УДК 519.719.325 DOI 10.17223/2226308X/10/23

УСЛОВИЕ ОДНОЗНАЧНОСТИ РАЗЛОЖЕНИЯ В СУММУ ФУНКЦИЙ ПРИ ЛИНЕЙНОЙ ЗАМЕНЕ ПЕРЕМЕННЫХ

А. В. Черемушкин

Рассматривается множество разложений двоичной функции в сумму функций от непересекающихся множеств переменных при различных линейных преобразованиях аргументов. Каждому такому разложению соответствует разложение векторного пространства в прямую сумму подпространств. Приведены условия, при которых такое разложение определяется однозначно с точностью до перестановки подпространств между собой.

Ключевые слова: *двоичные функции, разложение в прямую сумму, линейное преобразование.*

Пусть $\mathcal{F}_n = \{f : V_n \to \mathrm{GF}(2)\}$ — множество двоичных функций от n переменных, $n \geqslant 1$, $V_n = \mathrm{GF}(2)^n$ рассматривается как векторное пространство над полем $\mathrm{GF}(2)$, $\mathbf{H}_n$ — группа сдвигов пространства V_n. Для каждого целого $s \geqslant 0$ определим подпространство $\mathcal{U}_s = \{f : \deg f \leqslant s\}$ пространства функций $\mathcal{F}_n$, имеющих ограниченную степень нелинейности (не больше s). Заметим, что $\mathcal{U}_0 = \{0, 1\}$. При $s < 0$ положим $\mathcal{U}_s = \{0\}$ — нулевое подпространство. Обозначим $(\mathbf{H}_n)_f^{(s)}$ множество таких сдвигов $\begin{pmatrix} x \\ x \oplus a \end{pmatrix} \in \mathbf{H}_n$, что выполнено сравнение

$$f(x \oplus a) \equiv f(x) \pmod{\mathcal{U}_s}, \quad x \in V_n.$$

Пусть $0 \leqslant t \leqslant n-1$, $1 \leqslant k \leqslant n$. Будем говорить, что переменные $x_{k+1}, \ldots, x_n$ функции $f(x_1, \ldots, x_n)$ являются несущественными по модулю $\mathcal{U}_s$, если найдётся функция $h(x_1, \ldots, x_k)$, такая, что $f \oplus h \in \mathcal{U}_s$. Нетрудно видеть, что переменное x_n является несущественным для функции f по модулю $\mathcal{U}_s$, если и только если

$$\begin{pmatrix} x \\ x \oplus e_n \end{pmatrix} \in (\mathbf{H}_n)_f^{(s-1)}$$

при $e_n = (0, \ldots, 0, 1)$.

Будем говорить, что функция $f \in \mathcal{F}_n$ *линейно разложима в бесповторную сумму по модулю* $\mathcal{U}_s$, если при некотором линейном преобразовании A пространства V_n и $1 \leqslant k < n$ найдутся функции f_1 и f_2, для которых выполнено сравнение

$$f(xA) \equiv f_1(x_1, \ldots, x_k) \oplus f_2(x_{k+1}, \ldots, x_n) \pmod{\mathcal{U}_s}.$$

Заметим, что разложение двоичной функции в бесповторное произведение нелинейных неприводимых сомножителей изучалось в работе [1].

Случай, когда $s \leqslant 0$ и $k = 1$ ($k = n - 1$), рассмотрен в [2]. В этом случае пространство размерности $n - 1$ однозначно определено в том и только в том случае, когда у функции f_2 (f_1) все переменные существенны по модулю $\mathcal{U}_1$.

Для $s \leqslant 1$ и слагаемых второй степени ни о каком однозначном разложении в принципе не может быть и речи, так как таким функциям соответствуют квадратичные формы, которые имеют неприводимые группы инерции, в качестве которых выступают классические линейные группы.

В то же время для $s \leqslant 2$ и слагаемых степени три и выше при ограничениях на число существенных переменных по модулю $\mathcal{U}_s$ уже можно показать однозначность для разложения, имеющего максимальное число слагаемых.

Теорема 1. Если при $s \geqslant 2$ функция $f = f(x_1, \ldots, x_n)$ имеет тривиальную группу инерции $(\mathbf{H}_n)_f^{(s-1)}$ и линейно разложима в бесповторную сумму по модулю $\mathcal{U}_s$, то для этой функции найдётся линейное разложение по модулю $\mathcal{U}_s$ в бесповторную сумму линейно неразложимых (в бесповторную сумму) слагаемых, однозначно определённое в том смысле, что любое другое такое разложение соответствует тому же самому разложению пространства в прямую сумму подпространств, а соответствующие функции линейно эквивалентны по модулю $\mathcal{U}_s$.

Метод доказательства аналогичен тому, который применён в работе [3]. В качестве следствия получаем описание группы инерции таких функций в полной аффинной группе.

Следствие 1. Если в условиях теоремы 1 функция f представлена в виде суммы линейно неразложимых в бесповторную сумму по модулю $\mathcal{U}_s$ функций

$$f \equiv f_1 \oplus \cdots \oplus f_m \pmod{\mathcal{U}_s},$$

причём множество функций $\{f_1, \ldots, f_m\}$ разбивается на t классов аффинной эквивалентности по модулю $\mathcal{U}_s$: $\{f_{\mu_1}, \ldots, f_{\mu_p}\} \subseteq \mathcal{F}_{n_1}$, $\ldots$, $\{f_{\nu_1}, \ldots, f_{\nu_q}\} \subseteq \mathcal{F}_{n_t}$, то для группы инерции бесповторной суммы этих функций справедлив изоморфизм

$$\mathbf{AGL}\,(n,2)^{(s)}_{f_1\oplus\cdots\oplus f_m} \cong [\mathbf{AGL}\,(n_1,2)^{(s)}_{f_{\mu_1}}]\mathbf{S}_p \times \cdots \times [\mathbf{AGL}\,(n_t,2)^{(s)}_{f_{\nu_1}}]\mathbf{S}_q.$$

Здесь через $G_f^{(s)}$ обозначена группа инерции функции f по модулю $\mathcal{U}_s$ в группе G, а $[G]\mathbf{S}_p$ — операция экспоненцирования группы G с помощью симметрической группы S_p степени p. Аналогичное описание справедливо для полной линейной группы $\mathbf{GL}\,(n,2)$.

ЛИТЕРАТУРА

1. *Черемушкин А. В.* Однозначность разложения двоичной функции в бесповторное произведение нелинейных неприводимых сомножителей // Вестник Московского государственного университета леса «Лесной вестник». 2004. № 4(35). С. 86–90.
2. *Черемушкин А. В.* Методы аффинной и линейной классификации двоичных функций // Труды по дискретной математике. М.: Физматлит, 2001. Т. 4. С. 273–314.
3. *Черемушкин А. В.* К вопросу о линейной декомпозиции двоичных функций // Прикладная дискретная математика. 2016. № 1(31). С. 46–56.

УДК 512.55 DOI 10.17223/2226308X/10/24

ОПИСАНИЕ НЕКОТОРЫХ ДЕКОМПОЗИЦИЙ ДЛЯ КВАДРАТИЧНЫХ БУЛЕВЫХ ПОРОГОВЫХ ФУНКЦИЙ

А. Н. Шурупов

Приводятся необходимые и достаточные условия функциональной разделимости квадратичных булевых пороговых функций, задаваемых распавшейся на два константных блока квадратичной формой.

Ключевые слова: *функциональная разделимость, квадратичные булевы пороговые функции.*