

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

УДК 512.13

КЛАСС СБАЛАНСИРОВАННЫХ АЛГЕБРАИЧЕСКИХ ПОРОГОВЫХ ФУНКЦИЙ

Д. А. Сошин

ФГУП «НИИ «Квант», г. Москва, Россия

Предложен подход к построению класса сбалансированных алгебраических пороговых функций (АПФ). Функция k -значной логики f называется АПФ, если существуют целочисленные наборы $\mathbf{c} = (c_0, c_1, \dots, c_n)$, $\mathbf{b} = (b_0, b_1, \dots, b_k)$ и натуральный модуль m , такие, что $f(x_1, x_2, \dots, x_n) = \alpha$, если и только если $b_\alpha \leq r_m(c_0 + c_1x_1 + c_2x_2 + \dots + c_nx_n) < b_{\alpha+1}$ для любого $\alpha \in \Omega_k$, где $r_m(x)$ — функция приведения числа x по модулю m . Тройку $(\mathbf{c}; \mathbf{b}; m)$ будем называть структурой функции f . Центральным результатом работы является построенный класс сбалансированных АПФ, а именно: если для АПФ f , заданной структурой $((c_0, c_1, c_2, \dots, c_n); (0, p, 2p, \dots, kp); kp) = (\mathbf{c}, \mathbf{b}, m)$, существует $c_i = pq$ и $(q, k) = 1$, то такая функция сбалансированная. Сбалансированные функции данного класса могут быть использованы в качестве координатных функций подстановок.

Ключевые слова: алгебраические пороговые функции, сбалансированные функции.

DOI 10.17223/20710410/40/1

THE CLASS OF BALANCED ALGEBRAIC THRESHOLD FUNCTIONS

D. A. Soshin

*Technology Federal State Unitary Enterprise “Research Institute Kvant”, Moscow, Russia***E-mail:** danil_re@list.ru

The paper proposes an approach to the construction of a class of balanced algebraic threshold functions (ATF). The function f of k -valued logic is called ATF if there are sequences $\mathbf{c} = (c_0, c_1, \dots, c_n)$, $\mathbf{b} = (b_0, b_1, \dots, b_k)$ of integers and the natural modulus m such that $f(x_1, x_2, \dots, x_n) = \alpha \Leftrightarrow b_\alpha \leq (c_0 + c_1x_1 + c_2x_2 + \dots + c_nx_n) \bmod m < b_{\alpha+1}$ for any $\alpha \in \Omega_k = \{0, 1, \dots, k-1\}$. The triple $(\mathbf{c}; \mathbf{b}; m)$ is called the structure of the function f . The central result of the paper is a class of balanced ATF constructed in the following way: if an ATF f has a structure $(\mathbf{c}, \mathbf{b}, m) = ((c_0, c_1, c_2, \dots, c_n); (0, p, 2p, \dots, kp); kp)$ where $c_i = pq$ and $(q, k) = 1$, then this function is balanced. Such functions can be used as coordinate functions of substitutions.

Keywords: algebraic threshold functions, balanced functions.

Работа посвящена развитию методов синтеза биективных преобразований, задаваемых регулярными системами функций. В [2, 1] в качестве координатных функций подстановок предлагается использовать системы однотипных пороговых функций и системы алгебраических пороговых функций. Согласно критерию Хаффмана, координатные функции должны быть сбалансированными, поэтому на первом этапе должен быть решён вопрос описания классов сбалансированных функций. В работе построен класс сбалансированных АПФ, обобщающий результаты, полученные в [3]. Использование АПФ представляет практический интерес в связи с возможностью их эффективной реализации непосредственно в среде — носителе сигнала, а именно в оптической среде.

Алгебраические пороговые функции k -значной логики от n переменных AT_n^k расширяют класс пороговых функций T_n^k за счёт добавления модульной операции.

Определение 1. Функцию k -значной логики $f : \Omega_k^n \rightarrow \Omega_k$ назовём алгебраической пороговой, если существуют целочисленные наборы $\mathbf{c} = (c_0, c_1, \dots, c_n)$, $\mathbf{b} = (b_0, b_1, \dots, b_k)$ и натуральный модуль m , такие, что для любого $\alpha \in \Omega_k$ выполняется

$$f(x_1, x_2, \dots, x_n) = \alpha \Leftrightarrow b_\alpha \leq r_m(c_0 + c_1x_1 + c_2x_2 + \dots + c_nx_n) < b_{\alpha+1}, \quad (1)$$

где $r_m(x)$ — функция приведения числа x по модулю m , $r_m(x) \in \{0, 1, \dots, m-1\}$; $\Omega_k = \{0, 1, \dots, k-1\}$. Тройку $(\mathbf{c}, \mathbf{b}, m)$ будем называть структурой функции f .

