On the differential equivalence of APN functions[*]

Anastasiya Gorodilova

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

E-mail: gorodilova@math.nsc.ru

Abstract. C. Carlet, P. Charpin, V. Zinoviev in 1998 defined 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. This article defines the differentially equivalent functions as vectorial functions having equal associated Boolean functions. It is an open problem of great interest to describe the differential equivalence class for a given Almost Perfect Nonlinear (APN) function. We determined that each quadratic APN function G in n variables, $n \leq 6$, that is differentially equivalent to a given quadratic APN function F, can be represented as $G = F + A$, where A is affine. For the APN Gold function F, we completely described all affine functions A such that F and $F+A$ are differentially equivalent. This result implies that the class of APN Gold functions up to EA-equivalence contains the first infinite family of functions, whose differential equivalence class is non-trivial.

Keywords. Boolean function, Almost perfect nonlinear function, Almost bent function, Crooked function, Differential equivalence, Linear spectrum

1 Introduction

Optimal differential properties of Almost Perfect Nonlinear (APN) functions allow to use them as S-boxes in cryptographic applications (see [37] of K. Nyberg). To find the new constructions of APN functions is an actual problem.

In the well-known paper [16] of C. Carlet, P. Charpin and V. Zinoviev, it was 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. In [26] we determined that there do not exist two APN functions F and G such that $\gamma_F(a,b) = \gamma_G(a,b)+1$ for all $a, b \in \mathbb{F}_2^n$, $a \neq \mathbf{0}$, where $n \geq 2$. But for a given APN function in n variables, it always exists at least 2^{2n} distinct functions having the same associated function. The question arises: does it exist more than 2^{2n} such functions? Surprisingly, working on [26] we computationally found an example of such an APN function in 4 variables.

In this paper we introduce the definition of *differentially equivalent* functions as functions that have equal associated functions. Note that one of the open problems stated by C. Carlet [14]

[*]The author was supported by the Russian Foundation for Basic Research (projects no. 17-41-543364, 18-07-01394), by the program of fundamental scientific researches of the SB RAS I.5.1. (project 0314-2016-0017), by the Russian Ministry of Science and Education (the 5-100 Excellence Programme and the Project no. 1.12875.2018/12.1).

can be formulated as follows: is it possible to describe all differentially equivalent functions for a given APN function? An answer to this question can potentially lead to new APN functions. In this paper we study the mentioned problem for quadratic APN functions and more precisely for the APN Gold functions. Also we continue the research of the *linear spectrum* of a quadratic APN function F. The linear spectrum is a differential and EA-equivalence invariant, which allows us to obtain several nonequivalence results.

The definition of differential equivalence for an arbitrary vectorial function was generalized by C. Boura, A. Canteaut, J. Jean, V. Suder [5]. They called two functions *DDT-equivalent* if their difference distribution tables are equal. DDT-equivalence implies differential equivalence (that is called γ-equivalence in [5]), but the converse is not true [5]. In case of APN functions these equivalences coincide. Note that the term *differential equivalence with respect to a subspace* that is used by V. Suder in [39] describes another property.

Section 2 provides basic definitions related to APN functions. In section 3 we introduce the definition of the differential equivalence and describe its general properties. A conjecture about the differential equivalence of quadratic APN functions is formulated. Section 4 contains a new result of the APN Gold function $F(x) = x^{2^k+1}$ over the finite field $\mathbb{F}_{2^n}$ with $\gcd(k,n)$=1. We prove that up to extended affine equivalence (EA-equivalence), APN Gold functions with $k = n/2 - 1$, where $n = 4t$, form the first infinite family of functions that have a non-trivial differential equivalence class. Section 5 is devoted to several new properties of the associated Boolean function γ_F of a quadratic APN function F. In section 6 the linear spectrum of a quadratic APN function is studied and theorem about its zero values is proved. Section 7 contains the computational results obtained. Section 8 concludes the paper: it formulates the remaining open questions.

Note that this paper is an extended version of [27].

2 Definitions

2.1 Vectorial Boolean functions

Let $\mathbb{F}_{2^n}$ be the finite field of order 2^n and $\mathbb{F}_2^n$ be the n-dimensional vector space over $\mathbb{F}_2$. Let $\mathbf{0}$ denote the zero vector of $\mathbb{F}_2^n$ and $x \cdot y = x_1y_1 + \ldots + x_ny_n$ denote the *inner product* of vectors $x, y \in \mathbb{F}_2^n$. A mapping $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$ is called a *vectorial Boolean function* or a *(n,m)-function.* If $m = 1$, F is called *a Boolean function* in n variables. The *Hamming weight* $\mathrm{wt}(f)$ of a Boolean function f is defined as $\mathrm{wt}(f) = |\{x \in \mathbb{F}_2^n : \ f(x) = 1\}|$ and the *Hamming distance* between f and g is defined as $\mathrm{dist}(f,g) = |\{x \in \mathbb{F}_2^n : \ f(x) \neq g(x)\}|$. Any (n,m)-function F can be considered as a set of m Boolean functions that are called *coordinate functions* of F in the form $F(x) = (f_1(x), \ldots, f_m(x))$, where $x \in \mathbb{F}_2^n$. The *algebraic normal form* (ANF) of F is the following unique representation:

$$F(x) = \sum_{I \in \mathcal{P}(N)} a_I \big(\prod_{i \in I} x_i \big),$$

where $\mathcal{P}(N)$ is the power set of $N = \{1, \ldots, n\}$ and each a_I belongs to $\mathbb{F}_2^m$. Here $+$ denotes the coordinate-wise sum of vectors modulo 2. The *algebraic degree* of F is degree of its ANF: $\deg(F) = \max\{|I| : \ a_I \neq \mathbf{0},\ I \in \mathcal{P}(N)\}$. A function is called *affine* if its algebraic degree is not more than 1 or, equivalently, if $F(x + y) = F(x) + F(y) + F(\mathbf{0})$ for any $x, y \in \mathbb{F}_2^n$. An affine function F is *linear* if $F(\mathbf{0}) = \mathbf{0}$. 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 a (n,m)-function 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 is called *bent* if all its Walsh coefficients take only values $\pm 2^{n/2}$.

In this paper we consider only (n,n)-functions and Boolean functions. Further, by vectorial Boolean functions we mean only (n,n)-functions. It is convenient to identify the vector space $\mathbb{F}_2^n$ with the finite field $\mathbb{F}_{2^n}$ and to consider vectorial Boolean functions as mappings from $\mathbb{F}_{2^n}$ to itself. A function F has the unique representation as a univariate polynomial over $\mathbb{F}_{2^n}$ of degree not more than $2^n - 1$

$$F(x) = \sum_{i=0}^{2^n-1} \lambda_i x^i, \text{ where } \lambda_i \in \mathbb{F}_{2^n}.$$

It is known that the algebraic degree of F can be calculated as $\deg(F) = \max_{i=0,\dots,2^n-1}\{\mathrm{wt}(i) : \lambda_i \neq 0\}$, where $\mathrm{wt}(i)$ is a binary weight of an integer i. Thus, an affine function F is of the form $F(x) = \lambda + \sum_{i=0}^{n} \lambda_i x^{2^i}$, where $\lambda, \lambda_i \in \mathbb{F}_{2^n}$ (additionally, F is linear if $\lambda = 0$).

For a function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ it is usually considered the following representation that is called the *trace form* (it is not unique):

$$f(x) = \mathrm{tr}\big(\sum_{i\in CS} \lambda_i x^i + \lambda x^{2^n-1}\big),$$

where $\lambda_i, \lambda \in \mathbb{F}_{2^n}$, tr denotes the *trace function* $\mathrm{tr}(x) = x + x^2 + x^{2^2} + \ldots + x^{2^{n-1}}$ and CS is a set of representatives of *cyclotomic classes* modulo $2^n - 1$. Note that the trace function takes values only from $\mathbb{F}_2$ and it is a linear function. A cyclotomic class modulo $2^n - 1$ of an integer i is the set $C(i) = \{i \cdot 2^j \bmod (2^n - 1),\ j = 0, \ldots, n-1\}$. Cardinality of any cyclotomic class modulo $2^n - 1$ is at most n and divides n.

There are two definitions of equivalence of vectorial Boolean functions that are usually considered, when studying cryptographic functions. Let F and F' be (n,n)-functions. F and F' are called *extended affine equivalent* (EA-equivalent) if $F' = A' \circ F \circ A'' + A$, where A', A'' are affine permutations on $\mathbb{F}_2^n$ and A is an affine function on $\mathbb{F}_2^n$. Two functions F and F' are said to be *Carlet-Charpin-Zinoviev equivalent* (CCZ-equivalent) if their graphs $\mathcal{G}_F = \{(x, F(x)) : x \in \mathbb{F}_2^n\}$ and $\mathcal{G}_{F'} = \{(x, F'(x)) : x \in \mathbb{F}_2^n\}$ are affine equivalent [16].

