ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Июль—сентябрь 2006. Серия 1. Том 13, № 3. 13–26

УДК 519.716.325

ПОЛИНОМИАЛЬНЫЕ ОПЕРАТОРНЫЕ ПРЕДСТАВЛЕНИЯ ФУНКЦИЙ k-ЗНАЧНОЙ ЛОГИКИ*)

А. С. Зинченко, В. И. Пантелеев

Рассматривается обобщение операторного подхода при исследовании полиномиальных представлений функций k-значной логики. Основной идеей построения операторных полиномиальных форм служит представление базисных функций канонической формы в виде операторных образов фиксированной функции (системы функций) по определённому набору операторов (определённому оператору). Приводятся некоторые оценки сложности полученных полиномиальных представлений.

1. Основные понятия

Пусть $k \geqslant 2$ — простое число и $E_k = \{0, \ldots, k-1\}$. Функцией k-значной логики называется отображение $f : E_k^n \to E_k$, а n — её размерностью. Множество всех функций k-значной логики от n переменных обозначим через F_k^n. В дальнейшем вместо «функция k-значной логики» будем говорить просто «функция».

Для n-местной функции $f(x_1, ..., x_n)$ и набора $(\sigma_1, ..., \sigma_n)$ будем использовать обозначения $f(\widetilde{x})$ и $\widetilde{\sigma}$ соответственно.

Операции сложения $+$, вычитания $-$ и умножения $\cdot$ выполняются по модулю k. Операция $\oplus$ есть сложение по модулю 2. Также будем считать, что

$$x^0 = 1 \text{ и } x^n = \underbrace{x \cdot \ldots \cdot x}_{n}, \text{ если } n \neq 0.$$

Последовательность символов $t_1^{a_1} t_2^{a_2} \ldots t_n^{a_n}$ такая, что $t_i \in \{e, p, d\}$ и $a_i \in E_k$ при $i \in \{1, 2, \ldots, n\}$, называется *оператором* и обозначается через t, её члены называются *компонентами* оператора, t_i — *основанием* компоненты оператора, a_i — её *показателем*, а число n — *длиной* оператора [1].

*) Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований (проект 04–07–90178в).

Пустая последовательность задает единственный оператор длины 0. Обозначим его через $\varnothing$. Оператор длины n задает отображение из F_k^n в F_k^n по правилу $tf(\widetilde{x}) = f_n(\widetilde{x})$, где $f_n(\widetilde{x})$ определяется по индукции следующим образом: $f_0(\widetilde{x}) = f(\widetilde{x})$,

$$f_i(\widetilde{x}) = \begin{cases} f_{i-1}(\widetilde{x}), & \text{если } t_i = e \text{ или } a_i = 0; \\ \widehat{f}_{i-1}(\widetilde{x}), & \text{если } t_i = p \text{ и } a_i \neq 0; \\ f_{i-1}(\widetilde{x}) + \widehat{f}_{i-1}(\widetilde{x}), & \text{если } t_i = d \text{ и } a_i \neq 0, \end{cases}$$

где $\widehat{f}_{i-1}(\widetilde{x}) = f_{i-1}(x_1, \ldots, x_{i-1}, x_i + a_i, x_{i+1}, \ldots, x_n)$, $i \in \{1, \ldots, n\}$.

При $n = 1$ оператор e^a будем называть *тождественным*, p^a — оператором *сдвига*, а d^a — *разностным* оператором.

Обозначим $\underbrace{t^a(t^a(\ldots t^a}_{i}(f(x))\ldots)) = (t^a)^i f(x)$. Можно заметить, что

$$(p^a)^k f(x) = f(x) \text{ и } (d^a)^k f(x) = 2f(x).$$

Упорядоченное множество, состоящее из k^n операторов длины n, называется *пучком* операторов, число n называется *размерностью* этого пучка. Пучки операторов будем также называть операторными пучками или просто пучками. Для упорядочения операторов в пучке будем использовать наборы $\widetilde{0} = (0, 0, ..., 0)$, ..., $\widetilde{k-1} = (k-1, k-1, ..., k-1)$.

Пучок $O = (o_1^{i_1} \ldots o_n^{i_n} \mid (i_1, \ldots, i_n) \in E_k^n, o_i \in \{p, d\})$ называется *однородным*.

Среди однородных пучков выделим два:

$$P = (p^{i_1} ... p^{i_n} | (i_1, ..., i_n) \in E_k^n) \text{ и } D = (d^{i_1} ... d^{i_n} | (i_1, ..., i_n) \in E_k^n).$$

Будем рассматривать полиномиальные представления функций k-значной логики, имеющие вид многоместных сумм по модулю k, в которых элементарными слагаемыми являются:

1) операторные образы фиксированной функции $g(\widetilde{x})$ по заданному пучку T: $f(\widetilde{x}) = \sum\limits_{\widetilde{\sigma} \in E_k^n} c_{\widetilde{\sigma}} t^{\widetilde{\sigma}} g(\widetilde{x})$, $t^{\widetilde{\sigma}} \in T$, $c_{\widetilde{\sigma}} \in E_k$;

2) операторные образы системы функций $g_i(\widetilde{x})$ из G по оператору t: $f(\widetilde{x}) = \sum\limits_{\widetilde{\sigma} \in E_k^n} c_{\widetilde{\sigma}} t g_{\widetilde{\sigma}}(\widetilde{x})$, $g_{\widetilde{\sigma}}(\widetilde{x}) \in G$, $c_{\widetilde{\sigma}} \in E_k$.

При полиномиальном представлении функций можно выделить следующие проблемы: нахождение такого класса или классов полиномов, чтобы любая функция была представима полиномами этого класса (классов); оценка сложности таких представлений, например, с точки зрения числа слагаемых в полиноме.

