A NOTE ON THE PROPERTIES OF ASSOCIATED BOOLEAN FUNCTIONS OF QUADRATIC APN FUNCTIONS[1]

A. A. Gorodilova

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

E-mail: gorodilova@math.nsc.ru

Let F be a quadratic APN function in n variables. The associated Boolean function γ_F in $2n$ variables ($\gamma_F(a,b) = 1$ if $a \neq \mathbf{0}$ and equation $F(x) + F(x+a) = b$ has solutions) has the form $\gamma_F(a,b) = \Phi_F(a) \cdot b + \varphi_F(a) + 1$ for appropriate functions $\Phi_F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ and $\varphi_F : \mathbb{F}_2^n \to \mathbb{F}_2$. We summarize the known results and prove new ones regarding properties of Φ_F and φ_F. For instance, we prove that degree of Φ_F is either n or less or equal to $n - 2$. Based on computation experiments, we formulate a conjecture that degree of any component function of Φ_F is $n - 2$. We show that this conjecture is based on two other conjectures of independent interest.

Keywords: *a quadratic APN function, the associated Boolean function, degree of a function.*

Introduction

Let $\mathbb{F}_2^n$ be the n-dimensional vector space over $\mathbb{F}_2$. Let $\mathbf{0}$ denote the zero vector of $\mathbb{F}_2^n$ and $\mathbf{1}$ denote the vector with all 1s. By «+» we denote the coordinate-wise sum modulo 2 for vectors from $\mathbb{F}_2^n$. Let $x \cdot y = x_1 y_1 + \ldots + x_n y_n$ denote the *inner product* of vectors $x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n) \in \mathbb{F}_2^n$; $x \preceq y$ if $x_i \leqslant y_i$ for all $i = 1, \ldots, n$; and $\mathrm{wt}(x) = \sum_{i=1}^{n} x_i$ denote the *Hamming weight* of $x \in \mathbb{F}_2^n$. A set $M \subseteq \mathbb{F}_2^n$ forms a *linear subspace* if $x + y \in M$ for any $x, y \in M$; the *dimension* of M, $\dim(M)$, is the maximal number of linearly independent over $\mathbb{F}_2$ vectors from M. We consider *vectorial Boolean functions* $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$, $F = (f_1, \ldots, f_m)$, where $f_i : \mathbb{F}_2^n \to \mathbb{F}_2$, $i = 1, \ldots, m$, is a *coordinate* function of F. The *algebraic normal form* (ANF) of F is the following unique representation: $F(x) = \sum_{I \in \mathcal{P}(N)} a_I \left(\prod_{i \in I} x_i \right)$, where $\mathcal{P}(N)$ is the power set of $N = \{1, \ldots, n\}$ and $a_I \in \mathbb{F}_2^m$. The *algebraic degree* of F is degree of its ANF: $\deg(F) = \max\{|I| : a_I \neq \mathbf{0}, I \in \mathcal{P}(N)\}$. Function of algebraic degree at most 1 are called *affine* (they are *linear* in case of $F(\mathbf{0}) = \mathbf{0}$). Functions of algebraic degree 2 are called *quadratic*. The *Walsh transform* $W_f : \mathbb{F}_2^n \to \mathbb{Z}$ of a Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ is defined as $W_f(u) = \sum_{x \in \mathbb{F}_2^n} (-1)^{f(x)+u \cdot x}$. For F the *Walsh spectrum* consists of all *Walsh coefficients* $W_{F_v}(u)$, $u \in \mathbb{F}_2^n$, $v \in \mathbb{F}_2^m$, $v \neq \mathbf{0}$, where $F_v = v \cdot F$ is a *component* Boolean function of F.

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 two solutions. APN functions are of special interest for using as S-boxes in block ciphers

---

due to their optimal differential characteristics. Despite the fact that APN functions are intensively studied (see, for example, the book of L. Budaghyan [2], surveys of A. Pott [3], M. M. Glukhov [4], and M. E. Tuzhilin [5]), there are a lot of open problems on finding new constructions, classifications, etc.