Двойное неравенство (1) можно записать равносильным способом

$$b_\alpha \leq c_1x_1 + c_2x_2 + \dots + c_nx_n + mt < b_{\alpha+1} \quad (2)$$

для некоторого $t \in \mathbb{Z}$ [4].

Определение 2. Слоем $D_\alpha(f)$ (носителем значения α) пороговой функции f будем называть множество точек из Ω_k^n , в которых функция f принимает значение α , $\alpha \in \{0, \dots, k-1\}$.

Пример 1. Зададим 3-значную АПФ $f(x_1, x_2)$ её структурой

$$(\mathbf{c}; \mathbf{b}; m) = ((0, 2, 3); (0, 3, 6, 9); 9).$$

Выпишем неравенства, определяющие значения функции:

$$\begin{aligned} f(x_1, x_2) = 0 &\Leftrightarrow 0 \leq r_9(2x_1 + 3x_2) < 3; \\ f(x_1, x_2) = 1 &\Leftrightarrow 3 \leq r_9(2x_1 + 3x_2) < 6; \\ f(x_1, x_2) = 2 &\Leftrightarrow 6 \leq r_9(2x_1 + 3x_2) < 9. \end{aligned}$$

Представим функцию $f(x_1, x_2)$ в табличном виде:

		x_1		
		0	1	2
x_2	0	0	0	1
	1	1	1	2
	2	2	2	0

Функция $f(x_1, x_2)$ принадлежит классу AT_2^3 , но не классу T_2^3 . Действительно, любая пороговая функция является полностью монотонной [5], а при фиксациях $x_1 = 1$ и $x_1 = 2$ у функции f нарушается условие 1-монотонности.

Следующие два утверждения описывают подкласс BAT_n^k класса AT_n^k сбалансированных k -значных функций, представляющих практический интерес.

Теорема 1. Пусть $c_i \neq 0$, $i \in \{1, \dots, n\}$, тогда структура

$$((c_0, c_1, c_2, \dots, c_n); (0, c_i, 2c_i, \dots, kc_i); kc_i) \quad (3)$$

задаёт сбалансированную функцию, принадлежащую классу AT_n^k .

Доказательство. Рассмотрим функцию $f(x_1, x_2, \dots, x_n)$, заданную структурой (3). Для множества Ω_k^n справедливо разложение

$$\Omega_k^n = \bigsqcup_{\alpha=0}^{k-1} D_\alpha(f), \quad D_i(f) \cap D_j(f) = \emptyset \text{ при } i \neq j.$$

Для доказательства теоремы достаточно проверить равномощность всех $D_\alpha(f)$. Зафиксируем произвольное значение $d \in \{0, \dots, k-2\}$. Построим отображение

$$\varphi : D_d(f) \rightarrow D_{d+1}(f)$$

по следующему правилу. Для каждой точки $\mathbf{a} = (a_1, a_2, \dots, a_n) \in D_d(f)$

$$\varphi(a_1, \dots, a_{i-1}, a_i, a_{i+1}, \dots, a_n) = (a_1, \dots, a_{i-1}, a_i \oplus 1, a_{i+1}, \dots, a_n), \quad (4)$$

где $\oplus$ — сложение по модулю k . Покажем корректность задания отображения φ . Запишем сравнения (2) для функции $f(x_1, x_2, \dots, x_n)$, используя структуру (3):

$$\alpha c_i \leq c_0 + c_1 x_1 + c_2 x_2 + \dots + c_n x_n + kc_i t < (\alpha + 1)c_i, \quad (5)$$

$kc_i = m$, $\alpha c_i = b_\alpha$, $(\alpha + 1)c_i = b_{\alpha+1}$. Для точки $\mathbf{a} \in D_d(f)$ преобразуем сравнение (5), подставив вместо значения α значение d :

$$dc_i \leq c_0 + c_1 a_1 + c_2 a_2 + \dots + c_n a_n + kc_i t < (d + 1)c_i.$$

Ко всем частям двойного неравенства прибавим c_i :

$$(c_i + dc_i) \leq c_0 + c_1 a_1 + \dots + (c_i a_i + c_i) + \dots + c_n a_n + kc_i t < c_i + (d + 1)c_i.$$

