A new family of APN quadrinomials

Lilya Budaghyan[1], Tor Helleseth[1], and Nikolay Kaleyski[1]

[1]*Department of Informatics, University of Bergen*

***Abstract*—The binomial $B(x) = x^3 + \beta x^{36}$ (where β is primitive in $\mathbb{F}_{2^2}$) over $\mathbb{F}_{2^{10}}$ is the first known example of an Almost Perfect Nonlinear (APN) function that is not CCZ-equivalent to a power function, and has remained unclassified into any infinite family of APN functions since its discovery in 2006. We generalize this binomial to an infinite family of APN quadrinomials of the form $x^3 + a(x^{2^i+1})^{2^k} + bx^{3\cdot 2^m} + c(x^{2^{i+m}+2^m})^{2^k}$ from which $B(x)$ can be obtained by setting $a = \beta$, $b = c = 0$, $i = 3$, $k = 2$. We show that for any dimension $n = 2m$ with m odd and $3 \nmid m$, setting $(a, b, c) = (\beta, \beta^2, 1)$ and $i = m - 2$ or $i = (m - 2)^{-1} \mod n$ yields an APN function, and verify that for $n = 10$ the quadrinomials obtained in this way for $i = m - 2$ and $i = (m - 2)^{-1} \mod n$ are CCZ-inequivalent to each other, to $B(x)$, and to any other known APN function over $\mathbb{F}_{2^{10}}$.**

TABLE I
KNOWN INFINITE FAMILIES OF APN POWER FUNCTIONS OVER $\mathbb{F}_{2^n}$

Family	Exponent	Conditions	Algebraic degree	Source
Gold	$2^i + 1$	$\gcd(i, n) = 1$	2	[18], [22]
Kasami	$2^{2i} - 2^i + 1$	$\gcd(i, n) = 1$	$i + 1$	[19], [20]
Welch	$2^t + 3$	$n = 2t + 1$	3	[13]
Niho	$2^t + 2^{t/2} - 1$, t even $2^t + 2^{(3t+1)/2} - 1$, t odd	$n = 2t + 1$	$(t + 2)/2$ $t + 1$	[12]
Inverse	$2^{2t} - 1$	$n = 2t + 1$	$n - 1$	[2], [22]
Dobbertin	$2^{4i} + 2^{3i} + 2^{2i} + 2^i - 1$	$n = 5i$	$i + 3$	[14]

I. INTRODUCTION

Vectorial Boolean functions, or (n, m)-functions, are mappings between the vector spaces $\mathbb{F}_2^n$ and $\mathbb{F}_2^m$ for some positive integers n and m, where $\mathbb{F}_2$ is the finite field with two elements. Any such mapping can be understood as a transformation substituting a sequence of n bits (zeros and ones) with a sequence of m bits according to a given prescription, and for this reason (n, m)-functions naturally appear in different areas of computer science and engineering. In particular, (n, m)-functions are of critical importance in the field of cryptography: virtually all modern block ciphers incorporate an (n, m)-function (usually referred to as an "S-box" or "substitution box" in this context) as their only nonlinear component, and as such the security of the encryption directly depends on the properties of the (n, m)-function. Researchers have defined various properties which measure the resistance of an (n, m)-function to different kinds of cryptanalysis, including nonlinearity, differential uniformity, boomerang uniformity, algebraic degree, and so forth. The lower the differential uniformity of a function, in particular, the better its security against differential cryptanalysis [3], which is one of the most efficient attacks that can be employed against block ciphers. When $n = m$, which is the main case of our interest, the differential uniformity of any (n, n)-function is at least 2, and the (n, n)-functions meeting this bound are called almost perfect nonlinear (APN). Discovering new examples and constructions of APN functions is thus a matter of significant practical importance since they enable the design of new block ciphers. APN functions are interesting from a theoretical point of view as well, as they correspond to optimal objects within other areas of mathematics and computer science, e.g. coding theory, combinatorics, and projective geometry.