2. Существование полиномиальных представлений

Пучок операторов T размерности n назовём *базисным*, если существует такая функция $g \in F_k^n$, что любую функцию $f \in F_k^n$ можно представить в виде линейной комбинации операторных образов функции g по операторам из T.

Функция $f(\widetilde{x})$ называется *невырожденной*, если $\sum\limits_{\widetilde{\sigma} \in E_k^n} f(\widetilde{\sigma}) \neq 0$.

Существование базисных пучков следует из следующего утверждения.

Теорема 1 [2]. *Для любой функции $f \in F_k^n$ существует полиномиальное представление вида $f(\widetilde{x}) = \sum\limits_{o^{\widetilde{\sigma}} \in O} c_{\widetilde{\sigma}} o^{\widetilde{\sigma}} g(\widetilde{x})$, $c_{\widetilde{\sigma}} \in E_k$, тогда и только тогда, когда $g(\widetilde{x})$ является невырожденной.*

Однородные пучки являются не единственными базисными. Для описания базисных пучков дадим некоторые определения.

Для каждого оператора t^a длины 1 определим характеристики α и β следующим образом:

$$\alpha = \begin{cases} 0 & \text{при } a = 0; \\ 1 & \text{при } a \neq 0, \end{cases} \qquad \beta = \begin{cases} 0 & \text{при } t = p \text{ и } a \neq 0; \\ 1 & \text{в остальных случаях.} \end{cases}$$

Матрицей пучка $T = (t^{\widetilde{0}}, \ldots, t^{\widetilde{k-1}})$ операторов $t^{\widetilde{\sigma}} = t_1^{a_{1\sigma_1}} \ldots\ t_n^{a_{n\sigma_n}}$ длины n назовём матрицу $M_T = (m_{\widetilde{\sigma}\widetilde{\tau}})$ такую, что

$$m_{\widetilde{\sigma}\widetilde{\tau}} = (\alpha_{1\sigma_1})^{i(\tau_1)} \cdot \ldots \cdot (\alpha_{n\sigma_n})^{i(\tau_n)} \cdot (\beta_{1\sigma_1})^{i(\tau_1)\oplus 1} \cdot \ldots \\ \ldots \cdot (\beta_{n\sigma_n})^{i(\tau_n)\oplus 1} \cdot (k - a_{1\sigma_1})^{[\tau_1]} \cdot \ldots \cdot (k - a_{n\sigma_n})^{[\tau_n]},$$

где

$$i(a) = \begin{cases} 0 & \text{при } a = 0, \\ 1 & \text{при } a \neq 0; \end{cases}, \quad a^{[\tau]} = \begin{cases} 1 & \text{при } a = \tau \text{ или } \tau = 0, \\ 0 & \text{в остальных случаях.} \end{cases}$$

Теорема 2. *Если $T = (t^{\widetilde{0}}, \ldots, t^{\widetilde{k-1}})$ — пучок операторов длины n и $g(\widetilde{x}) \in F_k^n$, то любую функцию $f(\widetilde{x}) \in F_k^n$ можно представить в виде*

$$f(\widetilde{x}) = \sum_{\widetilde{\sigma} \in E_k^n} c_{\widetilde{\sigma}} t^{\widetilde{\sigma}} g(\widetilde{x}), \text{ где } c_{\widetilde{\sigma}} \in E_k,$$

тогда и только тогда, когда выполняются условия:

1) $\det M_T \neq 0$, 2) $g(\widetilde{x})$ — *невырожденная функция.*

Доказательство. Пусть $F_k[x_1,\dots,x_n]$ — кольцо многочленов от n переменных с коэффициентами из множества E_k.

Рассмотрим алгебру многочленов $A \simeq F_k[x_1,\dots,x_n]/(x_1^k-1,\dots, x_n^k-1)$.

Каждой k-значной функции $f(\widetilde{x})$ поставим в соответствие элемент $\widehat{f}(\widetilde{x}) \in A$, который определен следующим образом:

$$\widehat{f}(\widetilde{x}) = \sum_{\widetilde{\sigma}} f(\widetilde{\sigma}) \cdot x_1^{\sigma_1} \cdot \ldots \cdot x_n^{\sigma_n}.$$

Отображение $f(\widetilde{x}) \to \widehat{f}(\widetilde{x})$ линейно и взаимнооднозначно.

Покажем, что $\widehat{g}(x_1+r_1,\dots,x_n+r_n) = x_1^{k-r_1}\cdot\ldots\cdot x_n^{k-r_n}\widehat{g}(x_1,\dots,x_n)$. Действительно,

$$\begin{aligned}
\widehat{g}(x_1+r_1,\dots,x_n+r_n) &= \sum_{\widetilde{\sigma}} g(\sigma_1+r_1,\dots,\sigma_n+r_n)\cdot x_1^{\sigma_1}\cdot\ldots\cdot x_n^{\sigma_n} \\
&= \sum_{\widetilde{\sigma}} g(\sigma_1+r_1,\dots,\sigma_n+r_n)\cdot x_1^{\sigma_1+r_1-r_1}\cdot\ldots\cdot x_n^{\sigma_n+r_n-r_n} \\
&= x_1^{k-r_1}\cdot\ldots\cdot x_n^{k-r_n}\cdot\sum_{\widetilde{\sigma}} g(\sigma_1+r_1,\dots,\sigma_n+r_n)\cdot x_1^{\sigma_1+r_1}\cdot\ldots\cdot x_n^{\sigma_n+r_n} \\
&= x_1^{k-r_1}\cdot\ldots\cdot x_n^{k-r_n}\widehat{g}(x_1,\dots,x_n).
\end{aligned}$$

Пусть T — пучок операторов, по которому ведётся разложение. По определению пучок T является базисным тогда и только тогда, когда найдётся такая функция $g(\widetilde{x})$, что система $\{\widehat{t^0 g(\widetilde{x})},\dots,\widehat{t^{k-1}g(\widetilde{x})}\}$ образует базис алгебры A.

