Math-Net.Ru

Общероссийский математический портал

Р. Н. Забалуев, О сложности реализации полиномов Жегалкина, *Дискрет. матем.*, 2004, том 16, выпуск 1, 79–94

DOI: <https://doi.org/10.4213/dm143>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.162.127.20

26 апреля 2023 г., 08:31:17

О сложности реализации полиномов Жегалкина

© 2004 г. Р. Н. Забалуев

Показано, что сложность полинома Жегалкина степени k , $2 \leq k \leq n$, не превосходит величины

$$\sum_{i=0}^k C_n^i / \log_2 \sum_{i=0}^k C_n^i (1 + o(1)),$$

(при $n \rightarrow \infty$) и для почти всех таких полиномов сложность асимптотически совпадает с этой величиной. Также показано, что сложность каждого однородного полинома Жегалкина степени k (для большинства значений k) не превосходит величины

$$C_n^k / \log_2 C_n^k (1 + o(1)),$$

(при $n \rightarrow \infty$) и для почти всех таких полиномов сложность асимптотически совпадает с этой величиной.

1. Введение

В настоящей работе рассматривается сложность реализации (однородных) булевых функций, заданных полиномами Жегалкина степени k , схемами из функциональных элементов в базисе $\{\&, \oplus, 1\}$. Пусть полином $f(x_1, \dots, x_n)$ имеет вид

$$f(x_1, \dots, x_n) = \bigoplus_{\sigma_1, \dots, \sigma_n} c_{\sigma_1, \dots, \sigma_n} x_1^{\sigma_1} \dots x_n^{\sigma_n},$$

где $\sigma_i \in \{0, 1\}$, $1 \leq i \leq n$, $c_{\sigma_1, \dots, \sigma_n} \in \{0, 1\}$, $x^\sigma = x$ при $\sigma = 1$ и $x^\sigma = 1$ при $\sigma = 0$. Если коэффициент $c_{\sigma_1, \dots, \sigma_n}$ не равен нулю, то $c_{\sigma_1, \dots, \sigma_n} x_1^{\sigma_1} \dots x_n^{\sigma_n}$ называется мономом полинома f , $\sigma_1 + \dots + \sigma_n$ — степенью этого монома. Степень полинома f , $f \neq 0$, определяется как наибольшая из степеней его мономов. Если $f = 0$ или все мономы f имеют одну и ту же степень, то полином f называется однородным. Через $P_2^k[n]$ обозначим класс полиномов от n переменных, степень каждого из которых не превосходит k , а через $P_2^{k,h}[n]$ — класс однородных полиномов степени k от n переменных. Сложностью схемы из функциональных элементов будем называть число входящих в нее базисных элементов, сложность полинома (системы полиномов) определим как наименьшую из сложностей схем, реализующих этот полином (систему полиномов). Сложность схемы S обозначим через $L(S)$, а сложность полинома (системы полиномов) f — через $L(f)$. Функция, тождественно равная единице, является базисным элементом, поэтому $L(1) = 1$. Если Q — некоторый класс полиномов, тогда максимум сложностей $L(f)$ по всем полиномам f из Q назовем сложностью класса Q и обозначим ее через $L(Q)$. Пусть $W(n)$ — некоторый класс

полиномов, зависящих от n переменных, и $|W(n)|$ — число полиномов в этом классе. Будем говорить, что некоторое свойство выполнено для почти всех полиномов из класса $W(n)$, если для числа $V(n)$ полиномов, не обладающих этим свойством, справедливо соотношение $V(n)/|W(n)| \rightarrow 0$ при $n \rightarrow \infty$.

Очевидно, что каждый полином первой степени вычисляется с линейной сложностью. Любой полином f степени k можно записать в виде суммы однородных полиномов. В разделе 2 предложен способ представления полиномов, позволяющий сводить вычисления однородных полиномов к вычислению систем линейных функций. В разделе 3 доказано, что для каждого полинома $f \in P_2^{k,o}[n]$, $2 \leq k \leq n - \log n - 4 \log \log n$ (здесь и далее $\log$ означает $\log_2$), справедливо асимптотическое соотношение

$$L(f) \lesssim \frac{C_n^k}{\log C_n^k}$$

и для почти всех $f \in P_2^{k,h}[n]$ выполняется неравенство

$$L(f) \geq \frac{C_n^k}{\log C_n^k} (1 - \varepsilon_1(n)),$$

где $\varepsilon_1(n) \geq 0$ и стремится к нулю при $n \rightarrow \infty$. В разделе 4 данной работы показано, что для каждого полинома $f \in P_2^k[n]$ при $2 \leq k \leq n$ и $n \rightarrow \infty$ справедливо асимптотическое соотношение

$$L(f) \lesssim \sum_{i=0}^k C_n^i / \log \sum_{i=0}^k C_n^i,$$

и для почти всех $f \in P_2^k[n]$ выполняется неравенство

$$L(f) \geq \sum_{i=0}^k C_n^i / \log \sum_{i=0}^k C_n^i (1 - \varepsilon_2(n)),$$

где $\varepsilon_2(n) \geq 0$ и стремится к нулю при $n \rightarrow \infty$.

2. Прямоугольное представление полиномов Жегалкина

Для булева набора $\tilde{\sigma} = (\sigma_1, \dots, \sigma_n)$ через $\|\tilde{\sigma}\|$ обозначим норму набора, то есть число единиц в наборе $\tilde{\sigma}$, и положим

$$N(\tilde{\sigma}) = \sum_{i=1}^n \sigma_i 2^{i-1} + 1.$$

Пусть $\tilde{x} = (x_1, \dots, x_n)$, тогда для $i \leq j$ через $\tilde{x}_i^j$ обозначим набор $(x_i, \dots, x_j)$. В частности, если $1 \leq m \leq n-1$, то $\tilde{x}_1^m = (x_1, \dots, x_m)$ и $\tilde{x}_{m+1}^n = (x_{m+1}, \dots, x_n)$.

