Noname manuscript No.
(will be inserted by the editor)

The classification of quadratic APN functions in 7 variables

Konstantin Kalgin · Valeriya Idrisova

Received: date / Accepted: date

Abstract Almost perfect nonlinear functions possess optimal resistance to differential cryptanalysis and are widely studied. Most known APN functions are defined using their representation as a polynomial over a finite field and very little is known about combinatorial constructions of them on $\mathbb{F}_2^n$. In this work we propose two approaches for obtaining quadratic APN functions on $\mathbb{F}_2^n$. The first approach exploits a secondary construction idea, it considers how to obtain a quadratic APN function in $n+1$ variables from a given quadratic APN function in n variables using special restrictions on the new terms. The second approach is searching for quadratic APN functions that have a matrix representation partially filled with the standard basis vectors in a cyclic manner. This approach allows us to find a new APN function in 7 variables. We prove that the updated list of quadratic APN functions in dimension 7 is complete up to CCZ-equivalence.

Keywords Boolean function · APN function · quadratic function · differential uniformity · S-box

The work is supported by Mathematical Center in Akademgorodok under agreement No. 075-15-2019-1613 with the Ministry of Science and Higher Education of the Russian Federation and Laboratory of Cryptography JetBrains Research. We are grateful to the Supercomputing Center of the Novosibirsk State University for provided computational resources.

Konstantin Kalgin
Sobolev Institute of Mathematics,
Institute of Computational Mathematics and Mathematical Geophysics of the Siberian Branch of the RAS,
Novosibirsk State University, Novosibirsk, Russia
E-mail: kalginkv@gmail.com

Valeriya Idrisova
Sobolev Institute of Mathematics, Novosibirsk, Russia
E-mail: vvitkup@yandex.ru

1 Introduction

Vectorial Boolean functions are components of many block ciphers, and their properties affect the cryptographic strength of the corresponding cipher. Functions that show optimal resistance to differential attack [4] are called almost perfect nonlinear (APN) functions. APN functions have been widely studied since the 90's [47], but there is still a significant list [24] of important open questions, such as lower and upper bounds on the number of APN functions, the minimum distance between two APN functions, an upper bound on the algebraic degree of an APN function, the existence of bijective APN functions in even dimensions, etc. Moreover, at the moment we know more than 20 000 CCZ-inequivalent instances of APN functions, but only about 20 infinite families have been constructed so far [22]. In particular, finding a secondary construction of APN functions is a well-known open problem which was stated as Problem 3.8 in [24]. Another problem is to find new APN functions in the vector space $\mathbb{F}_2^n$ without using the finire field structure, since, to the best of our knowledge all the known constructions of this class are found only using their representation as polynomials over finite fields, and there are only a few combinatorial approaches to search for APN functions over $\mathbb{F}_2^n$. The classification of APN functions is another hard open problem. A complete classification of APN functions (up to CCZ-equivalence) was obtained up to 5 variables, and quadratic and cubic APN functions were classified for dimension 6. Also, quadratic APN polynomials over finite fields with binary coefficients have been classified up to $n = 9$.

This paper is devoted to methods of searching for APN functions and corresponding problems. We investigate a few combinatorial approaches to search for APN functions, in particular, quadratic APN functions. Moreover, we provide a complete classification of quadratic APN functions in dimension 7. Generally, quadratic APN functions are not suitable for use as S-boxes (components of symmetric ciphers that perform substitutions of bits) due to the low algebraic degree, but obtaining new quadratic representatives can lead us to other useful functions. This is also one of the topics that we discuss in our work. Moreover, this is especially important for even dimensions $n \geqslant 8$, since new APN permutations CCZ-equivalent to quadratic functions might be found in a similar way that this was done for dimension six [10].

We start in Section 2 by considering necessary definitions, discussing relevant open problems and surveying some results in this area. Further, we propose two approaches for generating quadratic APN functions on $\mathbb{F}_2^n$. The first approach is described in Section 3. It considers the algebraic normal form of a given quadratic APN function G in n variables and extends it into an ANF of a quadratic function F in $n+1$ variables, using special restrictions on the coefficients of the new terms. In Section 4 we propose another method to generate quadratic APN functions, which we call the cyclic approach. In this method we consider special matrices that are partially filled with the vectors of the standard basis, and search for corresponding APN functions using the same idea of restrictions. Using this approach we found one previously unknown (up

to CCZ-equivalence) quadratic APN function for $n = 7$. In Section 5 we show that the updated list of quadratic APN functions in 7 variables is complete up to CCZ-equivalence. Thus, all quadratic APN functions in 7 variables fall into exactly 488 distinct CCZ-classes. In Section 6 we observe that the quadratic parts of some non-quadratic APN functions have a low differential uniformity. Based on this, we introduce the notion of a stacked APN function and find such functions in dimensions up to 6 using quadratic APN functions obtained with some of the approaches mentioned above.

2 Preliminaries

2.1 Definitions

Let $\mathbb{F}_2$ be the finite field with two elements. Let $\mathbb{F}_2^n$ be the n-dimensional vector space over $\mathbb{F}_2$. A function F from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$, where n and m are positive integers, is called a *vectorial Boolean function*. If $m = 1$, such a function is called *Boolean*. Every vectorial Boolean function F can be represented as an ordered set of m *coordinate functions* $F = (f_1, \ldots, f_m)$, where f_i is a Boolean function in n variables. Any vectorial function F can be represented uniquely in its *algebraic normal form (ANF)*:

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

where $\mathcal{P}(N)$ is the power set of $N = \{1, \ldots, n\}$, $x = (x_1, x_2, \ldots, x_n)$ and $a_I \in \mathbb{F}_2^m$. The *algebraic degree* of a given function F is the degree of its ANF: $\deg(F) = \max\{|I| : a_I \neq 0, I \in \mathcal{P}(N)\}$. If the algebraic degree of a function F is at most 1 then F is called *affine*. If for an affine function F it holds $F(\mathbf{0}) = \mathbf{0}$ then F is called *linear*. If the algebraic degree of a function F is equal to 2 then F is called *quadratic*.

Let us further consider the case $m = n$ only. It is well known that we can put the finite field $\mathbb{F}_{2^n}$ in a one-to-one correspondence with the vector space $\mathbb{F}_2^n$ and consider a vectorial Boolean function as a function over $\mathbb{F}_{2^n}$. Then any vectorial function F has a unique *univariate polynomial representation* over $\mathbb{F}_{2^n}$:

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

2.2 APN functions

Let F be a vectorial Boolean function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$. For vectors $a, b \in \mathbb{F}_2^n$, where $a \neq 0$, consider the value

$$\delta_F(a, b) = \big| \{ \ x \in \mathbb{F}_2^n \ \big| \ F(x + a) + F(x) = b \} \big|.$$

Denote by Δ_F the following value:

$$\Delta_F = \max_{a \neq \mathbf{0},\ b \in \mathbb{F}_2^n} \delta_F(a, b).$$

Then F is called a *differentially Δ_F-uniform* function. The smaller the parameter Δ_F, the better the resistance of a cipher containing F as an S-box to differential attack [4]. The smallest possible value of Δ_F is equal to 2. In this case the function F is called *almost perfect nonlinear (APN)*. This notion was introduced by K. Nyberg [47], also differential properties of vectorial functions were investigated in the USSR, but these results were not published [37]. Despite extensive reserch, there are many important open problems. One of these problems is to find lower and upper bounds on the number of APN functions (most recent improvement of previous results was made in [45]). Another open problem is to find an upper bound on the algebraic degree of an APN function, for some partial answers see [12]. The minimum distance between two APN functions is also unknown, but there exist some results on this question [13], [42]. The problem on existence of bijective APN functions in even dimensions is referred as "Big APN problem" and widely mentioned [1]. For further details, we refer the reader to the reviews of C. Blondeau and K. Nyberg [5], C. Carlet [24], M. M. Glukhov [37], A. Pott [48], M. E. Tuzhilin [50] and to the books of L. Budaghyan [11], C. Carlet [25] for an exhaustive discussion of the topic.