Преобразовав последнее, получим

$$(d + 1)c_i \leq c_0 + c_1 a_1 + \dots + c_i(a_i + 1) + \dots + c_n a_n + kc_i t < (d + 2)c_i. \quad (6)$$

Сравнение (6) задаёт пределы, в которых лежит значение линейной формы функции $f(x_1, x_2, \dots, x_n)$ в точках $(a_1, a_2, \dots, a_{i-1}, a_i + 1, a_{i+1}, \dots, a_n)$, $a_i \in \{0, \dots, k-2\}$. Если координата a_i равна $k-1$, то (6) примет вид

$$(d + 1)c_i \leq c_0 + c_1 a_1 + \dots + c_i 0 + \dots + c_n a_n + kc_i t' < (d + 2)c_i, \quad (7)$$

где $t' = t + 1 \in \mathbb{Z}$. Объединяя (6) и (7), получим для любого $a_i \in \{0, \dots, k-1\}$

$$(d + 1)c_i \leq r_{kc_i}(c_0 + c_1 a_1 + \dots + c_i(a_i \oplus 1) + \dots + c_n a_n) < (d + 2)c_i.$$

Из последнего видно, что для указанных значений d выполняется

$$f(\varphi(a_1, a_2, \dots, a_n)) = d + 1,$$

откуда получаем, что вектор $\varphi(a_1, a_2, \dots, a_n)$ лежит в множестве $D_{d+1}(f)$.

Докажем, что отображение φ биективное. Для этого построим обратное отображение $\varphi^{-1} : D_{d+1}(f) \rightarrow D_d(f)$, положив для каждой точки $\mathbf{a} = (a_1, a_2, \dots, a_n)$, принадлежащей множеству $D_{d+1}(f)$,

$$\varphi(a_1, a_2, \dots, a_n) = (a_1, a_2, \dots, a_{i-1}, a_i \ominus 1, a_{i+1}, \dots, a_n), \quad (8)$$

где $\ominus$ — вычитание по модулю k . Корректность определения φ^{-1} проверяется аналогично φ . Из (4) и (8) получим $\varphi^{-1}\varphi(a_1, a_2, \dots, a_n) = (a_1, a_2, \dots, a_n)$, что свидетельствует о биективности φ и равномощности множеств $D_\alpha(f)$, $\alpha \in \{0, \dots, k-1\}$. ■

Обобщим результат, полученный в теореме 1. В доказательстве используется следствие из критерия о полноцикловости линейного конгруэнтного генератора. Напомним, что под последовательностью, порождённой линейным конгруэнтным генератором с параметрами X_0, a, q, m , понимается последовательность $\{X_i\}_{i \geq 0}$, удовлетворяющая следующему рекуррентному закону:

$$X_{i+1} = aX_i + q \pmod{m}, \quad i \geq 0. \quad (9)$$

Критерий полноцикловости [6, с. 36] при $a = 1$ имеет следующий вид:

Линейный конгруэнтный генератор вида (9) при $a = 1$ является полноцикловым тогда и только тогда, когда $(q, m) = 1$.

Теорема 2. Если для АПФ f , заданной структурой

$$((c_0, c_1, c_2, \dots, c_n); (0, p, 2p, \dots, kp); kp),$$

существует $c_i = pq$ и $(q, k) = 1$, то функция f сбалансированная.

Доказательство. Доказательство полностью повторяет логику доказательства теоремы 1 со следующими изменениями.

Отображение φ для любого d определяется условием

$$\varphi : D_d(f) \rightarrow D_{d \oplus q}(f).$$

Правило (4) при этом остаётся неизменным. Далее, в силу равенств $c_i = pq$ и $b_d = dp$, в (6) произведём соответствующие замены, в результате чего получим

$$(d + q)p \leq c_0 + c_1a_1 + \dots + c_i(a_i + 1) + \dots + c_na_n + kpt < (d + q + 1)p. \quad (10)$$

Остальные преобразования (10) повторяют логику доказательства теоремы 1 с учётом приведения, при необходимости, порогов в (10) по модулю kp .