Рассмотрим произвольный полином

$$f(x_1, \dots, x_n) = \bigoplus_{\sigma_1, \dots, \sigma_n} c_{\sigma_1, \dots, \sigma_n} x_1^{\sigma_1} \dots x_n^{\sigma_n} \quad (1)$$

Таблица 1.

		C_0		C_q		C_{n-m}
	x_n	0		σ_n		1
	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
	x_{m+1}	0		σ_{m+1}		1
	$x_1 \dots x_m$			.		
S_0	00 ... 0			.		
S_1	10 ... 0			.		
				.		
	0 ... 01			.		
				.		
S_p	$\sigma_1 \dots \sigma_m$	...	...	$c_{\tilde{\sigma}}$		
						
						
S_m	1 ... 1					

Полином f может быть задан таблицей с двумя входами (см. таблицу 1). В этой таблице каждой строке соответствует некоторый булев набор $\tilde{\sigma}_1^m = (\sigma_1, \dots, \sigma_m)$ (при этом будем подразумевать, что строке соответствует также конъюнкция вида $x_1^{\sigma_1} \dots x_m^{\sigma_m}$). Каждому столбцу в таблице соответствует набор $\tilde{\sigma}_{m+1}^n = (\sigma_{m+1}, \dots, \sigma_n)$ (соответствует конъюнкция $x_{m+1}^{\sigma_{m+1}} \dots x_n^{\sigma_n}$). На пересечении строки, соответствующей конъюнкции $x_1^{\sigma_1} \dots x_m^{\sigma_m}$, и столбца, соответствующего конъюнкции $x_{m+1}^{\sigma_{m+1}} \dots x_n^{\sigma_n}$, стоит константа $c_{\sigma_1, \dots, \sigma_m, \sigma_{m+1}, \dots, \sigma_n}$ из (1), на которую умножается конъюнкция $x_1^{\sigma_1} \dots x_m^{\sigma_m} \cdot x_{m+1}^{\sigma_{m+1}} \dots x_n^{\sigma_n}$ (далее, где нет специальных оговорок, под умножением будем понимать операцию конъюнкции, а под сложением сложение по модулю 2).

Далее вводится прямоугольное представление полиномов, которое позволит оптимально вычислять однородные полиномы. Разобьем строки матрицы M , составленной из значений коэффициентов $c_{\tilde{\sigma}_1^m}$ полинома f , на $m+1$ горизонтальную полосу S_p . Строка, соответствующая $\tilde{\sigma}_1^m$, попадает в полосу S_p , если $\|\tilde{\sigma}_1^m\| = p$ (то есть число единиц в наборе $\tilde{\sigma}_1^m$ равно p). Наборы $\tilde{\sigma}_1^m$ каждой горизонтальной полосы упорядочены в соответствии с их значениями $N(\tilde{\sigma}_1^m)$. По аналогии со строками разобьем столбцы матрицы M на $n-m+1$ вертикальную полосу C_q : столбец, соответствующий $\tilde{\sigma}_{m+1}^n$, попадает в полосу C_q , если $\|\tilde{\sigma}_{m+1}^n\| = q$. Наборы $\tilde{\sigma}_{m+1}^n$ каждой вертикальной полосы также упорядочены в соответствии с их значениями $N(\tilde{\sigma}_{m+1}^n)$. Прямоугольник (здесь и далее под прямоугольником будем подразумевать матрицу), образованный пересечениями строк из полосы S_p и столбцов из полосы C_q , обозначим как $A_{p,q}$. Введем полином $F_{p,q}(x_1, \dots, x_n)$, соответствующий прямоугольнику $A_{p,q}$:

$$F_{p,q} = \bigoplus_{\substack{\tilde{\sigma}_1^m = (\sigma_1, \dots, \sigma_m) \\ \|\tilde{\sigma}_1^m\| = p}} x_1^{\sigma_1} \dots x_m^{\sigma_m} \bigoplus_{\substack{\tilde{\sigma}_{m+1}^n = (\sigma_{m+1}, \dots, \sigma_n) \\ \|\tilde{\sigma}_{m+1}^n\| = q}} c_{\sigma_1, \dots, \sigma_m, \sigma_{m+1}, \dots, \sigma_n} x_{m+1}^{\sigma_{m+1}} \dots x_n^{\sigma_n}, \quad (2)$$

где коэффициенты $c_{\sigma_1, \dots, \sigma_m, \sigma_{m+1}, \dots, \sigma_n}$ входят в $A_{p,q}$, то есть полином $F_{p,q}$ является суммой

Таблица 2.

		C_0	C_1	C_2
	x_4	0	01	1
	x_3	0	10	1
	x_1x_2			
S_0	00	1	00	1
S_1	10	0	10	0
	01	0	10	1
S_2	11	0	00	0

некоторых мономов полинома f . Поэтому полином f может быть представлен в виде

$$f(x_1, \dots, x_n) = \bigoplus_{p=0}^m \bigoplus_{q=0}^{n-m} F_{p,q}. \quad (3)$$

Представление (3) будем называть прямоугольным представлением полинома f , число m назовем параметром этого представления.

В качестве примера рассмотрим полином от четырех переменных. Пусть

$$f(x_1, \dots, x_4) = 1 \oplus x_2x_3 \oplus x_1x_3 \oplus x_3x_4 \oplus x_2x_3x_4. \quad (4)$$

Зададим этот полином таблицей 2. В этой таблице на пересечении строк из горизонтальной полосы S_1 с номерами 1 и 2, относящихся к переменным x_1 и x_2 соответственно, и столбца из вертикальной полосы C_1 с номером 1, соответствующего переменной x_3 , стоят единицы, равные соответственно коэффициентам мономов x_1x_3 и x_2x_3 полинома f из (4). Аналогично, на пересечениях столбцов с номерами 1 из вертикальных полос C_0 и C_2 соответственно и строки с номером 1 из горизонтальной полосы S_0 , стоят единицы, равные коэффициентам монома нулевой степени и монома x_3x_4 ; на пересечении строки из S_1 с номером 2, соответствующей переменной x_2 , и столбца из C_2 , соответствующего конъюнкции x_3x_4 , стоит единица, равная коэффициенту монома $x_2x_3x_4$. Следующая запись есть прямоугольное представление полинома f

$$f = F_{0,0} \oplus F_{0,2} \oplus F_{1,2} \oplus F_{1,1},$$

куда входят только не тождественно нулевые функции $F_{0,0} \equiv 1$,

$$F_{0,2} = x_3x_4, \quad F_{1,2} = x_2x_3x_4, \quad F_{1,1} = x_1x_3 \oplus x_2x_3.$$