Well-known examples of constructions of APN functions are monomial functions over $\mathbb{F}_{2^n}$, they are provided in Table 1. Also, there exist many constructions and infinite families of APN functions over finite fields (for example, see [14], [15], [17], [18] and [19] of L. Budaghyan et al., the paper of Y. Edel et al. [32]). All known infinite families of quadratic APN polynomials are listed in Table 2. Several combinatorial approaches for searching for new APN functions from known ones have been proposed. An approach using special matrices was proposed in [52] and further developed in [53] and [54]. Y. Edel and A. Pott proposed the so-called switching method that searches for suitable coordinate functions in order to obtain a new APN function from a given one [31]. A combinatorial approach using subfunctions was proposed by A. Gorodilova [35]. V. Idrisova introduced an approach for finding APN permutations using 2-to-1 APN functions [40]. Recently, more than 13 000 new quadratic APN functions were found with a recursive tree search algorithm [2]. For more on constructions of APN functions the reader can consult [22].

2.3 Classifications of APN functions

Let us recall the main equivalence relations that preserve the APN property of a given vectorial Boolean function. Two vectorial Boolean functions F and G are *extended affine equivalent (EA-equivalent)* if $F = A_1 \circ G \circ A_2 + A$ where A_1, A_2 are affine permutations on $\mathbb{F}_2^n$ and A is an affine function. Two functions F and G are called *Carlet-Charpin-Zinoviev [26] equivalent (CCZ-equivalent)*

Table 1 Known APN power functions x^d on $\mathbb{F}_{2^n}$.

Functions	Exponents	Conditions	References
Gold	$d = 2^t + 1$	$\gcd(t, n) = 1$	[33], [47]
Kasami	$d = 2^{2t} - 2^t + 1$	$\gcd(t, n) = 1$	[41], [44]
Welch	$2^t + 3$	$n = 2t + 1$	[23], [28]
Niho	$2^t + 2^{\frac{t}{2}} - 1$, t even $2^t + 2^{\frac{3t+1}{2}} - 1$, t odd	$n = 2t + 1$	[29], [39]
Inverse	$2^{2t} - 1$	$n = 2t + 1$	[3], [47]
Dobbertin	$2^{4t} + 2^{3t} + 2^{2t} + 2^t - 1$	$n = 5t$	[30]

if their graphs $\Gamma_F = \{(x, F(x)) \mid x \in \mathbb{F}_2^n\}$ and $\Gamma_G = \{(x, G(x)) \mid x \in \mathbb{F}_2^n\}$ are affine equivalent, that is, there exists an affine permutation A of $\mathbb{F}_2^n \times \mathbb{F}_2^n$ such that $\{A(x, y) \mid (x, y) \in \Gamma_F\} = \Gamma_G$. Let us recall that in the case of quadratic APN functions, two APN functions are CCZ-equivalent if and only if they are EA-equivalent [51], but in general, CCZ-equivalence does not imply EA-equivalence. Also, there exists the notion of DDT-equivalence which applies to vectorial Boolean functions that share the same difference distribution table [6], [36]. It is an open question whether DDT-equivalence implies CCZ-equivalence.

To find a complete classification of APN functions under CCZ-equivalence is a complicated open question. M. Brinkmann and G. Leander found a complete classification of APN functions up to $n = 5$ [9]. When $n = 6$ APN functions have been classified only for algebraic degree up to 3 (the list can be found in [9] and a complete classification of cubics was described by P. Langevin in [46]). Also, M. Calderini provided all the representatives of the EA-classes of APN functions in 6 variables as well as partial results for 7, 8 and 9 variables [21]. Moreover, the classification for quadratic APN functions over $\mathbb{F}_{2^n}$ with coefficients from $\mathbb{F}_2$ up to $n = 9$ was obtained by Y. Yu et al. [53]. Until recently there were known 487 CCZ-classes of quadratic APN functions in 7 variables and 8179 CCZ-classes of quadratic APN functions in 8 variables; most of them were found in [52]. However, C. Beierle and G. Leander found 12921 new quadratic APN functions in dimension 8, 35 new quadratic APN functions in dimension 9 and five new quadratic APN functions in dimension 10 in their very recent breakthrough work [2]. In the conference version of this paper [43] we found a new APN function in 7 variables, later this function was also independently found in [2].

3 On a secondary approach to search for quadratic APN functions

Since EA-equivalence preserves the APN property, it is always possible to omit linear and constant terms in the algebraic normal form of a given APN function. We shall then consider quadratic vectorial Boolean functions that

Table 2 Known classes of quadratic APN polynomials on $\mathbb{F}_{2^n}$ inequivalent to power functions [22].

Functions	Conditions	References
$x^{2^s+1} + u^{2^k-1}x^{2^{ik}+2^{mk+s}}$	$n = pk$, $\gcd(k,p) = \gcd(s,pk) = 1$, $p \in \{3,4\}$, $i = sk \bmod p$, $m = p-i$, $n \geqslant 12$, u primitive in $\mathbb{F}^*_{2^n}$	[16]
$sx^{q+1} + x^{2^i+1} + x^{q(2^i+1)} + cx^{2^iq+1} + c^q x^{2^i+q}$	$q = 2^m$, $n = 2m$, $\gcd(i,m) = 1$, $c \in \mathbb{F}_{2^n}$, $s \in \mathbb{F}_{2^n} \setminus \mathbb{F}_q$, $X^{2^i+1} + cX^{2^i} + c^qX + 1$ has no solution x such that $x^{q+1} = 1$	[19]
$x^3 + a^{-1}Tr(a^3x^9)$	$a \neq 0$	[14]
$x^3 + a^{-1}Tr_n^3(a^3x^9 + a^6x^{18})$	$3 \mid n$, $a \neq 0$	[15]
$x^3 + a^{-1}Tr_n^3(a^6x^{18} + a^{12}x^{36})$	$3 \mid n$, $a \neq 0$	[15]
$ux^{2^s+1} + u^{2^k}x^{2^{-k}+2^{k+s}} + vx^{2^{-k}+1} + wu^{2^k+1}x^{2^s+2^{k+s}}$	$n = 3k$, $\gcd(k,3) = \gcd(s,3k) = 1$, $v, w \in \mathbb{F}_{2^k}$, $vw \neq 1$, $3 \mid (k+s)$, u primitive in $\mathbb{F}^*_{2^n}$	[7, 8]
$(x + x^{2^m})^{2^i+1} + u'(ux + u^{2^m}x^{2^m})^{(2^i+1)2^j} + u(x + x^{2^m})(ux + u^{2^m}x^{2^m})$	$n = 2m$, $m \geqslant 2$ even, $\gcd(i,m) = 1$ and $j \geqslant 2$ even, u primitive in $\mathbb{F}^*_{2^n}$, $u' \in \mathbb{F}_{2^m}$ not a cube	[55]
$L(x)^{2^i}x + L(x)x^{2^i}$	$n = km$, $m > 1$, $\gcd(n,i) = 1$, $L(x) = \sum_{j=0}^{k-1} a_j x^{2^{jm}}$ satisfies the conditions in Theorem 6.3 of [17]	[17]
$u(u^qx + x^qu)(x^q + x) + (u^qx + x^qu)^{2^{2i}+2^{3i}} + a(u^qx + x^qu)^{2^{2i}}(x^q + x)^{2^i} + b(x^q + x)^{2^i+1}$	$q = 2^m$, $n = 2m$, $\gcd(i,m) = 1$, u primitive in $\mathbb{F}^*_{2^n}$, $X^{2^i+1} + aX + b$ has no solution over $\mathbb{F}_{2^m}$	[49]
$x^3 + ax^{2^k(2^i+1)} + bx^{3\cdot 2^m} + cx^{2^{n+k}(2^i+1)}$	$n = 2m = 10$, $(a,b,c) = (\beta,0,0)$, $i = 3$, $k = 2$, $\mathbb{F}_4^* = \langle\beta\rangle$, or $n = 2m$, m odd, $3 \nmid m$, $(a,b,c) = (\beta,\beta^2,1)$ $\mathbb{F}_4^* = \langle\beta\rangle$, $i \in \{m-2, m, 2m-1, (m-2)^{-1} \bmod n\}$	[20]
$u[(u^qx + x^qu)^{2^i+1} + (u^qx + x^qu)(x^q + x)^{2^i} + (x^q + x)^{2^i+1}] + (u^qx + x^qu)^{2^{2i}+1} + (u^qx + x^qu)^{2^{2i}}(x^q + x) + (x^q + x)^{2^{2i}+1}$	$q = 2^m$, $n = 2m$, $gcd(3i,m) = 1$, u primitive in $\mathbb{F}^*_{2^n}$	[34]
$u[(u^qx + x^qu)^{2^i+1} + (u^qx + x^qu)(x^q + x)^{2^i} + (x^q + x)^{2^i+1}] + (u^qx + x^qu)^{2^{3i}}(x^q + x) + (u^qx + x^qu)(x^q + x)^{2^{3i}}$	m odd, $q = 2^m$, $n = 2m$, $gcd(3i,m) = 1$, u primitive in $\mathbb{F}^*_{2^n}$	[34]

