On values of vectorial Boolean functions and related problems in APN functions*

George Shushuev
Sobolev Institute of Mathematics, Novosibirsk, Russia
Novosibirsk State University, Novosibirsk, Russia

E-mail: shushuev@math.nsc.ru

Abstract. In this paper we prove that there are only differential 4-uniform functions which are on distance 1 from an APN function. Also we prove that there are no APN functions of distance 1 from another APN functions up to dimension 5. We determine some properties of the set of values of an arbitrary vectorial Boolean function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ in connection to the set of values of its derivatives. These results are connected to several open question concerning metric properties of APN functions.

Keywords: Vectorial Boolean function, APN function, differentially δ-uniform function.

1 Introduction

In this paper we deal with vectorial Boolean functions $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ that are also known as substitution boxes. Substitution boxes play a central role in the robustness of block ciphers in symmetric cryptography. The notion of differentially δ-uniform functions was introduced by K. Nyberg [1] in 1994.

A vectorial Boolean function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is called *differentially δ-uniform* if for any non-zero $a \in \mathbb{F}_2^n$ and for any $b \in \mathbb{F}_2^n$ the equation $F(x) \oplus F(x \oplus a) = b$ has at most δ solutions, where δ is a positive integer. *An order* of differential uniformity of a function F is the minimal possible δ such that F is differential δ-uniform.

The fewer the order of differential uniformity of substitution box that using in a cipher, the better the resistance of this cipher to differential attack [2]. The minimal possible value of δ is two. If $\delta = 2$, then a differentially δ-uniform function is called *almost perfect nonlinear* (APN) function. Classification of APN functions up to dimension five is given in [3], constructions of APN and differentially 4-uniform functions are presented in [4, 5]. Surveys of cryptographic functions can be found in [6, 7, 8]. In [9, 10] we studied distance between distinct APN functions.

In this paper we prove that there are only differential 4-uniform functions which are on distance 1 from an APN function and experimentally prove that the minimal distance between distinct APN functions up to dimestion 5 is equal to 2. Also we determine some properties of the set of values of an arbitrary vectorial Boolean function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ in connection to the set of values of its derivatives. The obtained results will help us with respect to metrical properties of the class of APN functions.

*The author was supported by the Russian Foundation for Basic Research (project no. 15-31-20635).

2 Preliminaries

For a vectorial Boolean function F and for any vector $a \in \mathbb{F}_2^n$ it is defined the set

$$B_a(F) = \{F(x) \oplus F(x \oplus a) \mid x \in \mathbb{F}_2^n\}.$$

The maximal possible cardinality of the set $B_a(F)$ is equal to 2^{n-1}. In particular, if it holds $|B_a(F)| = 2^{n-1}$ for any non-zero vector a, then the function F is an APN function, but if it holds $|B_a(F)| = 2^{n-1} - 1$ then the function F is a differential 4-uniformity function.

Let the sum of a vector $x \in \mathbb{F}_2^n$ and a set $A \subseteq \mathbb{F}_2^n$ be the shift of the set A:

$$x \oplus A = \{x \oplus a | a \in A\}.$$

Let the sum of two sets $A \subseteq \mathbb{F}_2^n$ and $B \subseteq \mathbb{F}_2^n$ be the set of all pairwise sums of elements of these sets,

$$A \oplus B = \{a \oplus b \mid a \in A, b \in B\}.$$

The set of all values of a vectorial Boolean function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is the *image* of the function F. Denote the image of a function F by $im(F)$.

A *distance* between vectorial Boolean functions F and G is called cardinality of the set $\{x \in \mathbb{F}_2^n \mid F(x) \neq G(x)\}$.

3 Vectorial Boolean functions on distance 1 from an APN function

Statement 1. *Let F be APN function of n variables, then on distance one from F there are only differential 4-uniform functions.*

Proof. Let F is APN function. So for all non-zero vector $a \in \mathbb{F}_2^n$ we have $|B_a(F)| = 2^{n-1}$. Consider the function G which coincide with F in each vectors except one $x' \in \mathbb{F}_2^n$. Let

$$\overline{B_a}(G) = \{G(x) \oplus G(x \oplus a) \mid x \in \mathbb{F}_2^n \backslash \{x', x' \oplus a\}\}.$$

For all non-zero vector $a \in \mathbb{F}_2^n$ the set $\overline{B_a}(F)$ coincide with $\overline{B_a}(G)$ and we have the equation $|\overline{B_a}(G)| = 2^{n-1} - 1$.

