Math-Net.Ru

Общероссийский математический портал

С. Н. Селезнева, О сложности распознавания полноты множеств булевых функций, реализованных полиномами Жегалкина, *Дискрет. матем.*, 1997, том 9, выпуск 4, 24–31

DOI: <https://doi.org/10.4213/dm507>

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: 35.173.219.12

26 апреля 2023 г., 12:05:58

О сложности распознавания полноты множеств булевых функций, реализованных полиномами Жегалкина

© 1997 г. С. Н. Селезнева

Доказано, что существует алгоритм, с полиномиальной временной сложностью определяющий, является ли множество булевых функций, реализованных полиномами Жегалкина, полным. Доказано также, что если числа l и r являются соответственно длиной и рангом полинома самодвойственной (четной) булевой функции, то верно неравенство $l \geq \sqrt{2^r} - 1$ ($l \geq \sqrt{2^r}$).

1. Основные понятия

Пусть $E_2 = \{0, 1\}$. Функцию $f = f(x_1, \dots, x_n)$, $n \geq 0$, определенную на E_2^n и принимающую значения из E_2 , назовем булевой. Множество всех булевых функций обозначим через P_2 . Будем рассматривать P_2 как функциональную систему с операциями суперпозиции [1]. Пусть $M \subseteq P_2$. Множество M называется полным, если любая булева функция может быть получена из функций M при помощи операций суперпозиции. Критерий полноты был получен Постом [2, 3]. Его формулировка использует следующие понятия.

Функция $f(x_1, \dots, x_n)$ называется

- (1) сохраняющей константу a из E_2 , если $f(a, \dots, a) = a$;
- (2) линейной, если $f(x_1, \dots, x_n)$ может быть представлена в виде

$$a_1 x_1 \oplus \dots \oplus a_n x_n, \quad a_i \in E_2, \quad i = 1, \dots, n;$$

- (3) монотонной, если

$$f(a_1, \dots, a_n) \leq f(b_1, \dots, b_n)$$

для всех $a_1, \dots, a_n, b_1, \dots, b_n$ таких, что $a_i \leq b_i$, $i = 1, \dots, n$;

- (4) самодвойственной, если

$$f(\bar{x}_1, \dots, \bar{x}_n) = \bar{f}(x_1, \dots, x_n).$$

Множества всех булевых функций, сохраняющих константу 0 (1), являющихся линейными, монотонными, самодвойственными обозначаются соответственно через T_0 (T_1), L , M , S .

Теорема 1 ([2]). Пусть $M \subseteq P_2$. Множество M полно тогда и только тогда, когда M не содержится ни в одном из множеств T_0, T_1, L, M, S .

Пусть теперь M конечно. Нас будет интересовать вопрос, с какой алгоритмической сложностью можно установить его полноту. Заметим, что названная сложность существенно зависит от способа реализации функций M . В работе рассматривается случай, когда функции реализуются полиномами Жегалкина.

Произведение вида $x_{i_1} \dots x_{i_r}$, в котором все сомножители различны, назовем (монотонной) элементарной конъюнкцией. Рангом элементарной конъюнкции назовем число ее сомножителей. Константу 1 будем считать вырожденной конъюнкцией ранга 0. Любую булеву функцию $f(x_1, \dots, x_n)$ можно представить в виде полинома

$$\sum_{i=1}^l K_i,$$

где K_i — различные элементарные конъюнкции, $i = 1, \dots, l$, $l \geq 0$. Он называется полиномом Жегалкина [4, 5] и для конкретной функции определяется с точностью до порядка слагаемых и сомножителей в слагаемых однозначно. Длиной полинома назовем число его слагаемых, рангом — максимальный ранг его слагаемых. Будем полагать, что 0 является вырожденным полиномом, длина которого равна 0. Ранг 0 не определен. Полином Жегалкина булевой функции $f(x_1, \dots, x_n)$ будем обозначать через $\Pi(f)$, $\Pi(0) = 0$.

Дальнейшее содержание работы устроено следующим образом. В разделах 2 и 3 исследуются некоторые свойства полиномов Жегалкина булевых функций. С использованием этих свойства в разделе 4 доказано, что временная сложность распознавания полноты множества булевых функций, реализованных полиномами Жегалкина, полиномиальна.