Finding new constructions of APN functions is difficult. APN functions have been known and studied since the early 90's [22] but, to date, only six infinite families of APN monomials and 11 infinite families of APN polynomials are known. Together, these cover only a miniscule fraction of all APN functions: for instance, more than 8000 CCZ-inequivalent APN functions have been constructed over $\mathbb{F}_2^8$ [25], yet none of them have been classified into general constructions yet. Finding new examples of infinite families is an area of intense ongoing research. Tables I and II list all currently known infinite families of APN functions.

When $n = m$, it is convenient to identify the vector space $\mathbb{F}_2^n$ with the finite field $\mathbb{F}_{2^n}$ and to consider mappings from $\mathbb{F}_{2^n}$ (instead of $\mathbb{F}_2^n$) to itself. The binomials $B'(x) = x^3 + \alpha^{36}x^{36}$ and $B(x) = x^3 + \alpha^{341}x^{36}$ (where α is a primitive element of $\mathbb{F}_{2^{10}}$) are known to be APN over $\mathbb{F}_{2^{10}}$ [16] and are remarkable as the first examples of APN functions that are CCZ-inequivalent to power functions. Since their discovery in 2006, a lot of work has been done on the construction of polynomial APN functions [4], [5], [7]–[11], [26] but the binomials $B(x)$ and $B'(x)$ have not been classified into any infinite family or construction to date. It is worth noting that the binomial $x^3 + wx^{258}$ over $\mathbb{F}_{2^{12}}$ (where $w \in \mathbb{F}_{2^{12}}$ has order 273 or 585) was also a sporadic, i.e., not belonging to any infinite family, APN polynomial, until it was classified into two infinite families, one for dimensions n that are multiples of 3, and one for dimensions n that are multiples of 4 [9].

Attempts to generalize $B(x)$ and $B'(x)$ to an infinite family have, to the best of our knowledge, so far only considered binomials of a similar form in higher dimensions [10], which has not resulted in any success thus far. In our work, we take a different approach, which involves expanding $B(x)$ and $B'(x)$

This paper was presented in part at the Fourth International Workshop on Boolean Functions and their Applications (BFA-2019) which took place in Florence, Italy on June 16-21, 2019

TABLE II
KNOWN INFINITE FAMILIES OF QUADRATIC APN POLYNOMIALS OVER $\mathbb{F}_{2^n}$

ID	Functions	Conditions	Source
F1-F2	$x^{2^s+1}+u^{2^k-1}x^{2^{ik}+2^{mk+s}}$	$n=pk, \gcd(k,3)=\gcd(s,3k)=1, p\in\{3,4\}, i=sk \bmod p, m=p-i, n\geq 12, u$ primitive in $\mathbb{F}_{2^n}^*$	[9]
F3	$sx^{q+1}+x^{2^i+1}+x^{q(2^i+1)}+cx^{2^iq+1}+c^qx^{2^i+q}$	$q=2^m, n=2m,$ $gcd(i,m)=1,$ $c\in\mathbb{F}_{2^n}, s\in\mathbb{F}_{2^n}\setminus\mathbb{F}_q, X^{2^i+1}+cX^{2^i}+c^qX+1$ has no solution x s.t. $x^{q+1}=1$	[8]
F4	$x^3+a^{-1}\mathrm{Tr}_1^n(a^3x^9)$	$a\neq 0$	[10]
F5	$x^3+a^{-1}\mathrm{Tr}_3^n(a^3x^9+a^6x^{18})$	$3\|n,$ $a\neq 0$	[11]
F6	$x^3+a^{-1}\mathrm{Tr}_3^n(a^6x^{18}+a^{12}x^{36})$	$3\|n, a\neq 0$	[11]
F7-F9	$ux^{2^s+1}+u^{2^k}x^{2^{-k}+2^{k+s}}+vx^{2^{-k}+1}+wu^{2^k+1}x^{2^s+2^{k+s}}$	$n=3k, \gcd(k,3)=\gcd(s,3k)=1, v,w\in\mathbb{F}_{2^k}, vw\neq 1, 3\|(k+s), u$ primitive in $\mathbb{F}_{2^n}^*$	[5]
F10	$(x+x^{2^m})^{2^k+1}+u'(ux+u^{2^m}x^{2^m})^{(2^k+1)2^i}+u(x+x^{2^m})(ux+u^{2^m}x^{2^m})$	$n=2m, m\geqslant 2$ even, $\gcd(k,m)=1$ and $i\geqslant 2$ even, u primitive in $\mathbb{F}_{2^n}^*$, $u'\in\mathbb{F}_{2^m}$ not a cube	[26]
F11	$a^2x^{2^{2m+1}+1}+b^2x^{2^{m+1}+1}+ax^{2^{2m}+2}+bx^{2^m+2}+(c^2+c)x^3$	$n=3m, m$ odd$, L(x)=ax^{2^{2m}}+bx^{2^m}+cx$ satisfies the conditions of Lemma 8 of [7]	[7]
F12	$u(u^qx+x^qu)(x^q+x)+(u^qx+x^qu)^{2^{2i}+2^{3i}}+a(u^qx+x^qu)^{2^{2i}}(x^q+x)^{2^i}+b(x^q+x)^{2^i+1}$	$q=2^m, n=2m, \gcd(i,m)=1,$ $x^{2^i+1}+ax+b$ has no roots in $\mathbb{F}_{2^m}$	[23]
F13	$x^3+a(x^{2^i+1})^{2^k}+bx^{3\cdot 2^m}+c(x^{2^{i+m}+2^m})^{2^k}$	$n=2m,$ $a,b,c\in\mathbb{F}_4$ satisfying the conditions of Corollary 1	new

