УДК 519.7

А. Н. Алексейчук, О. Н. Кулинич, В. В. Сокур, С. Н. Конюшок

ОЦЕНКИ СЛОЖНОСТИ И АЛГОРИТМЫ МИНИМИЗАЦИИ БУЛЕВЫХ ФУНКЦИЙ В КЛАССЕ КАНОНИЧЕСКИХ ПОЛЯРИЗОВАННЫХ ПОЛИНОМОВ

Канонические поляризованные полиномы (КПП) образуют специальный класс полиномиальных форм, интерес к исследованию которых обусловлен как традиционными задачами анализа сложности и классификации булевых функций (БФ) [1 – 4], так и вопросами, связанными с их реализацией на основе современных интегральных микросхем (программируемых логических матриц (ПЛМ) типа “и-исключающее или” [5]). Известно [1], что основу логического проектирования стандартных ПЛМ составляют традиционные алгоритмы минимизации дизъюнктивных нормальных форм (ДНФ) булевых функций. С другой стороны, многие функции, имеющие большую сложность в классе ДНФ, могут быть достаточно просто представлены в полиномиальном виде. Поэтому ПЛМ, содержащие в своем составе логические элементы “сложение по модулю 2”, в ряде случаев обладают определенными преимуществами [5].

Постоению алгоритмов минимизации и анализу сложности БФ в классе КПП посвящены работы [5 – 9] и другие. В настоящей статье получены новые границы функции Шеннона для сложности представления каноническими поляризованными полиномами n-местных БФ, имеющих степень нелинейности не более r. Указанные границы уточняют результаты [6, 7] и могут быть непосредственно использованы при оценке сложности БФ, принадлежащих некоторым другим классам. Предложен рекурсивный алгоритм вычисления коэффициентов всех КПП булевой функции f по вектору T_f ее значений, вычислительная сложность которого совпадает со сложностью алгоритма, описанного в [8]. На основе результатов [9] получена нижняя оценка сложности оптимальной схемы вычисления КПП произвольной БФ f, заданной вектором значений T_f.

Основные понятия и некоторые вспомогательные результаты.

Введем обозначения: V_n – пространство двоичных векторов длины n; F_n– множество булевых функций n переменных; $N_n = \{1, 2, \ldots, n\}$. Для любого вектора $\alpha = (\alpha_1, \ldots, \alpha_n) \in V_n$ обозначим $A_\alpha = \{i \in N_n: \alpha_i = 1\}$, $\overline{\alpha} = (\overline{\alpha_1}, \ldots, \overline{\alpha_n})$, $\|\alpha\| = \alpha_1 + \ldots + \alpha_n$. Запись $\alpha \le \beta$, где $\alpha, \beta \in V_n$ означает, что $\alpha_i \le \beta_i$ для всех $i \in N_n$.

Для любого $i \in N_n$ компоненты f^{x_i}, $f^{\overline{x_i}}$ и частная производная $\dfrac{df}{d\,x_i}$ БФ $f \in F_n$ по переменной x_i определяются соответственно равенствами [10]

$$f^{x_i} = f(x_1, \ldots, x_{i-1}, 1, x_{i+1}, \ldots, x_n),\ f^{\overline{x_i}} = f(x_1, \ldots, x_{i-1}, 0, x_{i+1}, \ldots, x_n),$$

$$\frac{df}{d\,x_i} = f^{x_i} \oplus f^{\overline{x_i}}.$$

Последнее соотношение индуктивно распространяется на произвольное подмножество переменных $x_1, \ldots, x_n$. А именно, для любого вектора $\alpha \in V_n$ полагаем $\frac{df}{d\alpha} = \frac{df}{dx_{i_1}}\left(\frac{df}{dx_{i_2}}\left(\ldots\frac{df}{dx_{i_k}}\right)\ldots\right)$, где $\{i_1, i_2, \ldots, i_k\} = A_\alpha$. Имеет место равенство [10]

$$\frac{df}{d\alpha}(x) = \sum_{c \in V_n:\ c \oplus x \le \alpha} \oplus\ f(c),\ x \in V_n. \qquad (1)$$

Непосредственно из (1) следует, что функция $\frac{df}{d\alpha}$ постоянна на смежных классах пространства V_n по подпространству $\{c \in V_n: c \le \alpha\}$ (не зависит от переменных с номерами из множества A_α).