3. Реализация однородных полиномов Жегалкина

В этом разделе доказываются оценки сложности реализации однородных полиномов $f(x_1, \dots, x_n)$ степени k в случае, когда

$$2 \leq k \leq n - \log n - 4 \log \log n.$$

Приведем несколько вспомогательных утверждений. Рассмотрим систему линейных функций

$$\alpha = \left\{ f_i(y_1, \dots, y_N) = \bigoplus_{1 \leq j \leq N} c_{ij} y_j \right\}_{i=1}^M,$$

где c_{ij} — булевы константы. Из результатов работы [5] вытекает следующее утверждение.

Предложение 1. Если $N = 2^{o(M)}$, $M = 2^{o(N)}$ и $NM \rightarrow \infty$, тогда выполнено асимптотическое неравенство

$$L(\alpha) \lesssim NM / \log(NM).$$

В [2] доказано следующее утверждение.

Предложение 2. Если

$$L = \sum_{i=1}^l L_i,$$

где $L_i \geq 3$, $i = 1, 2, \dots, l$, и $l \leq \log L$, начиная с некоторого L , тогда при $L \rightarrow \infty$

$$\frac{L}{\log L} \sim \sum_{i=1}^l \frac{L_i}{\log L_i}.$$

Теорема 1. Пусть $f(x_1, \dots, x_n) \in P_2^{k,h}[n]$, где

$$\log n \leq k \leq n - \log n - 4 \log \log n.$$

Тогда при $n \rightarrow \infty$ справедливо соотношение

$$L(f) \lesssim \frac{C_n^k}{\log C_n^k}.$$

Доказательство. Построим схему для реализации полинома f , используя его прямоугольное представление

$$f(x_1, \dots, x_n) = \bigoplus_{p=0}^m \bigoplus_{q=0}^{n-m} F_{p,q}. \quad (5)$$

В соответствующей этому представлению таблице прямоугольники $A_{p,q}$ состоят из одних нулей, если $p+q \neq k$. Значит, для таких p и q полиномы $F_{p,q}$ равны нулю. Поэтому будем строить схемы, вычисляющие только полиномы $F_{p,q}$, у которых $p+q = k$. Без ограничения общности считаем, что n и k четные (для остальных n и k доказательство меняется незначительно). Положим параметр m прямоугольного представления полинома f равным $n/2$. Рассмотрим два случая,

$$\log n \leq k \leq n/2 \quad (6)$$

и

$$n/2 < k \leq n - \log n - 4 \log \log n. \quad (7)$$

Пусть k удовлетворяет условию (6). Прямоугольнику $A_{p,q}$ соответствует полином

$$F_{p,q} = \bigoplus_{\substack{\tilde{\sigma}_1^{n/2} = (\sigma_1, \dots, \sigma_{n/2}) \\ \|\tilde{\sigma}_1^{n/2}\| = p}} x_1^{\sigma_1} \dots x_{n/2+1}^{\sigma_{n/2+1}} \bigoplus_{\substack{\tilde{\sigma}_{n/2+1}^n = (\sigma_{n/2+1}, \dots, \sigma_n) \\ \|\tilde{\sigma}_{n/2+1}^n\| = q}} c_{\sigma_1, \dots, \sigma_n} x_{n/2+1}^{\sigma_{n/2+1}} \dots x_n^{\sigma_n}. \quad (8)$$

Рассмотрим функцию

$$f_{p,q}(y_1, \dots, y_M, z_1, \dots, z_N) = \bigoplus_{1 \leq i \leq M} y_i \bigoplus_{1 \leq j \leq N} c_{ij} z_j,$$

где

$$M = C_{n/2}^p, \quad N = C_{n/2}^q,$$

и булев коэффициент c_{ij} равен такому коэффициенту $c_{\sigma_1, \dots, \sigma_n}$ в (8), что в прямоугольном представлении полинома f номер строки в группе S_p , соответствующей набору $\tilde{\sigma}_1^{n/2}$, равен i , а номер столбца в группе C_q , соответствующего набору $\tilde{\sigma}_{n/2+1}^n$, равен j . Пусть схема Σ_1 минимальной сложности вычисляет всевозможные конъюнкции $x_1^{\sigma_1} \dots x_{n/2}^{\sigma_{n/2}}$ и $x_{n/2+1}^{\sigma_{n/2+1}} \dots x_n^{\sigma_n}$ такие, что $\|\tilde{\sigma}_1^{n/2}\| \leq k$ и $\|\tilde{\sigma}_{n/2+1}^n\| \leq k$, тогда справедливо неравенство

$$L(\Sigma_1) \leq 2k \sum_{p=0}^k C_{n/2}^p. \quad (9)$$

Очевидно, что

$$L(f) \leq \sum_{p=0, p+q=k}^k L(f_{p,q}) + k + L(\Sigma_1).$$

Заметим, что общая площадь прямоугольников $A_{p,q}$, где $p+q=k$, равняется C_n^k , то есть

$$\sum_{p=0}^k C_{n/2}^p C_{n/2}^{k-p} = C_n^k. \quad (10)$$

Для $p = 2, \dots, k-2$ справедливы соотношения

$$N = C_{n/2}^p = 2^{o(M)}, \quad M = C_{n/2}^{k-p} = 2^{o(N)}, \quad NM \rightarrow \infty,$$