Note that $B_a(G) = \overline{B_a}(G) \cup \{G(x') \oplus G(x' \oplus a)\}$. Then for all values $G(x')$ (including one non equal to $F(x')$) and for all non-zero vector $a \in \mathbb{F}_2^n$ we have $|B_a(G)| \geq |\overline{B_a}(G)| = 2^{n-1} - 1$, i. e. function G is differentially 4-uniform. □

Since APN functions are differentially 4-uniform then statement 1 does not exclude the possibility of existence of APN functions on distance one from each other. An exception of this is equal to the fact that all functions distanced one from an APN function possess differentially uniformity of order 4.

We consider hypothesis that means that unite of shifted derivatives of an APN function coincides with the whole space $\mathbb{F}_2^n$. Further we will prove that this hypothesis is equivalent to the fact that there is no APN functions on distance 1 from any APN function.

Hypothesis 1. *If F is APN function in n variables, then the following expression is true:*

$$\bigcup_{a \in \mathbb{F}_2^n, a \neq 0} (B_a(F) \oplus F(x' \oplus a)) = \mathbb{F}_2^n \quad \forall x' \in \mathbb{F}_2^n. \tag{1}$$

Theorem 1. *The hypothesis 1 is true if and only if there are only functions with differential uniformity of order 4 on distance one from APN functions.*

Proof. Let a function F is an APN function. According to the statement 1 a function G coinciding with F in each vectors but one $x' \in \mathbb{F}_2^n$ is differentially 4-uniform.

We shall show that if the hypothesis 1 is true, then for any arbitrary value of the function G on the vector x', which is not equal to $F(x')$, function G is of differential uniformity order equals 4. A necessary and sufficient conduction for this to be true is existence of a vector $a \in \mathbb{F}_2^n$ for which the equality $|B_a(G)| = |\overline{B_a}(G)|$ is true. This requires that there is a sum $G(x') \oplus G(x' \oplus a)$ belonging to the set $\overline{B_a}(G)$.

Let $G(x') = v$. So the theorem is true if and only if the next statement is true:

$$\forall x' \in \mathbb{F}_2^n \;\; \forall v \in \mathbb{F}_2^n \backslash \{F(x')\} \;\; \exists a \in \mathbb{F}_2^n \backslash \{0\} : v \oplus G(x' \oplus a) \in \overline{B_a}(G).$$

Note that $B_a(F)$ is equal to $\overline{B_a}(G) \cup \{F(x') \oplus F(x' \oplus a)\}$ and for any vector v other than $F(x')$ the sum $v \oplus G(x' \oplus a)$ belongs $\overline{B_a}(G)$ if and only if $v \oplus F(x' \oplus a)$ belongs to $B_a(F)$. So we shall prove the next expression:

$$\forall x' \in \mathbb{F}_2^n \;\; \forall v \in \mathbb{F}_2^n \backslash \{F(x')\} \;\; \exists a \in \mathbb{F}_2^n \backslash \{0\} : v \oplus F(x' \oplus a) \in B_a(F).$$

Since $F(x') \oplus F(x' \oplus a)$ belongs to the set $B_a(F)$ by the definition, then the expression above is always true for any vector v equals to $F(x')$. So we can represent the statement to prove as follows:

$$\forall x' \in \mathbb{F}_2^n \;\; \forall v \in \mathbb{F}_2^n \;\; \exists a \in \mathbb{F}_2^n \backslash \{0\} : v \oplus F(x' \oplus a) \in B_a(F).$$

Let us express the vector v

$$\forall x' \in \mathbb{F}_2^n \;\; \forall v \in \mathbb{F}_2^n \;\; \exists a \in \mathbb{F}_2^n \backslash \{0\} : v \in B_a(F) \oplus F(x' \oplus a).$$

Now we obviously have that the statement to prove is represented in a convenient way:

$$\bigcup_{a \in \mathbb{F}_2^n, a \neq 0} (B_a(F) \oplus F(x' \oplus a)) = \mathbb{F}_2^n \quad \forall x' \in \mathbb{F}_2^n.$$

So there is only function with differential uniformity of order 4 on distance 1 from APN functions if and only if hypothesis 1 is true. □

As the corollary the hypothesis 1 is true if and only if there is no APN functions on distance 1 from an APN function.