Both these equivalences preserve the APN property of a function. But, in general, CCZ-equivalence modifies the algebraic degree of a function (in contrast to EA-equivalence). EA-equivalence is a particular case of CCZ-equivalence. In several cases they coincide, for example, for Boolean functions and vectorial bent Boolean functions as shown by L. Budaghyan and C. Carlet in [10]. Also, it was proved in [41] by S. Yoshiara that two quadratic APN functions are CCZ-equivalent if and only if they are EA-equivalent.

2.2 APN functions

A function F from $\mathbb{F}_2^n$ to itself is called *almost perfect nonlinear* (APN) 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. Equivalently, F is APN if $|B_a(F)| = |\{F(x) + F(x + a) : x \in \mathbb{F}_2^n\}| = 2^{n-1}$ for any nonzero vector a.

Although APN functions are intensively studied, it is very hard to give a complete description of the class. *Power*, or *monomial* functions, which are functions over $\mathbb{F}_{2^n}$ of the form $F(x) = x^d$, are the simplest candidates to study whether they are APN or not. It is known 6 classes of monomial APN functions, and there is a conjecture of H. Dobbertin [18] that this list is complete. Note that in 1964 V. A. Bashev and B. A. Egorov proved the APN property of the inverse function $F(x) = x^{2^n-2}$, for odd n (as M. M. Glukhov mentioned in [24]). Infinite families of APN polynomials were also found (see, for example, the book [9] of L. Budaghyan, surveys [38] of A. Pott, [24] of M. M. Glukhov, [40] of M. E. Tuzhilin).

Another longstanding problem in APN functions is the existence of APN permutations in even number of variables n. There are several partial nonexistence results on APN permutations (for example, [2], [23], [24], [31]) and the only APN permutation in even n was discovered in [8] for $n = 6$ by J. F. Dillon et al. In [32] V. Idrisova proposed two methods for searching APN permutations that are based on special symbol sequences generated by the invented algorithm.

Complete classifications over EA- and CCZ-equivalences of APN functions up to dimension 5 were obtained in [6] by M. Brinkman and G. Leander. For $n = 6$ there are also known all 13 CCZ-inequivalent quadratic APN functions (found in [7], verified in [21] by Y. Edel). In [43] Y. Yu, M. Wang, Y. Li developed a new approach for finding CCZ-inequivalent quadratic APN functions and presented 487 CCZ-inequivalent quadratic APN functions for $n = 7$ and 8179 ones for $n = 8$ (in updated version of [42]).

3 The differential equivalence of vectorial Boolean functions

In this section we introduce the definition of the differential equivalence of vectorial Boolean functions and consider its basic properties, mainly for quadratic functions.

3.1 Definition and basic properties of differential equivalence

Let F be a (n, n)-function. In [16] a Boolean function γ_F in $2n$ variables associated to F was introduced. It takes value 1 if and only if $a \neq \mathbf{0}$ and $F(x) + F(x + a) = b$ has solutions. It was shown that F is APN if and only if γ_F has the Hamming weight $2^{2n-1} - 2^{n-1}$.

Let us introduce the following definition.

Definition 1. *Two functions F, G from $\mathbb{F}_2^n$ to itself are called differentially equivalent if $\gamma_F = \gamma_G$. Denote the differential equivalence class of F by $\mathcal{DE}_F$.*

Problem 1. *[14] If we are given an APN function F, is it possible to find a systematic way to build another function G such that $\gamma_F = \gamma_G$?*

This open problem can be also formulated in terms of the differential equivalence: is it possible to describe the differential equivalence class of a given APN function? It is a rather natural question, but it seems to be difficult to find an answer for an arbitrary APN function. Indeed, we could not even say that the differential equivalence between two APN functions implies EA- or CCZ-equivalence between them. It makes this problem even more interesting since we potentially could find new APN functions by studying the differential equivalence classes of the known ones.

Let us denote the set $\{F(x) + F(x + a) : x \in \mathbb{F}_2^n\}$ by $B_a(F)$, where $a \in \mathbb{F}_2^n$.

Proposition 1. *Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be an APN function and $n > 1$. Then $F_{c,d}(x) = F(x + c) + d$ is differentially equivalent to F for all $c, d \in \mathbb{F}_2^n$ and all the functions $F_{c,d}$ are pairwise distinct.*

Proof. Let us consider $B_a(F_{c,d})$ for an arbitrary nonzero a from $\mathbb{F}_2^n$:

$$B_a(F_{c,d}) = \{F(x+c) + d + F(x+c+a) + d : \ x \in \mathbb{F}_2^n\} = B_a(F).$$

Thus, by definition F and $F_{c,d}$ are differentially equivalent for any $c, d \in \mathbb{F}_2^n$.

Suppose that there exist $c, d, c', d' \in \mathbb{F}_2^n$ such that $F_{c,d} = F_{c',d'}$. Then $F(x+c) + d = F(x+c') + d'$ for all $x \in \mathbb{F}_2^n$. Since $n > 1$, equation $F(x) + F(x+a) = b$ has at least 4 solutions if $a = c + c'$ and $b = d + d'$. Since F is APN, then $c = c'$ and $d = d'$. □ □

We will call the functions $F_{c,d}$ *trivially* differentially equivalent to F. The next proposition means that we only need to study the differential equivalence classes of the EA-equivalence representatives.

Proposition 2. *Let F, G be EA-equivalent functions from $\mathbb{F}_2^n$ to itself. Then $|\mathcal{DE}_F| = |\mathcal{DE}_G|$. Moreover, if $G = A' \circ F \circ A'' + A$ and $\mathcal{DE}_F = \{F_1, \ldots, F_k\}$, then $\mathcal{DE}_G = \{A' \circ F_1 \circ A'' + A, \ldots, A' \circ F_k \circ A'' + A\}$.*

Proof. Let us firstly note the following: if F and G are EA-equivalent and $G = A' \circ F \circ A'' + A$, then for all nonzero a

$$B_a(G) = A'\big(B_{A''(a)+A''(\mathbf{0})}(F)\big) + A'(\mathbf{0}) + A(a) + A(\mathbf{0}).$$

Thus, the statement is a straightforward corollary from this fact and the differential equivalence definition. □ □

There is the next natural question: "Is it true that an analogue of proposition 2 for CCZ-equivalent functions takes place?" Let us consider the case $n = 4$: there exist two EA-equivalence classes of APN functions and their representatives are CCZ-equivalent [6]. We computationally found that cardinalities of the differential equivalence classes of these two representatives are equal to each other (see section 7). So, such an analogue holds up to 4 variables.

3.2 The differential equivalence of quadratic APN functions

It is known that affine APN functions on $\mathbb{F}_2^n$ do not exist when $n > 1$. So quadratic APN functions are the simplest APN functions with the smallest possible algebraic degree. But even in this case APN functions are still not classified for an arbitrary number of variables. We can use the following useful property of quadratic functions: if F is a quadratic function, then $B_a(F)$ is an affine subspace for all nonzero $a \in \mathbb{F}_2^n$. If F is an APN function, then $B_a(F)$ is an affine hyperplane (i. e. it has cardinality 2^{n-1}) for all $a \neq \mathbf{0}$.

Let us consider the *crooked* functions. The definition of the *crooked* functions was introduced in connection with distance regular graphs by T. D. Bending and D. Fon-Der-Flaass in [1]. In [35] G. Kyureghyan generalized this definition to the following: a function F is called *crooked* if $B_a(F)$ is an affine hyperplane for all $a \neq \mathbf{0}$. Obviously, quadratic APN functions are always crooked. There is also a conjecture (proved for monomial functions [35] and binomial functions of the form $x^d + ux^e$ [4]):

Conjecture 1. *[35] All crooked functions are quadratic.*

If conjecture 1 is true, then for solving problem 1 for a quadratic APN function F, we only need to study which quadratic functions are differentially equivalent to F. The first natural step in this direction is to study whether function G that is EA-equivalent to F is also differentially equivalent to F.

We start to consider this question by studying when just an affine function is added to a given quadratic APN function. It is easy to see that the number of affine functions A such that $F + A \in \mathcal{DE}_F$, where F is a quadratic APN function, is an EA-equivalence invariant.

Note 1. *There exist at least 2^{2n} distinct affine functions A such that F and $F + A$ are differentially equivalent to any quadratic APN function F on $\mathbb{F}_2^n$. Indeed, $A^F_{c,d}(x) = F(x) + F(x + c) + d$ is affine for all $c, d \in \mathbb{F}_2^n$ and $F(x) + A^F_{c,d}(x) = F(x + c) + d$, which is differentially equivalent to F according to proposition 1. So, all these functions $A^F_{c,d}$ are distinct. And all corresponding $F + A^F_{c,d}$ are trivially differentially equivalent to F. The question arises: are there any other affine functions? Surprisingly, the answer is "no" for almost all quadratic APN functions up to 6 variables.*

Computationally (see section 7), we obtained the following result.

