2. Расстояние Хэмминга между функциями

Изучим теперь для двух функций f и g из разных классов величину $\rho(f, g)$.

Утверждение 2. Пусть отображение ψ_1 задано равенством (1) и $\psi_2(a) = a_{n-1}$, $f = f_{u,\psi_1}$, $g = f_{u,\psi_2}$. Тогда

$$2^{m-k+1} - \frac{(2^n-1)(2^{n-1}-1)}{3}2^{m/2-k+2} \leqslant \rho(f,g) \leqslant 2^{m-k+1} + \frac{(2^n-1)(2^{n-1}-1)}{3}2^{m/2-k+2}.$$

Обозначим через ε_1, ε_2 соответственно левую и правую части неравенства из утверждения 2.

Утверждение 3. Пусть отображение ψ_1 задано равенством (1), $\psi_2(a) = a_{n-1} \oplus \oplus a_{n-2} \oplus a_{n-3} \oplus \ldots \oplus a_{n-k}$, где $k \in \{3, \ldots, n\}$, $f = f_{u,\psi_1}$, $g = f_{u,\psi_2}$. Тогда

$$\begin{array}{ll} (2^{k-2}+1)\varepsilon_1 \leqslant \rho(f,g) \leqslant (2^{k-2}+1)\varepsilon_2 & \text{для нечётного } k; \\ (2^{k-2}-1)\varepsilon_1 \leqslant \rho(f,g) \leqslant (2^{k-2}-1)\varepsilon_2 & \text{для чётного } k. \end{array}$$

Заключение

В данной работе для класса булевых функций, построенных на основе двоичных разрядных последовательностей линейных рекуррент над кольцом $\mathbb{Z}_{2^n}$, получены оценки для веса функций, нелинейности и расстояний между функциями. Отметим, что ранее в работах [2–4] аналогичные вопросы были рассмотрены только для случая, когда ψ — линейное отображение по всем двоичным разрядам.

ЛИТЕРАТУРА

1. *Нечаев А. А.* Цикловые типы линейных подстановок над конечными коммутативными кольцами // Математический сборник. 1993. Т. 184. № 3. С. 21–56.
2. *Быльков Д. Н., Камловский О. В.* Параметры булевых функций, построенных с использованием старших координатных последовательностей линейных рекуррент // Математические вопросы криптографии. 2012. Т. 3. № 4. С. 25–53.
3. *Камловский О. В.* Нелинейность одного класса булевых функций, построенных с использованием двоичных разрядных последовательностей линейных рекуррент над кольцом $\mathbb{Z}_{2^n}$ // Математические вопросы криптографии. 2016. Т. 7. № 3. С. 29–46.
4. *Быльков Д. Н.* Об одном классе булевых функций, построенных с использованием старших разрядных последовательностей линейных рекуррент // Прикладная дискретная математика. Приложение. 2014. № 7. С. 59–60.

UDC 519.7 DOI 10.17223/2226308X/12/24

PROPERTIES OF ASSOCIATED BOOLEAN FUNCTIONS OF QUADRATIC APN FUNCTIONS[1]

A. A. Gorodilova

For a function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$, it is defined the associated Boolean function γ_F in $2n$ variables as follows: $\gamma_F(a, b) = 1$ if $a \neq \mathbf{0}$ and equation $F(x) + F(x + a) = b$ has solutions. A vectorial Boolean function F from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ is called almost perfect nonlinear (APN) if equation $F(x) + F(x + a) = b$ has at most 2 solutions for all vectors $a, b \in \mathbb{F}_2^n$, where a is nonzero. In case when F is a quadratic APN function its associated function has the form $\gamma_F(a, b) = \Phi_F(a) \cdot b + \varphi_F(a) + 1$ for appropriate

[1]The work is supported by RFBR, projects no. 18-31-00479 and 18-07-01394.

functions $\Phi_F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ and $\varphi_F : \mathbb{F}_2^n \to \mathbb{F}_2$. We study properties of functions Φ_F and φ_F, in particular their degrees.

Keywords: *APN functions, associated Boolean functions, differential equivalence.*

1. Introduction

Let $\mathbb{F}_2^n$ be the n-dimensional vector space over $\mathbb{F}_2$. Let $\mathbf{0}$ denote the zero vector of $\mathbb{F}_2^n$; $x \cdot y = x_1y_1 + \ldots + x_ny_n$ denote the *inner product* of vectors $x, y \in \mathbb{F}_2^n$. A set $M \subseteq \mathbb{F}_2^n$ form a *linear subspace* if $x + y \in M$ for any $x, y \in M$. Here $+$ denotes the coordinate-wise sum of vectors modulo 2. A mapping $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is a *Boolean function* of n variables. The *Hamming weight* of f is the number $\mathrm{wt}(f) = |\{x \in \mathbb{F}_2^n : \ f(x) = 1\}|$.

We consider a *vectorial Boolean function* $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$, $F = (f_1, \ldots, f_n)$, where f_i is the i-th *coordinate* function of F; a function $v \cdot F$ is a *component* function of F for a nonzero $v \in \mathbb{F}_2^n$. The *algebraic normal form* (ANF) of F is the following unique representation: $F(x) = \sum\limits_{I \in \mathcal{P}(N)} a_I \big(\prod\limits_{i \in I} x_i \big)$, where $\mathcal{P}(N)$ is the power set of $N = \{1, \ldots, n\}$ and each a_I belongs to $\mathbb{F}_2^n$. The *algebraic degree* of F is degree of its ANF: $\deg(F) = \max\{|I| : a_I \neq \mathbf{0}, I \in \mathcal{P}(N)\}$. Functions of algebraic degree 2 are called *quadratic*.