Рассмотрим операторные образы $\widehat{t^{\widetilde{\sigma}}g(\widetilde{x})}$.

При $n=1$ имеем:

$$\begin{aligned}
&\widehat{eg(x)} = \widehat{p^0 g(x)} = \widehat{d^0 g(x)} = \widehat{g}(x), \\
&\widehat{p^a g(x)} = \widehat{g}(x+a) = x^{k-a}\cdot\widehat{g}(x), \\
&\widehat{d^a g(x)} = \widehat{g}(x) + \widehat{g}(x+a) = (1+x^{k-a})\cdot\widehat{g}(x).
\end{aligned}$$

В общем виде имеем: $\widehat{t^a g(x)} = (\alpha x^{k-a}+\beta)\cdot\widehat{g}(x)$, где α и β — введённые выше характеристики оператора t^a.

При $n>1$ получаем

$$t_1^{a_1}\dots t_n^{a_n}\widehat{g(x_1,\dots,x_n)} = (\alpha_n x_n^{k-a_n}+\beta_n)\cdot t_1\dots t_{n-1}\widehat{g(x_1,\dots,x_n)}$$

$$= (\alpha_1 x_1^{k-a_1} + \beta_1) \cdot \ldots \cdot (\alpha_n x_n^{k-a_n} + \beta_n) \cdot \widehat{g}(x_1, \ldots, x_n)$$
$$= \prod_{i=1}^{n} (\alpha_i x_i^{k-a_i} + \beta_i) \cdot \widehat{g}(x_1, \ldots, x_n).$$

Пусть $\widehat{h^{\widetilde{\sigma}}}(\widetilde{x}) = \prod\limits_{i=1}^{n} (\alpha_{i\sigma_i} x_i^{k-a_{i\sigma_i}} + \beta_{i\sigma_i})$, тогда $\widehat{t^{\widetilde{\sigma}} g(\widetilde{x})} = \widehat{h^{\widetilde{\sigma}}}(\widetilde{x}) \cdot \widehat{g}(\widetilde{x})$.

Пучок T будет базисным тогда и только тогда, когда всевозможные линейные комбинации $t^{\widetilde{\sigma}} g(\widetilde{x})$ (операторных образов функции $g(\widetilde{x})$ по пучку T) дают все элементы множества F_k^n, что возможно тогда и только тогда, когда система элементов $\widehat{t^{\widetilde{\sigma}} g(\widetilde{x})}$ образует базис алгебры A.

С другой стороны, все элементы алгебры A могут быть получены, если элементы $\widehat{h^{\widetilde{\sigma}}}(\widetilde{x})$ образуют базис A и элемент $\widehat{g}(\widetilde{x})$ не является делителем нуля, что равносильно тому, что $\widehat{g}(\widetilde{x})$ обратим.

Определим условия, при которых система $\{\widehat{h^{\widetilde{\sigma}}}(\widetilde{x})\}$ образует базис алгебры A. Рассмотрим матрицу перехода от этой системы к базису $x_1^0 \cdot \ldots \cdot x_n^0, \ldots, x_1^{k-1} \cdot \ldots \cdot x_n^{k-1}$:

$$\begin{pmatrix} \widehat{h^{\widetilde{0}}}(\widetilde{x}) \\ \vdots \\ \widehat{h^{\widetilde{k-1}}}(\widetilde{x}) \end{pmatrix} = \begin{pmatrix} (\alpha_{10} x_1^{k-a_{10}} + \beta_{10}) \cdot \ldots \cdot (\alpha_{n0} x_n^{k-a_{n0}} + \beta_{n0}) \\ \vdots \\ (\alpha_{1k-1} x_1^{k-a_{1k-1}} + \beta_{1k-1}) \cdot \ldots \cdot (\alpha_{nk-1} x_n^{k-a_{nk-1}} + \beta_{nk-1}) \end{pmatrix}$$
$$= MP \cdot \begin{pmatrix} x_1^0 \cdot \ldots \cdot x_n^0 \\ \vdots \\ x_1^{k-1} \cdot \ldots \cdot x_n^{k-1} \end{pmatrix},$$

где MP — матрица перехода, состоящая из элементов вида

$$(\alpha_{1\sigma_1} x_1^{k-a_{1\sigma_1}} + \beta_{1\sigma_1}) \cdot \ldots \cdot (\alpha_{n\sigma_n} x_n^{k-a_{n\sigma_n}} + \beta_{n\sigma_n})$$
$$= \sum_{\tau_1, \ldots, \tau_n} (\alpha_{1\sigma_1})^{i(\tau_1)} \cdot \ldots \cdot (\alpha_{n\sigma_n})^{i(\tau_n)} \cdot (\beta_{1\sigma_1})^{i(\tau_1)\oplus 1} \cdot \ldots \cdot (\beta_{n\sigma_n})^{i(\tau_n)\oplus 1} \cdot$$
$$\cdot (k - a_{1\sigma_1})^{[\tau_1]} \cdot \ldots \cdot (k - a_{n\sigma_n})^{[\tau_n]} \cdot x_1^{\tau_1} \cdot \ldots \cdot x_n^{\tau_n}.$$

Таким образом, $MP = M_T$. Следовательно, система $\{\widehat{h^{\widetilde{\sigma}}}(\widetilde{x})\}$ образует базис алгебры A тогда и только тогда, когда $\det M_T \neq 0$.