have only quadratic terms in their ANF. The following result of T. Beth and C. Ding gives a necessary condition on the ANF of a given APN function.

Theorem 1 *(Theorem 6 in [3]) Let $F = (f_1, \ldots, f_n)$ be an APN function in n variables. Then every quadratic term x_ix_j, where $i \neq j$, appears in at least one coordinate function of F.*

Proof Without loss of generality consider an APN function F such that there is no quadratic term x_1x_2. Therefore, $F(x_1, x_2, 0, \ldots, 0) = a_0 + a_1x_1 + a_2x_2$, where

$a_0, a_1, a_2 \in \mathbb{F}_2^n$. Let $x = (0, 0, \ldots, 0), y = (1, 0, \ldots, 0)$ and $a = (0, 1, 0, \ldots, 0)$. Then $F(x)+F(x+a)+F(y)+F(y+a) = a_0+a_0+a_2+a_0+a_1+a_0+a_1+a_2 = 0$, thus, we have a contradiction to the definition of an APN function.

This property motivated us to suggest the following construction of quadratic APN functions. Let $G = (g_1, \ldots, g_n)$ be a quadratic APN function in n variables. Consider a vectorial Boolean function $F = (f_1, \ldots, f_n, f_{n+1})$ in $n + 1$ variables such that:

$$\begin{aligned} f_1 &= g_1 + \sum_{i=1}^{n} \alpha_{1,i} x_i x_{n+1}; \\ &\ldots \\ f_n &= g_n + \sum_{i=1}^{n} \alpha_{n,i} x_i x_{n+1}; \\ f_{n+1} &= g_{n+1} + \sum_{i=1}^{n} \alpha_{n+1,i} x_i x_{n+1}, \end{aligned} \tag{1}$$

where $\alpha_{1,i} \ldots, \alpha_{n+1,i} \in \mathbb{F}_2$ for $i = 1, \ldots, n$ and $g_{n+1} = \sum_{1 \leqslant j < k \leqslant n} \beta_{j,k} x_j x_k$ for some fixed $\beta_{j,k} \in \mathbb{F}_2$. Note that if $\alpha_{1,i}, \ldots, \alpha_{n,i}$ are such that each term $x_i x_{n+1}$ appears in at least one of the coordinate functions $f_1, \ldots, f_n$, then the necessary condition of Theorem 1 is satisfied for the constructed function F. Since an exhaustive search for the given APN function becomes infeasible starting from $n = 6$, we need to find some necessary and sufficient conditions on the new coefficients of F.

Let us denote the lexicographically ordered elements of $\mathbb{F}_2^n$ as $x^0, \ldots, x^{2^n-1}$. Since all the values $G(x^0), \ldots, G(x^{2^n-1})$ of the function G are known, we can represent values of the constructed function F only through the unknown coefficients $\alpha_{i,k}$ and some constant terms. Since F is an APN function, for a nonzero a all the sums $F(x) + F(x + a)$ and $F(y) + F(y + a)$, where $x \neq y$ and $x \neq y + a$, should be pairwise distinct. Then additional restrictions on the coefficients $\alpha_{i,k}$ can be obtained from this condition. For the convenient representation of these restrictions further we consider the following matrix approach that was also proposed by T. Beth and C. Ding in [3].

Each quadratic vectorial Boolean function G in n variables can be considered as a symmetric matrix $\mathcal{G} = (g_{ij})$, where each element $g_{ij} \in \mathbb{F}_2^n$ is a vector of the coefficients corresponding to the term $x_i x_j$ in the algebraic normal form of G and all the diagonal elements g_{ii} are null.

Example 1 Let us consider the function $G = (g_1, g_2, g_3) = (x_1x_2 + x_2x_3,$
$x_2x_3, x_1x_2 + x_1x_3) = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} \cdot x_1x_2 + \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \cdot x_1x_3 + \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} \cdot x_2x_3.$

Then the corresponding matrix $\mathcal{G}$ is the following:

$$\mathcal{G} = \begin{bmatrix} (000) & (101) & (001) \\ (101) & (000) & (110) \\ (001) & (110) & (000) \end{bmatrix}.$$

It is necessary to mention that matrices of a similar form were used in [52] and [53] to construct and classify a lot of new quadratic APN functions using the univariate representation. We refer the reader to the book of C. Carlet for more details on the link between the algebraic normal form and the univariate representation of a given vectorial Boolean function [25]. Using these matrices the APN property can be formulated in the following way:

Proposition 1 *Let $\mathcal{G}$ be the matrix that corresponds to the quadratic vectorial function G. Then the function G is APN if and only if $x\mathcal{G}a^T \neq 0$ for all $a, x \in \mathbb{F}_2^n \backslash \{0\}$ with $x \neq a$.*

Proof The proof follows directly from Theorem 10 of [3]. This theorem states that a permutation G is APN if and only if the rank of the matrix $\mathcal{G}a^T$ is equal to $n-1$ for any nonzero $a \in \mathbb{F}_2^n$. Since there is no a requirement for the function to be bijective in the original proof, it can be generalized to non-bijective vectorial Boolean functions.

In terms of matrices the method described in (1) can be considered as an extension of a given $\mathcal{G}$ with an extra bit that represents g_{n+1} in every element and an extra pair of row and column that represents the set of new terms $x_i x_{n+1}$.

Example 2 For the previously considered function $G = (g_1, g_2, g_3) = (x_1x_2 + x_2x_3, x_2x_3, x_1x_2 + x_1x_3)$ we choose null g_{n+1} and construct an APN function $F = (f_1, f_2, f_3, f_4)$ in 4 variables, where:
$f_1 = g_1 + x_3x_4$;
$f_2 = g_2$;
$f_3 = g_3 + x_2x_4$;
$f_4 = x_1x_4 + x_3x_4$.
Then the corresponding matrix $\mathcal{F}$ is the following:

$$\mathcal{F} = \begin{bmatrix} (0000) & (1010) & (0010) & (0001) \\ (1010) & (0000) & (1100) & (0010) \\ (0010) & (1100) & (0000) & (1001) \\ (0001) & (0010) & (1001) & (0000) \end{bmatrix}.$$

Consider a quadratic APN function G and the corresponding $n \times n$ matrix $\mathcal{G}$. Denote the vector of nonzero coefficients for the new variables by $\alpha = (\alpha_1, \ldots, \alpha_n)$, where $\alpha_i \in \mathbb{F}_2^{n+1}$. Let us fix g_{n+1} and construct an $(n+1)\times(n+1)$ matrix $\mathcal{F}$ by adding $(\alpha_1, \ldots, \alpha_n, 0)$ to $\mathcal{G}$ as the last column and the last row and adding a new bit to every element of $\mathcal{G}$ according to the choice of g_{n+1}. Let us denote by $\mathcal{G}'$ the submatrix (f_{ij}) of $\mathcal{F}$, such that $i, j < n+1$. Let

$B = (b_1, \ldots, b_m)$ be a vector of length m, where m is some positive integer and $b_i \in \mathbb{F}_2^n$, for $i = 1, \ldots, m$. Then $\langle B \rangle$ denotes the linear span of the set $\{b_1, \ldots, b_m\}$. Let F be the quadratic vectorial function corresponding to the constructed matrix $\mathcal{F}$. Then the following proposition is true.