Заметим, что преобразование Φ , действующее на множестве $\{D_i(f) : i=0, \dots, k-1\}$ и заданное по правилу

$$\Phi(D_i(f)) = D_{i \oplus q}(f),$$

удовлетворяет условиям критерия полноцикловости. Из биективности φ и того, что все множества $D_i(f)$ лежат на одном цикле преобразования Φ , следует их равномощность, при этом преобразование Φ можно записать $\Phi(D_i(f)) = \varphi(D_i(f))$. ■

При $q = 1$ утверждение теоремы 2 совпадает с теоремой 1.

Замечание 1. В соответствии с результатами [2] были найдены структуры 18 представителей сбалансированных геометрических типов булевых функций от четырёх переменных с номерами

$$\begin{array}{cccccc} 8.1.1.1, & 8.1.2.1, & 8.1.5.1, & 8.1.16.1, & 8.1.29.1, & 8.2.1.1, \\ 8.2.9.2, & 8.2.11.1, & 8.2.13.1, & 8.2.17.1, & 8.2.20.1, & 8.2.21.1, \\ 8.3.4.1, & 8.3.5.1, & 8.4.2.1, & 8.4.3.1, & 8.5.1.1, & 8.8.1.1. \end{array}$$

Непосредственной проверкой условий теоремы 2 установлено, что геометрические типы с номерами

8.1.1.1, 8.2.1.1, 8.2.13.1, 8.2.17.1, 8.2.20.1, 8.2.21.1,
8.3.4.1, 8.3.5.1, 8.4.2.1, 8.4.3.1, 8.5.1.1, 8.8.1.1

принадлежат классу BAT_4^2 .

ЛИТЕРАТУРА

1. Сошин Д. А. Построение подстановок на основе пороговых функций многозначной логики // Прикладная дискретная математика. 2016. № 2(32). С. 20–32.
2. Сошин Д. А. Задание подстановок алгоритмов блочного шифрования Магма и 2-ГОСТ с помощью алгебраических пороговых функций // Прикладная дискретная математика 2016. № 3(33). С. 53–66.
3. Сошин Д. А. Конструктивный метод синтеза сбалансированных k -значных алгебраических пороговых функций // Comp. Nanotechnol. 2015. No. 4. P. 31–36.
4. Глухов М. М., Елизаров В. П., Нечаев А. А. Алгебра. СПб.: Лань, 2015. 608 с.
5. Никонов В. Г., Никонов Н. В. Особенности пороговых представлений k -значных функций // Труды по дискретной математике. М.: Физматлит, 2008. Т. 11. № 1. С. 60–85.
6. Кнут Д. Э. Искусство программирования. Т. 2. Получисленные алгоритмы. 3-е изд. М.: Вильямс, 2007. 832 с.

REFERENCES

1. Soshin D. A. Postroenie podstanovok na osnove porogovykh funktsiy mnogoznachnoy logiki [Constructing substitutions on the basis of threshold functions of multivalued logic]. Prikladnaya Diskretnaya Matematika, 2016, no. 2(32), pp. 20–32. (in Russian)
2. Soshin D. A. Zadanie podstanovok algoritmov blochnogo shifrovania Magma i 2-GOST s pomochiu algebraicheskikh porogovykh funktsiy [The implementation of Magma and 2-GOST block cipher substitutions by algebraic threshold functions]. Prikladnaya Diskretnaya Matematika, 2016, no. 3(33), pp. 53–66. (in Russian)
3. Soshin D. A. Konstruktivnyy metod sinteza sbalansirovannykh k -znachnykh algebraicheskikh porogovykh funktsiy [The constructive method for synthesis of balanced k -valued algebraic threshold functions]. Comp. Nanotechnol., 2015, no. 4, pp. 31–36. (in Russian)
4. Glukhov M. M., Elizarov V. P., and Nechaev A. A. Algebra [Algebra]. St. Petersburg, Lan' Publ., 2015. 608 p. (in Russian)
5. Nikonov V. G. and Nikonov N. V. Osobennosti porogovykh predstavleniy k -znachnykh functions [Peculiarities of threshold representations of k -valued functions]. Proc. Discr. Math., Moscow, Fizmatlit Publ., 2008, vol. 11, no. 1, pp. 60–85. (in Russian)
6. Knuth D. E. The Art of Computer Programming. Vol. 2. Seminumerical Algorithms, 3rd Ed. Massachusetts, Addison-Wesley, 1997. 762 p.