Theorem 1. *Let F be a quadratic APN function in n variables, $n = 2, 3, 4, 5, 6$. Then each differentially equivalent to F quadratic APN function G is represented as follows: $G = F + A$, where A is an affine function. Moreover, the number K of such functions A equals to 2^{2n} for all functions except functions from two EA-equivalence classes with the following representatives:*
1) $n = 4$: APN Gold function $F(x) = x^3$, $K = 2^{10}$;
2) $n = 6$: APN function $F(x) = \alpha^7x^3 + x^5 + \alpha^3x^9 + \alpha^4x^{10} + x^{17} + \alpha^6x^{18}$, $K = 2^{13}$.

This means that we found all affine functions that do not change the associated Boolean function when adding to a quadratic APN function for a small number of variables up to 6. And we also computationally proved that there are no two differentially equivalent quadratic APN functions F and G such that $F + G$ is not an affine function. This results in the following conjecture.

Conjecture 2. *Let F be a quadratic APN function in n variables. Then each quadratic APN function G that is differentially equivalent to F, can be represented as follows: $G = F + A$, where A is an affine function.*

4 APN Gold functions

An APN Gold function is a quadratic monomial function of the form $F(x) = x^{2^k+1}$ over $\mathbb{F}_{2^n}$, where $\gcd(k, n) = 1$. It is easy to see that Gold functions are permutations if n is odd and 3-to-1 functions otherwise. It also has maximal possible nonlinearity (AB-functions) when n is odd [16].

APN Gold functions take a special place among APN functions. At first, these functions are the only *exceptional* monomial functions along with APN Kasami functions [29]. Also, despite the fact these functions seem to be rather simple (due to their small algebraic degree and the univariate representation), many other interesting constructions of APN functions have been found based on them (for example, [11], [12], [22]).

In [26] we tried to find an affine function A for a given quadratic APN function F such that $B_a(F+A) = \mathbb{F}_2^n \setminus B_a(F)$ for as many vectors a as possible. Working on [26], we found that for the APN Gold function in 4 variables there exist 2^{10} affine functions such that $B_a(F+A) = B_a(F)$ for all $a \in \mathbb{F}_2^4$. This shows that the differential equivalence class of quadratic APN function F is wider than the trivial class of cardinality 2^8.

In this section we prove that for an APN Gold function $F(x) = x^{2^k+1}$ there exist exactly $2^{2n+n/2}$ distinct affine functions A such that F and $F + A$ are differentially equivalent if $n = 4t$ for some t and $k = n/2 \pm 1$; otherwise the number of such affine functions is equal to 2^{2n}.

4.1 Preliminary lemma

Here we consider a lemma that is necessary for proving a new result on APN Gold functions.

Lemma 1. *Let n be an integer. Let $P_k^i = 2^i - 2^k - 1$, where $i = 0, \dots, n-1$ and k runs from 1 to $n-1$ except the case $k = n/2$ if n is even. Then the following statements hold:*
1) P_k^0 and P_k^k are in one cyclotomic class modulo $2^n - 1$ (say, C) for all k;
2) P_k^i and P_k^j are in distinct cyclotomic classes modulo $2^n - 1$ not equal to C for all $i \neq j$ and $i, j \neq 0, k$;
3) if n is odd, then $|C(P_k^i)| = n$ for all i and k;
4) if n is even, then $|C(P_k^i)| = n$ for all i and k except the following cases: $|C(P_{n/2-1}^{n-1})| = |C(P_{n/2+1}^{k-1})| = n/2$.

Proof. 1) Hereinafter, P_k^i means the representative of P_k^i congruence class modulo $2^n - 1$ belonging to the interval from 0 to $2^n - 2$. By definition, binary weights of $P_k^0 = -2^k$ and $P_k^k = -1$ are equal to $n - 1$. It is easy to see that all integers from 0 to $2^n - 2$ of binary weight $n - 1$ are in one cyclotomic class modulo $2^n - 1$ (say, C) of cardinality n.

2) Consider all integers P_k^i and their binary representations, see Table 1. The integers $P_k^1, \dots, P_k^{k-1}$ (we denote them by group A) have binary weights $n-k, \dots, n-2$ correspondingly. Thus, they belong to pairwise distinct cyclotomic classes modulo 2^n-1 not equal to C. Similarly, the integers $P_k^{k+1}, \dots,\ P_k^{n-1}$ (group B) belong to pairwise distinct cyclotomic classes modulo $2^n - 1$ not equal to C since their binary weights runs from k to $n - 2$.

The binary representation of P_k^i consists of two groups of consecutive 1s that have lengths $n - k$ and $i - 1$ if $i = 1, \dots k - 1$, and k and $i - k - 1$ if $i = k + 1, \dots, n - 1$. Two such integers belong to the same cyclotomic classes if lengths of consecutive 1s groups are equal. Thus, any two integers from groups A and B correspondingly belong to the distinct classes. Indeed, $n - k \neq k$ by proposition condition and $n - k \neq i - k - 1$ for all $i = k + 1, \dots, n - 1$.

3), 4) According to the previous studying of P_k^i binary representations, the only possible case when $|C(P_k^i)| \neq n$ is the following: if lengths of consecutive 1s groups in P_k^i are both equal to $n/2 - 1$. If n is odd, this case is not realized. If n is even, then these possibilities are the following: $i = n-1$ if $k = n/2-1$ and $i = k-1$ if $k = n/2+1$. In both these cases $P_k^i = 2^{n/2} P_k^i$ modulo $2^n - 1$ that completes the proof. □ □

4.2 The main result concerning APN Gold function

The associated Boolean function of an APN Gold function is known [16].

Proposition 3. [16] *Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a Gold function $F(x) = x^{2^k+1}$, where $gcd(k, n) = 1$. Then $\gamma_F(a, b) = \mathrm{tr}\big((a^{2^k+1})^{-1} b\big) + \mathrm{tr}(1) + 1$ if $a \neq 0$ and $\gamma_F(0, b) = 0$ for all $b \in \mathbb{F}_{2^n}$.*

Table 1: Binary representations of integers P_k^i.

i	$P_k^i = 2^i - 2^k - 1 \bmod(2^n - 1) = (b_{n-1}, \dots, b_k, \dots, b_0) \in \mathbb{F}_2^n$	$wt(P_k^i)$
0	1 1 ... 1 1 **0** 1 1 ... 1 1 1 1 1	$n-1$
1	1 1 ... 1 1 **1** 0 0 ... 0 0 0 0 0	$n-k$
2	1 1 ... 1 1 **1** 0 0 ... 0 0 0 1 0	$n-k+1$
3	1 1 ... 1 1 **1** 0 0 ... 0 0 1 1 0	$n-k+2$
...	...	...
$k-1$	1 1 ... 1 1 **1** 0 1 ... 1 1 1 1 0	$n-2$
k	1 1 ... 1 1 **1** 1 1 ... 1 1 1 1 0	$n-1$
$k+1$	0 0 ... 0 0 **0** 1 1 ... 1 1 1 1 1	k
$k+2$	0 0 ... 0 1 **0** 1 1 ... 1 1 1 1 1	$k+1$
...	...	...
$n-1$	0 1 ... 1 1 **0** 1 1 ... 1 1 1 1 1	$n-2$

The following theorem contains a new result on APN Gold functions.

Theorem 2. *Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be a Gold function $F(x) = x^{2^k+1}$, where $gcd(k, n) = 1$. Then the following statements hold:*
1) if $n = 4t$ for some t and $k = n/2 \pm 1$, then there exist exactly $2^{2n+n/2}$ distinct affine functions A such that F and $F + A$ are differentially equivalent; all of them are of the form $A(x) = \alpha + \lambda^{2^k} x + \lambda x^{2^k} + \delta x^{2^j}$, where $\alpha, \lambda, \delta \in \mathbb{F}_{2^n}$, $\delta = \delta^{2^{n/2}}$, and $j = k - 1$ for $k = n/2 + 1$ and $j = n - 1$ for $k = n/2 - 1$;
2) otherwise, there exist exactly 2^{2n} distinct affine functions A such that F and $F + A$ are differentially equivalent; all of them are of the form $A(x) = \alpha + \lambda^{2^k} x + \lambda x^{2^k}$, where $\alpha, \lambda \in \mathbb{F}_{2^n}$.

Proof. From proposition 3 we get that $\gamma_F(a, b) = \mathrm{tr}\big((a^{2^k+1})^{-1} b\big) + \mathrm{tr}(1) + 1$ if $a \neq 0$ and $\gamma_F(0, b) = 0$ for all $b \in \mathbb{F}_{2^n}$. Let A be an affine function from $\mathbb{F}_{2^n}$ to itself and L be its linear part, i. e. $L(x) = A(x) + A(0)$. Then

$$\gamma_{F+A}(a, b) = \gamma_F\big(a, b + L(a)\big) = \mathrm{tr}\big((a^{2^k+1})^{-1}(b + L(a)\big) + \mathrm{tr}(1) + 1$$

$$= \mathrm{tr}\big((a^{2^k+1})^{-1} b\big) + \mathrm{tr}\big(((a^{2^k+1})^{-1} L(a)\big) + \mathrm{tr}(1) + 1.$$

Thus, $\gamma_{F+A}(a, b) = \gamma_F(a, b) + \mathrm{tr}\big((a^{2^k+1})^{-1} L(a)\big)$. So, F and $F + A$ are differentially equivalent if and only if the linear part L of A satisfies the equality $\mathrm{tr}\big((a^{2^k+1})^{-1} L(a)\big) = 0$ for all $a \in \mathbb{F}_{2^n}$. Denote by N the number of such affine functions A.