Для описания обратимых элементов алгебры A сделаем линейную подстановку $x_i = y_i + 1$. Так как $(y+1)^k = 1 + y^k$, то получаем, что в новом базисе алгебра A будет иметь вид $A \simeq F_k[y_1, \ldots, y_n]/(y_1^k, \ldots, y_n^k)$ и

$$\widehat{f}(\widetilde{y}) \in A : \widehat{f}(\widetilde{y}) = \sum_{\widetilde{\sigma}} c_{\widetilde{\sigma}} \cdot y_1^{\sigma_1} \cdot \ldots \cdot y_n^{\sigma_n}.$$

Так как каждый элемент x_i переходит в $y_i + 1$, 1 переходит в 1, а всевозможные произведения элементов $x_1^{r_1} \cdot \ldots \cdot x_n^{r_n}$ перейдут в $(y_1 + 1)^{r_1} \cdot \ldots \cdot (y_n + 1)^{r_n}$, то каждый новый базисный элемент будет содержать единицу, и матрица перехода от базиса x_i к базису y_i будет иметь вид

$$MPP = \begin{pmatrix} 1 & \ldots & \ldots & \ldots \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \ldots & \ldots & \ldots \end{pmatrix}$$

(в первом столбце стоят только единицы). Тогда коэффициенты в новом базисе вычисляются по формуле

$$\left(c_{\widetilde{0}}, \ldots, c_{\widetilde{k-1}}\right) = \left(g(\widetilde{0}), \ldots, g(\widetilde{k-1})\right) \cdot MPP.$$

Следовательно, $c_{\widetilde{0}} = \sum\limits_{\widetilde{\sigma}} g(\widetilde{\sigma})$.

Рассмотрим случаи:

а) $c_{\widetilde{0}} = 0$. Тогда $y_1^{k-1} \cdot \ldots \cdot y_n^{k-1} \cdot \widehat{g}(\widetilde{y}) = y_1^{k-1} \cdot \ldots \cdot y_n^{k-1} \cdot \sum\limits_{\widetilde{\sigma}} c_{\widetilde{\sigma}} \cdot y_1^{\sigma_1} \cdot \ldots \cdot y_n^{\sigma_n} = \sum\limits_{\widetilde{\sigma}} c_{\widetilde{\sigma}} \cdot y_1^{\sigma_1 + k-1} \cdot \ldots \cdot y_n^{\sigma_n + k-1} = c_{\widetilde{0}} \cdot y_1^{k-1} \cdot \ldots \cdot y_n^{k-1} = 0$.

б) $c_{\widetilde{0}} \neq 0$. Для любого ненулевого многочлена $\widehat{f}(\widetilde{y})$ из алгебры A вида $\widehat{f}(\widetilde{y}) = \sum\limits_{\widetilde{\sigma}} c^*_{\widetilde{\sigma}} \cdot y_1^{\sigma_1} \cdot \ldots \cdot y_n^{\sigma_n}$ выберем ненулевой моном $c^*_{\widetilde{\tau}} \cdot y_1^{\tau_1} \cdot \ldots \cdot y_n^{\tau_n}$ минимально возможной степени $\tau_1 + \ldots + \tau_n$. Тогда коэффициент при $y_1^{\tau_1} \cdot \ldots \cdot y_n^{\tau_n}$ в $\widehat{f}(\widetilde{y}) \cdot \widehat{g}(\widetilde{y})$ будет равен $c_{\widetilde{0}} \cdot c^*_{\widetilde{\tau}}$, т. е. $\widehat{f}(\widetilde{y}) \cdot \widehat{g}(\widetilde{y}) \neq 0$. Следовательно, $\widehat{g}(\widetilde{y})$ не является делителем нуля. Таким образом, показано, что $\widehat{g}(\widetilde{y})$ обратим тогда и только тогда, когда $c_{\widetilde{0}} \neq 0$, что эквивалентно тому, что функция $g(\widetilde{y})$ невырожденна. Теорема 2 доказана.

Замечание 1. При вычислении элементов матрицы пучка M_T при $k = 2$ множитель $(k - a_{1\sigma_1})^{[\tau_1]} \cdot \ldots \cdot (k - a_{n\sigma_n})^{[\tau_n]}$ можно опускать в силу полилинейности всех булевых функций.

Теорема 3. *Пусть T — класс операторов и $G = \{g_{\widetilde{0}}, ..., g_{\widetilde{k-1}}\}$ — базис пространства всех n-местных функций k-значной логики, $k > 2$. Тогда для любой функции $f(\widetilde{x})$ и любого $t \in T$ существует единственное полиномиальное представление*

$$P_t : f(\widetilde{x}) = \sum_{\widetilde{\sigma} \in E_k^n} c_{\widetilde{\sigma}}^{(\widetilde{a})} t g_{\widetilde{\sigma}}(\widetilde{x}), \tag{1}$$

где $\widetilde{a}$ является показателем оператора t, а $c_{\widetilde{\sigma}}^{(\widetilde{a})} \in E_k$.

Доказательство. Для любого оператора $t = t_1^{a_1} \dots t_n^{a_n}$ существует обратный к нему оператор $(t)^{-1} : (t)^{-1}(tf) = f$, $(t)^{-1} = (t_1^{a_1})^{-1} \dots (t_n^{a_n})^{-1}$, где $(e^a)^{-1} = e^a$, $(p^0)^{-1} = p^0$, $(d^0)^{-1} = d^0$ и если $a \neq 0$, то $(p^a)^{-1} = p^{k-a}$, $(d^a)^{-1} = ((k+1)/2) \cdot (d^a)^{k-1}$.

Рассмотрим функцию $h(x_1, \dots, x_n) = t^{-1} f(x_1, \dots, x_n)$. Так как G — базис, то каждая функция единственным образом представима в виде линейной комбинацией базисных функций. Пусть

$$h(x_1, \dots, x_n) = \sum_{\widetilde{\sigma} \in E_k^n} c_{\widetilde{\sigma}} g_{\widetilde{\sigma}}(\widetilde{x}).$$

Тогда $f(x_1, \dots, x_n) = th(x_1, \dots, x_n) = \sum\limits_{\widetilde{\sigma} \in E_k^n} c_{\widetilde{\sigma}} t g_{\widetilde{\sigma}}(\widetilde{x})$. Теорема 3 доказана.