A function F from $\mathbb{F}_2^n$ to itself is called *almost perfect nonlinear* (APN) (according to K. Nyberg [1]) if for any $a, b \in \mathbb{F}_2^n$, $a \neq \mathbf{0}$, equation $F(x) + F(x + a) = b$ has at most 2 solutions. APN functions are of special interest for using as S-boxes in block ciphers due to their optimal differential characteristics. Despite to fact that APN functions are intensively studied (see, for example, survey [2] of M. M. Glukhov), there are a lot of open problems on finding new constructions, classifications, etc.

In [3] C. Carlet, P. Charpin, and V. Zinoviev introduced the *associated Boolean function* $\gamma_F(a, b)$ in $2n$ variables for a given vectorial Boolean function F from $\mathbb{F}_2^n$ to itself. It takes value 1 if $a \neq \mathbf{0}$ and equation $F(x) + F(x + a) = b$ has solutions. It is easy to see that F is APN if and only if $\mathrm{wt}(\gamma_F) = 2^{2n-1} - 2^{n-1}$.

Two functions are called *differentially equivalent* [4] (or *γ-equivalent* according to K. Boura et al. [5]) if their associated functions coincide. The problem of describing the differential equivalence class of an APN function remains open even for quadratic case. That is why we are interested in obtaining some properties of γ_F. We will focus on quadratic APN functions.

Let F be a quadratic APN function. Then γ_F is of the form $\gamma_F(a, b) = \Phi_F(a) \cdot b + \varphi_F(a) + 1$, where $\Phi_F : \mathbb{F}_2^n \to \mathbb{F}_2^n$, $\varphi_F : \mathbb{F}_2^n \to \mathbb{F}_2$ are uniquely defined from

$$\{F(x) + F(x + a) : x \in \mathbb{F}_2^n\} = \{y \in \mathbb{F}_2^n : \ \Phi_F(a) \cdot y = \varphi_F(a)\}$$

for all $a \neq \mathbf{0}$ and $\Phi_F(\mathbf{0}) = \mathbf{0}$, $\varphi_F(\mathbf{0}) = 1$.

2. Properties of Φ_F and φ_F

In this section, we summarize known results and present new ones about properties of Φ_F and φ_F. As it usually happens the cases of even and odd number of variables are different.

P r o p e r t y 1: the image set of Φ_F.

Theorem 1 [3, 6]. Let F be a quadratic APN function in n variables.

1) If n is odd, then Φ_F is a permutation.
2) If n is even, then the preimage Φ_F of any nonzero vector is a linear subspace of even dimension together with the zero vector.

Corollary 1. Let F be a quadratic APN function. Then Φ_F takes an odd number of distinct nonzero values.

P r o p e r t y 2: the degree of Φ_F.

Theorem 2 [4]. Let F be a quadratic APN function in n variables, $n \geqslant 3$, n is odd. Then $\deg(\Phi_F) \leqslant n-2$.

Theorem 3. Let F be a quadratic APN function in n variables, $n \geqslant 4$, n is even. Then each coordinate function of Φ_F is represented as $(\Phi_F)_i(x) = f_i(x) + \lambda_i\big(x_2 \dots x_n + x_1x_3 \dots x_n + \dots + x_1x_2 \dots x_{n-1} + x_1 \dots x_n\big)$, where $\deg(f_i) \leqslant n-2$ and $\lambda_i \in \mathbb{F}_2$.

Remark 1. For all known quadratic APN functions in not more than 11 variables, we computationally verified that

— for even n, the case $\deg((\Phi_F)_i) = n$ is not realized;
— any component function of Φ_F has degree exactly $n-2$.

Based on computational experiments we can formulate the following

Hypothesis 1. Let F be a quadratic APN function in n variables, $n \geqslant 3$. Then $\deg(v \cdot \Phi_F) = n-2$ for any nonzero $v \in \mathbb{F}_2^n$.

P r o p e r t y 3: the degree of φ_F.

Proposition 1. Let F be a quadratic APN function in n variables, n is even. Then $\deg(\varphi_F) = n$, or, equivalently, $\mathrm{wt}(\varphi_F)$ is odd.

The case of odd n remains open, but based on our computational experiments we can formulate the following

Hypothesis 2. Let F be a quadratic APN function in n variables, n is odd. Then $\deg(\varphi_F) < n$, or, equivalently, $\mathrm{wt}(\varphi_F)$ is even.

REFERENCES

1. *Nyberg K.* Differentially uniform mappings for cryptography. EUROCRYPT'93, LNCS, 1994, vol. 765, pp. 55–64.
2. *Glukhov M. M.* O priblizhenii diskretnykh funktsiy lineynymi funktsiyami [On the approximation of discrete functions by linear functions]. Matematicheskie Voprosy Kriptografii, 2016, vol. 7, no. 4, pp. 29–50. (in Russian)
3. *Carlet C., Charpin P., and Zinoviev V.* Codes, bent functions and permutations suitable for DES-like cryptosystems. Designs, Codes and Cryptography, 1998, vol. 15, iss. 2, pp. 125–156.
4. *Gorodilova A.* On the differential equivalence of APN functions. Cryptography and Communications, 2019. `https://link.springer.com/article/10.1007/s12095-018-0329-y`.
5. *Boura C., Canteaut A., Jean J., and Suder V.* Two notions of differential equivalence on S-boxes. Designs, Codes and Cryptography, 2019, vol. 87, iss. 2–3, pp. 185–202.
6. *Gorodilova A.* Lineynyy spektr kvadratichnykh APN-funktsiy [The linear spectrum of quadratic APN functions]. Prikladnaya Diskretnaya Matematika, 2016, no 4(34), pp. 5–16. (in Russian)