Proposition 2 *F is APN if and only if $\alpha a'$ does not belong to $\langle \mathcal{G}' a'^T \rangle$ for any $a' \in \mathbb{F}_2^n$, $a' \neq 0$.*

Proof Let us note that $\mathcal{F} = \begin{bmatrix} \mathcal{G}' & \alpha^T \\ \alpha & 0 \end{bmatrix}$. Consider some $x = (x', \beta)$, $a = (a', \gamma)$ for $\beta, \gamma \in \{0, 1\}$, $x', a' \in \mathbb{F}_2^n$ and $\alpha = (\alpha_1, \ldots, \alpha_n)$, where $\alpha_i \in \mathbb{F}_2^{n+1}$. Then we can write $x\mathcal{G}a^T = (x', \beta) \begin{bmatrix} \mathcal{G}' & \alpha^T \\ \alpha & 0 \end{bmatrix} (a', \gamma)^T = x'\mathcal{G}'a'^T + \gamma(\alpha x') + \beta(\alpha a')$.

Let us prove that if the function F ia APN then $\alpha a'$ does not belong to $\langle \mathcal{G}' a'^T \rangle$ for any $a' \in \mathbb{F}_2^n$, $a' \neq 0$. Since the function F is APN, from Proposition 1, we have that $x\mathcal{G}a^T \neq 0$ for all $x \neq a$, where $a, x \in \mathbb{F}_2^n \backslash \{0\}$. Let $\gamma = 0, \beta = 1$, therefore, $x\mathcal{G}a^T = x'\mathcal{G}'a'^T + \alpha a' \neq 0 \Rightarrow x'\mathcal{G}'a'^T \neq \alpha a'$ for all x'. It can be seen that all possible x' give us all possible vectors of $\langle \mathcal{G}' a'^T \rangle$, therefore, $\alpha a'$ does not belong to $\langle \mathcal{G}' a'^T \rangle$ for any $a' \in \mathbb{F}_2^n$, $a' \neq 0$.

Suppose that we have that $\alpha a' \notin \langle \mathcal{G}' a'^T \rangle$, i.e., $\alpha a' \neq x'\mathcal{G}'a'^T$ for all $a' \in \mathbb{F}_2^n \backslash \{0\}$ and all x', and we want to prove that the relation $x\mathcal{G}a^T \neq 0$ holds for all nonzero x and a such that $x \neq a$. There are 4 possible cases for the choice of β and γ:

1) $\beta = 0, \gamma = 0$. Therefore, $x\mathcal{G}a^T = x'\mathcal{G}'a'^T \neq 0$ since G is an APN function and we have that $a' \neq 0$, $x' \neq 0$, $a' \neq x'$, since we consider only the case $a \neq 0$, $x \neq 0$ and $a \neq x$ due to Proposition 2.

2) $\beta = 1, \gamma = 0$. Therefore, $x\mathcal{G}a^T = x'\mathcal{G}'a'^T + \alpha a' \neq 0$ since we have that $\alpha a' \notin \langle \mathcal{G}' a'^T \rangle$ for all $a' \in \mathbb{F}_2^n$, $a' \neq 0$. As we showed above, we also do not consider the case $a' = 0$ since $\gamma = 0$.

3) $\beta = 0, \gamma = 1$. Therefore, $x\mathcal{G}a^T = x'\mathcal{G}'a'^T + \alpha x' \neq 0$ as we have seen in the previous case (we just need to denote x' by a' since the matrix $\mathcal{G}'$ is symmetric).

4) $\beta = 1, \gamma = 1$. Therefore, $x\mathcal{G}a^T = x'\mathcal{G}'a'^T + \alpha x' + \alpha a'$. Let us note that $x'\mathcal{G}'x'^T$ is equal to 0 since the matrix $\mathcal{G}'$ is symmetric and the main diagonal is zero, so, we can write $x'\mathcal{G}'a'^T + \alpha x' + \alpha a' = x'\mathcal{G}'a'^T + x'\mathcal{G}'x'^T + \alpha x' + \alpha a' = x'\mathcal{G}'(a' + x')^T + \alpha(a' + x')$. Since we consider the case $a \neq x$ then $a' \neq x'$ as well. So, $(a' + x') \neq 0$ and if we denote $(a' + x')$ by a'' we obtain case 2 again. This proves the statement.

Remark 1 Let us note that Proposition 2 shows how to obtain restrictions on the new coefficients in a convenient form. Our algorithm for searching for APN functions using these restrictions is very similar to Algorithm 1 in [52], but in our work we start from a $n \times n$ matrix corresponding to an APN function in n variables, add an extra bit to each element that corresponds to g_{n+1} and search through all possible values of the elements in the last column in order

to construct a $(n+1) \times (n+1)$ matrix corresponding to an APN function in $n+1$ variables. In [52] the authors started from a $n \times n$ matrix corresponding to an APN function and searched through all possible evaluations of the last column (or last few columns) in order to construct a $n \times n$ matrix.

Let us show that our method can be also extended to the case when G is not an APN function, but the ANF of G and g_{n+1} together contain all possible quadratic terms. The following proposition describes a necessary condition on the choice of such functions.

Proposition 3 *Let G be a quadratic vectorial function in n variables and F be an APN function in $n+1$ variables that is obtained from G using the method from (1). Then $\Delta_G \leqslant 4$.*

Proof Consider the vectorial function $F = (f_1, \ldots, f_n, f_{n+1})$ that is obtained from the vectorial function $G = (g_1, \ldots, g_n)$ using the method described in (1). Then for all arguments $x = (x_1, \ldots, x_{n+1})$ such that $x_{n+1} = 0$, we have that $F(x) = (g_1(x), \ldots, g_n(x), g_{n+1}(x))$, where g_{n+1} is a coordinate function that was added according to the method. Since the function $F(x)$ satisfies the APN property for all nonzero $a = (a_1, \ldots, a_{n+1})$ such that $a_{n+1} = 0$ and any $b \in \mathbb{F}_2^{n+1}$, the equation $F(x) + F(x+a) = b$ has no more than 2 solutions x such that $x_{n+1} = 0$. Therefore, for any nonzero $a = (a_1, \ldots, a_n)$ and any $b \in \mathbb{F}_2^n$, the equation $G(x) + G(x+a) = b$ has no more than 4 solutions and G is APN or differentially 4-uniform.

For example, for a differentially 4-uniform function $G = (g_1, g_2, g_3, g_4, g_5)$, where:

$g_1 = x_1x_2 + x_3x_5 + x_4x_5$;
$g_2 = x_1x_3 + x_4x_5$;
$g_3 = x_2x_3 + x_1x_4 + x_3x_5 + x_4x_5$;
$g_4 = x_2x_4 + x_1x_5 + x_4x_5$;
$g_5 = x_3x_4 + x_2x_5 + x_4x_5$,

and g_6 contains all the terms x_ix_j, where $i < j \leqslant n$, we obtained all 13 CCZ-classes of APN functions in 6 variables among the constructed functions.