2. Некоторые свойства самодвойственных булевых функций

Пусть $f(x_1, \dots, x_n) \in P_2$, через $f^+(x_1, \dots, x_n)$ обозначим $f(\bar{x}_1, \dots, \bar{x}_n)$. Булеву функцию $f(x_1, \dots, x_n)$ назовем четной, если

$$f(x_1, \dots, x_n) = f^+(x_1, \dots, x_n).$$

Множество всех четных булевых функций обозначим через H .

Пусть K_1, K_2 — элементарные конъюнкции. Обозначим через $\wedge(K_1, K_2)$ элементарную конъюнкцию, составленную из общих сомножителей K_1 и K_2 . По определению положим, что $\wedge(1, K_1) = 1$ для любой элементарной конъюнкции K_1 , $\wedge(K_1, K_2) = 1$, если K_1 и K_2 не имеют общих сомножителей. Будем обозначать через $K_1 < K_2$ тот факт, что каждый сомножитель K_1 содержится также в K_2 , но не наоборот. По определению положим, что $1 < K_1$ для любой элементарной конъюнкции K_1 , не равной 1.

Пусть $f(x_1, \dots, x_n) \in P_2$, K — элементарная конъюнкция.

Положим $k(K, f)$, равным 1, если K является слагаемым $\Pi(f)$, и равным 0 в противном случае.

Положим $\text{ind}(K, f) = 0$, если число таких слагаемых K_i полинома $f(x_1, \dots, x_n)$, что $K < K_i$, четно, и $\text{ind}(K, f) = 1$ в остальных случаях.

Лемма 1. Функция $f(x_1, \dots, x_n) \in P_2$ является самодвойственной тогда и только тогда, когда $k(K, \bar{f}) = k(K, f^+)$ для любой элементарной конъюнкции K .

Функция $f(x_1, \dots, x_n) \in P_2$ является четной тогда и только тогда, когда $k(K, f) = k(K, f^+)$ для любой элементарной конъюнкции K .

Доказательство. Утверждение леммы 1 следует из определений самодвойственной и четной функций и однозначности представления булевой функции полиномом Жегалкина.

Пусть

$$f(x_1, \dots, x_n) \in P_2, \quad \Pi(f) = \sum_{i=1}^l K_i.$$

Пусть $f_i(x_1, \dots, x_n) = K_i$, $i = 1, \dots, l$. Тогда $\Pi(f^+)$ может быть получен из суммы

$$\sum_{i=1}^l \Pi(f_i^+),$$

с использованием правила $K \oplus K = 0$, верного для любой элементарной конъюнкции K . Заметим также, что $\Pi(f_i^+)$ содержит всевозможные элементарные конъюнкции K , такие, что $K < K_i$ или $K = K_i$. Следовательно, если K — элементарная конъюнкция, то $k(K, \bar{f}) = k(K, f^+)$ тогда и только тогда, когда $\text{ind}(K, f) = 0$ при $K \neq 1$ и $\text{ind}(1, f) = 1$.

Лемма 2. Пусть $f(x_1, \dots, x_n) \in H$,

$$f(x_1, \dots, x_n) = x_i g(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n) \oplus h(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n).$$

Тогда

$$g(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n) \in H.$$

Доказательство. Так как $f(x_1, \dots, x_n) \in H$, в силу леммы 1 $k(K, f) = k(K, f^+)$ для любой элементарной конъюнкции K вида $x_i K_1$, где K_1 не содержит x_i . Так как

$$f(x_1, \dots, x_n) = x_i g(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n) \oplus h(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n),$$

справедливо представление

$$\begin{aligned} f^+(x_1, \dots, x_n) &= (x_i \oplus 1)g^+(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n) \\ &\quad \oplus h^+(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n) \\ &= x_i g^+(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n) \\ &\quad \oplus g^+(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n) \\ &\quad \oplus h^+(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n). \end{aligned}$$

Следовательно, $k(K_1, g) = k(K_1, g^+)$ для любой элементарной конъюнкции K_1 , не содержащей x_i . Очевидно, что если элементарная конъюнкция K_2 содержит сомножитель x_i , то $k(K_2, g) = k(K_2, g^+) = 0$. Следовательно, по лемме 1

$$g(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n) \in H.$$

Лемма 3. Пусть $f(x_1, \dots, x_n) \in H$ и $\Pi(f) \neq 0$. Тогда в $\Pi(f)$ найдутся такие слагаемые K_1 и K_2 (не обязательно различные), что $\wedge(K_1, K_2) = 1$.