Рассмотрим для каждого фиксированного $\sigma \in V_n$ систему БФ

$$(x_\alpha^{\overline{\sigma}} : \alpha \in V_n), \qquad (2)$$

где $x_\alpha^{\overline{\sigma}} = \prod_{i \in A_\alpha} x_i^{\overline{\sigma i}}$, $x_i^{\overline{\sigma i}} = \overline{x_i}$, если $\sigma_i = 1$; $x_i^{\overline{\sigma i}} = x_i$ – в противном случае, $i \in \overline{1, n}$.

Полиномиальное разложение вида

$$f(x) = \sum_{\alpha \in V_n} \oplus\ p_{\alpha,\sigma}\, x_\alpha^{\overline{\sigma}} \qquad (3)$$

называется *каноническим полиномом, поляризованным по вектору* $\sigma \in V_n$ (или *обобщенной формой Рида-Мюллера*) БФ $f = f(x_1, \ldots, x_n)$ [5, 6].

Используемые ниже свойства КПП булевых функций собраны в следующей теореме, вытекающей из ряда результатов, приведенных в [10].

Теорема 1 [10]**.** Справедливы следующие утверждения:

а) для любого $\sigma \in V_n$ система (2) является базисом векторного пространства F_n; в частности, для любой БФ $f \in F_n$ коэффициенты $p_{\alpha,\sigma}$, $\alpha, \sigma \in V_n$ разложения (3) однозначно определяются функцией f и совпадают с коэффициентами $p_\alpha^{f_\sigma}$, $\alpha, \sigma \in V_n$ полинома Жегалкина БФ $f_\sigma(x) = f(x \oplus \sigma)$, $x \in V_n$;

б) для любых $\alpha, \sigma \in V_n$ имеют место равенства

$$p_{\alpha,\sigma} = \frac{df}{d\alpha}(\sigma) \equiv \left\| f_\sigma^{\overline{\alpha}} \right\| (\mathrm{mod}\ 2), \qquad (4)$$

где $f_\sigma^{\overline{\alpha}}$ – подфункция БФ f, получаемая путем фиксации переменных с номерами из множества A_α^- соответствующими значениями координат вектора σ.

Обозначим $l_f(\sigma)$ вес вектора $(p_\alpha^{f_\sigma} : \alpha \in V_n)$, равный числу ненулевых слагаемых в выражении (3) поляризованного по вектору σ канонического полинома БФ f. Число $l_f(\sigma)$ называется *длиной* булевой функции f_σ. *Сложность* $l(f)$ БФ f в классе канонических поляризованных полиномов определяется равенством

$$l(f) = \min\{l_f(\sigma): \sigma \in V_n\}. \quad (5)$$

Для любого класса K булевых функций обозначим

$$L_K(n) = \max\{l(f): f \in K \cap F_n\} \quad (6)$$

функцию Шеннона [6] для оценки сложности представления n-местных БФ из класса K каноническими поляризованными полиномами.

К числу основных задач исследования сложности БФ в классе КПП относятся задачи

1) разрабоки эффективных алгоритмов вычисления коэффициентов $p_{\alpha,\sigma}$, α, $\sigma \in V_n$ всех 2^n канонических поляризованных полиномов БФ f, а также алгоритмов построения оптимальных (имеющих наименьшее число ненулевых слагаемых) КПП вида (3) функций $f \in F_n$;

2) нахождения нетривиальных границ значений $l(f)$, $L_K(n)$ для булевых функций f, принадлежащих различным классам K.

Для криптографических приложений представляет определенный интерес исследование полиномиальных форм вида (3), реализующих функции, описываемые в терминах ограничений на коэффициенты Уолша, степень нелинейности, значения весов частных производных данной БФ и т.д. Примерами могут служить классы максимально нелинейных функций, функций, свободных от корреляций [3], удовлетворяющих критерию распространения [2] и некоторые другие классы БФ.