into APN polynomials with more than two terms, and then generalizing these polynomials to higher dimensions. Based on our experiments, we arrive at a family of quadrinomials of the form

$$x^3+a(x^{2^i+1})^{2^k}+bx^{3\cdot 2^m}+c(x^{2^{i+m}+2^m})^{2^k}$$

in which $B(x)$ corresponds to the coefficients$(a,b,c)=(\beta,0,0)$ and the exponents $i=3$, $k=2$. We show that the coefficients $(a,b,c)=(\beta,\beta^2,1)$, where β is primitive in $\mathbb{F}_{2^2}$, and exponents $i=m-2$, $i=(m-2)^{-1} \mod n$, $i=m$ or $i=n-1$ in the case of even k, or $i=m+2$, $i=(m+2)^{-1} \mod n$, or $i=n-1$ in the case of odd k, where $n=2m$ and m is odd with $3\nmid m$, give rise to APN functions. Furthermore, in the case of $n=10$, we show that for $i=m-2$ and $i=(m-2)^{-1}$, these APN functions are CCZ-inequivalent to each other or to any other known APN function over $\mathbb{F}_{2^{10}}$, including $B(x)$ and $B'(x)$. For $i=m$ and $i=n-1$ the functions are equivalent to representatives from the known families.

The condition $3\nmid m$ is needed since β is a cube in $\mathbb{F}_{2^n}$ if and only if $3\mid m$. Indeed, β is a cube in $\mathbb{F}_{2^n}$ if and only if $\beta^{(2^n-1)/d}=1$, where $d=\gcd(2^n-1,3)$; see e.g. [21]. For even n, $\gcd(2^n-1,3)=3$. The rest follows by observing that for $n=2m$, $(2^n-1)/3\equiv 0 \pmod{2^n-1}$ if and only if $3\mid m$, and since $\beta^3=1$.

II. PRELIMINARIES

Let n be a positive integer. We denote by $\mathbb{F}_{2^n}$ the finite field with 2^n elements, and by $\mathbb{F}_{2^n}^*$ the set of its non-zero elements, i.e., its multiplicative group. For $m\mid n$, we denote by $\mathrm{Tr}_m^n:\mathbb{F}_{2^n}\rightarrow\mathbb{F}_{2^m}$, resp. $\mathrm{N}_m^n:\mathbb{F}_{2^n}\rightarrow\mathbb{F}_{2^m}$ the trace function $\mathrm{Tr}_m^n(x)=\sum_{i=0}^{n/m-1}x^{2^{mi}}$, resp. the *norm function* $\mathrm{N}_m^n(x)=\prod_{i=0}^{n/m-1}x^{2^{mi}}$ from $\mathbb{F}_{2^n}$ into its subfield $\mathbb{F}_{2^m}$. We will only work with fields of even dimension $n=2k$; given some element $x\in\mathbb{F}_{2^n}$, we denote $\overline{x}=x^{2^k}$, and refer to $\overline{x}$ as the *conjugate* of x.