Доказательство. Так как $\Pi(f) \neq 0$, найдутся такие значения $a_1, \dots, a_n$ из E_2 переменных $x_1, \dots, x_n$, что $f(a_1, \dots, a_n) \neq 0$. Если $a_i = 0$ при $i = 1, \dots, n$, то $\Pi(f)$ содержит 1 в качестве слагаемого. Пусть $K_1 = K_2 = 1$. Очевидно, что $\wedge(1, 1) = 1$.

В противном случае, пусть $J_0 \subseteq \{1, \dots, n\}$ и J_0 в точности содержит номера тех $a_1, \dots, a_n$, которые равны 0, $J_1 = \{1, \dots, n\} \setminus J_0$. Множества J_0, J_1 непусты, так как $f(0, \dots, 0) = f(1, \dots, 1) = 0$.

Так как $f(a_1, \dots, a_n) = 1$, в $\Pi(f)$ входит хотя бы одно слагаемое, не содержащее переменные с номерами из J_0 . Обозначим его через K_1 . Пусть $b_1 = \bar{a}_1, \dots, b_n = \bar{a}_n$. Так как $f(x_1, \dots, x_n)$ — четная функция, то $f(b_1, \dots, b_n) \neq 0$. Следовательно, в $\Pi(f)$ входит хотя бы одно слагаемое, не содержащее переменные с номерами из J_1 . Обозначим его через K_2 . По построению $\wedge(K_1, K_2) = 1$.

Лемма 4. Пусть $f(x_1, \dots, x_n) \in H$. Тогда для любой элементарной конъюнкции K верно следующее утверждение: если в $\Pi(f)$ найдется слагаемое K_0 такое, что $K < K_0$ или $K = K_0$, то в $\Pi(f)$ также найдутся слагаемые K_1 и K_2 (не обязательно различные) такие, что $K = \wedge(K_1, K_2)$.

Доказательство. Если $K = 1$, то утверждение леммы 4 следует из леммы 3.

Проведем доказательство индукцией по n для случая, когда $K \neq 1$. Пусть $n \leq 2$. Тогда $f(x_1, x_2) = x_1 \oplus x_2$, или $f(x_1, x_2) = x_1 \oplus x_2 \oplus 1$, или f равна константе. Во всех этих случаях лемма 4 верна. Пусть лемма 4 верна для $k < n$. Установим ее справедливость для $k = n$. Пусть

$$f(x_1, \dots, x_n) = x_i g(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n) \oplus h(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n),$$

причем ясно, что такое представление всегда возможно. Согласно лемме 2 функция $g(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n)$ является четной. По индуктивному предположению для любой элементарной конъюнкции K верно, что если в $\Pi(g)$ найдется такое слагаемое K_0 , что $K < K_0$ или $K = K_0$, то в $\Pi(g)$ найдутся также слагаемые K_1 и K_2 такие, что $\wedge(K_1, K_2) = K$. Следовательно, для любой элементарной конъюнкции $x_i K$ верно утверждение леммы 4.

Теорема 2. Если $f(x_1, \dots, x_n)$ — четная функция и $\Pi(f) \neq 0$, то для чисел l и r , являющихся соответственно длиной и рангом $\Pi(f)$, верно неравенство $l \geq \sqrt{2^r}$.

Если $f(x_1, \dots, x_n)$ — самодвойственная функция и $\Pi(f) \neq 0$, то для чисел l и r , являющихся соответственно длиной и рангом $\Pi(f)$ верно неравенство $l \geq \sqrt{2^r - 1}$.

Доказательство. Докажем первое утверждение. Так как ранг $\Pi(f)$ равен r , в $\Pi(f)$ найдется слагаемое K_0 , ранг которого равен r . Следовательно, число различных элементарных конъюнкций K таких, что $K < K_0$ или $K = K_0$, равно 2^r .

Так как длина $\Pi(f)$ равна l , число всевозможных элементарных конъюнкций вида $\wedge(K_1, K_2)$, где K_1, K_2 — слагаемые $\Pi(f)$, не больше, чем l^2 . Утверждение леммы 4 требует, чтобы выполнялось неравенство $2^r \leq l^2$, то есть $l \geq \sqrt{2^r}$.

Докажем второе утверждение. Пусть

$$g(x_1, \dots, x_n) = f(x_1, \dots, x_n) \oplus x_1.$$

Утверждение следует из доказанного выше, если заметить, что $g(x_1, \dots, x_n)$ является четной, и $\Pi(f)$ и $\Pi(g)$ отличаются только слагаемым ранга 1, а их длины отличаются не более, чем на 1.

