7. *Фомин Д. Б.* Об алгебраической степени и дифференциальной равномерности подстановок пространства V_{2m}, построенных с использованием $(2m, m)$-функций. // Матем. вопр. криптогр. 2020. Т. 11. № 4. С. 133–149.
8. *Carlet C., Tang D., Tang X., and Liao Q.* New construction of differentially 4-uniform bijections // LNCS. 2013. V. 8567. P. 22–38.

УДК 519.719.325 DOI 10.17223/2226308X/14/10

УСЛОВИЕ ОДНОЗНАЧНОСТИ РАЗЛОЖЕНИЯ В ПРОИЗВЕДЕНИЕ ФУНКЦИЙ p-ЗНАЧНОЙ ЛОГИКИ ПРИ ЛИНЕЙНОЙ ЗАМЕНЕ ПЕРЕМЕННЫХ

А. В. Черемушкин

Рассматривается множество разложений функции p-значной логики в произведение 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 разложение определяется однозначно с точностью до перестановки подпространств между собой.

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

Пусть $n \geqslant 1$, $V_n = \mathbb{Z}_p^n$ рассматривается как векторное пространство над полем $\mathbb{Z}_p$, $\mathcal{F}_n = \{f : V_n \to \mathbb{Z}_p\}$ — множество функций от n переменных.

Пусть $1 \leqslant k \leqslant n$. Говорят, что переменные $x_{k+1}, \ldots, x_n$ функции $f(x_1, \ldots, x_n)$ являются несущественными, если найдётся функция $h(x_1, \ldots, x_k)$, такая, что $f = h$. Нетрудно видеть, что переменная x_n является несущественной для функции f, если и только если $f(x + e^n) = f(x)$ при $e^n = (0, \ldots, 0, 1)$.

Пусть $(\mathbf{H}_n)_f$ — группа инерции функции f в группе сдвигов $\mathbf{H}_n$, т. е. множество таких сдвигов $\begin{pmatrix} x \\ x+a \end{pmatrix} \in \mathbf{H}_n$, что выполнено сравнение $f(x + a) = f(x)$, $x \in V_n$. Условие тривиальности группы инерции $(\mathbf{H}_n)_f$ равносильно тому, что у всех функций, полученных из f всевозможными линейными заменами переменных, все переменные будут существенными.

Назовём *носителем функции* $f : V_n \to \mathbb{Z}_p$ множество векторов, на которых она принимает ненулевые значения:

$$f^{-1}(*) = \{a \in V_n : f(a) \neq 0\}.$$

Если носитель функции содержится в некотором многообразии размерности k, то это позволяет сводить задачу исследования функции от n переменных к задаче исследования функции от $n - k$ переменных.

Лемма 1. Пусть функция $f : V_n \to \mathbb{Z}_p$ не является константой. Если носитель $f^{-1}(*)$ функции f содержится в многообразии $L + a \subset V_n$, $1 \leqslant \dim L \leqslant n - 1$, то существует линейное преобразование A пространства V_n, функция $h : \mathbb{Z}_p^{n-k} \to \mathbb{Z}_p$ и элементы $a_1 \ldots, a_k \in \mathbb{Z}_p$, $k = n - \dim L$, такие, что функцию $f(xA)$ можно представить в виде

$$f(xA) = J_{a_1}(x_1) \ldots J_{a_k}(x_k) h(x_{k+1}, \ldots, x_n),$$

где

$$J_a(x_i) = \begin{cases} 1, & x_i = a, \\ 0, & x_i \neq a. \end{cases}$$

Лемма 2. Пусть разложение функции f по первой переменной имеет вид

$$f(x_1, x_2, \ldots, x_n) = \sum_{a_1=0}^{p-1} J_{a_1}(x_1) f_{a_1}(x_2, \ldots, x_n). \tag{1}$$

Тогда:

1) если $f(x_1, x_2, \ldots, x_n) = J_{a_1}(x_1) f_{a_1}(x_2, \ldots, x_n)$, то множество $f^{-1}(*)$ содержится в гиперплоскости, задаваемой уравнением $(x, e^1) = a_1$;
2) если в разложении (1) имеется не менее двух ненулевых слагаемых, то множество $f^{-1}(*)$ содержится в гиперплоскости в том и только в том случае, когда все множества $f_{a_1}^{-1}(*)$, $0 \leqslant a_1 \leqslant p-1$, одновременно содержатся в одной гиперплоскости.

Будем говорить, что функция $f \in \mathcal{F}_n$ *линейно разложима в бесповторное произведение*, 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

$$f(xA) = f_1(x_1, \ldots, x_k) f_2(x_{k+1}, \ldots, x_n).$$

С данным разложением связаны разложения вида $f = h_1 h_2$, где $h_i = c_i f_i$; $c_i \in \mathbb{Z}_p$, $i = 1, 2$, и выполнено условие $c_1 c_2 = 1$.