An (n,n)-function is any mapping $F:\mathbb{F}_{2^n}\rightarrow\mathbb{F}_{2^n}$. Any such function can be expressed as a polynomial of the form $F(x)=\sum_{i=0}^{2^n-1}a_ix^i$, for $a_i\in\mathbb{F}_{2^n}$. This is the *univariate representation* of F, and it is unique. The *algebraic degree* of F, denoted $\deg(F)$, is the largest binary weight of an exponent i with $a_i\neq 0$ in the univariate representation, where the *binary weight* of an integer is the number of ones in its binary notation, i.e., the minimum number of distinct powers of two that sum up to it. Functions of algebraic degree 1, 2, and 3 are called *affine*, *quadratic*, and *cubic*, respectively. An affine function F satisfying $F(0)=0$ is called *linear*.

Given an (n,n)-function F, we denote by $\Delta_F(a,b)$ the number of solutions x to the equation $D_aF(x)=b$, where $D_aF(x)=F(x+a)+F(x)$ is the *derivative* of F in direction $a\in\mathbb{F}_{2^n}$. The largest value of $\Delta_F(a,b)$ among all $a\neq 0$ and all b is denoted by Δ_F and is called the *differential uniformity* of F. If $\Delta_F=2$, we say that F is *almost perfect nonlinear (APN)*.

The *Walsh transform* of $F:\mathbb{F}_{2^n}\rightarrow\mathbb{F}_{2^n}$ is the integer-valued function $W_F(a,b)=\sum_{x\in\mathbb{F}_{2^n}}(-1)^{b\cdot F(x)+a\cdot x}$ for $a,b\in\mathbb{F}_{2^n}$, where the scalar product can be defined as $a\cdot b=\mathrm{Tr}_1^n(ab)$ for $a,b\in\mathbb{F}_{2^n}$ without losing generality. The values of $W_F(a,b)$ for $a,b\in\mathbb{F}_{2^n}$ are the *Walsh coefficients* of F, and the multiset $\{W_F(a,b):a,b\in\mathbb{F}_{2^n}\}$ is called the *Walsh spectrum* of F. The multiset $\{|W_F(a,b)|:a,b\in\mathbb{F}_{2^n}\}$ of the absolute values of the Walsh transform is the *extended Walsh spectrum*.

Two designs, $\mathrm{dev}(G_F)$ and $\mathrm{dev}(D_F)$, can be associated with a given APN function F over $\mathbb{F}_{2^n}$ [17]. In both cases, the set of points is $\mathbb{F}_{2^n}^2$. The set of blocks of $\mathrm{dev}(G_F)$, resp.

$\mathrm{dev}(D_F)$ is $\{(x+a, F(x)+b) : x \in \mathbb{F}_{2^n}\}$ for $a, b \in \mathbb{F}_{2^n}$, resp. $\{(x+y+a, F(x)+F(y)+b) : x, y \in \mathbb{F}_{2^n}, x \neq y\}$ for $a, b \in \mathbb{F}_{2^n}$. The rank of the incidence matrix of $\mathrm{dev}(G_F)$, resp. $\mathrm{dev}(D_F)$ is called the *Γ-rank*, resp. *Δ-rank* of F.

Since the number of distinct (n,n)-functions, viz. $(2^n)^{2^n}$, grows rapidly with the dimension, (n,n)-functions are classified only up to a suitable equivalence relation which preserves the properties being studied. The most general known equivalence relation which preserves the differential uniformity is the so-called *Carlet-Charpin-Zinoviev equivalence (CCZ-equivalence)*: we say that two (n,n)-functions F and F' are CCZ-equivalent if there is an affine permutation $\mathcal{L}$ of $\mathbb{F}_{2^n}^2$ which maps the graph $G_F = \{(x, F(x)) : x \in \mathbb{F}_{2^n}\}$ of F to the graph $G_{F'}$ of G. Deciding whether two given functions F and F' are CCZ-equivalent computationally is a difficult problem in general, and is typically resolved via code isomorphism. More precisely, a linear code $\mathcal{C}_F$ with the generating matrix

$$\mathcal{C}_F = \begin{pmatrix} 1 & 1 & \dots & 1 \\ 0 & \alpha & \dots & \alpha^{2^n-1} \\ F(0) & F(\alpha) & \dots & F(\alpha^{2^n-1}) \end{pmatrix}$$

can be associated with any given (n,n)-function F, where α is the primitive element of $\mathbb{F}_{2^n}$. Then F and F' are CCZ-equivalent if and only if $\mathcal{C}_F$ and $\mathcal{C}_{F'}$ are isomorphic [6].