In [6], C. Carlet, P. Charpin, and V. Zinoviev introduced the *associated Boolean function* $\gamma_F : \mathbb{F}_2^{2n} \to \mathbb{F}_2$ for a given vectorial Boolean function F from $\mathbb{F}_2^n$ to itself; $\gamma_F(a, b) = 1$ if and only if $a \neq \mathbf{0}$ and equation $F(x) + F(x + a) = b$ has solutions.

Two functions are called *differentially equivalent* [7] (or γ-equivalent according to K. Boura et al. [8]), if their associated Boolean 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 the set $B_a(F) = \{F(x) + F(x + a) : x \in \mathbb{F}_2^n\}$ is a linear subspace of dimension $n - 1$ or its complement for a nonzero $a \in \mathbb{F}_2^n$. Using this fact, γ_F can be uniquely represented in 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 defined from $B_a(F) = \{y \in \mathbb{F}_2^n : \Phi_F(a) \cdot y = \varphi_F(a)\}$ for all $a \neq \mathbf{0}$; and $\Phi_F(\mathbf{0}) = \mathbf{0}$, $\varphi_F(\mathbf{0}) = 1$. Note that $B_a(F)$ is a linear subspace if and only if $\varphi_F(a) = 0$. It is easy to see that $(F(x) + F(x + a) + F(a) + F(\mathbf{0})) \cdot \Phi_F(a) = \mathbf{0}$ for all $x \in \mathbb{F}_2^n$ by definition.

In this paper we study the properties of functions Φ_F and φ_F.

1. 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.

1.1. The image set of Φ_F

According to [9], let us denote $A_v^F = \{a \in \mathbb{F}_2^n : \Phi_F(a) = v\}$.

Theorem 1 [6, 9]. 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.

Note that state 1 in Theorem 1 means also that γ_F is a bent function of Maiorana—McFarland type (readers may find details regarding bent functions in [10]).

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

Proof. By definition of Φ_F, we have $\Phi_F(\mathbf{0}) = \mathbf{0}$.

If n is odd, then Φ_F is a permutation [6]. Hence, the proposition holds.

Let n be even. It is known [9] that the preimage set $A_v^F = \{x \in \mathbb{F}_2^n : \Phi_F(x) = v\}$ for any nonzero $v \in \mathbb{F}_2^n$ represents a linear subspace of even dimension together with the zero vector. Let $\Phi_F \in \{\mathbf{0}, v_1, \ldots, v_m\}$, where v_i, $i = 1, \ldots, m$, are pairwise distinct nonzero vectors. We need to prove that m is odd. We have

$$2^n - 1 = |A_{v_1}^F| + \ldots + |A_{v_m}^F| = 2^{\lambda_1} - 1 + \ldots + 2^{\lambda_m} - 1 = 2^{\lambda_1} + \ldots + 2^{\lambda_m} - m,$$

where λ_i, $i = 1, \ldots, m$, are nonzero even numbers. Since $2^n - 1$ is odd, then m is also odd. ∎

1.2. 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.

Proof. It is known [9] that $A_v^F \cup \{\mathbf{0}\}$ is a linear subspace of even dimension if n is even for any nonzero $v \in \mathbb{F}_2^n$. Also [9], there exists $c_v \in \mathbb{F}_2^n$ such that $\varphi_F|_{A_v^F} = c_v \cdot x|_{A_v^F}$. Hence, $\mathrm{wt}(\varphi_F|_{A_v^F})$ is an even number equal to 0 or $2^{\dim(A_v^F \cup \{\mathbf{0}\})-1}$ for any nonzero v and $\varphi_F(\mathbf{0}) = 1$ by definition. Thus, $\mathrm{wt}(\varphi_F)$ is odd. It is widely known that $\mathrm{wt}(f)$ is odd if and only if $\deg(f) = n$ for any Boolean function in n variables. ∎

The case of odd n remains open. Based on our computational experiments for all known quadratic APN functions of not more than 11 variables, we can formulate the following

Conjecture 1. 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.