Note that there are APN functions on distance 2 from an APN function. For instance functions $F = (0, 0, 1, 2, 1, 4, 2, 4)$ and $G = (0, 0, 1, 2, 1, 4, 4, 2)$ differ in the two last vectors and both are APN functions. Finally note that there are not only APN functions correspond to expression (1). For instance function $H = (0, 1, 15, 0, 12, 2, 4, 6, 6, 4, 6, 3, 8, 12, 11, 1)$ is function with differential uniformity of order 4 and (1) is true for H.

4 Distance between APN functions of small dimensions

Statement 1. *If vectorial Boolean functions F and G are EA-equivalent and (1) is true for F then (1) is true for G.*

Proof. We shall prove that if functions F and G are EA-equivalent then function $G = A_1 \circ F \circ A_2 \oplus A$ satisfies the equation (1) if and only if F satisfies the equation (1). It is known that

$$B_a(G) = A_1(B_{A_2(a)\oplus A_2(0)}(F)) \oplus A_1(0) \oplus A(a) \oplus A(0).$$

Let consider

$$G(x' \oplus a) = A_1(F(A_2(x' \oplus a)) \oplus A(x' \oplus a)) =$$
$$A_1(F(A_2(x') \oplus A_2(a) \oplus A_2(0)) \oplus A(x') \oplus A(a) \oplus A(0))).$$

Summing and reducing like terms we obtain

$$B_a(G) \oplus G(x' \oplus a) =$$
$$A_1(B_{A_2(a)\oplus A_2(0)}(F) \oplus F(A_2(x') \oplus A_2(a) \oplus A_2(0)) \oplus A_1(0) \oplus A(x') =$$
$$A_1(B_b(F) \oplus F(y' \oplus b)) \oplus const.$$

Remark that since A_2 is a permutation we have $y' = A_2(x')$ and $b = A_2(a) \oplus A_2(0)$ take any value from $\mathbb{F}_2^n$ if x' and a take any value from $\mathbb{F}_2^n$. Also we see that b is equal to zero if and only if a is equal to zero. Since A_1 is a permutation we see that for any y' of the set $\mathbb{F}_2^n$ we have

$$\bigcup_{b\in\mathbb{F}_2^n, b\neq 0} (B_b(G) \oplus F(y' \oplus b)) = \bigcup_{b\in\mathbb{F}_2^n, b\neq 0} (A_1(B_b(F) \oplus F(y' \oplus b)) \oplus const) =$$
$$const \oplus \bigcup_{b\in\mathbb{F}_2^n, b\neq 0} (A_1(B_b(F) \oplus F(y' \oplus b))) = \mathbb{F}_2^n.$$

□

Since by [3] classes of EA-equivalence of APN functions that cover all APN functions up to dimension 5 and classes of EA-equivalence that cover all quadratic APN functions in dimension 6 are known, we experimentally obtain the next statement by checking representatives of corresponding EA-equivalence classes:

Statement 2. *Hypothesis 1 is true for APN functions up to dimension 5, for all quadratic APN functions of dimension 6 and some EA-equivalence classes of APN functions in dimension 7 and 8 from the article [5].*

As the corollary there are no APN functions on distance 1 from an another APN function up to dimension 5.

5 Sum of vectorial Boolean function's values

In this section we determine requirements for an image of vectorial Boolean function which it should requires to the set of all derivatives coincides with the whole space $\mathbb{F}_2^n$.

Lemma 1. *Let $A, B \subseteq \mathbb{F}_2^n$, $|A| \geq 2^{n-1}$ and $|B| \geq 2^{n-1} + 1$. Then $A \oplus B = \mathbb{F}_2^n$.*

Proof. Since $|A| \geq 2^{n-1}$, for all $x \in \mathbb{F}_2^n$ it holds $|x \oplus A| \geq 2^{n-1}$. Suppose $(x \oplus A) \cap B = \varnothing$. Hence $x \oplus A \subseteq \mathbb{F}_2^n \backslash B$ but $|\mathbb{F}_2^n \backslash B| \leq 2^{n-1} - 1$. We obtain a contradiction, therefore for any $x \in \mathbb{F}_2^n$ it holds that $(x \oplus A) \cap B \neq \varnothing$ hence for any $x \in \mathbb{F}_2^n$ there exist $a \in A, b \in B$ such that $x \oplus a = b$, in other words, $x = a \oplus b$. □

Theorem 2. *Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a vectorial Boolean function,*