Various CCZ-invariants, i.e., properties that remain invariant under CCZ-equivalence, can be used to show that a pair of (n,n)-functions is CCZ-inequivalent. These include the differential uniformity, the extended Walsh spectrum and the Γ- and Δ-ranks. In particular, it is known that if F and F' are CCZ-equivalent, then they must necessarily have e.g. the same Γ-rank. Thus, if two functions have distinct Γ-ranks, then they are definitely CCZ-inequivalent (although the converse does not hold in general).

A special cases of CCZ-equivalence is the so-called *extended affine equivalence (EA-equivalence)*. Two (n,n)-functions F and F' are said to be EA-equivalent if $F' = A_1 \circ F \circ A_2 + A$ for affine $A_1, A_2, A : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ with A_1, A_2 bijective.

III. A NEW FAMILY OF APN QUADRINOMIALS

Let β denote the primitive element of $\mathbb{F}_{2^2}$. Note that $\overline{\beta} = \beta^2$. We know that $B(x) = x^3 + \beta x^{36}$ and $B'(x) = x^3 + \alpha^{11} x^{341}$, where α is primitive in $\mathbb{F}_{2^{10}}$ are APN over $\mathbb{F}_{2^{10}}$ [16] but have not been classified into any infinite family yet. By means of the code isomorphism test, we establish that $B(x)$ and $B'(x)$ are CCZ-equivalent, and henceforth concentrate on $B(x)$ only. We look for polynomials $P(x)$ with a small number of terms such that $B(x) + P(x)$ is APN. We do not find any non-trivial (that is, not arising from simple EA-equivalence) monomial $P(x)$ for which $B(x) + P(x)$ is APN. We do, however, come across binomials $P(x)$ for which $B(x) + P(x)$ is APN and is CCZ-inequivalent to any known APN function over $\mathbb{F}_{2^{10}}$. A detailed description of the tests that we performed for disproving CCZ-equivalence can be found at the end of this section after Theorem 2.

Observation 1. *The quadrinomials $x^3 + \beta x^{36} + \beta^2 x^{96} + x^{129}$ and $x^3 + \beta x^{129} + \beta^2 x^{96} + x^{36}$ are APN over $\mathbb{F}_{2^{10}}$, and are CCZ-inequivalent to each other and to any other known APN function over $\mathbb{F}_{2^{10}}$.*

Note that $96 \equiv 332 \mod (2^{10} - 1)$ and $129 \equiv 3632 \mod (2^{10} - 1)$, i.e., $x^{96} = \overline{x^3}$, and $x^{129} = \overline{x^{36}}$ and, conversely, $x^{36} = \overline{x^{129}}$. Furthermore, $36 = 4 \cdot 9 = 4 \cdot (2^3 + 1)$. It is thus natural to consider functions of the form

$$C_i(x) = x^3 + \beta x^{2^i+1} + \beta^2 \overline{x^3} + \overline{x^{2^i+1}} \tag{1}$$

for $0 \leq i \leq n-1$. The APN-ness of such functions can be characterized by the solvability of the following system of equations.