Let $A(x) = \alpha + L(x) = \alpha + \sum_{i=0}^{n-1} \lambda_i x^{2^i}$ be an affine function, where $\alpha, \lambda_i \in \mathbb{F}_{2^n}$, $i = 0, \dots, n - 1$. Then the following equalities hold for all $a \in \mathbb{F}_{2^n}$:

$$\mathrm{tr}\big((a^{2^k+1})^{-1} L(a)\big) = \mathrm{tr}\big(\sum_{i=0}^{n-1} \lambda_i a^{2^i} (a^{2^k+1})^{-1}\big) = \sum_{i=0}^{n-1} \mathrm{tr}(\lambda_i a^{2^i - 2^k - 1}) = 0.$$

The last equality represents a polynomial equation in variable a of degree not more than $2^n - 1$ that has 2^n solutions. So, all its coefficients must be equal to 0. Let us find the coefficients of all monomials x^d, $d = 0, \dots, 2^n - 1$. For this, we need to study cyclotomic classes of all exponents $P_k^i = 2^i - 2^k - 1$, $i = 0, \dots, n-1$, for a given k. Lemma 1 (1,2) gives us that there are only two exponents P_k^0 and P_k^k that belong to one cyclotomic class modulo $2^n - 1$. So, this means that there is a relation between λ_0 and λ_k in the form $\lambda_0 = (\lambda_k)^{2^k}$ for all n since $P_k^0 = 2^k P_k^k \pmod{(2^n-1)}$. To study the other coefficients consider the following cases.

Case 1. If n is odd, then according to lemma 1 (2,3) $\lambda_i = 0$ if $i \neq 0, k$. Thus, $N = 2^{2n}$ since we can choose such α, λ_k that they are arbitrary elements from $\mathbb{F}_{2^n}$.

Let n be even, $n = 2\ell$. There are two different possibilities.

Case 2. If ℓ is odd, then $\gcd(n, n/2 \pm 1) = 2$. So, we do not consider $k = n/2 \pm 1$ by theorem condition and as a result $\lambda_i = 0$ if $i \neq 0, k$ according to lemma 1 (4). Similarly to case 1, $N = 2^{2n}$.

Case 3. If ℓ is even, then $\gcd(n, n/2 \pm 1) = 1$.

- If $k \neq n/2 \pm 1$, then according to lemma 1 (4) we have $\lambda_i = 0$ if $i \neq 0, k$. Thus, $N = 2^{2n}$.
- If $k = n/2 + 1$, then according to lemma 1 (4) we have $\lambda_i = 0$ if $i \neq 0, k-1, k$ and $\lambda_{k-1} = (\lambda_{k-1})^{2^{n/2}}$. Since the number of elements $x \in \mathbb{F}_{2^n}$ satisfying the equality $x = x^{2^{n/2}}$ is equal to $2^{n/2}$, we have $N = 2^{2n+n/2}$.
- If $k = n/2 - 1$, then according to lemma 1 (4) we have $\lambda_i = 0$ if $i \neq 0, k, n-1$ and $\lambda_{n-1} = (\lambda_{n-1})^{2^{n/2}}$. Similarly to the previous, $N = 2^{2n+n/2}$. □ □

Theorem 2 shows that the class of APN Gold functions contains the first infinite family of quadratic APN functions whose differential equivalence class is wider than trivial class of cardinality 2^{2n} (see note 1). Indeed, the cardinality of $\mathcal{DE}_F$, where $F(x) = x^{2^{n/2\pm1}+1}$, $n = 4t$, is greater or equal to $2^{2n+n/2}$ (since theorem 2 (1) describes only differentially equivalent to F functions of special form). Note that functions $F(x) = x^{2^{n/2\pm1}+1}$ are in the same EA-equivalence class for any n.

Also, APN Gold functions $F(x) = x^{2^{n/2-1}+1}$, $n = 4, 8$, are the only functions up to EA-equivalence (except one function in 6 variables) among all known quadratic APN functions in $2, \dots, 8$ variables that have more than 2^{2n} affine functions preserving the associated Boolean functions when adding to the original functions (see theorem 1 and section 7). That is why we may call this property of APN Gold functions remarkable.

5 Properties of the associated Boolean function

In this section we get several properties of the associated Boolean function for 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

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

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 $(F(x) + F(x+a) + F(a) + F(\mathbf{0})) \cdot \Phi_F(a) = 0$ for all $x \in \mathbb{F}_2^n$ by definition.

Let us denote

$$A_v^F = \{a \in \mathbb{F}_2^n : \ \Phi_F(a) = v\}$$

for $v \in \mathbb{F}_2^n$. In [35] G. Kyureghyan considered two sets $T_F(v)$ and $\overline{T}_F(v)$ for a quadratic APN function F. In terms of this work, them can be expressed as follows: $T_F(v) = \{a \in A_v^F : \ \varphi_F(a) =$

$0\} \cup \{\mathbf{0}\}$ and $\overline{T}_F(v) = \{a \in A_v^F : \varphi_F(a) = 1\}$. It is known [35] that if F is crooked, then $T_F(v)$ is a subspace and $\overline{T}_F(v)$ is either empty or is a coset of $T_F(v)$ for any v. Thus, we can get the following two propositions for quadratic APN functions (that are crooked by definition).

Proposition 4. *Let F be a quadratic APN function in n variables. Then $A_v^F \cup \{\mathbf{0}\}$ is a linear subspace for any vector $v \in \mathbb{F}_2^n$, $v \neq \mathbf{0}$, and $A_{\mathbf{0}}^F = \{\mathbf{0}\}$.*

Proof. It is a direct corollary of proposition 1 [35]. □ □

Proposition 5. *Let F be a quadratic APN function in n variables. Then there exists $c_v \in \mathbb{F}_2^n$ for any vector $v \in \mathbb{F}_2^n$ such that $\varphi_F(x)|_{A_v^F} = c_v \cdot x|_{A_v^F}$.*

Proof. It is a direct corollary of proposition 1 [35]. □ □

It is known the following statement.

Proposition 6. [16] *Let F be a quadratic APN function in n variables, n is odd. Then Φ_F is a permutation; therefore, γ_F is a bent function of Maiorana–McFarland type.*

Thus, when n is odd, all A_v^F, $v \in \mathbb{F}_2^n$, are pairwise distinct and each of them consists of one element. We prove the following theorem for even n.

Theorem 3. *Let F be a quadratic APN function in n variables, n is even. Then dimension of $A_v^F \cup \{\mathbf{0}\}$ is even for any $v \in \mathbb{F}_2^n$.*

Proof. Step 1. The Walsh coefficients of F and γ_F are connected by the following rule [16] (here $F_v = v \cdot F$ is a component function of F):

$$W_{\gamma_F}(u, v) = 2^{2n}\delta(u, v) - (W_{F_v}(u))^2 + 2^n, \tag{1}$$

where $\delta(u, v) = 1$ if $(u, v) = (\mathbf{0}, \mathbf{0})$ and $\delta(u, v) = 0$ otherwise.

All component functions F_v, $v \neq \mathbf{0}$, are quadratic since APN functions do not have affine component functions [15]. Then $W_{F_v} \in \{0, \pm 2^{k_v}\}$ for all $v \neq \mathbf{0}$, where k_v is an integer, $n/2 \leq k_v \leq n - 1$ [17]. Let us consider $W_{\gamma_F}(u, v)$ according to equality (1):

If $v = \mathbf{0}$, then

- $u = \mathbf{0}$: $W_{\gamma_F}(u, v) = 2^{2n} - 2^{2n} + 2^n = 2^n$;
- $u \neq \mathbf{0}$: $W_{\gamma_F}(u, v) = 0 - 0 + 2^n = 2^n$.

If $v \neq \mathbf{0}$, then

- $W_{F_v}(u) = 0$: $W_{\gamma_F}(u, v) = 0 - 0 + 2^n = 2^n$;
- $W_{F_v}(u) = \pm 2^{k_v}$: $W_{\gamma_F}(u, v) = 0 - 2^{2k_v} + 2^n = 2^n - 2^{2k_v}$.