Замечание 2. При $k = 2$ теорема 3 справедлива, если в основании операторов встречаются только p и e.

3. Некоторые оценки сложности полиномиальных представлений

Пусть $P_t(f)$ — полином, представляющий функцию f. Сложностью $L(P_t(f))$ полинома $P_t(f)$ будем называть число слагаемых в нём. Число $LK(f) = \min\limits_{P_t(f) \in K} L(P_t(f))$ назовём сложностью функции f в классе полиномов K. Сложностью класса функций S в классе полиномов K назовём число $LK(S) = \max\limits_{f \in S} LK(f)$.

Если $S = F_k^n$, то используем обозначение $LK(n)$.

Ниже будем рассматривать два класса полиномов: $K = K_T^G$ — линейные комбинации образов функций из базиса G по операторам из T и $K = K_T^g$ — линейные комбинации образов невырожденной функции g по пучку из класса T.

Среди всевозможных базисов выделим два:

$$G_1 = \{x_1^0 \cdot \dots \cdot x_n^0, \dots, x_1^{k-1} \cdot \dots \cdot x_n^{k-1}\} \text{ и}$$

$$G_2 = \{p^{i_1} \dots p^{i_n} g(x_1, \dots, x_n) | (i_1, \dots, i_n) \in E_k^n\},$$

где g — невырожденная функция. Первый базис состоит из произведений степеней переменных, второй — из сдвигов функции g.

Разложения по операторам из класса P и базису G_1 позволяют получить представления, называемые *поляризованными* полиномами. Для булевых функций в [3] были получены точные оценки сложности поляризованных полиномов Жегалкина (форм Рида-Маллера):

$$LK_P^{G_1}(n) = \left\lfloor \frac{2}{3} 2^n \right\rfloor,$$

а в [4, 5] оценки сложности функции Шеннона для поляризованных полиномов при $k \geqslant 3$ имеют вид

$$(k-1)^n \leqslant LK_P^{G_1}(n) < \frac{k(k-1)}{k(k-1)+1}k^n.$$

Для класса D и базиса G_1 по аналогии с [3, 4] можно получить верхнюю оценку.

Теорема 4. *При любом* $n \geqslant 1$

$$LK_D^{G_1}(n) \leqslant \frac{k(k-1)}{k(k-1)+1}k^n - \frac{(k-1)^{n+1}}{k^{n-1}(k^2-k+1)}, \quad k \geqslant 3.$$

Доказательство. Сначала заметим, что для любого произведения вида $x_1^{\beta_1} \cdot ... \cdot x_n^{\beta_n} x_{n+1}^{\beta_{n+1}}$ и оператора $t_{n+1} = d^{\alpha_1}...d^{\alpha_n}d^{\alpha_{n+1}}$ справедливо равенство

$$t_{n+1}(x_1^{\beta_1} \cdot ... \cdot x_n^{\beta_n} x_{n+1}^{\beta_{n+1}}) = d^{\alpha_1}...d^{\alpha_n}(x_1^{\beta_1} \cdot ... \cdot x_n^{\beta_n}) \cdot d^{\alpha_{n+1}}(x_{n+1}^{\beta_{n+1}})$$

Кроме того, если при $i \neq 0$ для функции $f(x_1, ..., x_{n-1}, x_n)$ имеется 2 полиномиальных представления

$$\begin{aligned} f(x_1, ..., x_{n-1}, x_n) &= A(x_1, ..., x_{n-1})d^0(x_n^{k-1}) + B(x_1, ..., x_{n-1})d^0(x_n^{k-2}) \\ &+ C(x_1, ..., x_{n-1})d^0(x_n^{k-3}) + ... + D(x_1, ..., x_{n-1})d^0(x_n^0) \\ \text{и } f(x_1, ..., x_{n-1}, x_n) &= A_i(x_1, ..., x_{n-1})d^i(x_n^{k-1}) + B_i(x_1, ..., x_{n-1})d^i(x_n^{k-2}) \\ &+ C_i(x_1, ..., x_{n-1})d^i(x_n^{k-3}) + ... + D_i(x_1, ..., x_{n-1})d^i(x_n^0), \end{aligned}$$

то $A_i = 2^{-1}A, B_i = 2^{-1}B + i2^{-2}A$.

Доказательство утверждения теоремы проведём индукцией по n. Идеи индуктивного перехода взяты из [3, 4].

При $n = 1$ имеем

$$\frac{k(k-1)}{k(k-1)+1}k^1 - \frac{(k-1)^{1+1}}{k^{1-1}(k^2-k+1)} = k-1 \leqslant k-1,$$

так как среди чисел $A, B, 2^{-1}B + i2^{-2}A$ $(i = 1, ..., k-1)$ обязательно встретится 0.

Пусть

$$\begin{aligned} f(x_1, ..., x_n, x_{n+1}) &= A(x_1, ..., x_n)x_{n+1}^{k-1} + B(x_1, ..., x_n)x_{n+1}^{k-2} \\ &+ C(x_1, ..., x_n)x_{n+1}^{k-3} + ... + D(x_1, ..., x_n)x_{n+1}^0. \end{aligned}$$

По индуктивному предположению для функции $A(x_1,..,x_n)$ существует оператор $t_n = d^{i_1}...d^{i_n}$ такой, что $L(P_t(A)) \leqslant LK_D^{G_1}(n-1)$.

Пусть $P_{t_n}(A), P_{t_n}(B)$ — полиномы, представляющие функции A и B соответственно. Каждое слагаемое в этих полиномах является произведением монома $t_n(x_1^{\alpha_1} \cdot ... \cdot x_n^{\alpha_n})$ на некоторый коэффициент $a_{\alpha_1...\alpha_n} \in E_k$.

Множество всех мономов из $P_{t_n}(A)$ разделим на k частей. Для удобства части занумеруем числами 0, 1, ..., $k-1$.