1. *If $2^{n-1} < |im(F)| < 2^n$, then*

$$\bigcup_{a \in \mathbb{F}_2^n, a \neq 0} B_a(F) = \mathbb{F}_2^n.$$

2. *If $|im(F)| = 2^n$, i.e. F is one-to-one function, then*

$$\bigcup_{a \in \mathbb{F}_2^n, a \neq 0} B_a(F) = \mathbb{F}_2^n \backslash \{0\}.$$

Proof. Let

$$\bigcup_{a \in \mathbb{F}_2^n, a \neq 0} B_a(F) = M.$$

Firstly prove that it holds the equality $\bigcup_{a \in \mathbb{F}_2^n} B_a(F) = \mathbb{F}_2^n$ and then consider the union without $B_0(F)$. By the definition,

$$M \cup B_0(F) = \bigcup_{a \in \mathbb{F}_2^n} B_a(F) = \bigcup_{x,a \in \mathbb{F}_2^n} \{F(x) \oplus F(x \oplus a)\}.$$

Since the union over all $x, a \in \mathbb{F}_2^n$ is considered, then for every x sum $x \oplus a$ can take any value from $\mathbb{F}_2^n$ and that is why this union is equal to the sum of function's images, and by the Lemma is equal to $\mathbb{F}_2^n$:

$$\bigcup_{x,a \in \mathbb{F}_2^n} \{F(x) \oplus F(x \oplus a)\} = im(F) \oplus im(F) = \mathbb{F}_2^n.$$

Now we remove $B_0(F)$ from the union. We can do it because $B_0(F) = F(x) \oplus F(x \oplus 0)$ is zero for all x. The set M does not contain zero if and only if for any $x, a \in \mathbb{F}_2^n$ such that a is not equal to zero, it follows that $F(x) \neq F(x \oplus a)$, which is equivalent that F is a one-to-one function. From the other hand, if F is not one-to-one function then for any $x \in \mathbb{F}_2^n$ there exists non-zero vector $a \in \mathbb{F}_2^n$ such that $F(x) = F(x \oplus a)$ and zero is contained in M. □

The following example shows us that the condition on cardinality of function's image cannot be reduced. There is a function F such that $|im(F)| = 2^{n-1}$ and $\bigcup_{a \in \mathbb{F}_2^n, a \neq 0} B_a(F) \neq \mathbb{F}_2^n$. For example APN function $F : \mathbb{F}_2^3 \to \mathbb{F}_2^3$ given by the following vector of values $(0, 0, 1, 2, 1, 4, 2, 4)$. In this case $|im(F)| = 2^2$ and

$$\bigcup_{a \in \mathbb{F}_2^n, a \neq 0} B_a(F) = \mathbb{F}_2^n \backslash \{7\}.$$

References

[1] Nyberg K., Differentially uniform mapping for cryptography // EUROCRYPT'93. — 1994 — P. 55–64.

[2] Biham E., Shamir A., Differential cryptoanalysis of DES-like cryptosystems // J. Cryptology, 1991, 4 — P. 3–72.

[3] Brinkmann M., Leander G., On the classification of APN functions up to dimension five // Designs, Codes and Cryptography., 2008, V. 49 — P. 273 – 288.

[4] Carlet C., More constructions of APN and differentially 4-uniform functions by concatenation // Sci. China Math., 2013, V. 56(7) — P. 1373 – 1384.

[5] Yu Y., Wang M., Li Y., A matrix approach for constructing quadratic APN functions // Des. Codes Cryptogr., 2014, V. 73 — P. 587 – 600.

[6] Glukhov M. M., Planar mappings of finite fields and their generalizations // Presentation for the conference "Algebra and Logic: theory and applications", (Krasnoyarsk, Russia. July 21–27, 2013) in Russian.

[7] Budaghyan L., Construction and Analysis of Cryptographic Functions: Habilitation Thesis. // University of Paris 8. Sept. 2013. 192 pages.

[8] Carlet C., Vectorial Boolean functions for cryptography // Boolean Models and Methods in Mathematics, Computer Science, and Engineering / Eds. P. Hammer, Y. Crama. Cambridge Univ. Press, 2010. Chapter 9. P. 398–472.

[9] Shushuev G.I., Vectorial Boolean functions on distance one from APN functions // Prikl. Diskr. Mat. Suppl., 2014, 7. — P. 36–37.

[10] Shushuev G.I., On properties of the set of values of an arbitrary vectorial Boolean functions // Prikl. Diskr. Mat. Suppl., 2015, 8. — P. 51–53.