Step 2. From the other hand, $W_{\gamma_F}(u, v) = -2^n \sum_{a \in A_v^F} (-1)^{\varphi_F(a) + u \cdot a}$ if $v \neq \mathbf{0}$. Indeed, consider W_{γ_F} using $\gamma_F(a, b) = b \cdot \Phi_F(a) + \varphi_F(a) + 1$:

$$W_{\gamma_F}(u, v) = \sum_{a,b \in \mathbb{F}_2^n} (-1)^{b \cdot \Phi_F(a) + \varphi_F(a) + 1 + u \cdot a + v \cdot b}$$

$$= - \sum_{a \in \in \mathbb{F}_2^n} (-1)^{\varphi_F(a) + u \cdot a} \sum_{b \in \in \mathbb{F}_2^n} (-1)^{b \cdot \Phi_F(a) + v \cdot b}$$

$$= \sum_{b \in \mathbb{F}_2^n} (-1)^{v \cdot b} - \sum_{a \in \mathbb{F}_2^n, a \neq \mathbf{0}} (-1)^{\varphi_F(a) + u \cdot a} \sum_{b \in \mathbb{F}_2^n} (-1)^{b \cdot \Phi_F(a) + v \cdot b}.$$

If $v = \mathbf{0}$, then $W_{\gamma_F}(u,v) = 2^n - 0 = 2^n$, since $\Phi_F(a) \neq \mathbf{0}$ when $a \neq \mathbf{0}$.

If $v \neq \mathbf{0}$, then $W_{\gamma_F}(u,v) = 0 - 2^n \sum_{a \in \mathbb{F}_2^n : \Phi_F(a) = v} (-1)^{\varphi_F(a) + u \cdot a}$.

Step 3. We have $W_{\gamma_F}(u,v) = -2^n \sum_{a \in A_v^F} (-1)^{\varphi_F(a) + u \cdot a}$. According to proposition 5, there exists $c_v \in \mathbb{F}_2^n$ for any vector $v \in \mathbb{F}_2^n$ such that $\varphi_F(x)|_{A_v^F} = c_v \cdot x|_{A_v^F}$. Then $W_{\gamma_F}(c_v, v) = -2^n |A_v^F|$. According to step 1, we have the only possible case: $-2^n |A_v^F| = 2^n - 2^{2k_v}$. This results in $|A_v^F| + 1 = 2^{2k_v - n}$ or $\dim(A_v^F \cup \{\mathbf{0}\}) = 2k_v - n$. Since n is even, we get the required statement. □ □

Let us prove the following auxiliary statement.

Proposition 7. *Let F be a quadratic APN function in n variables. Then, for any nonzero vector $v \in \mathbb{F}_2^n$, the set $\{x \in \mathbb{F}_2^n : \ v \cdot \Phi_F(x) = 0\}$ is represented as $\bigcup_{i \in I} M_i$, where M_i is a linear subspace of dimension 2, and $M_i \cap M_j = \{\mathbf{0}\}$, $i, j \in I$, $i \neq j$.*

Proof. Let $v \neq \mathbf{0}$ and $v \cdot \Phi_F(x) = 0$, where $x \in \mathbb{F}_2^n$, $x \neq \mathbf{0}$. This means that there exists a vector $y \in \mathbb{F}_2^n$ such that $v = F(y) + F(y+x) + F(x) + F(0)$ (since F is an APN function, there is no such a vector z that is not equal to y or $y + x$). This implies $v \cdot \Phi_F(y) = 0$ and $v \cdot \Phi_F(x+y) = 0$ by definition of Φ_F. Thus, the set $\{x, y, x+y\}$ together with the zero vector forms the required linear subspace of dimension 2. □ □

We get the following upper bound on the algebraic degree of Φ_F for odd n.

Theorem 4. *Let F be a quadratic APN function in n variables, n is odd, $n \geq 3$. Then* $\deg(\Phi_F) \leq n - 2$.

Proof. Let $v \in \mathbb{F}_2^n$ be an arbitrary nonzero vector. We prove that $\deg(v \cdot \Phi_F) \leq n - 2$ and as a result $\deg(\Phi_F) \leq n - 2$. We use the following widely known equality for counting the ANF coefficients of a Boolean function f in n variables:

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

Since Φ_F is a permutation by proposition 6, then $v \cdot \Phi_F$ is balanced for any nonzero vector $v \in \mathbb{F}_2^n$. This implies $W_{v \cdot \Phi_F}(\mathbf{0}) = 0$ and $\deg(v \cdot \Phi_F) < n$.

Let v be a nonzero vector from $\mathbb{F}_2^n$. Let us prove that $\deg(v \cdot \Phi_F) \neq n - 1$. This means that $g_{v \cdot \Phi_F}(a^k) = 0$ for all $a^k \in \mathbb{F}_2^n$ such that $\mathrm{wt}(a^k) = n - 1$, $k = 1, \ldots, n$. Equivalently, $\sum_{b \preceq (a^k + \mathbf{1})} W_{v \cdot \Phi_F}(b) = W_{v \cdot \Phi_F}(\mathbf{0}) + W_{v \cdot \Phi_F}(e^k) = W_{v \cdot \Phi_F}(e^k)$ is divided by 8 according to (2), where e^k is the vector with one nonzero coordinate k. Indeed,

$$W_{v \cdot \Phi_F}(e^k) = \sum_{x \in \mathbb{F}_2^n} (-1)^{v \cdot \Phi_F(x) + x \cdot e^k} =$$

$$\sum_{x \in \mathbb{F}_2^n : \ v \cdot \Phi_F(x) = 0} (-1)^{x \cdot e^k} + \sum_{x \in \mathbb{F}_2^n : \ v \cdot \Phi_F(x) = 1} (-1)^{1 + x \cdot e^k} = 4|M| - 2^n,$$

where

$$M = \{x \in \mathbb{F}_2^n : \ v \cdot \Phi_F(x) = 0, \ x \cdot e^k = 0\}.$$

We need to prove that $|M|$ is even. By proposition 7, $\{x \in \mathbb{F}_2^n \mid v \cdot \Phi_F(x) = 0\} = \bigcup_{i \in I} M_i$, where M_i is a linear subspace of dimension 2, and $M_i \cap M_j = \{\mathbf{0}\}$, $i, j \in I$, $i \neq j$. Note that the number of vectors $x \in \mathbb{F}_2^n$ such that $v \cdot \Phi_F(x) = 0$ is equal to 2^{n-1} since Φ_F is a permutation. So, $|I| = (2^{n-1} - 1)/3$ and it is an odd integer. Let $M_i = \{\mathbf{0}, x^i, y^i, x^i + y^i\}$, $i \in I$. For any $i \in I$, there is an odd number (one or three) of nonzero vectors $x \in M_i$ such that $x_k = 0$. Thus, $|M|$ is even since we have an odd number of nonzero vectors belonging to M and $\mathbf{0} \in M$. □ □

Note 2. *The bound of theorem 4 is tight for all known quadratic APN functions in not more than 8 variables (including also even numbers). Moreover, it holds that all their component functions are of degree $n - 2$. For example, for an APN Gold function we have $\Phi_F(a) = (a^{2^k+1})^{-1}$, $\Phi_F(\mathbf{0}) = \mathbf{0}$, and $\deg(\Phi_F) = n - 2$.*

6 The linear spectrum of a quadratic Boolean function

In this section we introduce the notion of the linear spectrum of a quadratic APN function as a new combinatorial characteristics of the function.

Let F be a quadratic APN function in n variables and $L : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a linear function. Then $B_a(F + L)$ equals either $B_a(F)$ or $\mathbb{F}_2^n \setminus B_a(F)$ for all $a \in \mathbb{F}_2^n$.

Let us denote $k_L^F = |\{a \in \mathbb{F}_2^n \setminus \{\mathbf{0}\} : \ B_a(F) = B_a(F+L)\}|$. If γ_F is represented as $\gamma_F(a, b) = \Phi_F(a) \cdot b + \varphi_F(a) + 1$, then $\gamma_{F+L}(a, b) = \gamma_F(a, b + L(a)) = \Phi_F(a) \cdot b + \Phi_F(a) \cdot L(a) + \varphi_F(a) + 1$.

Thus,

$$k_L^F = |\{a \in \mathbb{F}_2^n \setminus \{\mathbf{0}\} : \ \Phi_F(a) \cdot L(a) = 0\}|. \tag{3}$$

Definition 2. *The linear spectrum of a quadratic APN function F in n variables is vector $\Lambda^F = (\lambda_0^F, \ldots, \lambda_{2^n-1}^F)$, where λ_k^F is the number of linear functions L such that $k_L^F = k$.*

It is easy to see that $\sum_{k=0}^{2^n-1} \lambda_k^F = 2^{n^2}$.

The notion of the linear spectrum is essentially arisen while studying quadratic APN functions. Let us describe two directions of studying APN functions, to which the linear spectrum is especially important.

The first direction is the following. In [26] it was suggested an approach for finding iterative constructions of APN function. In particular, to get a quadratic APN function S in $n + 1$ variables, one needs to take two admissible (see definition 4 [26]) quadratic functions F and G in n variables such that $F+G$ is an affine function. We can formulate this statement (assertion 7 [26]) in terms of this paper as follows. Two functions F and $F+L$ are not admissible if $k_L^F > 2^{n-1}$, where F is a quadratic APN function and L is a linear function. Thus, we are interested in possible values of k_L^F .