В нулевую часть занесём мономы, которые не встречаются среди слагаемых в $P_t(B)$, в первую — такие мономы, отношение коэффициентов перед которыми в $P_t(B)$ и $P_t(A)$ равно $(k-1)2^{-1}$, во вторую — такие мономы, отношение коэффициентов перед которыми в $P_t(B)$ и $P_t(A)$ равно $(k-2)2^{-1}$, и т. д., в $(k-1)$-ю — такие мономы, отношение коэффициентов перед которыми в $P_t(B)$ и $P_t(A)$ равно 2^{-1}.

Очевидно, что из всех k частей можно выбрать $k-1$ частей таких, что общее число мономов не превосходит $\frac{k-1}{k} LK_D^{G_1}(n-1)$. Пусть i — номер отсутствующей части. В ней содержится не менее $\frac{1}{k} LK_D^{G_1}(n)$ мономов.

Возьмём оператор $t_{n+1} = d^{i_1}...d^{i_n}d^i$. Пусть

$$P_{t_{n+1}}(f) = A_i d^i(x_{n+1}^{k-1})_i + B_i d^i(x_{n+1}^{k-2}) + C_i d^i(x_{n+1}^{k-3}) + ...$$

Тогда $A_i = P_{t_n}(A)$, $B_i = 2^{-1}(i2^{-1}P_{t_n}(A) + P_{t_n}(B)$ и сумма длин A_i и B_i не превосходит

$$LK_D^{G_1}(n-1) + (k^n - \frac{1}{k} LK_D^{G_1}(n-1)).$$

С учётом того, что длина оставшейся части в $P_{t_{n+1}}(f)$ не превосходит $(k-2)k^n$, получаем нужный результат. Теорема 4 доказана.

В следующей теореме содержится нижняя оценка.

Теорема 5. *При любом $n \geqslant 1$ справедливо неравенство*

$$LK_D^{G_1}(n) \geqslant (\frac{k+1}{2})^n, \quad k \geqslant 3.$$

Доказательство. Рассмотрим функцию $f(x) = x^{k-1} + x^{k-3} + ... + x^2 + 1$ и покажем, что её сложность равна $(k+1)/2$. Пусть для разностного оператора d^a разложение (1) имеет вид

$$d^a : f(x) = \sum_{i=0}^{k-1} c_i^{(a)} d^a x^i. \qquad (2)$$

При $a = 0$ среди коэффициентов разложения содержится $(k+1)/2$ ненулевых элементов, так как $d^0(f(x)) = f(x)$. Покажем, что в остальных разложениях число ненулевых коэффициентов не меньше $(k+1)/2$.

Применив к левой и правой части (2) $(d^a)^{k-1}$, получаем

$$(d^a)^{k-1}(f(x)) = (d^a)^{k-1}\left(\sum_{i=0}^{k-1} c_i^{(a)} d^a x^i\right) = \sum_{i=0}^{k-1} c_i^{(a)} (d^a)^k x^i = \sum_{i=0}^{k-1} 2c_i^{(a)} x^i.$$

Покажем, что в левой части коэффициенты при чётных степенях x отличны от 0. Действительно,

$$\begin{aligned}(d^a)^{k-1}(x)^t &= \sum_{j=0}^{k-1} \binom{k-1}{j} (x+aj)^t \\ &= \sum_{j=0}^{k-1} \binom{k-1}{j} \sum_{p=0}^{t} \binom{t}{p} x^p (ja)^{t-p} = \sum_{p=0}^{t} \binom{t}{p} a^{t-p} x^p \sum_{j=0}^{k-1} \binom{k-1}{j} j^{t-p}.\end{aligned}$$

При $p = t$ справа остается x^t, а при чётном p, отличном от t, имеем

$$\begin{aligned}\sum_{j=0}^{k-1} \binom{k-1}{j} j^{(t-p)} &= \binom{k-1}{0} 0^{(t-p)} + \sum_{j=1}^{\frac{k-1}{2}} \binom{k-1}{j} j^{(t-p)} \\ &+ \sum_{j=1}^{\frac{k-1}{2}} \binom{k-1}{k-j} (k-j)^{(t-p)} = \sum_{j=0}^{\frac{k-1}{2}} \left(\binom{k-1}{j} + \binom{k-1}{k-j}\right) j^{(t-p)} \\ &= \sum_{j=1}^{\frac{k-1}{2}} \binom{k}{j} j^{(t-p)} = 0.\end{aligned}$$

Таким образом, мы показали, что в остальных разложениях число ненулевых коэффициентов не меньше $(k+1)/2$. Поэтому $LK_D^{G_1}(1) \geqslant (k+1)/2$.

Для получения функции от n переменных сложности $((k+1)/2)^n$ достаточно рассмотреть функцию $g(\widetilde{x}) = f(x_1)f(x_2)\dots f(x_n)$, где $f(x)$ — функция, построенная при доказательстве теоремы в случае $n = 1$. Теорема 5 доказана.

В следующей теореме приводится точная оценка функции Шеннона для полиномиальных форм (1) по оператору из класса O и системе G_2.

Теорема 6. *При любом* $n \geqslant 1$

$$LK_O^{G_2}(n) = k^n, \quad k \geqslant 3.$$

Доказательство. Полином из $K_O^{G_2}$, представляющий функцию $f(\widetilde{x})$, имеет вид

$$f(\widetilde{x}) = \sum_{i=0}^{k^n-1} c_i^{(\widetilde{a})} t g_i(\widetilde{x}), \tag{3}$$

где $\widetilde{a}$ — показатель оператора t и $g_i \in G_2$, $c_i^{(\widetilde{a})} \in E_k$.

Рассмотрим случай $n = 1$, тогда $g_i(x) = p^i g(x) = g(x + i)$.