Построение эффективных алгоритмов минимизации или оценок сложности булевых функций в классе КПП предполагает проведение предварительного исследования спектров длин $l_f(\sigma)$, $\sigma \in V_n$ канонических поляризованных полиномов функций $f \in F_n$. На конкретных примерах БФ нетрудно убедиться в том, что в общем случае длины полиномов (3), реализующих данную булеву функцию, могут существенно отличаться друг от друга. С другой стороны, ясно, что числа $l_f(\sigma)$, $\sigma \in V_n$ не могут принимать произвольные натуральные значения (в интервале от 1 до 2^n).

Следующее утверждение показывает, что вектор $(l_f(\sigma): \sigma \in V_n)$ однозначно определяет булеву функцию $f \in F_n$.

Утверждение 1. Для любой БФ $f \in F_n$ справедливы равенства

$$f(\sigma) \equiv l_f(\bar{\sigma}) \pmod 2, \ \sigma \in V_n. \quad (7)$$

Доказательство. Из определения функций системы (2) и соотношений (1), (3), (4) вытекают следующие равенства, связывающие коэффициенты $p_{\alpha,\sigma}$ канонических поляризованных полиномов функции f со значениями функций f_σ, $\sigma \in V_n$:

$$f_\sigma(x) = \sum_{\alpha \le x} \oplus p_{\alpha,\sigma}, \quad p_{x,\sigma} = \sum_{\alpha \le x} \oplus f_\sigma(\alpha), \; x \in V_n. \tag{8}$$

Полагая в первом из равенств (8) $x = (1, 1, \ldots, 1)$, получим соотношения

$$f(\bar{\sigma}) = \sum_{\alpha \in V_n} \oplus p_{\alpha,\sigma} \equiv l_f(\sigma) \pmod 2, \; \sigma \in V_n,$$

равносильные (7). Утверждение доказано.

Оценки сложности булевых функций в классе КПП.

Обозначим $R(r, n)$ множество булевых функций n переменных, имеющих степень нелинейности не более r (код Рида-Маллера порядка r и длины 2^n), $0 \le r \le n$. Положим $L(r, n) = \max\{l(f): f \in R(r, n)\}$, $L(n) = L(n, n)$, $n = 1, 2, \ldots$. Непосредственно из определения следует, что

$$1 = L(0, n) \le n = L(1, n) \le L(2, n) \le \ldots \le L(n-1, n) \le L(n) \tag{9}$$

для всех натуральных n.

Явное выражение функции $L(n)$ получено в [6] и независимо в [7]:

$$L(n) = \tfrac{1}{3}(2^{n+1} - 1), \text{ если } n \text{ нечетно}, \; L(n) = \tfrac{1}{3}(2^{n+1} - 2), \text{ если } n \text{ четно}. \tag{10}$$

В [6] показано также, что $L(n) = L_B(n)$, где B – класс симметрических функций.

Следующая теорема устанавливает верхнюю границу сложности БФ $f \in R(r, n)$, $1 \le r \le n$, совпадающую при $r = n$ со значением $L(n)$, определяемым по формуле (10).

Теорема 2. Для любых $1 \le r \le n$, $f \in R(r, n)$, $i \in N_n$ справедливо неравенство

$$l(f) \le \sum_{k=0}^{r} \binom{n-1}{k} + \left[\tfrac{1}{2} l\left(\frac{df}{dx_i}\right) \right]. \tag{11}$$

Доказательство. Не ограничивая общности рассуждений, будем считать, что $i = 1$. Для любого вектора $\sigma = (\sigma_2, \ldots, \sigma_n) \in V_{n-1}$ обозначим f_σ^0, f_σ^1 соответственно функции $(f^{\overline{x_1}})_\sigma$, $(f^{x_1})_\sigma$. Положим $D_\sigma = f_\sigma^0 \oplus f_\sigma^1$, $\sigma(0) = (0, \sigma_2, \ldots, \sigma_n)$, $\sigma(1) = (1, \sigma_2, \ldots, \sigma_n)$.