The second direction is to find the linear spectrum coefficient $\lambda_{2^n-1}^F$ for a quadratic APN function F in n variables. It is equal to the number of linear functions L such that F and $F + L$ are differentially equivalent. As we computationally obtained (see theorem 1, section 3.2), there are no two differentially equivalent quadratic APN functions in small number of variables up to 6 such that their sum is not affine. So, $\lambda_{2^n-1}^F$ multiplied by 2^n seems to show how many differentially equivalent functions to F exist. Also, the next proposition states that the linear spectrum is invariant under EA- and differential equivalences and it can be used for obtaining nonequivalence results.

Proposition 8. *The linear spectrum of a quadratic APN function is*
1) a differential equivalence invariant;
2) a EA-equivalence invariant.

Proof. 1) It follows from definitions of the differential equivalence and the linear spectrum.

2) Let $G = A' \circ F \circ A'' + A$, where F, G are quadratic APN functions in n variables, A', A'' are affine permutations, A is an affine function. Then $B_a(G) = A'\big(B_{A''(a)+A''(\mathbf{0})}(F)\big) + A'(\mathbf{0}) + A(a) + A(\mathbf{0})$. Hence, $k_L^F = k_{L'}^G$ for any linear function L since $B_a(F) = B_a(F + L)$ if and only if $B_a(G) = B_a(G + L')$, where $L'(x) = A'\big(L(x)\big) + A'(\mathbf{0})$. As long as A' is a permutation, then L' runs through the set of all linear functions when looking all linear functions L. Thus, by definition of the linear spectrum, we have $\Lambda^F = \Lambda^G$. □ □

Proposition 9. *Let F be a quadratic APN function in n variables, $n > 1$. Then $\lambda_{2^n-1}^F \geq 2^n$.*

Proof. It is a direct corollary of the fact from note 1 with a remark that here we consider just linear functions (not affine). □ □

Let us prove the following theorem on zero values of the linear spectrum.

Theorem 5. *Let F be a quadratic APN function in n variables, $n > 1$. Then the following statements hold:*
1) $\lambda_k^F = 0$ for all even k, $0 \leq k \leq 2^n - 2$;
2) if n is even, then $\lambda_k^F = 0$ for all $0 \leq k < (2^n - 1)/3$.

Proof. 1) Let n be odd. By equality (3) we have $k_L^F = |\{a \in \mathbb{F}_2^n \setminus \{\mathbf{0}\} : \Phi_F(a) \cdot L(a) = 0\}|$ for any linear function L. Equivalently, $k_L^F = 2^n - 1 - \mathrm{wt}(f)$, where $f(a) = \Phi_F(a) \cdot L(a)$. Since $\deg(\Phi_F) \leq n - 2$ by theorem 4 and L is linear, then $\deg(f) \leq n - 1$. This implies that $\mathrm{wt}(f)$ is even and k_L^F is odd. The proof for even n is contained in item 2).

2) Let $\gamma_F(a, b) = \Phi_F(a) \cdot b + \varphi_F(a) + 1$. Recall $A_v^F = \{a \in \mathbb{F}_2^n : \Phi_F(a) = v\}$ for a vector $v \in \mathbb{F}_2^n$. By theorem 3, dimension of linear subspace $A_v^F \cup \{\mathbf{0}\}$ is even. Hence, the minimum possible nonzero $|A_v^F|$ is equal to 3. Moreover, if $|A_v^F| > 3$, then A_v^F can be represented as the union of sets $A_{v,i}^F$, $i = 1, \ldots, |A_v^F|/3$, such that $A_{v,i}^F \cup \mathbf{0}$ is a linear subspace of dimension 2.

Let $M \cup \{\mathbf{0}\}$ be a linear subspace of dimension 2 that coincides with A_v^F or with $A_{v,i}^F$ for some i if $|A_v^F| > 3$. Note that there are exactly $(2^n - 1)/3$ such subspaces M. Then $\Phi_F(a) \cdot L(a)|_M = c \cdot L(a)|_M$ is a linear Boolean function, where $c = \Phi_F(a)$, $a \in M$. Hence, $\Phi_F(a) \cdot L(a) = 0$ either for all three vectors $a \in M$ or for only one. Since $(2^n - 1)/3$ is odd, then according to (3) we get that k_L^F is odd that completes the proof of item 1). Moreover, there are at least $(2^n - 1)/3$ nonzero vectors $a \in \mathbb{F}_2^n$ such that $\Phi_F(a) \cdot L(a) = 0$. This means that $\lambda_k^F = 0$ for all $0 \leq k < (2^n - 1)/3$. □ □

Note 3. *It is possible to make the upper bound of theorem 5 (2) even stronger. For this one should find cardinalities of the sets A_v^F, $v \in \mathbb{F}_2^n$, for a quadratic APN function F. This can be done by the following algorithm:*

1. *Let $d = (2^n - 1)/3$ and v be the first vector in all ordered nonzero vectors from $\mathbb{F}_2^n$.*

2. *If $|A_v^F| > 3$, then replace the current d by $d - |A_v^F|/3 + 2^{\dim(A_v^F \cup \{\mathbf{0}\}) - 1} - 1$. Take the next vector v and repeat step 2 until all vectors v will be looked.*

Table 2: Value distribution of Φ_F for even n.

n	# EA classes		$\#\{v \in \mathbb{F}_2^n : \ \lvert A_v^F\rvert = k\}$	
			$k = 3$	$k = 15$
4	1		5	–
6	13	for 12 classes:	21	–
		for 1 class:	16	1
8	≥ 8179	for 7680 classes:	85	–
		for 487 classes:	80	1
		for 12 classes:	75	2

This algorithm provides the final bound: $\lambda_k^F = 0$ for all k, $0 \leq k < d$. The algorithm is correct since we can consider the whole set A_v^F instead of $A_{v,i}^F$, $i = 1, \ldots, |A_v^F|/3$, in the proof of the theorem 5.

We computationally found the linear spectra of all quadratic APN functions in $3, 4, 5, 6$ variables, see section 7.

7 Computational results

Here we present results that were obtained using computer calculations. Recall that the exact number of EA-equivalence classes of quadratic APN (n, n)-functions is known for all n from 2 to 6 ([6], [7], [21]). For n equal to $7, 8$ there are known partial results from [43] and updated version of [42]. We took representatives of EA-equivalence classes of APN functions from [6] (note that the function N13 in Table 5 [6] is not quadratic) and updated version of [42].

7.1 Value distribution of Φ_F

By proposition 6, Φ_F is a permutation for a quadratic APN function F in n variables, when n is odd. According to theorem 3, the preimage $\Phi_F^{-1}(v)$ for any nonzero $v \in \mathbb{F}_2^n$, where n is even, is either the empty set or forms a linear subspace of even dimension together with the zero vector. We computationally found value distribution of Φ_F for all known quadratic APN functions in 4, 6, 8 variables (Table 2).

7.2 The linear spectra of quadratic APN functions

We obtained the linear spectra of all quadratic APN functions in $3, 4, 5, 6$ variables as listed in Tables 3, 4, 5, 6. Calculations for $n = 6$ were conducted using supercomputer NKS-30T SSCC SB RAS.

Note 4. *We obtained that the linear spectra of EA-equivalence representatives of quadratic APN functions in $5, 6$ variables are pairwise distinct except two functions N3 and N10 in Table 6 for $n = 6$, which have equal spectra. Moreover, the bound from theorem 5 (2) with the algorithm of note 3 is tight for all considered n. Note 3 is actual for only one function in 6 variables: one set A_v^F of the APN function N11 in Table 6 is of cardinality 15.*

Table 3: The linear spectrum of quadratic APN functions in 3 variables.

N	Λ^F							
1.	0	56	0	280	0	168	0	8

Table 4: The linear spectrum of quadratic APN functions in 4 variables.

N	Λ^F															
1.	0	0	0	0	0	15552	0	25920	0	17280	0	5760	0	960	0	64

7.3 Differentially equivalent APN functions in a small number of variables

Here we summarize the obtained computational results about the differential equivalence classes of APN functions in $n = 2, 3, 4, 5, 6, 7, 8$ variables.

Result 1. Table 7 illustrates a classification under the differential equivalence of **all** APN functions in small number of variables $n = 2, 3, 4$. For these dimensions we see that differential equivalence between two functions implies also their EA-equivalence.

Result 2. Further we study how many affine functions A in n variables exist for a given **quadratic** APN function such that F and $F + A$ belong to the same differential equivalence class.

At first we present mathematical background for our search. Let F be a quadratic APN function, A be an affine function from $\mathbb{F}_2^n$ to itself and $L(x) = A(x) + A(\mathbf{0})$. Then $\gamma_{F+A}(a, b) = \gamma_F(a, b + L(a)) = \gamma_F(a, b) + \Phi_F(a) \cdot L(a)$.

Thus, F and $F + A$ are differentially equivalent if and only if

$$\Phi_F(a) \cdot L(a) = 0 \text{ for all } a \in \mathbb{F}_2^n. \tag{4}$$

The equalities (4) form the system of equations over n^2 binary variables $\ell_{i,j}$, $i, j = 1, \ldots, n$, if we represent L as $L(x) = (\sum_{i=1}^n \ell_{1,i} x_i, \ldots, \sum_{i=1}^n \ell_{n,i} x_i)$. Let r be rank of this system. Then there exist exactly $2^{n^2 - r + n}$ affine functions A such that F and $F + A$ are differentially equivalent.