Remark 2 It can be seen that any quadratic APN function in n variables can be obtained using the method described in (1) from a quadratic APN or differential 4-uniform function in $n-1$ variables.

It is also worth mentioning that when $n = 3, 4$ and 5 for all possible (up to CCZ-equivalence [9]) quadratic APN functions we obtained all the possible quadratic APN functions for $4, 5$ and 6 variables, respectively.

Note that for a given APN function G in n variables we have $2^{\frac{(n^2-n)}{2}}$ possibilities to choose g_{n+1}. It is interesting to see how the choice of g_{n+1} affects the possibility of obtaining an APN function F in $n+1$ variables, the number of such constructed functions and the variety of different CCZ-classes among the obtained functions. For example, when $n = 5$ and g_{n+1} is null, all known quadratic APN functions give us only one CCZ-class of APN functions in 6 variables (class 11 in the list from [9]). At the same time, when

g_{n+1} contains all quadratic terms $x_i x_j$, these functions give 13 CCZ-classes of quadratic APN functions in 6 variables. Unfortunately, for $n \geqslant 7$ it becomes harder to choose the proper initial function and g_{n+1} and to obtain a large amount of generated functions. It seems that the method from (1) is not so efficient on large dimensions.

OPEN QUESTION Q1: How to choose properly the initial function G in this approach? It seems that for most APN functions in n variables it is possible to find corresponding APN functions in $n+1$ variables for some g_{n+1}, but we have found one counterexample for $n = 6$. That function is the APN function #11 in the classification [9].

OPEN QUESTION Q2: Given an APN (or differentially 4-uniform) function G, how to choose the function g_{n+1} in such a way that the number of CCZ-classes of obtained APN functions is maximal?

4 On a cyclic approach to search for quadratic APN functions

As noted earlier, each row and each column of a symmetric matrix corresponding to an APN function in n variables consists of $n-1$ linearly independent vectors from $\mathbb{F}_2^n$. Let us introduce another approach for constructing quadratic APN functions using the matrix representation from the previous section. Let $\{e_1, \ldots, e_n\}$ be the standard basis of $\mathbb{F}_2^n$. For the given n, consider the following matrix with elements from $\mathbb{F}_2^n$:

$$\mathcal{T} = \begin{bmatrix} 0 & e_1 & e_2 & e_3 & \ldots & e_{n-2} & e_{n-1} \\ e_1 & 0 & e_3 & e_4 & \ldots & e_{n-1} & e_n \\ e_2 & e_3 & 0 & e_5 & \ldots & e_n & t_{3,n} \\ e_3 & e_4 & e_5 & 0 & \ldots & t_{4,n-1} & t_{4,n} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ e_{n-2} & e_{n-1} & e_n & t_{n-1,4} & \ldots & 0 & t_{n-1,n} \\ e_{n-1} & e_n & t_{n,3} & t_{n,4} & \ldots & t_{n,n-1} & 0 \end{bmatrix},$$

where $t_{i,j} = t_{j,i}$ and $t_{i,j}$ denote some unknown elements in $\mathbb{F}_2^n$. Our aim is to find the values of the unknown matrix elements such that the matrix $\mathcal{T}$ represents an APN function. We can apply the approach with restrictions from the previous section.

Let us consider the following procedure.

1. Without loss of generality consider the first unknown element of the matrix $\mathcal{T}$, that is $t_{3,n}$. According to Proposition 2 the last column of $\mathcal{T}$ should satisfy $(e_{n-1}, e_n, t_{3,n}, \ldots, 0)a' \notin \langle \mathcal{T}' a'^T \rangle$, where $a' \in \mathbb{F}_2^{n-1}$, $a' \neq 0$ and $\mathcal{T}' = \mathcal{T} \setminus (e_{n-1}, e_n, t_{3,n}, \ldots, 0)$.
2. We consider all $a' = a'_1, \ldots, a'_{n-1}$ such that $a'_3 = 1$ and $a'_i = 0$, if $i > 3$, and obtain restrictions on the value of $t_{3,n}$ that are independent from any other unknown element of $\mathcal{T}$.

Repeating this procedure step by step for every new element after fixing values of previous variables $t_{i,j}$ allows us to obtain all possible assignments for the given matrix $\mathcal{T}$.

For $n = 3, 4$ and 5 this construction covered all CCZ-classes of quadratic APN functions. For $n = 6$ it covered 11 out of 13 CCZ-classes. Unfortunately, for larger dimensions the number of generated functions dropped dramatically and the construction covers only 7 CCZ-classes for $n = 7$ and only one class for $n = 8$. As a consequence, we consider the following generalization of this construction.

For the given n consider the same matrix $\mathcal{T}$. Suppose that $\mathcal{T}$ contains k unknown elements. Consider the subdiagonal that contains all elements e_n in $\mathcal{T}$. It is easy to see that we can remove any element e_n from this subdiagonal and apply the above procedure to the new matrix with $k + 1$ unknown elements. Moreover, we can remove any number of elements from $\mathcal{T}$ and the more elements that are removed, the more APN functions can be constructed using this matrix.

For $n = 6$ we removed one element e_n from this subdiagonal in $\mathcal{T}$. Applying the above procedure to the new matrix resulted in covering all 13 CCZ-classes of quadratic APN functions. For $n = 7$ we removed all elements e_n from the mentioned subdiagonal and generated more than two million quadratic APN functions. We have found a new CCZ-class for $n = 7$ among the obtained functions. Here we provide a representative of this class in the univariate form:

$F(x) = a^{100}x + a^{88}x^2 + a^{89}x^3 + a^{107}x^4 + a^{57}x^5 + a^{98}x^6 + a^{56}x^8 + a^9x^9 + a^{58}x^{10} + a^{60}x^{12} + a^{109}x^{16} + a^{47}x^{17} + a^{44}x^{18} + a^{27}x^{20} + a^{91}x^{24} + a^{71}x^{32} + a^{96}x^{33} + a^{101}x^{34} + a^7x^{36} + a^{12}x^{40} + a^{34}x^{48} + a^{66}x^{64} + a^4x^{65} + a^4x^{66} + a^{73}x^{68} + a^{73}x^{72} + a^{56}x^{80} + a^{20}x^{96}$,

where a is the primitive element whose minimal polynomial over $\mathbb{F}_{2^7}$ is $x^7 + x + 1$.

5 Classification of quadratic APN functions in dimension 7

Let us recall that APN functions are classified completely only up to $n = 5$. APN functions in 6 variables are classified for the case of algebraic degree no greater than 3. We complete the classification of quadratic APN functions for $n = 7$.

Given a quadratic APN function F, let $\mathcal{F}$ be its corresponding symmetric matrix. It can be seen that the first row of $\mathcal{F}$ is equal to (0 1 2 4 8 16 32) (that is the row $(0\ e_1\ e_2\ e_3\ e_4\ e_5)$ in decimal notation) up to EA-equivalence, since we can map any set of $(n - 1)$ linearly independent elements to the standard basis.

It was shown in [52] (see Corollary 1) that if the APN functions F and G are EA-equivalent, then for their matrices $\mathcal{F}$ and $\mathcal{G}$ the following relation holds:

$$\mathcal{G} = L(P\mathcal{F}P^t),$$

where P is an invertible matrix with elements from $\mathbb{F}_2$ and L is a linear permutation on $\mathbb{F}_2^n$. Let us briefly describe the procedure of finding a lexicographically minimal matrix in the EA-class. Our aim is to transform the first k (for $n = 7$ we considered the case $k = 2$) rows of a given matrix in order to obtain lexicographically minimal ones using only transformations that preserve EA-equivalence.