1.3. The degree of Φ_F

Theorem 2 [7]. Let F be a quadratic APN function in n variables, $n \geqslant 3$, n is odd. Then $\deg(\Phi_F) \leqslant n - 2$.

The following theorem contains a similar bound for even n.

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 $(\Phi_F)_i(x) = f_i(x) + \lambda_i\big(x_2 \dots x_n + x_1 x_3 \dots x_n + \dots + x_1 x_2 \dots x_{n-1} + x_1 \dots x_n\big)$, where $\deg(f_i) \leqslant n - 2$ and $\lambda_i \in \mathbb{F}_2$.

Proof. Let $L : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a linear function. Then it is easy to see that

$$\gamma_{F+L}(a,b) = \gamma_F(a, b+L(a)) = (b+L(a))\cdot\Phi_F(a)+\varphi_F(a)+1 = b\cdot\Phi_F(a)+\varphi_F(a)+L(a)\cdot\Phi_F(a)+1.$$

Hence, $\Phi_{F+L} = \Phi_F$ and $\varphi_{F+L} = \varphi_F + L \cdot \Phi_F$. By Proposition 1, $\deg(\varphi_F) = \deg(\varphi_{F+L}) = n$, since $F+L$ is also a quadratic APN function. Thus, $\deg(L\cdot\Phi_F) < n$ for any linear function L.

Suppose that $\deg(\Phi_F) = n$. This means that there exists a coordinate function $(\Phi_F)_i$ of degree n. Let us represent

$$(\Phi_F)_i(x) = f_i(x) + a_1 x_2 \dots x_n + a_2 x_1 x_3 \dots x_n + \dots + a_n x_1 x_2 \dots x_{n-1} + x_1 \dots x_n,$$

where $\deg(f_i) \leqslant n - 2$ and $a_1, \dots, a_n \in \mathbb{F}_2$.

— If $a_j = 0$, then $\deg(L \cdot \Phi_F) = n$ for $L = (0, \dots, 0, x_j, 0, \dots, 0)$, where x_j is the i-th coordinate function of L. Hence, we get a contradiction.

— If $a_j = 1$ for all j, then it is easy to see that we will always have $\deg(L \cdot \Phi_F) < n$ for any linear function L.

Suppose that $\deg(\Phi_F) = n - 1$. Similarly,

$$(\Phi_F)_i(x) = f_i(x) + a_1 x_2 \dots x_n + a_2 x_1 x_3 \dots x_n + \dots + a_n x_1 x_2 \dots x_{n-1},$$

where at least one coefficient is equal to 1, say a_j. Then $\deg(L \cdot \Phi_F) = n$ for $L = (0, \dots, 0, x_j, 0, \dots, 0)$, where x_j is the i-th coordinate function of L. Hence, we get a contradiction.

Thus, $(\Phi_F)_i$ is of degree not more than $n - 2$ or all monomials of degree $n - 1$ and n are included in the ANF of $(\Phi_F)_i$. ∎

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 our computational experiments we can formulate the following

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

2. Does the equality $\deg(\Phi_F) = n - 2$ hold?

In this section we study the following question: "Is conjecture 2 true or not?".

For example, consider an APN Gold function $F(x) = x^{2^k+1}$, $\gcd(n, k) = 1$ (the function is given as a function over the finite field of order 2^n). Its associated Boolean function is known [6]: $\gamma_F(a, b) = \mathrm{tr}((a^{2^k+1})^{-1}b) + \mathrm{tr}(1) + 1$ (here tr is the absolute trace function in the finite field of order 2^n). So, we have $\Phi_F(a) = (a^{2^k+1})^{-1}$, $\Phi_F(0) = 0$, and as it is easy to see $\deg(\Phi_F) = n - 2$ (since it is well-known that the degree of a function $F(x) = x^d$ is equal to the 2-weight of the integer d modulo 2^n).

We wonder whether conjecture 2 is true or not for arbitrary n. Let us focus on the case of odd n since in this case we have the bound of Theorem 2. For even case, the consideration could be rather similar but with assumption that $\deg(\Phi_F)$ is not equal to n, that is only a conjecture up to now.