(а) При $t = p^a$ равенство (3) принимает вид

$$f(x) = \sum_{i=0}^{k-1} c_i^{(a)} p^a g(x+i) = \sum_{i=0}^{k-1} c_i^{(a)} g(x+i+a) = \sum_{i=0}^{k-1} c_{k+i-a}^{(0)} g(x+i).$$

Таким образом, рассмотрев полином по оператору t^0, в котором $c_i^{(0)} \neq 0$ при любом $i \in \{0, ..., k-1\}$, получаем сложность, равную k.

(б) При $t = d^a$ равенство (3) принимает вид

$$f(x) = \sum_{i=0}^{k-1} c_i^{(a)} d^a g(x+i) = \sum_{i=0}^{k-1} c_i^{(a)} (g(x+i) + g(x+i+a)) = \sum_{i=0}^{k-1} (c_i^{(a)} + c_{i-a}^{(a)}) g(x+i).$$

Рассмотрим функцию $f(x) = c_{k-1}^{(0)} x^{k-1} + x^{k-2} + \ldots + x + 1$. Найдем $c_{k-1}^{(0)}$ такой, что $c_i^{(a)} \neq 0$ для любых $a, i \in E_k$.

Имеем $c_i^{(0)} = c_i^{(a)} + c_{i-a}^{(a)}$, т. е.

$$\left(c_{k-1}^{(0)}, \ldots, c_0^{(0)}\right) = M_a \cdot \begin{pmatrix} c_{k-1}^{(a)} \\ \vdots \\ c_0^{(a)} \end{pmatrix},$$

где $M_a = \{m_{ij}^{(a)}\}$ — квадратная матрица порядка k, в которой

$$m_{ij}^{(a)} = \begin{cases} 1 & \text{при } i = j \text{ или } i = j - a; \\ 0 & \text{в остальных случаях.} \end{cases}$$

Для нахождения коэффициентов $(c_{k-1}^{(a)}, \ldots, c_0^{(a)})$ построим матрицу M_a^{-1}, обратную к матрице M_a.

Введём обозначения: $u = \frac{k+1}{2}, v = \frac{k-1}{2}$.

Так как в j-й строке матрицы M_a в позициях j и $j+a$ находятся единицы, то в j-м столбце матрицы M_a^{-1} в позициях j и $j+a$ находится элемент u. Все остальные строки матрицы M_a при умножении на j-й столбец матрицы M_a^{-1} должны давать 0, т. е. при $i \neq j$ в i-й и $(i+a)$-й позициях находятся u и v. Таким образом, в каждом столбце матрицы M_a^{-1} имеется u вхождений элемента u и v вхождений элемента v. Тогда

$$c_i^{(a)} = \begin{cases} vc_{k-1}^{(0)} + 2u, & \text{если в первой позиции } i\text{-й строки матрицы} \\ & M_a^{-1} \text{ находится } v; \\ uc_{k-1}^{(0)}, & \text{если в первой позиции } i\text{-й строке матрицы} \\ & M_a^{-1} \text{ находится } u. \end{cases}$$

Отсюда следует, что $c_i^{(a)} \neq 0$ тогда и только тогда, когда

$$\begin{cases} vc_{k-1}^{(0)} + 2u \neq 0, \\ uc_{k-1}^{(0)} \neq 0; \end{cases} \quad \text{или} \quad \begin{cases} c_{k-1}^{(0)} \neq 2, \\ c_{k-1}^{(0)} \neq 0. \end{cases}$$

Таким образом, построена функция одной переменной сложности k.

Используя произведение функций одной переменной, построенных в пунктах (а) и (б), получаем точное значение сложности $LK_O^{G_2}(n)$ при $n > 1$. Теорема 6 доказана.

По определению сложность функции f в классе базисных пучков B зависит от выбора функции g. Интересен вопрос о соотношении сложностей класса всех функций k-значной логики в полиномах по разным функциям. Ответ на него дает теорема 7, но сначала докажем следующее утверждение.

Лемма. *Для любого базисного пучка операторов T и любого оператора s найдутся $c_{\widetilde{0}}, \ldots, c_{\widetilde{k-1}} \in E_k$ такие, что для любой функции $f(\widetilde{x})$ имеет место разложение $sf(\widetilde{x}) = \sum\limits_{\widetilde{\sigma} \in E_k^n} c_{\widetilde{\sigma}} t^{\widetilde{\sigma}} f(\widetilde{x})$.*

Доказательство. Будем использовать обозначения из теоремы 2. Если оператор $s = s_1^{a_1} \ldots s_n^{a_n}$, то $\widehat{sf}(\widetilde{x}) = \prod\limits_{i=1}^{n} (\alpha_i x_i^{a_i} + \beta_i) \widehat{f}(\widetilde{x})$. Рассмотрим правую часть равенства:

$$\left(c_{\widetilde{0}}, \quad \ldots, \quad c_{\widetilde{k-1}}\right) \cdot \begin{pmatrix} \widehat{t^{\widetilde{0}} f(\widetilde{x})} \\ \vdots \\ \widehat{t^{\widetilde{k-1}} f(\widetilde{x})} \end{pmatrix} = \left(c_{\widetilde{0}}, \quad \ldots, \quad c_{\widetilde{k-1}}\right) \cdot \begin{pmatrix} \widehat{h^{\widetilde{0}}} \cdot \widehat{f}(\widetilde{x}) \\ \vdots \\ \widehat{h^{\widetilde{k-1}}} \cdot \widehat{f}(\widetilde{x}) \end{pmatrix}$$

$$= \left(c_{\widetilde{0}}, \quad \ldots, \quad c_{\widetilde{k-1}}\right) \cdot M_T \cdot \begin{pmatrix} x_1^0 \cdot \ldots \cdot x_n^0 \\ \vdots \\ x_1^{k-1} \cdot \ldots \cdot x_n^{k-1} \end{pmatrix} \cdot \widehat{f}(\widetilde{x}).$$