Proposition 1. *Let $n = 2m$, $3 \nmid m$, m odd, and let $C_i(x)$ be defined as in* (1)*. Consider the system E_i defined by*

$$\begin{cases} a^3(x^2 + x) \in \beta \cdot \mathbb{F}_{2^m} \\ a^{2^i+1}(x^{2^i} + x) \in \beta \cdot \mathbb{F}_{2^m}. \end{cases} \tag{2}$$

Given some integer $1 \leq i \leq n-1$, the function defined by $C_i(x)$ is APN over $\mathbb{F}_{2^n}$ if, for any $a \in \mathbb{F}_{2^n}^*$, the system E_i from (2) *only has trivial solutions in x, i.e., only $x \in \mathbb{F}_2$ can be a solution to E_i.*

Proof. Note that C_i is quadratic, so that proving its APN-ness is equivalent to showing that the equation $D_a C_i(ax) = D_a C_i F(0)$ has only $x \in \mathbb{F}_2$ as solutions for $a \neq 0$. The expression $D_a C_i(ax) + D_a C_i F(0)$ takes the form

$$a^3(x^2+x) + \beta a^{2^i+1}(x^{2^i}+x) + \beta^2 \overline{a^3(x^2+x)} + \overline{a^{2^i+1}(x^{2^i}+x)}.$$

For simplicity, denote $A = a^3(x^2+x)$ and $B = a^{2^i+1}(x^{2^i} + x)$. Then the equation $D_a C_i(ax) + D_a C_i(0) = 0$ becomes

$$A + \beta B + \beta^2 \overline{A} + \overline{B} = 0. \tag{3}$$

Taking the conjugate of (3) and multiplying it by β, we get $\beta^2 A + \beta B + \beta \overline{A} + \overline{B} = 0$, and, adding this to (3), we obtain $\beta A + \overline{A} = 0$ which implies $\beta^2 A = \beta \overline{A}$, hence $\beta^2 A = \overline{\beta^2 A}$ and thus $\beta^2 A \in \mathbb{F}_{2^m}$, i.e., $A \in \beta \cdot \mathbb{F}_{2^m}$. Multiplying the identity $\beta A + \overline{A} = 0$ by β^2 and substituting it back into (3), we obtain $\beta B + \overline{B} = 0$, so that we also have $B \in \beta \cdot \mathbb{F}_{2^m}$. The two inclusions, viz. $A \in \beta \cdot \mathbb{F}_{2^m}$ and $B \in \beta \cdot \mathbb{F}_{2^m}$, are precisely the equations in the system (2). Therefore, under the hypothesis, $D_a C_i(ax) + D_a C_i(0) = 0$ can only have trivial solutions, and thus $C_i(x)$ is APN. □

Next, we determine values of i for which system (2) only has trivial solutions. According to our experimental results, which encompass dimensions up to 46, there are precisely four such values of i for any given dimension n satisfying the conditions of Proposition 1. Two of these give rise to APN functions equivalent to some of the previously known ones, while the other two lead to infinite constructions of APN functions whose instances for $n = 10$, i.e the quadrinomials from Observation 1, are CCZ-inequivalent to any known APN function over $\mathbb{F}_{2^{10}}$.

In the proof of Theorem 2 we will need the following auxiliary results.

Lemma 1. *Let $n = 2m$ for m odd, and suppose that for some $c \in \mathbb{F}_{2^n}$ with $\mathrm{Tr}_1^n(c) = 0$ we have*

$$c(c + c^2 + c^4 + \cdots + c^{2^{m+1}}) \in \mathbb{F}_{2^m}. \tag{4}$$

Then c is a cube.

Proof. First, observe that all elements of $\mathbb{F}_{2^m}$ are cubes due to $(2^m - 1, 3) = 1$ for m odd.

For convenience, let us denote by $h(c) = c + c^2 + \cdots + c^{2^{m-1}}$ the "half-trace" function. Then (4) can be written as $ch(c) + c^{2^m+1} + c^{2^{m+1}+1} \in \mathbb{F}_{2^m}$, and since $c^{2^m+1} = \mathrm{N}_m^n(c)$ is an element of $\mathbb{F}_{2^m}$, this becomes simply

$$ch(c) + c^{2^{m+1}+1} \in \mathbb{F}_{2^m}. \tag{5}$$

Observe that $h(c) + \overline{h(c)} = \mathrm{Tr}_1^n(c)$, and since $\mathrm{Tr}_1^n(c) = 0$ by assumption, we have $h(c) = \overline{h(c)}$. Conjugating (5), we get $h(c)(c + \overline{c}) = c\overline{c}(c + \overline{c})$, and, assuming that $c \neq \overline{c}$ (for otherwise c is already in $\mathbb{F}_{2^m}$ and thus a cube), this becomes $h(c) = c\overline{c}$.