For all possible values of the first two rows of the matrix $\mathcal{F}$ such that the condition from Proposition 1 is true, we implement a search through all possible matrices P of the form

$$P = \begin{bmatrix} x & x & 0 & 0 & 0 & 0 & 0 \\ x & x & 0 & 0 & 0 & 0 & 0 \\ * & * & x & x & x & x & x \\ * & * & x & x & x & x & x \\ * & * & x & x & x & x & x \\ * & * & x & x & x & x & x \\ * & * & x & x & x & x & x \end{bmatrix},$$

where the upper left 2×2 square and the lower right 5×5 square are invertible matrices and the lower left part can be any 5×2 matrix. We consider such matrices P since our aim is to find the minimal values of the first two rows for a given EA-class and we want only these two rows to interact with each other (since we do not know the rest of the rows when $k = 2$). For each matrix P we perform the following steps:

P1: Search through all possible L such that the first row of $\mathcal{G}$ is equal to (0 1 2 4 8 16 32);

P2: If P and L are such that $\mathcal{G} < \mathcal{F}$ lexicographically, we discard $\mathcal{F}$.

We implemented the above procedure and obtained that there are only five possible options for the second row of a given quadratic matrix up to EA-equivalence. We list below these options and the number of EA-inequivalent APN functions that have such a lexicographically minimal matrix:

1. Case (1 0 4 8 16 32 64) contains 3 quadratic APN functions up to EA-equivalence (all are equivalent to monomial functions);
2. Case (1 0 4 6 16 32 64) contains 2 functions;
3. Case (1 0 4 6 16 32 24) contains no functions;
4. Case (1 0 4 6 16 26 64) contains 220 functions;
5. Case (1 0 4 6 16 24 64) contains 263 functions.

Thus, there exist only 488 quadratic APN functions up to CCZ-equivalence, and the updated list is complete.

For $n = 8$ we implemented the procedure as well. There exist 11 possible options for the second row of a given quadratic matrix (while the first row is equal to (0 1 2 4 8 16 32 64)):

1. Case (1 0 4 8 16 32 64 128);
2. Case (1 0 4 8 16 32 64 18);
3. Case (1 0 4 8 16 32 64 6);

4. Case (1 0 4 6 16 32 64 128);
5. Case (1 0 4 6 16 32 64 24);
6. Case (1 0 4 8 16 32 24 128);
7. Case (1 0 4 8 16 26 64 128);
8. Case (1 0 4 8 16 26 64 104);
9. Case (1 0 4 8 16 24 64 128);
10. Case (1 0 4 8 16 24 64 98);
11. Case (1 0 4 8 16 24 64 96).

The number of EA-inequivalent APN functions for each case is being computed at the moment.

6 Using of quadratic functions to search for APN fuctions of higher algebraic degree

In this section we disscuss possible approaches for the use of quadratic functions with low differential uniformity to search for APN fuctions of higher algebraic degree. Also, we introduce the notion of a stacked APN function as an APN function of algebraic degree d such that eliminating monomials of degrees $k+1,\ldots,d$ for any $k<d$ results in an APN function of algebraic degree k.

6.1 The differential uniformity of the quadratic parts of APN functions and the class of stacked APN functions

Let F be a vectorial Boolean function of algebraic degree d. Then it can be represented as the sum $F=F^{(c)}+F^{(1)}+F^{(2)}+\ldots+F^{(d)}$, where each function $F^{(j)}$ contains only monomials of algebraic degree j in its algebraic normal form and $F^{(c)}$ is a constant term. We observe that if F is an APN function then its quadratic part $F^{(2)}$ has a low differential uniformity. In particular, we can state the following proposition based on our computational results:

Proposition 4 *Let F be an APN function from $\mathbb{F}_2^4$ to $\mathbb{F}_2^4$. Then $\Delta_{F^{(2)}}\leqslant 4$.*

Some sporadic examples of non-quadratic APN functions in $5,6$ and 7 variables have a quadratic part with differential uniformity not greater than 4. For the Dillon APN permutation P of $\mathbb{F}_2^6$ [10], the value $\Delta_{P^{(2)}}$ is equal to 8. When $n=8,9$ there also exist APN functions F (e.g. the Kasami power functions for $n=8$ and the inverse function for $n=9$) such that $\Delta_{F^{(2)}}=8$. Nevertheless, for these large dimensions the differential uniformity of the quadratic parts is still quite low. Further we consider only functions without affine terms. The observation on low differential uniformity of the quadratic parts of APN functions motivated us to introduce a new subclass of APN functions.

Definition 1 Let $F = F^{(2)}+\ldots+F^{(d)}$ be an APN function of algebraic degree d. If all functions $F - F^{(d)}$, $F - F^{(d)} - F^{(d-1)}, \ldots, F - F^{(d)} - F^{(d-1)} - \ldots - F^3$ are APN functions, then F is called a *stacked APN function.*

Let us describe one of the possible approaches to construct stacked APN functions of algebraic degree 3. Let h be a cubic Boolean function in n variables with no affine or quadratic terms, i.e. a homogenous one. Let us call a vectorial function H a *cubic shift* if $H = h \cdot v$ for a nonzero vector v in $\mathbb{F}_2^n$. In 2009, Y. Edel and A. Pott introduced a new approach for searching for APN functions, the so-called *switching method* [31]. It is necessary to mention that the same principle was previously used to construct an infinite family of APN polynomials in [14]. This approach describes how to find new APN functions from known ones by changing their coordinate functions. In particular, the following result for functions of the form $F + f \cdot v$ was obtained.

Theorem 2 *(Theorem 3 in [31]) Let F be an APN function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$. Let v be a nonzero vector in $\mathbb{F}_2^n$, and h be a Boolean function in n variables. Then the function $F + h \cdot v$ is an APN function if and only if*

$$h(x) + h(x + a) + h(y) + h(y + a) = 0$$

for all x, y, a such that

$$F(x) + F(x + a) + F(y) + F(y + a) = 0$$

and $x \neq y$, $x \neq y + a$.

The next property directly follows from Theorem 2 and it is also described in [13] (see Section V "Single shift"):

Proposition 5 *Let F be an APN function in n variables. Let v be a nonzero vector in $\mathbb{F}_2^n$, and h_1, h_2 be different Boolean functions in n variables. If both $F + h_1 \cdot v$ and $F + h_2 \cdot v$ are APN functions, then the function $F + h_1 \cdot v + h_2 \cdot v$ is also APN.*

The next simple corollary follows from Proposition 5 and allows us to potentially reduce the complexity of an exhaustive search for all suitable cubic shifts.

Corollary 1 *Let F be a quadratic APN function in n variables. Suppose that there exist homogenous cubic Boolean functions h_1, h_2 such that both $F + h_1 \cdot v$ and $F + h_2 \cdot v$ are APN. Then, there exist Boolean functions h, where $h = h_1$ or $h = h_2$ or $h = h_1 + h_2$, such that h contains an even (or, equivalently, an odd) number of monomials and $F + h \cdot v$ is an APN function.*

For $n = 4, 5$ we implemented a search for cubic APN functions $F = F^{(2)} + F^{(3)}$ such that $F^{(3)}$ is some cubic part and $F^{(2)}$ is a quadratic APN function constructed using the cyclic matrix $\mathcal{T}$ from the previous section. For $n = 6$ we implemented a similar search, but $F^{(3)}$ was a cubic shift since it is computationally hard to search through all possible cubic parts. We found a

Table 3 Examples of stacked cubic APN functions (both F and $F^{(2)}$ are APN).