Справедливы соотношения

$$f_{\sigma(0)}(x_1, \ldots, x_n) = x_1 D_\sigma(x_2, \ldots, x_n) \oplus f_\sigma^0(x_2, \ldots, x_n),$$

$$f_{\sigma(1)}(x_1, \ldots, x_n) = x_1 D_\sigma(x_2, \ldots, x_n) \oplus f_\sigma^1(x_2, \ldots, x_n),$$

из которых вытекают следующие равенства, связывающие длины рассматриваемых функций:

$$l_f(\sigma(0)) = l_D(\sigma) + l_{f^{\overline{x_1}}}(\sigma), \; l_f(\sigma(1)) = l_D(\sigma) + l_{f^{x_1}}(\sigma), \sigma \in V_{n-1}. \tag{12}$$

Обозначим a_σ, b_σ, c_σ соответственно число конъюнкций, являющихся общими слагаемыми полиномов Жегалкина функций f_σ^0 и D_σ, f_σ^1 и D_σ, f_σ^0 и f_σ^1. В силу (12) и равенства

$$l_D(\sigma) = a_\sigma + b_\sigma \tag{13}$$

имеют место соотношения

$$l_f(\sigma(0)) = 2a_\sigma + b_\sigma + c_\sigma,\ l_f(\sigma(1)) = 2b_\sigma + a_\sigma + c_\sigma,\ \sigma \in V_{n-1}. \tag{14}$$

Положим $s(r, n) = \sum_{k=0}^{r} \binom{n-1}{k}$. Поскольку $a_\sigma + b_\sigma + c_\sigma$ есть число конъюнкций, каждая из которых является слагаемым полинома Жегалкина хотя бы одной из функций f_σ^0, f_σ^1, то в силу условий $f \in R(r, n)$, f_σ^0, $f_\sigma^1 \in R(r, n-1)$ справедливо неравенство

$$a_\sigma + b_\sigma + c_\sigma \le s(r, n). \tag{15}$$

Подставляя (15) в (14), получим

$$l_f(\sigma(0)) \le s(r, n) + a_\sigma,\ l_f(\sigma(1)) \le s(r, n) + b_\sigma,\ \sigma \in V_{n-1}. \tag{16}$$

Складывая неравенства (16), с учетом (13) и соотношений $l_f(\sigma(0)) \ge l(f)$, $l_f(\sigma(1)) \ge l(f)$ получим верхнюю оценку (11) сложности БФ f.

Теорема доказана.

Следствие 1. Для любых $1 \le r \le n$ имеет место неравенство

$$L(r, n) \le \sum_{k=0}^{r} \binom{n-1}{k} + \left\lfloor \tfrac{1}{2} L(r-1, n-1) \right\rfloor \tag{17}$$

Обозначим через H класс *четных* булевых функций, то есть функций $f \in F_n$, удовлетворяющих условию $f(x) = f(\bar{x})$, $x \in V_n$, $n = 1, 2, \ldots$.

Следствие 2. Справедливы следующие соотношения:

$$L(n-2, n) \le L(n) - 2,\ n \ge 3, \tag{18}$$

$$L(n-1, n) = L(n) = L_H(n),\ n \ge 2. \tag{19}$$

Доказательство. Докажем неравенство (18), используя индукцию по n. При $n = 3$ имеем $3 = L(1, 3) \le L(3) - 2 = 5 - 2$. Далее, последовательно применяя неравенство (17), предположение индукции и соотношения (10), получим оценки

$$L(n-2, n) \le 2^{n-1} - 1 + \left\lfloor \tfrac{1}{2} L(n-3, n-1) \right\rfloor \le 2^{n-1} - 1 + \left\lfloor \tfrac{1}{2} (L(n-1) - 2) \right\rfloor = L(n) - 2,$$

из которых следует (18).

Для доказательства равенств (19) рассмотрим последовательность БФ $\{f^{(n)}: n = 2, 3, \ldots\}$, определяемых по формулам

$$f^{(2)}(x_1, x_2) = \overline{x_1}\,\overline{x_2} \oplus 1, \tag{20}$$

$$f^{(n+1)}(x_1, \ldots, x_{n+1}) = x_1 f^{(n)}(x_1, \ldots, x_n) \oplus f^{(n)}(\overline{x_1}, \ldots, \overline{x_n}),\ n = 2, 3, \ldots. \tag{21}$$

Положим $h^{(n)}(x_1, \ldots, x_n) = f^{(n)}(x_1, \ldots, x_n) \oplus f^{(n)}(\overline{x_1}, \ldots, \overline{x_n})$, $n = 2, 3, \ldots$. Нетрудно видеть, что

$$h^{(n)} \in H_n \cap R(n-1, n). \tag{22}$$

Кроме того, как показано в [7], для любого $\sigma \in V_n$ $l_{h^{(n)}}(\sigma) \geq \frac{1}{3}(2^{n+1}-1)$ при нечетном n и $l_{h^{(n)}}(\sigma) \geq \frac{1}{3}(2^{n+1}-2)$ при четном n. Отсюда в силу (10) имеем

$$l(h^{(n)}) = L(n),\ n \geq 2. \tag{23}$$

Равенства (19) следуют непосредственно из (18), (22), (23).