Обозначим через $l^*(r)$ наименьшую длину полинома четной функции, ранг которого равен r .

Предложение 1. *Справедливо соотношение*

$$l^*(r) \asymp \sqrt{2^r}.$$

Доказательство. В самом деле, рассмотрим

$$f(x_1, \dots, x_k, x_{k+1}, \dots, x_{2k}) = \bar{x}_1 \dots \bar{x}_k x_{k+1} \dots x_{2k} \vee x_1 \dots x_k \bar{x}_{k+1} \dots \bar{x}_{2k}.$$

Очевидно, что функция $f(x_1, \dots, x_{2k})$ четная, длина $\Pi(f)$ равна $2 \cdot 2^k - 2$, а ранг равен $(2k - 1)$. Следовательно, $\sqrt{2^r} \leq l^*(r) \leq 2 \cdot 2^{(r+1)/2} - 2$, и $l^*(r) \asymp \sqrt{2^r}$.

3. Одно свойство полиномов Жегалкина

Пусть $a_1, \dots, a_n \in E_2$. Будем писать $K \leftrightarrow (a_1, \dots, a_n)$, если элементарная конъюнкция K в точности состоит из всех таких переменных x_i , что $a_i = 1$. По определению положим, что $1 \leftrightarrow (0, \dots, 0)$.

Пусть $f(x_1, \dots, x_n) \in P_2$. Назовем $(a_1, \dots, a_n)$ нижней единицей $f(x_1, \dots, x_n)$, если $f(a_1, \dots, a_n) = 1$ и $f(b_1, \dots, b_n) = 0$ для таких $b_1, \dots, b_n$ из E_2 , что $b_i \leq a_i$ при $i = 1, \dots, n$ и $b_i < a_i$ хотя бы для одного i из $\{1, \dots, n\}$.

Будем писать $K \preceq \Pi(f)$, если элементарная конъюнкция K является слагаемым $\Pi(f)$ и в $\Pi(f)$ нет слагаемого K_1 такого, что $K_1 < K$.

Лемма 5. *Пусть $f(x_1, \dots, x_n) \in P_2$, K — элементарная конъюнкция и $a_1, \dots, a_n \in E_2$. Тогда если $K \leftrightarrow (a_1, \dots, a_n)$, то $K \preceq \Pi(f)$ тогда и только тогда, когда $(a_1, \dots, a_n)$ — нижняя единица $f(x_1, \dots, x_n)$.*

Доказательство. Докажем достаточность. Если $K \leftrightarrow (a_1, \dots, a_n)$ и $K \preceq \Pi(f)$, то, очевидно, $f(a_1, \dots, a_n) = 1$. Если $b_1, \dots, b_n \in E_2$, $b_i \leq a_i$ при $i = 1, \dots, n$ и $b_i < a_i$ хотя бы для одного i из $\{1, \dots, n\}$, то $f(b_1, \dots, b_n) = 0$. Следовательно, $(a_1, \dots, a_n)$ — нижняя единица $f(x_1, \dots, x_n)$.

Докажем необходимость. Пусть $K \leftrightarrow (a_1, \dots, a_n)$ и $(a_1, \dots, a_n)$ — нижняя единица $f(x_1, \dots, x_n)$. Пусть $\mathcal{K}$ — множество всех слагаемых $\Pi(f)$, которые обращаются в 1 при значениях переменных $x_1, \dots, x_n$, равных соответственно $a_1, \dots, a_n$. Так как $f(a_1, \dots, a_n) = 1$, то $\mathcal{K}$ непусто. Выберем в $\mathcal{K}$ такую элементарную конъюнкцию K_0 , что для любой K из $\mathcal{K}$ неверно, что $K < K_0$. Пусть $b_1, \dots, b_n \in E_2$ и $K_0 \leftrightarrow (b_1, \dots, b_n)$. Заметим, что $f(b_1, \dots, b_n) = 1$. Очевидно также, что $b_i \leq a_i$ при $i = 1, \dots, n$. Так как $(a_1, \dots, a_n)$ — нижняя единица $f(x_1, \dots, x_n)$, то, следовательно, $b_i = a_i$ при $i = 1, \dots, n$, то есть $K_0 \leftrightarrow (a_1, \dots, a_n)$ и $K_0 = K$. По построению $K_0 \preceq \Pi(f)$. Следовательно, $K \preceq \Pi(f)$.

