(Q(E,\gamma_0,\ldots,\gamma_{N-1})\,) \\
&\qquad= \sum_{n=3}^{k+l} \sum_{E\in R_{k,l}\cap\{0,\ldots,N-1\}^{k+l},\ n(E)=n} \mathbf{P}\,(Q(E,\gamma_0,\ldots,\gamma_{N-1})\,) \\
&\leqslant \sum_{n=3}^{k+l} \sum_{E\in R_{k,l}\cap\{0,\ldots,N-1\}^{k+l},\ n(E)=n} p^{m(E)} \leqslant \sum_{n=3}^{k+l} \sum_{C(E)\subset R_{k,l},\ n(E)=n} N^n p^{m(E)} \\
&\qquad\leqslant \sum_{n=3}^{k+l} \sum_{C(E)\subset R_{k,l},\ n(E)=n} (pN^{\rho(k,l)})^{m(E)},
\end{aligned}$$

где в предпоследнем переходе использовалось неравенство леммы 1, а в последнем — лемма 4 и определение (5).

Положим $p = \bigl(\frac{k+l}{ek^2l^2}\bigr)N^{-\rho(k,l)}$ и продолжим оценку, используя неравенство леммы 3:

$$\sum_{n=3}^{k+l} \sum_{C(E)\subset R_{k,l},\ n(E)=n} (pN^{\rho(k,l)})^{m(E)} \leqslant \sum_{n=3}^{k+l} \sum_{C(E)\subset R_{k,l},\ n(E)=n} \left(\frac{k+l}{ek^2l^2}\right)^{m(E)}$$

$$\leqslant \sum_{n=3}^{k+l} C_{k^2l^2}^{k+l-n} \left(\frac{k+l}{ek^2l^2}\right)^{k+l-1} \leqslant \sum_{n=3}^{k+l} \left(\frac{ek^2l^2}{k+l-n}\right)^{k+l-n} \left(\frac{k+l}{ek^2l^2}\right)^{k+l-1}$$
$$= \sum_{n=3}^{k+l} \left(\frac{k+l}{ek^2l^2}\right)^{n-1} \left(1+\frac{n}{k+l-n}\right)^{k+l-n} \leqslant \sum_{n=3}^{k+l} \left(\frac{k+l}{ek^2l^2}\right)^{n-1} e^n$$
$$= e\sum_{n=3}^{k+l} \left(\frac{k+l}{k^2l^2}\right)^{n-1} \leqslant \frac{e(k+l)}{k^2l^2} \leqslant e/4,$$

где использовались известные неравенства $C_n^m \leqslant \left(\frac{en}{m}\right)^m$ и $(1+1/x)^x < e$ при $x > 0$, а величина x^x при $x = 0$ полагается равной 1 (она присутствует в форме $(k+l-n)^{k+l-n}\,|_{n=k+l}$).

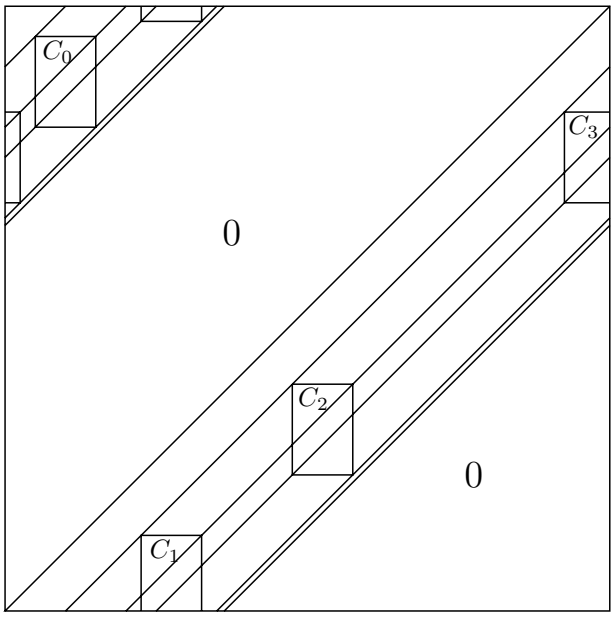

Рис. 1

Таким образом, как следует из сделанного перед формулировкой теоремы замечания, случайная циркулянтная матрица Γ (порядка $2N$) с вероятностью не менее $(4-e)/4$ не содержит ни одной единичной подматрицы размера $k \times l$, т. е. является (k,l)-редкой. С учётом леммы 6 заключаем, что с положительной вероятностью она одновременно является (k,l)-редкой и имеет вес $2N\gamma \geqslant 2N(pN - 2\sqrt{pN}) = \Omega(pN^2)$. Теорема 3 доказана.