Отметим, что с помощью рассуждений, использованных выше при доказательстве неравенства (11), в ряде случаев можно получить более точные верхние границы функции Шеннона $L_K(n)$ для сложности БФ, принадлежащих данному классу K. Как правило, улучшить оценки (11), (17) удается в том случае, когда функции $f \in K$ допускают определенного вида декомпозицию, например, имеют большой индекс линейности [2] или могут быть представлены в виде линейной комбинации $f(y, z_1, \ldots, z_t) = \varphi_1(y)g_1(z_1) \oplus \ldots \oplus \varphi_t(y)g_t(z_t)$ БФ, зависящих от попарно непересекающихся наборов y, z_1, …, z_t булевых переменных.

Обозначим $K_{n,t}$ множество булевых функций $f \in F_n$ вида

$$f(x, y) = x_1\varphi_1(y) \oplus \ldots \oplus x_t\varphi_t(y) \oplus \psi(y),\ x = (x_1, \ldots, x_t) \in V_t,\ y \in V_{n-t}. \tag{24}$$

Наибольшее натуральное t, для которого существуют БФ $\varphi_1, \ldots, \varphi_t, \psi \in F_{n-t}$ такие, что f имеет вид (24), называется *индексом линейности* функции f [2]. Следующее утверждение, доказательство которого по существу аналогично доказательству теоремы 2, устанавливает оценки функции Шеннона $L^{(t)}(n) \overset{\text{def}}{=} \max\{l(f)\colon f \in K_{n,t}\}$ для сложности БФ, имеющих индекс линейности не менее t.

Утверждение 2. Для любых $1 \leq t \leq n$ справедливы неравенства

$$(t+1)L(n-t) \leq L^{(t)}(n) \leq t2^{n-t} + L(n-t-1). \tag{25}$$

Нижняя граница (25) функции $L^{(t)}(n)$ доказывается путем оценки сложности БФ $f(x, y) = (x_1 \oplus \ldots \oplus x_t)\, f^{(n-t)}(y) \oplus f^{(n-t)}(\bar{y})$, $x \in V_t$, $y \in V_{n-t}$, где функции $f^{(n-t)}$, $1 \leq t \leq n$, $n = 2, 3, \ldots$ определяются по формулам (20), (21) (см. [6, 7]). Отметим также, что при $t = 1$ верхняя граница $L^{(t)}(n)$ совпадает с функцией Шеннона (10) для сложности всех БФ n переменных в классе КПП.

Алгоримы вычисления значений частных производных и минимизации БФ в классе КПП.

Известные алгоритмы [8, 9] построения оптимальных канонических поляризованных полиномов, реализующих произвольную БФ $f \in F_n$, предполагают вычисление значений всех частных производных функции f с последующим определением КПП вида (3), имеющего наименьшее число ненулевых слагаемых. Формально указанные алгоритмы являются схемами вычисления [1] системы

$$\left(\frac{d(\cdot)}{d\alpha}(\sigma)\colon\ \alpha, \sigma \in V_n\right) \tag{26}$$

булевых функций, зависящих от 2^n переменных: координат вектора T_f значений БФ $f \in F_n$ [8] или координат вектора P_f коэффициентов полинома

Жегалкина этой функции [9]. Вычислительная сложность алгоритмов определяется числом операций сложения по модулю 2, выполняемых в процессе вычисления коэффициентов КПП функции f по векторам T_f, P_f соответственно.

В статье [8] представлен алгоритм, основанный на отождествлении вектора значений произвольной БФ $f \in F_n$ с локальным кодом подходящей симметрической функции $S(f)$, зависящей от $2^n - 1$ переменных. С использованием полученных в [8] соотношений, связывающих частные производные БФ f и $S(f)$, построена схема вычисления системы функций (26) со сложностью $T(n) = 2^{2n-1} - 2^{n-1}$.