4. О сложности распознавания свойств булевых функций

В качестве алгоритмической модели будем использовать детерминированные многоленточные машины Тьюринга (МТ). Определения понятий, относящихся к МТ, можно найти, например, в [6].

Пусть $A = \{x, 0, 1, \dots, \oplus\}$ — алфавит символов МТ. Словом в алфавите A назовем произвольную конечную (в том числе и пустую) последовательность символов A . Пусть A^* — множество всех слов в алфавите A , через ϵ обозначим пустое слово. Если слово $\alpha \in A^*$, то через $|\alpha|$ обозначим число символов в нем, $|\epsilon| = 0$. Под временной сложностью МТ будем понимать функцию зависимости числа тактов ее работы от числа символов входного слова. Если временная сложность МТ не больше полинома некоторой степени, то назовем ее полиномиальной.

Обозначим через $\mathcal{P}_2$ множество всех конечных подмножеств P_2 . Пусть s отображает $P_2 \cup \mathcal{P}_2$ в A^* следующим образом: $s(0) = 0$, $s(1) = 1$;
 $s(f) = xa_1a_2\dots a_t$, где $a_j \in \{0, 1\}$ при $j = 1, 2, \dots, t$ и

$$i = \sum_{j=1}^t a_j 2^{t-j},$$

если $\Pi(f) = x_i$;

$s(f) = s(x_{i_1})s(x_{i_2})\dots s(x_{i_r})$, если $\Pi(f) = K$, $K = x_{i_1}x_{i_2}\dots x_{i_r}$, $r \geq 2$;

$s(f) = s(K_1) \oplus s(K_2) \oplus \dots \oplus s(K_l)$, если $\Pi(f) = \sum_{i=1}^l K_i$, $l \geq 2$;

$s(M) = s(f_1), s(f_2), \dots, s(f_m)$, если $M = \{f_1, f_2, \dots, f_m\}$.

Пусть $\mathcal{P} \subseteq A^*$ и $\alpha \in \mathcal{P}$ тогда и только тогда, когда $\alpha = s(M)$, где $M \in \mathcal{P}_2$.

Пусть $\mathcal{F} \subseteq A^*$ и $\alpha \in \mathcal{F}$ тогда и только тогда, когда $\alpha = s(f)$, где $f \in P_2$.

Очевидно, что существуют МТ, для любого α из A^* определяющие, принадлежит ли α множествам $\mathcal{P}$ и $\mathcal{F}$ соответственно, с временной сложностью, не большей, чем $O(|\alpha|)$.

Пусть $\mathcal{A} \subseteq \mathcal{P}$ и α , равное $s(M)$, принадлежит $\mathcal{A}$, тогда и только тогда, когда M полно.

Пусть $\mathcal{A}_s \subseteq \mathcal{F}$ и α , равное $s(f)$, принадлежит $\mathcal{A}_s$ тогда и только тогда, когда f самодвойственна.

Пусть $\mathcal{A}_m, \mathcal{A}_l, \mathcal{A}_{t_0}, \mathcal{A}_{t_1} \subseteq \mathcal{F}$ и определяются по аналогии с $\mathcal{A}_s$ соответственно для монотонных, линейных, сохраняющих 0 и сохраняющих 1 функций.

Предложение 2. Пусть $\mathcal{A}_{t_0}, \mathcal{A}_{t_1}, \mathcal{A}_l$ — определенные выше подмножества $\mathcal{F}$. Существуют МТ, для любого α из $\mathcal{F}$ определяющие, принадлежит ли α множествам $\mathcal{A}_{t_0}, \mathcal{A}_{t_1}, \mathcal{A}_l$ соответственно, с временной сложностью, не большей, чем $O(|\alpha|)$.

Доказательство очевидно.

Лемма 6. Пусть $\mathcal{A}_s$ — определенное выше подмножество $\mathcal{F}$. Существует МТ, для любого α из $\mathcal{F}$ определяющая, принадлежит ли α множеству $\mathcal{A}_s$, с временной сложностью, не большей, чем $O(|\alpha|^4)$.

Доказательство. Пусть $\alpha \in \mathcal{F}$, то есть $\alpha = s(f)$ для некоторой $f(x_1, \dots, x_n)$ из P_2 . Пусть

$$\Pi(f) = \sum_{i=1}^l K_i.$$

Заметим, что $|\alpha| \geq l$. Требуемую МТ можно построить, используя следующий алгоритм.