значит, применимо предложение 1. Поэтому верно соотношение

$$L(f_{p,k-p}) \lesssim C_{n/2}^p C_{n/2}^{k-p} / \log(C_{n/2}^p C_{n/2}^{k-p}) + 2C_{n/2}^p - 1, \quad p = 2, \dots, k-2. \quad (11)$$

Если p равно одному из четырех значений 0, 1, $k-1$ или k , то справедливы соотношения

$$L(f_{p,k-p}) \leq C_{n/2}^p (C_{n/2}^{k-p} - 1) + 2C_{n/2}^p - 1 \sim C_{n/2}^p C_{n/2}^{k-p}. \quad (12)$$

Очевидно, что при $1 \leq k \leq n/2$ и достаточно больших n верно неравенство

$$k+1 \leq \log C_n^k. \quad (13)$$

Отсюда, из предложения 2 и (10) получим соотношение

$$\sum_{p=2}^{k-2} C_{n/2}^p C_{n/2}^{k-p} / \log(C_{n/2}^p C_{n/2}^{k-p}) \lesssim \frac{C_n^k}{\log C_n^k}.$$

Поэтому из (9), (11) и (12) вытекает следующая оценка для сложности функции f :

$$L(f) \lesssim \frac{C_n^k}{\log C_n^k} + 2 \sum_{p=2}^{k-2} C_{n/2}^p + 2C_{n/2}^k + 2C_{n/2}^1 C_{n/2}^{k-1} + k + 2k \sum_{p=0}^k C_{n/2}^p.$$

Если $\log n \leq k \leq \lfloor n/4 \rfloor$, тогда

$$2k \sum_{p=0}^k C_{n/2}^p \leq \frac{2k(k+1)C_n^k}{2^k} \lesssim \frac{C_n^k}{\log^2 C_n^k}.$$

Если $\lfloor n/4 \rfloor < k \leq n/2$, то

$$2k \sum_{p=0}^k C_{n/2}^p \leq 2k2^{n/2} \lesssim \frac{C_n^{\lfloor n/4 \rfloor}}{n^2} \leq \frac{C_n^k}{\log^2 C_n^k};$$

а также

$$2C_{n/2}^1 C_{n/2}^{k-1} \leq \frac{nC_n^{k-1}}{2^{k-1}} = \frac{nkC_n^k}{2^{k-1}(n-k+1)} \lesssim \frac{C_n^k}{\log^2 C_n^k}.$$

Поэтому справедливо асимптотическое неравенство

$$L(f) \lesssim \frac{C_n^k}{\log C_n^k}.$$

Пусть теперь значения k удовлетворяют условию (7). Рассуждения этого случая проводятся по аналогии с предыдущим за исключением вычисления конъюнкций. Прямоугольное представление полинома f здесь выглядит так:

$$f = \bigoplus_{p=0}^{n-k} F_{n/2-p, k-n/2+p}.$$

Пусть схема Σ_1 минимальной сложности вычисляет всевозможные конъюнкции $x_1^{\sigma_1} \dots x_{n/2}^{\sigma_{n/2}}$ и $x_{(n/2)+1}^{\sigma_{(n/2)+1}} \dots x_n^{\sigma_n}$ такие, что $\|\tilde{\sigma}_1^{n/2}\| \geq k - n/2$ и $\|\tilde{\sigma}_{n/2+1}^n\| \geq k - n/2$. Тогда справедлива цепочка неравенств

$$L(\Sigma_1) \leq n \sum_{p=k-n/2}^{n/2} C_{n/2}^p \leq n \sum_{p=0}^{n-k} C_{n/2}^p.$$

Для $k = \lfloor n - \log n - 4 \log \log n \rfloor$ проверим, что $L(\Sigma_1) \lesssim C_n^k / \log^2 C_n^k$. Действительно, верны соотношения

$$\begin{aligned} L(\Sigma_1) &\leq n \sum_{p=0}^{n-k} C_{n/2}^p \lesssim n(n-k+1)C_{n/2}^{n-k} \\ &\leq n(n-k+1) \frac{C_n^{n-k}}{2^{n-k}} \lesssim \frac{C_n^{n-k}}{\log^3 n} = o(C_n^{n-k} / \log C_n^{n-k}). \end{aligned}$$

Очевидно, что эта же оценка для $L(\Sigma_1)$ верна и при $n/2 < k < \lfloor n - \log n - 4 \log \log n \rfloor$. Теорема доказана.

Теорема 2. Пусть $f(x_1, \dots, x_n) \in P_2^{k,h}[n]$, где $2 \leq k \leq \log n$. Тогда

$$L(f) \lesssim \frac{C_n^k}{\log C_n^k}.$$

Доказательство. Утверждение этой теоремы следует из работы В. В. Кочергина [1], но так как эта работа объемна и трудно доступна, приведем здесь независимое доказательство.

Сведем вычисление полинома f к вычислению системы линейных функций. В полиноме f сгруппируем мономы, содержащие переменную x_1 , и вынесем x_1 за скобки. Полученный в скобках полином $f_{x_1}^{k-1}(x_2, \dots, x_n)$ имеет степень, не большую $k-1$, и зависит от переменных $x_2, \dots, x_n$; индекс x_1 в обозначении указывает на то, что полином $f_{x_1}^{k-1}(x_2, \dots, x_n)$ умножается только на x_1 . Среди оставшихся мономов, уже не содержащих x_1 , сгруппируем те, которые содержат x_2 , вынесем за скобки x_2 и в скобках получим полином $f_{x_2}^{k-1}(x_3, \dots, x_n)$ степени, не большей $k-1$. По аналогии для переменных $x_3, \dots, x_{n-k+1}$ получаются полиномы $f_{x_3}^{k-1}(x_4, \dots, x_n), \dots, f_{x_{n-k+1}}^{k-1}(x_{n-k+2}, \dots, x_n)$ степени, не большей $k-1$. Тогда полином f можно представить следующим образом:

$$f = \bigoplus_{i_1=1}^{n-k+1} x_{i_1} f_{x_{i_1}}^{k-1}(x_{i_1+1}, \dots, x_n). \quad (14)$$