Приведем еще один (имеющий сложность $T(n)$) алгоритм вычисления коэффициентов КПП (3) булевой функции $f \in F_n$, заданной вектором значений T_f. Обозначим f_1 и f_0 соответственно f^{x_1} - и $f^{\overline{x_1}}$ -компоненту БФ f; положим $D = f_1 \oplus f_0$. Рассмотрим матрицу $M_f = (\frac{df}{d\alpha}(\sigma))_{\alpha,\sigma \in V_n}$, составленную из значений частных производных функции f. Аналогично определим матрицы M_{f_1}, M_{f_0}, M_D. Нетрудно убедиться в справедливости следующего равенства:

$$M_f = \begin{pmatrix} M_{f_0} & M_{f_1} \\ M_D & M_D \end{pmatrix}. \qquad (27)$$

Предлагаемый алгоритм вычисления элементов матрицы (27) по вектору $T_f = (T_{f_0}, T_{f_1})$ представляет собой рекурсивную процедуру $\Re(n)$, входными данными которой являются булевы векторы длины 2^n.

1. При $n = 1$ положить $D = f_1 \oplus f_0$; определить M_f по формуле (27).

2. При $n > 1$ вычислить с использованием процедуры $\Re(n-1)$ матрицы M_{f_0}, M_{f_1}; вычислить M_D по формуле $M_D = M_{f_0} \oplus M_{f_1}$ и определить матрицу M_f по формуле (27).

Обозначим $t(n)$ вычислительную сложность описанной процедуры $\Re(n)$. Справедливы равенства $t(1) = 1$, $t(n) = 2t(n-1) + 2^{2(n-1)}$, $n > 1$, из которых следует, что

$$t(n) = 2^{2n-1} - 2^{n-1}, n = 1, 2, \ldots.$$

В [9] предложен оптимальный (в классе схем вычисления) алгоритм нахождения значений всех частных производных булевой функции n переменных, реализованной полиномом Жегалкина. Сложность этого алгоритма равна $T_0(n) = 3^n - 2^n$.

Обозначим $T^*(n)$ наименьшее число операций сложения по модулю 2 в алгоритмах (схемах) вычисления коэффициентов КПП булевых функций $f \in F_n$, заданных с помощью векторов значений T_f. Из результатов, полученных в [9], вытекает следующее утверждение.

Утверждение 3. Для любого натурального $n \geq 2$ справедливы неравенства

$$3^n - 2^n \leq T^*(n) \leq 3^n + 2^{n-1}(n-2). \qquad (28)$$

Вопрос о совпадении $T^*(n)$ с нижней границей (28) остается в настоящее время открытым.

1. *Сэвидж Дж.Э.* Сложность вычислений: Пер. с англ. – М.: Факториал, 1998. – 368 с.

2. *Ященко В.В.* О критерии распространения булевых функций и бент-функциях // Проблемы передачи информации. – 1997. – Т. 33. – В. 1. – С. 75-86.

3. *Xiao G.Z., Massey J.L.* A special characterization of correlation-immune combining functions // IEEE Trans. Inform. Theory. – 1988. – 34, № 3. – P. 569-571.

4. *Tsai C., Marek-Sadovska M.* Boolean functions classification via fixed polarity Reed-Muller forms // IEEE Trans. on Comput. – 1997. – 46, № 2. – P. 173-186.

5. *Sasao T., Besslich P.* On the complexity of mod-2 sum PLA's // IEEE Trans. on Comput. – 1990. – 39, № 2. – P. 262-266.

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

7. *Алексейчук А.Н.* О сложности булевых функций в классе канонических поляризованных полиномов // Кибернетика и системный анализ. – 2000. – № 3. – С. 179-183.

8. *Августь Л.В.* Полиномиальное разложение булевых функций методом "тройного треугольника" // Автоматика и вычисл. техника. – 1996. – № 2. – С. 12-24.

9. *Алексейчук А.Н.* О сложности вычисления значений частных производных булевых функций, реализованных полиномами Жегалкина // Кибернетика и системный анализ. – 2001. – № 5. – С. 30-37.

10. *Бохман Д., Постхоф Х.* Двоичные динамические системы: Пер. с нем. – М.: Энергоатомиздат, 1986. – 401 с.