Рассматриваем K_i , $i = 1, \dots, l$. Для любой элементарной конъюнкции K такой, что $K < K_i$, проверяем условие $\text{ind}(K, f) = 0$ при $K \neq 1$ и $\text{ind}(1, f) = 1$. Невыполнение этого условия означает несамодвойственность $f(x_1, \dots, x_n)$. Несамодвойственность $f(x_1, \dots, x_n)$ также будет иметь место, если для некоторого i число элементарных конъюнкций K таких, что $K < K_i$ или $K = K_i$, будет больше, чем $(l+1)^2$.

Если будут рассмотрены все слагаемые $\Pi(f)$ и не будет установлена несамодвойственность $f(x_1, \dots, x_n)$, то $f(x_1, \dots, x_n)$ является самодвойственной.

Временная сложность такой проверки не больше, чем $Cl(l+1)^2|\alpha|$, где C — некоторая константа.

Правильность алгоритма следует из леммы 1 и теоремы 2.

Лемма 7. Пусть $\mathcal{A}_m$ — определенное выше подмножество $\mathcal{F}$. Существует МТ, для любого α из $\mathcal{F}$ определяющая, принадлежит ли α множеству $\mathcal{A}_m$, с временной сложностью, не большей, чем $O(|\alpha|^3)$.

Доказательство. Пусть $\alpha \in \mathcal{F}$, то есть $\alpha = s(f)$ для некоторой $f(x_1, \dots, x_n)$ из P_2 . Пусть

$$\Pi(f) = \sum_{i=1}^l K_i.$$

Заметим, что $|\alpha| \geq l$. Требуемую МТ можно построить, используя следующий алгоритм.

Находим все нижние единицы $f(x_1, \dots, x_n)$, используя утверждение леммы 5. Временная сложность, требуемая для их нахождения, не больше, чем $Cl|\alpha|$, где C — некоторая константа.

Пусть число нижних единиц равно m , причем $m \leq l$. Упорядочиваем их произвольным образом. Рассматриваем i -ю нижнюю единицу $(a_1, \dots, a_n)$, $i = 1, \dots, m$. Пусть K_0 такая элементарная конъюнкция, что $K_0 \leftrightarrow (a_1, \dots, a_n)$. В $\Pi(f)$ вычеркиваем все переменные, являющиеся сомножителями в K_0 . В оставшейся записи приводим подобные слагаемые по правилу $K \oplus K = 0$, верному для любой элементарной конъюнкции K . В результате получаем полином некоторой функции $g(x_1, \dots, x_n)$, причем, если $g(x_1, \dots, x_n) \neq 0$, то $f(x_1, \dots, x_n)$ немонотонна.

Если будут рассмотрены все нижние единицы $f(x_1, \dots, x_n)$ и не будет установлена немонотонность, то $f(x_1, \dots, x_n)$ является монотонной. Временная сложность выполнения этих операций не больше, чем $Cm(|\alpha| + l|\alpha|)$, где C — некоторая константа.

Теорема 3. Пусть $\mathcal{A}$ — определенное выше подмножество $\mathcal{F}$. Существует МТ, для любого α из $\mathcal{F}$ определяющая, принадлежит ли α множеству $\mathcal{A}$, с временной сложностью, не большей, чем $O(|\alpha|^4)$.

Доказательство. Теорема 3 следует из теоремы 1, предложения 2 и лемм 6 и 7.

Список литературы

1. Яблонский С. В., Гаврилов Г. П., Кудрявцев В. Б. *Функции алгебры логики и классы Поста*. Наука, Москва, 1966.
2. Post E. Introduction to a general theory of elementary propositions. *Amer. J. Math.* (1921) **43**, 163–185.
3. Post E. *Two-valued Iterative Systems of Mathematical Logic*. Princeton Univ. Press, Princeton, 1941.
4. Жегалкин И. И. О технике вычислений предложений в символической логике. *Матем. сб.* (1927) **34**, 9–28.
5. Жегалкин И. И. Арифметизация символической логики. *Матем. сб.* (1928) **35**, №3–4.
6. Ахо А., Хопкрофт Дж., Уллман Дж. *Построение и анализ вычислительных алгоритмов*. Мир, Москва, 1979.

Статья поступила 27.04.1994.

Переработанный вариант поступил 17.10.1997.