S t e p 1. Let F be a quadratic APN function of n variables, n is odd, $n \geqslant 5$; v be a nonzero vector from $\mathbb{F}_2^n$. We need to prove that $\deg(v \cdot \Phi_F) = n - 2$ for any nonzero $v \in \mathbb{F}_2^n$.

We use the following widely known equality for counting the ANF coefficients of a Boolean function f in n variables:

$$g_f(a) = \left(2^{\mathrm{wt}(a)-1} - 2^{\mathrm{wt}(a)-n-1} \sum_{b \preceq (a+\mathbf{1})} W_f(b) \right) \bmod 2. \tag{1}$$

We need to show that there exists a vector a^v with $\mathrm{wt}(a^v) = n - 2$ such that $g_{v \cdot \Phi_F}(a^v) = 1$. Equivalently, that there exist coordinates i, j, $1 \leqslant i \neq j \leqslant n$, such that

$$\sum_{b \preceq (a^v+\mathbf{1})} W_{v \cdot \Phi_F}(b) = W_{v \cdot \Phi_F}(\mathbf{0}) + W_{v \cdot \Phi_F}(e^i) + W_{v \cdot \Phi_F}(e^j) + W_{v \cdot \Phi_F}(e^i + e^j)$$

is not divided by 16 according to (1). Here e^i is the vector with 1 in the i-th coordinate and 0s in other coordinates. Let us introduce the following sets:

$$M^i = \{ x \in \mathbb{F}_2^n : v \cdot \Phi_F(x) = 0, \; x \cdot e^i = 0 \},$$
$$M^j = \{ x \in \mathbb{F}_2^n : v \cdot \Phi_F(x) = 0, \; x \cdot e^j = 0 \},$$
$$M^{ij} = \{ x \in \mathbb{F}_2^n : v \cdot \Phi_F(x) = 0, \; x \cdot (e^i + e^j) = 0 \}.$$

Then, we have

$$\sum_{b \preceq (a^v+\mathbf{1})} W_{v \cdot \Phi_F}(b) = 4|M^i| - 2^n + 4|M^j| - 2^n + 4|M^{ij}| - 2^n =$$

$$= 4(|M^i| + |M^j| + |M^{ij}|) - 3 \cdot 2^n = 4(2^{n-1} + 2|M_0^{ij}|) - 3 \cdot 2^n = 8|M_0^{ij}| - 2^{n-1},$$

where $M_0^{ij} = \{ x \in \mathbb{F}_2^n : v \cdot \Phi_F(x) = 0, \; x \cdot e^i = 0, \; x \cdot e^j = 0 \}$.

S t e p 2. Thus, we need to prove that there exist coordinates i, j, $1 \leqslant i \neq j \leqslant n$, such that $|M_0^{ij}|$ is odd (since we consider $n \geqslant 5$). From [7, prop. 7], we know that $M = \{ x \in \mathbb{F}_2^n : v \cdot \Phi_F(x) = 0 \} = \bigcup_{\ell \in I} A_\ell$, where A_ℓ is a linear subspace of dimension 2,

and $A_\ell \cap A_k = \{\mathbf{0}\}$, $\ell, k \in I$, $\ell \neq k$. Since Φ_F is a permutation, then $|M| = 2^{n-1}$ and $|I| = (2^{n-1} - 1)/3$.