На следующем этапе полиномы степени, не большей $k-1$, в этом представлении разложим до полиномов степени, не большей $k-2$, а именно: полиномы вида $f_{x_{i_1}}^{k-1}(x_{i_1+1}, \dots, x_n)$ раскладываются так:

$$f_{x_{i_1}}^{k-1}(x_{i_1+1}, \dots, x_n) = \bigoplus_{i_2=i_1+1}^{n-k+2} x_{i_2} f_{x_{i_1} x_{i_2}}^{k-2}(x_{i_2+1}, \dots, x_n),$$

где индекс $x_{i_1} x_{i_2}$ в обозначении полинома $f_{x_{i_1} x_{i_2}}^{k-2}(x_{i_2+1}, \dots, x_n)$ степени, не большей $k-2$, указывает на то, что этот полином в представлении f умножается только на конъюнкцию $x_{i_1} x_{i_2}$. Подставляя в (14) вместо полиномов степени $k-1$ их разложения, получим новое представление полинома f

$$f = \bigoplus_{i_1=1}^{n-k+1} x_{i_1} \bigoplus_{i_2=i_1+1}^{n-k+2} x_{i_2} f_{x_{i_1} x_{i_2}}^{k-2}(x_{i_2+1}, \dots, x_n). \quad (15)$$

Шаг за шагом перейдем к представлению, содержащему линейные полиномы:

$$f = \bigoplus_{i_1=1}^{n-k+1} x_{i_1} \bigoplus_{i_2=i_1+1}^{n-k+2} x_{i_2} \dots \times \bigoplus_{i_{k-2}=i_{k-3}+1}^{n-2} x_{i_{k-2}} \bigoplus_{i_{k-1}=i_{k-2}+1}^{n-1} x_{i_{k-1}} f_{x_{i_1} x_{i_2} \dots x_{i_{k-1}}}^1(x_{i_{k-1}+1}, \dots, x_n) \dots, \quad (16)$$

(линейные полиномы $f_{x_{i_1} x_{i_2} \dots x_{i_{k-1}}}^1(x_{i_{k-1}+1}, \dots, x_n)$ являются однородными). Обозначим через $S(l)$, $l = 1, \dots, n-k+1$, количество построенных полиномов вида

Таблица 3.

x_k	x_{k+1}	x_{k+2}	$\dots$	x_n
$z_{p_1,1}$	$z_{1,2}$	$z_{1,3}$	$\dots$	$z_{1,n-k+1}$
0	$z_{2,2}$	$z_{2,3}$	$\dots$	$z_{2,n-k+1}$
			$\dots$	
0	$z_{p_2,2}$	$z_{p_2,3}$	$\dots$	$z_{p_2,n-k+1}$
0	0	$z_{p_2+1,3}$	$\dots$	$z_{p_2+1,n-k+1}$
			$\dots$	
0	0	$z_{p_3,3}$	$\dots$	$z_{p_3,n-k+1}$
			$\dots$	
0	0	0	$\dots$	$z_{p_{n-k+1},n-k+1}$

$f_{x_{i_1} x_{i_2} \dots x_{i_{k-1}}}^1(x_{i_{k-1}+1}, \dots, x_n)$, формально зависящих от последних l переменных. Из коэффициентов при переменных $x_k, \dots, x_n$ полиномов $f_{x_{i_1} x_{i_2} \dots x_{i_{k-1}}}^1(x_{i_{k-1}+1}, \dots, x_n)$ в представлении (16) составим ступенчатую таблицу из $n - k + 1$ столбцов (таблица 3). В таблице 3 сначала выписаны коэффициенты полиномов, зависящих от $n - k + 1$ переменных, затем коэффициенты полиномов, зависящих от $n - k$ переменных, и так далее до коэффициентов полиномов от одной переменной; коэффициенты одного полинома выписаны в одной строке под соответствующими переменными, а также дополнены нулями недостающие элементы. На углах ступеней стоят элементы $z_{p_j, j}$, $1 \leq j \leq n - k + 1$, где

$$p_j = \sum_{i=n-k-j+2}^{n-k+1} S(i),$$

в частности,

$$p_1 = S(n - k + 1) = 1, \quad p_{n-k+1} = \sum_{i=1}^{n-k+1} S(i)$$

(величина p_{n-k+1} является высотой таблицы).

Для того, чтобы вычислить полином f , вычислим p_{n-k+1} полиномов степени не выше первой из представления (16) и проделаем соответствующие этому представлению умножения и сложения (пусть эти сложения и умножения выполняет схема Σ минимальной сложности). Значение полинома степени не выше первой, соответствующего какой-либо строке, есть сумма произведений коэффициентов этой строки и значений соответствующих переменных. Построение схемы, вычисляющей эти суммы, основывается на конструкциях, аналогичных конструкциям О. Б. Лупанова [4].

Разобьем матрицу M коэффициентов таблицы 3 на вертикальные полосы V_b по s столбцов; последняя полоса может содержать меньшее число столбцов. Через d обозначим количество полос V_b , то есть $d = \lceil (n - k + 1)/s \rceil$. Для каждой полосы V_b вычислим систему y_b , состоящую из всех линейных функций, сохраняющих ноль, зависящих от переменных, соответствующих полосе V_b , причем существенных переменных среди них не более k . Очевидно, что

$$|y_b| \leq \sum_{i=1}^k C_s^i.$$

Рис. 1.

Пусть Σ_γ — схема минимальной сложности, вычисляющая все системы γ_b . Тогда

$$L(\Sigma_\gamma) \leq d \sum_{i=1}^k i C_s^i.$$

Матрицу M разобьем также на a горизонтальных полос A_t по m строк; последняя может содержать меньшее число строк. Прямоугольник, находящийся на пересечении горизонтальной полосы A_t и вертикальной полосы V_b обозначим через $D_{t,b}$ (см. рис. 1).