We computationally studied ranks of system (4) for all known EA-equivalence classes of quadratic APN functions in $2, \ldots, 8$ variables. Our computational results are listed in Table 8. As we can see, for almost all considered EA-equivalence classes in n variables with representative F there exist exactly 2^{2n} trivial affine functions A such that F and $F + A$ are differentially equivalent. The exceptional cases from Table 8 are the following functions in even number of variables:

$n = 4$: APN Gold function x^3;
$n = 6$: 4th APN function from [7] $\alpha^7 x^3 + x^5 + \alpha^3 x^9 + \alpha^4 x^{10} + x^{17} + \alpha^6 x^{18}$;
$n = 8$: APN Gold function x^9.

Table 5: The linear spectra of quadratic APN functions in 5 variables.

N	N[6]	Λ^F															
1.	1.	0	0	0	0	0	5952	0	84320	0	605120	0	2737920	0	6249600	0	9663072
		0	8035200	0	4563200	0	1331264	0	252960	0	25792	0	0	0	0	0	32
2.	2.	0	0	0	0	0	6944	0	74400	0	649760	0	2618880	0	6457920	0	9413088
		0	8243520	0	4444160	0	1375904	0	243040	0	26784	0	0	0	0	0	32

Table 6: The linear spectra of quadratic APN functions in 6 variables.

N	N[6]	Λ^F							
1.	1.	0 0	0 0	0 0	0 0	0 0	0 0	0 0	0 0
		0 0	0 0	0 2565573	0 17869363	0 59537331	0 125825973	0 188763661	0 213866654
		0 190026141	0 135740661	0 79238211	0 38171835	0 15254095	0 5076811	0 1405263	0 325493
		0 62735	0 10311	0 1500	0 190	0 18	0 4	0 0	0 1
2.	2.	0 0	0 0	0 0	0 0	0 0	0 0	0 0	0 0
		0 0	0 0	0 2553543	0 17877699	0 59589621	0 125781705	0 188741889	0 213800958
		0 190121337	0 135798669	0 79173675	0 38162187	0 15236991	0 5094747	0 1409499	0 327285
		0 59859	0 11151	0 882	0 126	0 0	0 0	0 0	0 1
3.	3.	0 0	0 0	0 0	0 0	0 0	0 0	0 0	0 0
		0 0	0 0	0 2542806	0 17905671	0 59586660	0 125776980	0 188633340	0 213945417
		0 190123668	0 135775332	0 79089192	0 38209626	0 15282540	0 5048316	0 1425060	0 329238
		0 54684	0 11340	0 1890	0 63	0 0	0 0	0 0	0 1
4.	4.	0 0	0 0	0 0	0 0	0 0	0 0	0 0	0 0
		0 0	0 0	0 2554340	0 17874904	0 59587206	0 125810414	0 188677693	0 213867958
		0 190098845	0 135772125	0 79211561	0 38138853	0 15249741	0 5086925	0 1411959	0 326341
		0 62023	0 9639	0 1151	0 135	0 9	0 1	0 0	0 1
5.	5.	0 0	0 0	0 0	0 0	0 0	0 0	0 0	0 0
		0 0	0 0	0 2557241	0 17872451	0 59577007	0 125814360	0 188696571	0 213867180
		0 190078715	0 135775295	0 79212625	0 38139345	0 15258109	0 5082923	0 1411065	0 325759
		0 61833	0 9853	0 1346	0 128	0 16	0 1	0 0	0 1
6.	6.	0 0	0 0	0 0	0 0	0 0	0 0	0 0	0 0
		0 0	0 0	0 2560448	0 17872948	0 59553053	0 125832589	0 188720207	0 213854452
		0 190068147	0 135758015	0 79225563	0 38153459	0 15254401	0 5079821	0 1408589	0 325919
		0 62817	0 9957	0 1289	0 133	0 14	0 2	0 0	0 1
7.	7.	0 0	0 0	0 0	0 0	0 0	0 0	0 0	0 0
		0 0	0 0	0 2554224	0 17872307	0 59600606	0 125785578	0 188702449	0 213850382
		0 190100817	0 135791481	0 79195077	0 38133595	0 15258913	0 5085601	0 1412147	0 325797
		0 61795	0 9659	0 1255	0 126	0 13	0 1	0 0	0 1
8.	8.	0 0	0 0	0 0	0 0	0 0	0 0	0 0	0 0
		0 0	0 0	0 2567716	0 17858235	0 59557665	0 125814883	0 188753869	0 213881510
		0 190016913	0 135750653	0 79230265	0 38172707	0 15255327	0 5075247	0 1408231	0 323437
		0 63067	0 10415	0 1455	0 206	0 20	0 2	0 0	0 1
9.	9.	0 0	0 0	0 0	0 0	0 0	0 0	0 0	0 0
		0 0	0 0	0 2555995	0 17877082	0 59574886	0 125801851	0 188718247	0 213851252
		0 190094459	0 135757863	0 79214449	0 38150271	0 15253395	0 5080817	0 1412525	0 325359
		0 62017	0 9901	0 1312	0 131	0 11	0 0	0 0	0 1
10.	10.	0 0	0 0	0 0	0 0	0 0	0 0	0 0	0 0
		0 0	0 0	0 2542806	0 17905671	0 59586660	0 125776980	0 188633340	0 213945417
		0 190123668	0 135775332	0 79089192	0 38209626	0 15282540	0 5048316	0 1425060	0 329238
		0 54684	0 11340	0 1890	0 63	0 0	0 0	0 0	0 1
11.	11.	0 0	0 0	0 0	0 0	0 0	0 0	0 0	0 0
		0 0	0 0	0 0	0 10089045	0 53809170	0 134516080	0 209269815	0 227340608
		0 184963439	0 119789795	0 66717075	0 34914745	0 17946799	0 8758623	0 3769445	0 1351275
		0 395005	0 92041	0 16273	0 2310	0 275	0 5	0 0	0 1
12.	12.	0 0	0 0	0 0	0 0	0 0	0 0	0 0	0 0
		0 0	0 0	0 2579442	0 17845114	0 59521616	0 125838552	0 188808200	0 213899042
		0 189939792	0 135702744	0 79305436	0 38173660	0 15256304	0 5072200	0 1396584	0 327292
		0 62320	0 12040	0 1218	0 266	0 0	0 0	0 0	0 2
13.	14.	0 0	0 0	0 0	0 0	0 0	0 0	0 0	0 0
		0 0	0 0	0 2554106	0 17873083	0 59600915	0 125783545	0 188687890	0 213892662
		0 190078149	0 135762125	0 79218325	0 38152995	0 15239255	0 5085771	0 1413065	0 327485
		0 61575	0 9519	0 1237	0 110	0 10	0 0	0 1	0 1

Note. All values in the table must be multiplied by 64.

Table 7: Cardinalities of differential equivalence classes of APN functions on $\mathbb{F}_2^n$.

n	# APN functions	EA	deg	# differential equivalence classes with cardinalities
2	192	x^3	2	12 classes of 2^4 functions
3	688128	x^3	2	10752 classes of 2^6 functions
4	18 940 805 775 360	x^3	2	1 156 055 040 classes of 2^{10} functions
		f [12]	3	17 340 825 600 classes of 2^{10} functions

Here $f(x) = x^3 + (x^2 + x + 1)tr(x^3)$.

Table 8: Total numbers of affine functions A on $\mathbb{F}_2^n$ such that F and $F + A$ are differentially equivalent, where F is a EA-equivalence representative of quadratic APN functions.

n	# EA classes	# affine functions A: $F + A \in \mathcal{DE}_F$
2	1	2^4
3	1	2^6
4	1	2^{10}
5	2	for all 2 classes: 2^{10}
6	13	for 12 classes: 2^{12}; for 1 class: 2^{13}
7	≥ 487	for all known 487 classes: 2^{14}

8	≥ 8179	for 1 class from known 8179: 2^{20}
		for other 8178 classes: 2^{16}

Result 3. As we know from section 6, the linear spectrum of a quadratic APN function is a differential equivalence invariant. Thus, we can state (see Tables 5, 6) that there are no two quadratic differentially equivalent APN functions in $n = 5, 6$ variables that belong to distinct EA-equivalence classes except possibly functions N3 and N10 in Table 6 (since they have equal spectra). But we succeeded to check that this possibility is not realized. The next question was to understand what quadratic APN functions from the same EA-equivalence class are differentially equivalent. Surprisingly, it happened that if any two quadratic APN functions F and G are in the same differential equivalence class, then $F + G$ is affine.

Our computational proofs of result 3 were based on theorem 3 and the following fact: if F and G are EA-equivalent, then Φ_F and Φ_G are linear equivalent, i. e. $\Phi_G = L' \circ \Phi_F \circ L''$, where L', L'' are linear permutations.

We summarized computational results in theorem 1 in section 3.2.