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$F(x)$	0	0	0	1	0	2	4	7	0	4	6	3	8	14	11	12
$F^{(2)}(x)$	0	0	0	1	0	2	4	7	0	4	6	3	8	14	10	13
x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
$F(x)$	0	0	0	1	0	2	4	7	0	4	10	15	19	21	28	27
	0	8	16	25	11	1	29	22	15	3	17	28	31	17	6	9
$F^{(2)}(x)$	0	0	0	1	0	2	4	7	0	4	10	15	19	21	29	26
	0	8	16	25	11	1	31	20	15	3	21	24	23	25	9	6
x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
$F(x)$	0	0	0	1	0	2	4	13	0	4	8	7	16	22	28	27
	0	8	16	19	9	3	29	22	45	33	53	56	52	58	40	45
	0	16	60	45	26	8	34	59	55	35	3	28	61	43	13	26
	5	29	41	58	22	12	62	37	31	3	59	38	28	2	60	41
$F^{(2)}(x)$	0	0	0	1	0	2	4	7	0	4	8	13	16	22	28	27
	0	8	16	25	9	3	29	22	45	33	53	56	52	58	40	39
	0	16	60	45	26	8	34	49	55	35	3	22	61	43	13	26
	5	29	41	48	22	12	62	37	31	3	59	38	28	2	60	35

large amount of cubic stacked APN functions for $n = 4, 5, 6$. Some examples are listed in Table 3.

It is worth mentioning that for quadratic APN functions from the different CCZ-classes for $n = 6$ we have found more than 70 000 cubic stacked APN functions. All these functions belong to the same CCZ-class that is the only known class of APN functions in 6 variables that does not contain quadratic functions (class number 13 in the list from [9]), despite the fact that all 14 CCZ-classes contains cubic representatives [21].

6.2 A generalization of the switching method to differentially 4-uniform functions

Here we show that the switching method mentioned earlier can be applied not only to APN functions, but also to differentially 4-uniform functions.

Proposition 6 *Let F be a vectorial Boolean function in n variables. Let v be a nonzero vector in $\mathbb{F}_2^n$, and h be a Boolean function in n variables, such that $F + h \cdot v$ is an APN function. Then there exists a vectorial function G, such that G is EA-equivalent to F and $G + h \cdot e_1$ is APN, where e_1 is a vector from the standard basis.*

Proof Consider the bijective linear mapping L such that $L(v) = e_1$. Then $L(F + h \cdot v) = L(F) + h \cdot e_1 = G + h \cdot e_1$ and G is EA-equivalent to F.

It is interesting that for $n = 4, 6$ we found cubic APN functions C such that $C = F + h \cdot e_1$, where F is APN and h is a homogenous cubic function only one of whose terms in ANF has a nonzero coefficient. An example of such F and C for $n = 4$ can be found in Table 3. An example for $n = 6$ is the following:

$c_1 = x_1x_2 + x_4x_6 + x_5x_6 + x_2x_3x_5$;
$c_2 = x_1x_3 + x_3x_5 + x_4x_5 + x_2x_6 + x_5x_6$;
$c_3 = x_2x_3 + x_1x_4 + x_4x_5 + x_5x_6$;
$c_4 = x_2x_4 + x_1x_5 + x_3x_5 + x_2x_6 + x_3x_6 + x_4x_6 + x_5x_6$;
$c_5 = x_3x_4 + x_2x_5 + x_3x_5 + x_4x_5 + x_1x_6 + x_2x_6 + x_3x_6 + x_5x_6$;
$c_6 = x_3x_5 + x_2x_6 + x_5x_6$.

Remark 3 Let F be an APN function in n variables. Let $G = F + f \cdot e_1$ for some Boolean function f, then $\Delta_G \leqslant 4$, since changing one coordinate of an APN function can not increase the differential uniformity more than two times [14]. This implies the following result:

Corollary 2 *Let F be a vectorial Boolean function in n variables. Let v be a nonzero vector in $\mathbb{F}_2^n$, and h be a Boolean function in n variables, such that $F + h \cdot v$ is an APN function. Then $\Delta_F \leqslant 4$.*

This corollary implies that the switching method for obtaining APN functions can be applied only to APN and differentially 4-uniform functions. The following analog of Theorem 2 for differentially 4-uniform functions is also known from [13]:

Theorem 3 *Let F be a differentially 4-uniform function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$. Let v be a nonzero vector in $\mathbb{F}_2^n$, and h be a Boolean function in n variables. Then the function $F + h \cdot v$ is APN if and only if the following conditions hold:*

$$C1.\ h(x) + h(x + a) + h(y) + h(y + a) = 0$$

for all x, y, a such that

$$F(x) + F(x + a) + F(y) + F(y + a) = v$$

and $x \neq y$, $x \neq y + a$.

$$C2.\ Zh(x) + h(x + a) + h(y) + h(y + a) = 1$$

for all x, y, a such that

$$F(x) + F(x + a) + F(y) + F(y + a) = 0$$

and $x \neq y$, $x \neq y + a$.

Remark 4 These observations emphasize the possible role of quadratic APN and differentially 4-uniform functions in obtaining new APN functions of higher algebraic degree and motivates further research in this direction.

OPEN QUESTION Q3: Do there exist stacked APN functions of algebraic degree higher than 3?

OPEN QUESTION Q4: Do there exist stacked APN functions for dimensions larger than 6?

7 Conclusion

In this paper we considered two combinatorial approaches that allow to search for quadratic APN functions using special matrices. Given a quadratic APN function in n variables, the first approach searches for quadratic APN functions in $n+1$ variables using special restrictions that can be described in terms of matrices. The second approach uses matrices of a cyclic form to generate quadratic APN functions. Using these approaches we found a new APN function in 7 variables. Moreover, we obtained a complete classification of quadratic APN functions up to CCZ-equivalence in dimension 7. Also, we noted that the quadratic parts of some APN functions have a low differential uniformity and introduced the notion of stacked APN functions.

Acknowledgements We sincerely thank the anonymous reviewers for their careful reading of this manuscript and suggesting substantial improvements. We would like to cordially thank Natalia Tokareva for her valuable remarks. We are much indebted to the reviewers of the SETA-2020 conference for their helpful reviews. We are grateful to Anastasia Gorodilova and Nikolay Kolomeec for their useful observations and fruitful discussions. The work is supported by the Mathematical Center in Akademgorodok under agreement No. 075-15-2019-1613 with the Ministry of Science and Higher Education of the Russian Federation and Laboratory of Cryptography JetBrains Research. We are grateful to the Supercomputing Center of the Novosibirsk State University for the provided computational resources.

References

1. Agievich S., Gorodilova A., Kolomeec N., Nikova S., Preneel B., Rijmen V., Shushuev G., Tokareva N., Vitkup V.: Problems, solutions and experience of the first international students Olympiad in cryptography. Prikladnaya Diskretnaya Matematika 3(29), 5-28 (2015)
2. Beierle C., Leander G.: New Instances of Quadratic APN Functions. CoRR abs/2009.07204 (2020).
3. Beth T., Ding C.: On almost perfect nonlinear permutations. Advances in Cryptology, EUROCRYPT'93, Lecture Notes in Computer Science, vol. 765, pp. 65-76 (1993).
4. Biham E., Shamir A.: Differential cryptanalysis of DES-like cryptosystems. Journal of Cryptology, vol. 4(1), pp. 3-72 (1991).
5. Blondeau C., Nyberg K.: Perfect nonlinear functions and cryptography. Finite Fields and Their Applications, vol.32 (March), pp. 120-147(2015).
6. Boura C., Canteaut A., Jean J., Suder V.: Two notions of differential equivalence on Sboxes. Des. Codes Cryptogr. 87, 185202 (2019).
7. Bracken C., Byrne E., Markin N. and McGuire G.: New Families of Quadratic Almost Perfect Nonlinear Trinomials and Multinomials. Finite Fields and their Applications 14(3), pp. 703-714 (2008).