Множество ненулевых столбцов каждого прямоугольника $D_{t,b}$ разобьем на группы одинаковых, пусть это будут группы $W_{t,b,\bar{\tau}}$, число групп равно числу различных ненулевых столбцов $\bar{\tau}$ из $D_{t,b}$. Переменные, соответствующие столбцам каждой группы $W_{t,b,\bar{\tau}}$, сложим по модулю 2, используя уже вычисленные функции системы γ_b , результат сложения обозначим как $w_{t,b,\bar{\tau}}$. Существенной длиной полосы A_t будем называть величину l_t , равную числу переменных, от которых зависит полином, соответствующий верхней строке полосы A_t . Тогда первые $n - k + 1 - l_t$ элементов каждой строки из A_t являются нулевыми. Поэтому полоса A_t содержит не более l_t ненулевых столбцов $\bar{\tau}$. Пусть $\Sigma_{t,1}$ — схема минимальной сложности, вычисляющая величины $w_{t,b,\bar{\tau}}$ для всех ненулевых наборов $\bar{\tau}$ во всех прямоугольниках $D_{t,b}$ из полосы A_t , тогда

$$L(\Sigma_{t,1}) \leq \left(\frac{l_t}{s} + 1 \right) \frac{s}{k} \leq \frac{l_t}{k} + \frac{s}{k}.$$

Положим

$$w_{t,\bar{\tau}} = \bigoplus_b w_{t,b,\bar{\tau}},$$

где суммирование ведется по таким b , что прямоугольник $D_{t,b}$ содержит хотя бы один ненулевой набор $\bar{\tau}$. Если $\Sigma_{t,2}$ — схема минимальной сложности, выполняющая эти сложения для всех различных $\bar{\tau}$ в полосе A_t , то

$$L(\Sigma_{t,2}) \leq l_t 2^m / s.$$

Теперь значение каждого полинома, соответствующего строке из полосы A_t , есть значение некоторых значений $w_{t,\bar{\tau}}$. Пусть $\Sigma_{t,3}$ — схема минимальной сложности, вычисляющая полином, соответствующий одной строке, из некоторых сумм $w_{t,\bar{\tau}}$, тогда

$$L(\Sigma_{t,3}) \leq 2^m.$$

Таким образом, m полиномов, соответствующих строкам полосы A_t , вычисляются со сложностью, не превосходящей величины

$$\frac{l_t}{k} + \frac{s}{k} + \frac{l_t}{s} 2^m + m 2^m. \quad (17)$$

Пусть Σ_M — схема минимальной сложности, вычисляющая полиномы, соответствующие строкам матрицы M . Оценим величину $L(\Sigma_M)$ сначала при $k \geq 3$, а потом при $k = 2$.

Пусть $k \geq 3$. Тогда справедливо неравенство

$$L(\Sigma_M) \leq \sum_{l=1}^{n-k+1} \left(\frac{S(l)}{m} + 1 \right) \left(\frac{l}{k} + \frac{s}{k} + \frac{l}{s} 2^m + m 2^m \right) + d \sum_{i=1}^k i C_s^i,$$

Действительно, число a горизонтальных полос существенной длины l в матрице M не больше $S(l)/m + 1$, и поэтому M содержит не больше $\sum_{l=1}^{n-k+1} (S(l)/m + 1)$ горизонтальных полос A_l . Положим

$$s = \lceil n / \log^3 n \rceil, \quad m = \lfloor \log n - 6 \log \log n \rfloor.$$

Тогда

$$\begin{aligned} L(\Sigma_M) &\lesssim \sum_{l=1}^{n-k+1} \left(\frac{S(l)}{\log n} + 1 \right) \left(\frac{l}{k} + \frac{n}{k \log^3 n} + (\log^3 n + \log n) \frac{n}{\log^6 n} \right) + \frac{dk^2 s^k}{k!} \\ &\lesssim \sum_{l=1}^{n-k+1} \frac{S(l)}{\log n} \left(\frac{l}{k} + \frac{3n}{\log^3 n} \right) + \sum_{l=1}^{n-k+1} \left(\frac{l}{k} + \frac{3n}{\log^3 n} \right) + \frac{k^2 n^k}{k! \log^{3(k-1)} n}. \end{aligned} \quad (18)$$

Для оценки этой суммы докажем некоторые соотношения.

Нетрудно установить справедливость равенства

$$\sum_{i_1=1}^{n-k+1} \sum_{i_2=i_1+1}^{n-k+2} \dots \sum_{i_{k-2}=i_{k-3}+1}^{n-2} \sum_{i_{k-1}=i_{k-2}+1}^{n-1} \sum_{i_k=i_{k-1}+1}^n 1 = C_n^k. \quad (19)$$

Для этого рассмотрим полином степени k

$$f' = \bigoplus_{\sigma_1 + \dots + \sigma_n = k} x_1^{\sigma_1} \dots x_n^{\sigma_n}.$$

Его представление (16) запишется так:

$$f' = \bigoplus_{i_1=1}^{n-k+1} x_{i_1} \bigoplus_{i_2=i_1+1}^{n-k+2} x_{i_2} \dots \bigoplus_{i_{k-2}=i_{k-3}+1}^{n-2} x_{i_{k-2}} \bigoplus_{i_{k-1}=i_{k-2}+1}^{n-1} x_{i_{k-1}} (x_{i_{k-1}+1} \oplus \dots \oplus x_n) \dots \quad (20)$$

В правой части этой записи операции конъюнкции и сложения по модулю 2 заменим операциями обычного умножения и суммирования соответственно, а вместо переменных подставим единицы. Получим сумму

$$s' = \sum_{i_1=1}^{n-k+1} \sum_{i_2=i_1+1}^{n-k+2} \dots \sum_{i_{k-2}=i_{k-3}+1}^{n-2} \sum_{i_{k-1}=i_{k-2}+1}^{n-1} \sum_{i_k=i_{k-1}+1}^n 1,$$