Приравняв правую и левую части, получаем

$$\prod_{i=1}^{n}(\alpha_i x_i^{a_i} + \beta_i)\widehat{f}(\widetilde{x}) = \left(c_{\widetilde{0}}, \quad \ldots, \quad c_{\widetilde{k-1}}\right) \cdot M_T \cdot \begin{pmatrix} x_1^0 \cdot \ldots \cdot x_n^0 \\ \vdots \\ x_1^{k-1} \cdot \ldots \cdot x_n^{k-1} \end{pmatrix} \cdot \widehat{f}(\widetilde{x}).$$

Если $\widehat{f}(\widetilde{x}) = 0$, то равенство выполняется при любых значениях $c_{\widetilde{\sigma}}$. В противном случае уравнение имеет единственное решение, так как M_T невырожденная, а $(x_1^0 \cdot \ldots \cdot x_n^0, \ldots, x_1^{k-1} \cdot \ldots \cdot x_n^{k-1})$ является базисом. Лемма доказана.

Теорема 7. *Для любого класса B базисных пучков операторов значение функции Шеннона $LK_B^g(n)$ не зависит от выбора функции $g(\widetilde{x})$.*

Доказательство. Рассмотрим базисный пучок T операторов и две невырожденных функции $g_1(x_1, ..., x_n)$ и $g_2(x_1, ..., x_n)$. Операторные образы этих функций ($\{t^{\widetilde{0}} g_1(\widetilde{x}), \ldots, t^{\widetilde{k-1}} g_1(\widetilde{x})\}$ и $\{t^{\widetilde{0}} g_2(\widetilde{x}), \ldots, t^{\widetilde{k-1}} g_2(\widetilde{x})\}$) являются базисами линейного пространства всех функций k-значной логики от n переменных. Поэтому найдется такое единственное линейное преобразование φ, переводящее один базис в другой, что $\varphi(t^{\widetilde{\sigma}} g_1) = t^{\widetilde{\sigma}} g_2$.

По лемме существуют $c_{\widetilde{0}}, \ldots, c_{\widetilde{k-1}} \in E_k$ такие, что имеет место разложение

$$sf(\widetilde{x}) = \sum_{\widetilde{\sigma} \in E_k^n} c_{\widetilde{\sigma}} t^{\widetilde{\sigma}} f(\widetilde{x}).$$

Тогда

$$\varphi(sg_1(\widetilde{x})) = \varphi\left(\sum_{\widetilde{\sigma} \in E_k^n} c_{\widetilde{\sigma}} t^{\widetilde{\sigma}} g_1(\widetilde{x})\right) = \sum_{\widetilde{\sigma} \in E_k^n} \varphi(c_{\widetilde{\sigma}} t^{\widetilde{\sigma}} g_1(\widetilde{x}))$$
$$= \sum_{\widetilde{\sigma} \in E_k^n} c_{\widetilde{\sigma}} \varphi(t^{\widetilde{\sigma}} g_1(\widetilde{x})) = \sum_{\widetilde{\sigma} \in E_k^n} c_{\widetilde{\sigma}} t^{\widetilde{\sigma}} g_2(\widetilde{x}) = sg_2(\widetilde{x}).$$

Рассмотрим произвольную функцию $f(\widetilde{x})$. Для любого пучка $T \in B$ имеем

$$\varphi(f(\widetilde{x})) = \varphi\left(\sum_{\widetilde{\sigma} \in E_k^n} c_{\widetilde{\sigma}} t^{\widetilde{\sigma}} g_1(\widetilde{x})\right) = \sum_{\widetilde{\sigma} \in E_k^n} c_{\widetilde{\sigma}} \varphi(t^{\widetilde{\sigma}} g_1(\widetilde{x})) = \sum_{\widetilde{\sigma} \in E_k^n} c_{\widetilde{\sigma}} t^{\widetilde{\sigma}} g_2(\widetilde{x}).$$

Поэтому сложности полиномов, порождённых пучком по функции $g_1(\widetilde{x})$ для $f(\widetilde{x})$ и этим же пучком по функции $g_2(\widetilde{x})$ для $\varphi(f(\widetilde{x}))$, совпадают, т. е.

$$LK_B^{g_1}(f) = LK_B^{g_2}(\varphi(f)).$$

Так как преобразование φ невырожденное, то $\varphi(F_k^n) = F_k^n$. Следовательно, $LK_B^{g_1}(n) = LK_B^{g_2}(n)$. Теорема 7 доказана.

ЛИТЕРАТУРА

1. Избранные вопросы теории булевых функций. Под редакцией Винокурова С. Ф., Перязева Н. А. М.: Физматлит, 2001.

2. Пантелеев В. И. Полиномиальные разложения k-значных функций по невырожденным функциям // Математические заметки. 1994. Т. 55, вып. 1. С. 144–149.

3. Перязев Н. А. Сложность булевых функций в классе полиномиальных поляризованных форм // Алгебра и логика. 1995. Т. 34, № 3. С. 323–326.

4. Селезнева С. Н. О сложности представления функций многозначных логик поляризованными полиномами // Дискретная математика. 2002. Т. 14, вып. 2. С. 48–53.

5. Селезнева С. Н. О сложности поляризованных полиномов функций многозначных логик, зависящих от одной переменной // Дискретная математика. 2004. Т. 16, вып. 2. С. 117–120.

Адреса авторов:

Зинченко А. С.

Иркутский гос. пед. ун-т,
факультет математики, физики
и информатики,
ул. Н. Набережная, 6,
664003, Иркутск, Россия.
E-mail: azinchenko@mail.com

Пантелеев В. И. А. С.

Иркутский гос. ун-т,
Институт математики и экономики,
ул. К. Маркса, 1,
664000, Иркутск, Россия.
E-mail: vp@math.isu.ru

Статья поступила
12 октября 2005 г.