Теорема 1. Если функция $f = f(x_1, \ldots, x_n)$ имеет тривиальную группу инерции $(\mathbf{H}_n)_f$, её носитель не содержится ни в какой гиперплоскости и она линейно разложима в бесповторное произведение, то для этой функции найдётся линейное разложение в бесповторное произведение линейно неразложимых (в бесповторное произведение) сомножителей, 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 с точностью до константного сомножителя.

Заметим, что для случая $p = 2$ разложение двоичной функции в бесповторное произведение нелинейных неразложимых сомножителей изучено в работе автора [1]. В настоящей работе применяется аналогичный метод доказательства.

В качестве следствия получаем описание группы инерции таких функций в полной аффинной группе.

Следствие 1. Если в условиях теоремы функция f представлена в виде произведения линейно неразложимых в бесповторное произведение функций

$$f = f_1 \cdot \ldots \cdot f_m,$$

причём множество функций $\{f_1, \ldots, f_m\}$ разбивается на t классов аффинной эквивалентности с точностью до константного сомножителя:

$$\{f_{\mu_1}, \ldots, f_{\mu_r}\} \subseteq \mathcal{F}_{n_1}, \ldots, \{f_{\nu_1}, \ldots, f_{\nu_q}\} \subseteq \mathcal{F}_{n_t},$$

то для группы инерции бесповторного произведения этих функций справедлив изоморфизм

$$\mathbf{AGL}\,(n, p)_{f_1 \cdot \ldots \cdot f_m} \cong [\mathbf{AGL}\,(n_1, p)_{f_{\mu_1}}]\mathbf{S}_r \times \cdots \times [\mathbf{AGL}\,(n_t, p)_{f_{\nu_1}}]\mathbf{S}_q.$$

Здесь через G_f обозначена группа инерции функции f в группе G; $[G]\mathbf{S}_r$ — операция экспоненцирования группы G с помощью симметрической группы $\mathbf{S}_r$ степени r. Аналогичное описание справедливо для полной линейной группы $\mathbf{GL}(n,p)$.

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.

УДК 519.7 DOI 10.17223/2226308X/14/11

О ПРОИЗВОДНЫХ БУЛЕВЫХ БЕНТ-ФУНКЦИЙ[1]

А. С. Шапоренко

Бент-функция может быть определена как булева функция $f(x)$ от n переменных (n чётно), такая, что для любого ненулевого вектора y её производная $D_yf(x) = f(x) \oplus f(x \oplus y)$ сбалансирована — принимает значения 0 и 1 одинаково часто. Справедливо ли, что любая сбалансированная функция — производная некоторой бент-функции? Эта задача рассмотрена для частного случая — аффинных функций. Доказано, что любая неконстантная аффинная функция от $n \geqslant 4$ (n чётно) переменных является производной для $(2^{n-1}-1)|\mathcal{B}_{n-2}|^2$ бент-функций, где $\mathcal{B}_{n-2}$ — класс бент-функций от $n-2$ переменных. Получены итерационные нижние границы для числа бент-функций.

Ключевые слова: *бент-функции, булевы функции, производные бент-функций, нижние границы для числа бент-функций.*

Пусть $\langle x, y\rangle$ — скалярное произведение двоичных векторов по модулю 2. Функция $f : \mathbb{Z}_2^n \to \mathbb{Z}_2$ называется *булевой функцией* от n переменных. Булева функция от чётного числа переменных называется бент-функцией, если она максимально нелинейна [1]. Обозначим через $\mathcal{B}_n$ множество бент-функций от n переменных.

Шифры, в которых применяются бент-функции, более устойчивы к *линейному криптоанализу* [2], потому что бент-функции крайне плохо аппроксимируются аффинными функциями. Бент-функции используются в структуре блочного шифра CAST как координатные функции S-блоков [3], а также для построения регистра сдвига с нелинейной обратной связью в поточном шифре Grain [4]; они связаны также с некоторыми объектами теории кодирования, например с кодами Рида — Маллера [5].

Другое определение бент-функции — булева функция $f(x)$ от n переменных (n чётно), такая, что для любого ненулевого вектора y её производная $D_yf(x) = f(x) \oplus f(x \oplus y)$ сбалансирована — принимает значения 0 и 1 одинаково часто [5]. Справедливо ли, что любая сбалансированная функция — производная некоторой бент-функции? В [6] показано, что любая сбалансированная функция g от $n \leqslant 6$ переменных степени не выше $n/2-1$, такая, что $g(x) = g(x \oplus y)$ для всех x при некотором y, является производной некоторой бент-функции от n переменных. В данной работе эта задача рассмотрена для частного случая сбалансированых функций — аффинных: $\ell_{a,b}(x) = \langle a, x\rangle \oplus b$, где $a \in \mathbb{Z}_2^n$ — ненулевой вектор и $b \in \mathbb{Z}_2$.

Теорема 1. Любая неконстантная аффинная функция $\ell_{a,b}(x)$ от $n \geqslant 4$ (n чётно) переменных является производной для $(2^{n-1}-1)|\mathcal{B}_{n-2}|^2$ бент-функций.

[1]Работа выполнена в рамках госзадания ИМ СО РАН (проект № 0314-2019-0017) при поддержке лаборатории криптографии JetBrains Research.