которая равна числу мономов полинома f' , то есть $s' = C_n^k$. Теперь заметим, что сумма $\sum_{l=1}^{n-k+1} l S(l)$ также равна числу мономов полинома f' . Поэтому справедливо равенство

$$\sum_{l=1}^{n-k+1} l S(l) = C_n^k. \quad (21)$$

Для величины p_{n-k+1} , равной количеству полиномов $f_{x_{i_1} x_{i_2} \dots x_{i_{k-1}}}^1(x_{i_{k-1}+1}, \dots, x_n)$ из представления (16), справедливо равенство

$$p_{n-k+1} = \sum_{i_1=1}^{n-k+1} \sum_{i_2=i_1+1}^{n-k+2} \dots \sum_{i_{k-2}=i_{k-3}+1}^{n-2} \sum_{i_{k-1}=i_{k-2}+1}^{n-1} 1. \quad (22)$$

Действительно, в представлении (16) заменим единицами обозначения полиномов $f_{x_{i_1} x_{i_2} \dots x_{i_{k-1}}}^1(x_{i_{k-1}+1}, \dots, x_n)$, затем поступим так же, как и при доказательстве формулы (19), операции конъюнкции и сложения по модулю 2 заменим операциями обычного умножения и суммирования соответственно, а вместо переменных подставим единицы. В результате получим сумму, равную количеству полиномов $f_{x_{i_1} x_{i_2} \dots x_{i_{k-1}}}^1(x_{i_{k-1}+1}, \dots, x_n)$ из представления (16), которая будет иметь такой же вид, как и правая часть из (22). Теперь нетрудно получить равенство

$$p_{n-k+1} = C_{n-1}^{k-1}, \quad (23)$$

нужно лишь в (19) вместо n и k подставить $n-1$ и $k-1$ соответственно. Так как

$$p_{n-k+1} = \sum_{i=1}^{n-k+1} S(i),$$

верны соотношения

$$\sum_{i=1}^{n-k+1} S(i) = C_{n-1}^{k-1} \leq \frac{n^{k-1}}{(k-1)!}.$$

Отсюда, из (18) и (21) вытекает асимптотическое неравенство

$$L(\Sigma_M) \lesssim \frac{C_n^k}{k \log n} + \frac{3n^k}{(k-1)! \log^4 n} + \frac{n^2}{2k} + \frac{3n^2}{\log^3 n} + \frac{k^2 n^k}{k! \log^{3(k-1)} n}.$$

При $k \leq \log n$ выполнены соотношения

$$C_n^k \sim n^k/k!, \quad \log C_n^k \sim \log n^k,$$

откуда следует, что

$$L(\Sigma_M) \lesssim \frac{C_n^k}{\log C_n^k}.$$

Далее оценим величину $L(\Sigma_M)$ при $k=2$. Число строк в матрице M равно $n-1$. Поэтому число a горизонтальных полос A_t не больше $(n-1)/m+1$. Положим

$$s = \lceil n/\log^2 n \rceil, \quad m = \lfloor \log n - 3 \log \log n \rfloor.$$

Для существенной длины l_t полосы A_t , $1 \leq t \leq a$, справедливо неравенство

$$l_t \leq n-1-(t-1)m.$$

Отсюда и из (17) вытекают соотношения

$$\begin{aligned}
 L(\Sigma_M) &\leq \sum_{t=1}^a \left(\frac{l_t}{2} + \frac{s}{2} + \frac{l_t}{s} 2^m + m 2^m \right) + d \sum_{i=1}^k i C_s^i \\
 &\lesssim \sum_{t=1}^a \left(\frac{n-1-(t-1)m}{2} + \frac{s}{2} + \frac{n-1-(t-1)m}{s} 2^m + m 2^m \right) + d 4 C_s^2 \\
 &\lesssim \frac{n^2}{4m} + \frac{ns}{2m} + \frac{n^2 2^m}{2sm} + n 2^m + 2ds^2 \\
 &\lesssim \frac{n^2}{4 \log n} \sim \frac{C_n^2}{\log C_n^2}.
 \end{aligned}$$

Поэтому при $k \geq 2$

$$L(\Sigma_M) \lesssim \frac{C_n^k}{\log C_n^k}.$$

Теперь оценим сложность минимальной схемы Σ , которая выполняет умножения и сложения из представления (16) полинома f . Пусть это представление содержит A умножений. Тогда сложений в этом представлении будет менее A . Поэтому

$$L(\Sigma) \leq 2A.$$

Найдем количество умножений в (16). Когда мы получали это представление, мы сначала получили представление (14), куда входит A_{k-1} умножений, где A_{k-1} равно количеству полиномов степени $k-1$ вида $f_{x_{i_1}}^{k-1}(x_{i_1+1}, \dots, x_n)$. Затем получили представление (15), куда помимо A_{k-1} умножений входит еще A_{k-2} умножений, где A_{k-2} равно количеству полиномов степени $k-2$ вида $f_{x_{i_1} x_{i_2}}^{k-2}(x_{i_2+1}, \dots, x_n)$. Шаг за шагом получили представление (16), где число умножений A равно сумме $\sum_{j=1}^{k-1} A_j$, A_j — число полиномов степени $k-j$ вида $f_{x_{i_1} x_{i_2} \dots x_{i_j}}^{k-j}(x_{i_j+1}, \dots, x_n)$ в промежуточных представлениях. Заметим, что $A_1 = p_{n-k+1}$. Для каждого числа A_j выполнены соотношения

$$A_j = \sum_{i_1=1}^{n-k+1} \sum_{i_2=i_1+1}^{n-k+2} \dots \sum_{i_{j-1}=i_{j-2}+1}^{n-k+j-1} \sum_{i_j=i_{j-1}+1}^{n-k+j} 1 = C_{n-k+j}^j,$$

которые доказываются так же, как равенства (22) и (23) для величины p_{n-k+1} . Поэтому для числа A справедлива оценка

$$A = \sum_{j=1}^{k-1} A_j = \sum_{j=1}^{k-1} C_{n-(k-j)}^j \leq k C_{n-1}^{k-1} = o(C_n^k / \log C_n^k).$$

В итоге заключаем, что при $k \geq 2$

$$L(f) \lesssim L(\Sigma_M) + L(\Sigma) \lesssim \frac{C_n^k}{\log C_n^k}.$$

Теорема доказана.