8 Conclusion

In this paper we introduced the definition of the differential equivalence of vectorial Boolean functions and considered its basic properties in general and quadratic cases. We studied functions that are obtained by adding affine functions to a given Gold function. And this allowed us to start analyzing the differential equivalence classes of APN Gold functions. This theoretical result and computer calculations for a small number of variables showed a remarkable property of APN

Gold functions, which is not usual for almost all known quadratic APN functions.

Also, we formulated a conjecture about the differential equivalence of quadratic APN functions that would be interesting to study further. It states that if two quadratic APN functions are differentially equivalent, then their sum is an affine function. But the most exciting problem that remains open about the differential equivalence in common case is the existence of two differentially equivalent APN functions that are not CCZ-equivalent. The positive answer to this question can give a new method for constructing APN functions inequivalent to the known ones.

Acknowledgements. The author would like to thank Natalia Tokareva, Nikolay Kolomeec and Valeriya Idrisova for fruitful discussions related to this work. The author is also very grateful to the reviewers for the valuable comments and remarks.

References

[1] Bending T. D., Fon-Der-Flaass D.: Crooked functions, bent functions, and distance regular graphs. Electron. J. Combin. 5 (1) (1998) R34.

[2] Berger T.P., Canteaut A., Charpin P., Laigle-Chapuy Y.: On almost perfect nonlinear functions over $\mathbb{F}_2^n$. IEEE Trans. Inf. Theory 52, 4160–4170 (2006).

[3] Beth T., Ding C.: On almost perfect nonlinear permutations. Advances in Cryptology-EUROCRYPT'93, Lecture Notes in Computer Science, 765, Springer-Verlag, New York, pp. 65–76 (1993).

[4] Bierbrauer J., Kyureghyan G. M.: Crooked binomials. Des. Codes Cryptogr. 46, 269–301 (2008).

[5] Boura C., Canteaut A., Jean J., Suder V.: Two Notions of Differential Equivalence on Sboxes. Extended abstract of The Tenth International Workshop on Coding and Cryptography 2017 (September 18-22, 2017, Saint-Petersburg, Russia).

[6] Brinkman M., Leander G.: On the classification of APN functions up to dimension five. Proc. of the International Workshop on Coding and Cryptography 2007 dedicated to the memory of Hans Dobbertin. Versailles, France, 39–48 (2007).

[7] Browning K. A., Dillon J. F., Kibler R. E., McQuistan M. T.: APN Polynomials and Related Codes. Journal of Combinatorics, Information and System Science, Special Issue in honor of Prof. D.K Ray-Chaudhuri on the occasion of his 75th birthday, vol. 34, no. 1-4, pp. 135–159 (2009).

[8] Browning K. A., Dillon J. F., McQuistan M. T., Wolfe A. J.: An APN Permutation in Dimension Six. Post-proceedings of the 9-th International Conference on Finite Fields and Their Applications Fq'09, Contemporary Math., AMS, v. 518, pp. 33–42 (2010).

[9] Budaghyan L.: Construction and analysis of cryptographic functions. Springer International Publishing, VIII, 168, 2014.

[10] Budaghyan L., Carlet C.: CCZ-equivalence of single and multi output Boolean functions. Post-proceedings of the 9-th International Conference on Finite Fields and Their Applications Fq'09, Contemporary Math., AMS, v. 518, pp. 43–54 (2010).

[11] Budaghyan L., Carlet C., Leander G.: Constructing new APN functions from known ones. Finite Fields and Their Applications. 15(2), 150–159 (2009).

[12] Budaghyan L., Carlet C., Pott A.: New classes of almost bent and almost perfect nonlinear polynomials. IEEE Trans. Inform. Theory 52, 1141–1152 (2006).

[13] Canteaut A., Charpin P., Dobbertin H.: Binary m-sequences with three-valued crosscorrelation: a proof of Welch conjecture, IEEE Trans. Inf. Theory. 46(1), 4–8 (2000).

[14] Carlet C.: Open Questions on Nonlinearity and on APN Functions. Arithmetic of Finite Fields, Lecture Notes in Computer Science. 9061, 83–107 (2015).

[15] Carlet C. Vectorial Boolean functions for cryptography. Ch. 9 of the monograph "Boolean Methods and Models in Mathematics, Computer Science, and Engineering", Cambridge Univ. Press, 2010, pp. 398–472.

[16] Carlet C., Charpin P., Zinoviev V.: Codes, bent functions and permutations suitable for DES-like cryptosystems. Des. Codes Cryptogr. 15, 125–156 (1998).

[17] Carlet C., Prouff E.: On plateaued functions and their constructions. Proceedings of Fast Software Encryption 2003, Lecture notes in computer science. 2887, 54–73 (2003).

[18] Dobbertin H.: Almost perfect nonlinear functions over $GF(2^n)$: the Niho case. Inform. and Comput. 151, 57–72 (1999).

[19] Dobbertin H.: Almost perfect nonlinear power functions on $GF(2^n)$: the Welch case. IEEE Trans. Inf. Theory. 45(4), 1271–1275 (1999).

[20] Dobbertin H.: Almost perfect nonlinear power functions over $GF(2^n)$: a new case for n divisible by 5. Proceedings of Finite Fields and Applications FQ5, pp. 113–121 (2000).

[21] Edel Y.: Quadratic APN functions as subspaces of alternating bilinear forms. Contact Forum Coding Theory and Cryptography III, Belgium (2009), pp. 11–24 (2011).

[22] Edel Y., Pott A.: A new almost perfect nonlinear function which is not quadratic. Advances in Mathematics of Communications. 3(1), 59–81 (2009).

[23] Glukhov M. M.: On the matrices of transitions of differences for some modular groups. Matematicheskie Voprosy Kriptografii. 4(4), 27–47 (2013) (in Russian).

[24] Glukhov M. M.: On the approximation of discrete functions by linear functions. Matematicheskie Voprosy Kriptografii. 7(4), 29–50 (2016) (in Russian).

[25] Gold R.: Maximal recursive sequences with 3-valued recursive crosscorrelation functions. IEEE Trans. Inform. Theory. 14, 154–156 (1968).

[26] Gorodilova A.A.: Characterization of almost perfect nonlinear functions in terms of subfunctions. Discrete Mathematics and Applications. 26(4), 193–202 (2016).

[27] Gorodilova A.A.: On a remarkable property of APN Gold functions // Cryptology ePrint Archive, Report 2016/286 (2016).

[28] Gorodilova A.: The linear spectrum of quadratic APN functions. Prikladnaya Diskretnaya Matematika. 4(34), 3–16 (2016) (in Russian).

[29] Hernando F., McGuire G.: Proof of a conjecture on the sequence of exceptional numbers, classifying cyclic codes and APN functions. Journal of Algebra. 343(1), 78–92 (2011).

[30] Hollmann H., Xiang Q.: A proof of the Welch and Niho conjectures on crosscorrelations of binary m-sequences. Finite Fields and Their Applications. 7, 253–286 (2001).

[31] Hou X.-D.: Affinity of permutations of $\mathbb{F}_2^n$. Discret. Appl. Math. 154, 313–325 (2006).

[32] Idrisova V.: On an algorithm generating 2-to-1 APN functions and its applications to "the big APN problem". Cryptogr. Commun. (2018).

[33] Janwa H., Wilson R.: Hyperplane sections of Fermat varieties in P^3 in char. 2 and some applications to cyclic codes. Proceedings of AAECC-10, LNCS, vol. 673, Berlin, Springer-Verlag, pp. 180–194 (1993).

[34] Kasami T.: The weight enumerators for several classes of subcodes of the second order binary Reed-Muller codes. Inform. and Control. 18, 369–394 (1971).

[35] Kyureghyan G.: Crooked maps in F_2^n. Finite Fields Their Appl. 13(3), 713–726 (2007).

[36] Nyberg K.: Perfect nonlinear S-boxes. In: Davies, D.W. (ed.) EUROCRYPT 1991. LNCS, vol. 547, pp. 378–386. Springer, Heidelberg (1991).

[37] Nyberg K.: Differentially uniform mappings for cryptography. Advances in Cryptography, EUROCRYPT'93, Lecture Notes in Computer Science. 765, 55–64 (1994).

[38] Pott A.: Almost perfect and planar functions. Des. Codes Cryptogr. 78, 141–195 (2016).

[39] Suder V.: Antiderivative functions over F_{2^n}. Des. Codes Cryptogr. 82, 435–447 (2017).

[40] Tuzhilin M. E.: APN functions. Prikladnaya Diskretnaya Matematika. 3, 14–20 (2009) (in Russian).

[41] Yoshiara S.: Equivalences of quadratic APN functions. J. Algebr. Comb. 35, 461–475 (2012).

[42] Yu Y., Wang M., Li Y.: A matrix approach for constructing quadratic apn functions. Cryptology ePrint Archive, Report 2013/007 (2013). http://eprint.iacr.org/.

[43] Yu Y., Wang M., Li Y.: A matrix approach for constructing quadratic APN functions. Des. Codes Cryptogr. 73, 587–600 (2014).