Let us consider an arbitrary $A_\ell = \{\mathbf{0}, x^\ell, y^\ell, x^\ell + y^\ell\}$. Then for any distinct coordinates i, j of $x^\ell, y^\ell, x^\ell + y^\ell$ we have the following situations (without permutations of rows):

$$
\begin{array}{cccccccccc}
& ij & & ij & & ij & & ij & & ij \\
x^\ell & 00 & & 00 & & 00 & & 00 & & 01 \\
y^\ell & 00 & \text{or} & 01 & \text{or} & 10 & \text{or} & 11 & \text{or} & 10 \\
x^\ell + y^\ell & 00 & & 01 & & 10 & & 11 & & 11
\end{array}
$$

Hence, the number of $x^\ell, y^\ell, x^\ell + y^\ell$ together with $\mathbf{0}$ that belong to the set M_0^{ij} is equal to $1 + 3 \cdot N_3^{ij} + 1 \cdot N_1^{ij} + 0 \cdot N_0^{ij}$, where $N_3^{ij} + N_1^{ij} + N_0^{ij} = |I| = (2^{n-1} - 1)/3$, and N_k^{ij}, $k = 0, 1, 3$, is the number of A_ℓ, $\ell \in I$, having exactly k vectors with both coordinates i and j equal to 0. Thus, $|M_0^{ij}|$ is odd if and only if N_0^{ij} is odd.

S t e p 3. Now, we need to prove that there exist coordinates i, j, $1 \leqslant i \neq j \leqslant n$, such that N_0^{ij} is odd. We found the following interesting property (computationally verified for $n = 5$) that we formulate as a conjecture.

Conjecture 3. Let $M = \bigcup_{\ell \in I} A_\ell$, where A_ℓ is a linear subspace of dimension 2, and $A_\ell \cap A_k = \{\mathbf{0}\}$, $\ell, k \in I$, $\ell \neq k$, $|I| = (2^{n-1} - 1)/3$. Then the set M is a hyperplane $\{x \in \mathbb{F}_2^n : x_m = 0\}$ for some coordinate m if and only if the number of subspaces A_ℓ without elements having both coordinates i and j equal to 0 is even for any distinct coordinates i, j.

S t e p 4. If Conjecture 3 is true, then we need to prove that $M = \{x \in \mathbb{F}_2^n : v \cdot \Phi_F(x) = 0\}$ cannot be a hyperplane $\{x \in \mathbb{F}_2^n : x_m = 0\}$ for some coordinate m.

Conjecture 4. Let F be a quadratic APN function in n variables, $n \geqslant 5$. Then $\{x \in \mathbb{F}_2^n : v \cdot \Phi_F(x) = 0\}$ is not a linear subspace.

We computationally verified this property for all known quadratic APN functions for $n = 5, \ldots, 11$ and formulate the conjecture.

Thus, by proving Conjectures 3 and 4, we can prove the starting Conjecture 2. Unfortunately, each of them remains open up to now.

Conclusion

The following question is open: what properties must a Boolean function satisfy in order to be the associated function for some vectorial function? Even a partial answer to the question provides a potential method to find new APN functions if we can choose "admissible" Boolean functions as γ_F. For example, using the algorithm from [8] for reconstructing APN functions from its associated functions. Another reason why we study the properties of associated functions is that they may lead to new results in the differential equivalence classification of APN functions.

REFERENCES

1. *Nyberg K.* Differentially uniform mappings for cryptography. Advances in Cryptography, EUROCRYPT'93, LNCS, 1994, vol. 765, pp. 55–64.

2. *Budaghyan L.* Construction and Analysis of Cryptographic Functions. Springer International Publishing, 2014. 168 p.

3. *Pott A.* Almost perfect and planar functions. Designs, Codes and Cryptography, 2016, vol. 78, pp. 141–195.

4. *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)

5. *Tuzhilin M. E.* Pochti sovershennye nelineynye funktsii [APN-functions]. Prikladnaya Diskretnaya Matematika, 2009, no. 3 (5), pp. 14–20. (in Russian)

6. *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.

7. *Gorodilova A.* On the differential equivalence of APN functions. Cryptography and Communications, 2019, vol. 11, iss. 4, pp. 793–813.

8. *Boura C., Canteaut A., Jean J., and Suder V.* Two notions of differential equivalence on Sboxes. Designs, Codes and Cryptography, 2019, vol. 87, iss. 2–3, pp. 185–202.

9. *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)

10. *Tokareva N.* Bent Functions, Results and Applications to Cryptography. Acad. Press. Elsevier, 2015. 230 p.