8. Bracken C., Byrne E., Markin N. and McGuire G.:A Few More Quadratic APN Functions. Cryptography and Communications 3(1), 43-53, (2011).
9. Brinkmann M., Leander G.: On the classification of APN functions up to dimension five. Des. Codes Cryptogr., vol. 49, Issue 13, pp. 273-288 (2008).
10. 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, vol. 518, pp. 33-42 (2010).
11. Budaghyan L.: Construction and analysis of cryptographic functions. Springer International Publishing, VIII, 168 pp. (2014).
12. Budaghyan L., Carlet C., Helleseth T., Li N. and Sun B.: On Upper Bounds for Algebraic Degrees of APN Functions. IEEE Transactions on Information Theory, vol. 64, no. 6, pp. 4399-4411 (2018).
13. Budaghyan L., Carlet C., Helleseth T. and Kaleyski N.: On the Distance Between APN Functions. IEEE Transactions on Information Theory, vol. 66, no. 9, pp. 5742-5753 (2020).
14. Budaghyan L., Carlet C., Leander G.: Constructing new APN Functions from known ones. Finite Fields and Their Applications, vol. 15, I. 2, pp. 150-159 (2009).
15. Budaghyan L., Carlet C. and Leander G.: On a construction of quadratic APN functions. 2009 IEEE Information Theory Workshop, Taormina, pp. 374-378 (2009).
16. Budaghyan L., Carlet C. and Leander G.: Two classes of quadratic APN binomials inequivalent to power functions. IEEE Trans. Inform. Theory 54 (9), pp. 4218-4229, (2008).
17. Budaghyan L., Calderini M., Carlet C., Coulter R. S. and Villa I.: Constructing APN Functions Through Isotopic Shifts. IEEE Transactions on Information Theory, vol. 66, no. 8, pp. 5299-5309 (2020).
18. Budaghyan L., Carlet C. and Pott A.: New classes of almost bent and almost perfect nonlinear polynomials. IEEE Transactions on Information Theory, vol. 52, no. 3, pp. 1141-1152 (2006).
19. Budaghyan L. and Carlet C.: Classes of Quadratic APN Trinomials and Hexanomials and Related Structures. IEEE Transactions on Information Theory, vol. 54, no. 5, pp. 2354-2357 (2008).
20. Budaghyan L., Helleseth T. and Kaleyski N.: A new family of APN quadrinomials. IEEE Trans. Inform. Theory 66, no. 11, pp. 7081-7087, (2020).
21. Calderini M.: On the EA-classes of known APN functions in small dimensions. Cryptogr. Commun., vol. 12, pp. 821-840 (2020).
22. Calderini M., Budaghyan L. and Carlet C. On known constructions of APN and AB functions and their relation to each other. Cryptology ePrint Archive, Report 2020/1444.
23. Canteaut A., Charpin P., Dobbertin H.: Binary m-sequences with three-valued cross-correlation: a proof of Welch conjecture, IEEE Trans. Inf. Theory., vol. 46(1), pp. 4-8 (2000).
24. Carlet C.: Open Questions on Nonlinearity and on APN Functions. Arithmetic of Finite Fields. WAIFI 2014. Lecture Notes in Computer Science, vol. 9061, pp. 83-107 (2015).
25. 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, pp. 398-472 (2010).
26. Carlet C., Charpin P., Zinoviev V.: Codes, bent functions and permutations suitable for DES-like cryptosystems. Des. Codes Cryptogr., vol. 15, pp. 125-156 (1998).
27. Dobbertin, H.: One-to-One Highly Nonlinear Power Functions on $GF(2^n)$. Appl. Algebra Eng. Commun. Comput., vol. 9(2), pp. 139-152 (1998).
28. Dobbertin H.: Almost perfect nonlinear power functions on $GF(2^n)$: the Welch case. IEEE Trans. Inf. Theory., vol. 45(4), pp. 1271-1275 (1999).
29. Dobbertin H.: Almost perfect nonlinear functions over GF$GF(2^n)$: the Niho case. Inform. and Comput., vol.151, pp. 57-72 (1999).
30. 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).
31. Edel Y., Pott A.: A new almost perfect nonlinear function which is not quadratic. Advances in Mathematics of Communications, vol. 3 (1), pp. 59-81 (2009).
32. Edel Y., Kyureghyan G. and Pott A.: A new APN function which is not equivalent to a power mapping. IEEE Transactions on Information Theory, vol. 52, no. 2, pp. 744-747 (2006).

33. Gold R.: Maximal recursive sequences with 3-valued recursive crosscorrelation functions. IEEE Trans. Inform. Theory, vol. 14, pp.154-156 (1968).
34. F. Göloğlu. Gold-hybrid APN functions. Preprint (2020)
35. Gorodilova A A.: Characterization of almost perfect nonlinear functions in terms of subfunctions, Diskr. Mat., vol. 27(3), pp. 3-16 (2015); Discrete Math. Appl., vol. 26(4), pp. 193-202 (2016).
36. Gorodilova, A.: On the differential equivalence of APN functions. Cryptography and Communications, 11, pp. 793-813 (2019).
37. Glukhov M. M.: On the approximation of discrete functions by linear functions. Matematicheskie Voprosy Kriptografii, vol. 7(4), pp. 29-50 (2016) (in Russian).
38. Glukhov M. M.: On the matrices of transitions of differences for some modular groups. Matematicheskie Voprosy Kriptografii, vol. 4(4), pp. 27-47 (2013) (in Russian).
39. Hollmann H., Xiang Q.: A proof of the Welch and Niho conjectures on crosscorrelations of binary m-sequences. Finite Fields and Their Applications, vol. 7, pp. 253-286 (2001).
40. Idrisova V.: On an algorithm generating 2-to-1 APN functions and its applications to the big APN problem. Cryptography and Communications, 11, pp. 21-39 (2019).
41. 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, Lecture Notes in Computer Science, vol. 673, Berlin, Springer-Verlag, pp. 180-194 (1993).
42. Kaleyski N. S.: Changing APN functions at two points. Cryptography and Communications, 11, pp. 1165-1184 (2019).
43. Kalgin K., Idrisova V.: On secondary and cyclic approaches to search for quadratic APN functions. Proceedings of the 11th international conference on Sequences and Their Applications — SETA-2020 (Saint-Petersburg, Russia, September 22-25, 2020).
44. Kasami T.: The weight enumerators for several classes of subcodes of the second order binary Reed-Muller codes. Inform. and Control. 18, pp. 369-394 (1971).
45. Kaspers C., Zhou Y.: The Number of Almost Perfect Nonlinear Functions Grows Exponentially. J Cryptol, vol. 34 (4), published online (2021).
46. Langevin P., Saygi Z. and Saygi E.: Classification of APN cubics in dimension 6 over GF(2): http://langevin.univ-tln.fr/project/apn-6/apn-6.html
47. Nyberg K.: Differentially uniform mappings for cryptography. Advances in Cryptography, EUROCRYPT'93, Lecture Notes in Computer Science, vol. 765, pp. 55-64 (1994).
48. Pott A.: Almost perfect and planar functions. Designs, Codes and Cryptography 78(1), pp. 141-195 (2016).
49. Taniguchi H.: On some quadratic APN functions. Designs, Codes and Cryptography 87, pp. 1973-1983 (2019).
50. Tuzhilin M. E.: APN functions. Prikladnaya Diskretnaya Matematika, vol. 3, pp. 14-20 (2009) (in Russian).
51. Yoshiara S.: Equivalences of quadratic APN functions. Journal of Algebraic Combinatorics, 35, pp. 461-475 (2012).
52. Yu Y., Wang M., Li Y.: A matrix approach for constructing quadratic APN functions. Des. Codes Cryptogr. 73, pp. 587-600 (2014).
53. Yu Y., Kaleyski N. S., Budaghyan L., Li Y.: Classification of quadratic APN functions with coefficients in GF(2) for dimensions up to 9. Finite Fields and Their Applications, 68, pp. 101-733 (2020).
54. Yu Y., Perrin L.: Constructing More Quadratic APN Functions with the QAM Method. Cryptology ePrint Archive, Report 2021/574 (2021).
55. Zhou Y. and Pott A.: A New Family of Semifields with 2 Parameters. Advances in Mathematics, 234, pp. 43-60 (2013).