Следующая теорема является следствием теорем 1 и 2.

Теорема 3. Пусть $f(x_1, \dots, x_n) \in P_2^{k,h}[n]$, $2 \leq k \leq n - \log n - 4 \log \log n$. Тогда

$$L(f) \lesssim \frac{C_n^k}{\log C_n^k}.$$

Замечание 1. Из мощностных соображений сложность $L(P_2^{k,h}[n])$, $2 \leq k \leq n$, оценивается снизу величиной $C_n^k / \log C_n^k (1 - \varepsilon_3(n))$, где $\varepsilon_3(n) \geq 0$ и стремится к нулю при $n \rightarrow \infty$ (см., например, теорему Д.1 в [3]). Из доказательства этой теоремы следует, что доля полиномов из класса $P_2^{k,h}[n]$, сложность которых менее $C_n^k / \log C_n^k (1 - \varepsilon_3(n))$, стремится к нулю. Отсюда получаем следующее утверждение.

Следствие 1. Пусть $f \in P_2^{k,h}[n]$, $2 \leq k \leq n - \log n - 4 \log \log n$. Тогда

$$L(f) \lesssim \frac{C_n^k}{\log C_n^k},$$

и для почти всех $f \in P_2^{k,o}[n]$ выполняется неравенство

$$L(f) \geq \frac{C_n^k}{\log C_n^k} (1 - \varepsilon_3(n)),$$

где $\varepsilon_3(n) \geq 0$ и стремится к нулю при $n \rightarrow \infty$.

4. Реализация полиномов Жегалкина

Теорема 4. Пусть $2 \leq k \leq n$. Тогда для каждого полинома $f \in P_2^k[n]$ при $n \rightarrow \infty$ справедливо соотношение

$$L(f) \lesssim \sum_{i=0}^k C_n^i / \log \sum_{i=0}^k C_n^i,$$

и для почти всех $f \in P_2^k[n]$ выполняется неравенство

$$L(f) \geq \sum_{i=0}^k C_n^i / \log \sum_{i=0}^k C_n^i (1 - \varepsilon(n)),$$

где $\varepsilon(n) \geq 0$ и стремится к нулю при $n \rightarrow \infty$.

Доказательство. Полином f из класса $P_2^k[n]$ можно представить в виде

$$f = \bigoplus_{i=1}^k g_i \oplus c,$$

где $g_i \in P_2^{i,h}[n]$, $c \in \{0, 1\}$.

Рассмотрим два случая:

$$2 \leq k \leq n - \log n - 4 \log \log n$$

(24)

и

$$n - \log n - 4 \log \log n < k \leq n. \quad (25)$$

Пусть k удовлетворяет (24). Очевидно, что при этих значениях k верно неравенство

$$k \leq \log \sum_{i=2}^k C_n^i.$$

Отсюда, из теоремы 3 и предложения 2 следует, что

$$L(f) \lesssim k + n + \sum_{i=2}^k \frac{C_n^i}{\log C_n^i} \lesssim k + n + \sum_{i=2}^k C_n^i / \log \sum_{i=2}^k C_n^i \lesssim \sum_{i=0}^k C_n^i / \log \sum_{i=0}^k C_n^i. \quad (26)$$

Пусть теперь k удовлетворяет условию (25). Из рассмотрения предыдущего случая следует, что сумма

$$\sum_{i=2}^{\lfloor n - \log n - 4 \log \log n \rfloor} g_i$$

вычисляется со сложностью L_1 , где

$$L_1 \lesssim \sum_{i=0}^k C_n^i / \log \sum_{i=0}^k C_n^i.$$

Вычислим систему полиномов

$$\alpha = \{g_i\}, \quad n - \log n - 4 \log \log n \leq i \leq k,$$

последовательно выполняя операции $\oplus$ и $\wedge$. Следовательно,

$$L(\alpha) \leq n \sum_{i=0}^{\lfloor \log n + 4 \log \log n \rfloor} C_n^{n-i} \leq 2n \log n \cdot C_n^{2 \log n} = o \left(\sum_{i=0}^k C_n^i / \log \sum_{i=0}^k C_n^i \right).$$

Поэтому справедливы соотношения

$$L(f) \lesssim k + n + L_1 + L(\alpha) \lesssim \sum_{i=0}^k C_n^i / \log \sum_{i=0}^k C_n^i.$$

Нижнюю оценку для $f \in P_2^k[n]$, $2 \leq k \leq n$, легко получить стандартным образом из мощностных соображений:

$$L(f) \geq \sum_{i=0}^k C_n^i / \log \sum_{i=0}^k C_n^i (1 - \varepsilon(n))$$

где $\varepsilon(n) \geq 0$ и стремится к нулю при $n \rightarrow \infty$. (см., например, теорему Д.1. в [3]), причем из доказательства этой теоремы следует, что доля полиномов, сложность которых менее $\sum_{i=0}^k C_n^i / \log \sum_{i=0}^k C_n^i$, стремится к нулю.

Теорема доказана.

Список литературы

1. Кочергин В. В., О сложности вычислений в конечных абелевых группах. *Матем. вопросы киберн.* (1990) **4**, 178–217.
2. Липатов Е. П., Об одном случае неравномерного локального кодирования. *Пробл. киберн.* (1977) **26**, 95–107.
3. Лупанов О. Б., Об одном подходе к синтезу управляющих систем — принципе локального кодирования. *Пробл. киберн.* (1965) **14**, 31–110.
4. Лупанов О. Б., О синтезе некоторых классов управляющих систем. *Пробл. киберн.* (1963) **10**, 63–97.
5. Pippenger N., On the evaluation of powers and monomials. *SIAM J. Comput.* (1980) **9**, 230–250.

Статья поступила 13.11.2003.