4. Следствия

Из теоремы 3 и леммы 5 вытекает

Следствие 1. *Существует (k,l)-редкая циркулянтная матрица порядка N и веса $\Omega\big(\frac{k+l}{k^2l^2}N^{2-\frac{k+l+2}{kl}}\big)$.*

В случае $k=l=\Theta(\log N)$ вес циркулянтной матрицы из этого следствия равен $\Omega\left(N^2\log^{-3}N\right)$. Отсюда и из оценок сложности систем булевых сумм с (k,l)-редкими матрицами [6] (см. также [2, 11]) получаем

Следствие 2. *Существует циркулянтная матрица порядка N такая, что для сложности соответствующей ей системы булевых сумм справедливы оценки: $\Omega\left(N^2\log^{-4}N\right)$ при реализации вентильными схемами глубины 2, $\Omega\left(N^2\log^{-5}N\right)$ — схемами над базисом $\{\vee\}$ или вентильными схемами, $\Omega\big(N^2\log^{-6}N\big)$ — для числа дизъюнкторов при реализации схемами над базисом $\{\vee,\wedge\}$.*

При том же выборе параметров для определённой во введении величины $\lambda(N)$ с учётом [1] имеем

Следствие 3. $\lambda(N)=\Omega\big(\frac{N}{(\log N)^6\log\log N}\big)$.

Булева свёртка порядка N — это функция

$$U_N(x_0,\dots,x_{N-1},y_0,\dots,y_{N-1})=(u_0,\dots,u_{2N-2}),\quad u_k=\bigvee_{i+j=k}x_iy_j.$$

Циклическая булева свёртка порядка N определяется как

$$Z_N(x_0,\dots,x_{N-1},y_0,\dots,y_{N-1})=(z_0,\dots,z_{N-1}),\ \ z_k=\bigvee_{i+j\equiv k \bmod N}x_iy_j.$$

дизъюнкторов в схеме, реализующей функцию f над базисом $\{\vee,\wedge\}$, то прямо из определений функций свёртки легко вывести соотношения

$$V(Z_N)\leqslant V(U_N)+N-1,\quad V(U_N)\leqslant V(Z_{2N-1}).$$

Циклическую булеву свёртку (с точностью до перестановки компонент) можно интерпретировать как систему булевых сумм переменных x_0, $\dots,x_{N-1}$ с переменной циркулянтной матрицей, определяемой строкой $y_{N-1},\dots,y_0$. Так как сложность схемы (в данном случае, в смысле меры $V(f)$) не возрастает при подстановке констант вместо некоторых входов, заключаем, что сложность циклической свёртки порядка N не меньше, чем сложность системы булевых сумм с произвольной циркулянтной матрицей порядка N. Используя следствие 2, получаем

Следствие 4. $V(U_N)$, $V(Z_N)=\Omega\left(N^2\log^{-6}N\right)$.

ЛИТЕРАТУРА

1. **Гашков С. Б., Сергеев И. С.** О сложности линейных булевых операторов с редкими матрицами // Дискрет. анализ и исслед. операций. — 2010. — Т. 17, № 3. — С. 3–18.
2. **Гринчук М. И.** О сложности реализации циклических булевых матриц вентильными схемами // Изв. вузов. Математика. — 1988. — Т. 7. — С. 39–44.
3. **Коршунов А. Д.** Монотонные булевы функции // Успехи мат. наук. — 2003. — Т. 58, вып. 5. — С. 89–162.
4. **Лупанов О. Б.** О вентильных и контактно-вентильных схемах // Докл. АН СССР. — 1956. — Т. 111, № 6. — С. 1171–1174.
5. **Лупанов О. Б.** Асимптотические оценки сложности управляющих систем. — М.: Изд-во МГУ, 1984. — 138 с.
6. **Мельхорн К.** Некоторые замечания, касающиеся булевых сумм // Кибернетический сборник. Вып. 18. — М.: Мир, 1981. — С. 39–45.
7. **Эрдеш П., Спенсер Дж.** Вероятностные методы в комбинаторике. — М.: Мир, 1976. — 130 с.
8. **Blum N.** On negations in Boolean networks. — Berlin; Heidelberg: Springer-Verl., 2009. — P. 18–29. (Lect. Notes Comput. Sci.; Vol. 5760.)
9. **Gardner R. J., Gronchi P.** A Brunn–Minkowski inequality for the integer lattice // Trans. Amer. Math. Soc. — 2001. — Vol. 353, N 10. — P. 3995–4024.
10. **Ruzsa I. Z.** Sum of sets in several dimensions // Combinatorica. — 1994. — Vol. 14. — P. 485–490.
11. **Wegener I.** The complexity of boolean functions. — Stuttgart: Wiley, 1987. — 470 p.

Гринчук Михаил Иванович,
e-mail: grinchuk@nw.math.msu.su
Сергеев Игорь Сергеевич,
e-mail: isserg@gmail.com

Статья поступила
27 января 2011 г.