From the definition of $h(c)$, we clearly have $h(c) + h(c)^2 = c + \overline{c}$. Hence $c + \overline{c} = c\overline{c} + c^2\overline{c}^2$, from which we get $c + \overline{c} + c\overline{c} + c^2 = c^2\overline{c}^2 + c^2$ by adding c^2 to both sides, and, finally, $(c+\overline{c})(1+c) = c^2(1+\overline{c}^2)$. Now, observe that $(1+\overline{c}^2)/(1+c) = (1+c)^{2^{m+1}-1}$, which is s cube for m odd, and that $c + \overline{c}$ lies in $\mathbb{F}_{2^m}$ and is thus a cube. Hence c^2, and thus also c is a cube, which completes the proof. □

Theorem 1. *[24] Let t_1 and t_2 denote the zeros of $t^2 + bt + a^3$ in $\mathbb{F}_{2^n}$ where $n = 2m$ and $a \in \mathbb{F}_{2^m}$, $b \in \mathbb{F}_{2^m}^*$. Let $f(x) = x^3 + ax + b$, then*

- *f has three zeros in $\mathbb{F}_{2^m}$ if and only if $\mathrm{Tr}_1^m(\frac{a^3}{b^2} + 1) = 0$ and t_1, t_2 are cubes in $\mathbb{F}_{2^m}$ (if m is even), $\mathbb{F}_{2^n}$ (if m is odd).*
- *f has exactly one zero in $\mathbb{F}_{2^m}$ if and only if $\mathrm{Tr}_1^m(\frac{a^3}{b^2} + 1) = 1$.*
- *f has no zeros in $\mathbb{F}_{2^m}$ if and only if $\mathrm{Tr}_1^m(\frac{a^3}{b^2} + 1) = 0$ and t_1, t_2 are not cubes in $\mathbb{F}_{2^m}$ (if m is even), $\mathbb{F}_{2^n}$ (if m is odd).*

Lemma 2. *[15] Let r, n be positive integers, and let $a, b, c \in \mathbb{F}_{2^n}$. Then the quadratic polynomial $Q(x) = x^{2^r+1} + ax^{2^r} + bx + c$ has either 0, 1, 2, or $2^{r_0} + 1$ roots $x \in \mathbb{F}_{2^n}$, where $r_0 = \gcd(r, n)$.*

Using Lemma 2, we can obtain the following.

Lemma 3. *Let m and i be positive integers such that $\gcd(m, i) = 1$ and let $S \in \mathbb{F}_{2^m} \setminus \{0, 1\}$. Then the polynomial*

$$P(N) = (S^{2^i} + S)N^{2^{2i}} + (S^{2^{2i}} + S)N^{2^i} + (S^{2^{2i}} + S^{2^i})N$$

in N has four roots, viz. $N = 0$, $N = 1$, $N = S$, and $N = S + 1$.

Proof. Note that for $S \notin \{0, 1\}$ the coefficients of P are all non-zero. Dividing P by N and substituting $t = N^{2^i-1}$, we obtain a new polynomial $P'(t) = at^{2^i+1} + bt + c$, with $a = (S^{2^i} + S)$, $b = (S^{2^{2i}} + S)$ and $c = (S^{2^{2i}} + S^{2^i})$. Since $\gcd(i, m) = 1$ from the hypothesis, by Lemma 2 $P'(t)$ can have at most three roots. Due to $\gcd(i, m) = 1$, every element in $\mathbb{F}_{2^m}$ has a unique $(2^i - 1)$-st root, and hence every root t of P' corresponds to a unique root N of P. It remains to verify that for $N \in \{0, 1, S, S + 1\}$, $P(N)$ does indeed evaluate to zero. □

We are now ready to prove the main result.

Theorem 2. *Let $n = 2m$ with m odd and $3 \nmid m$. Then the system E_i from (2) does not have any solutions $x \notin \mathbb{F}_2$ for the following values of i:*

1) $i = m - 2$;
2) $i = m$;
3) $i = (m - 2)^{-1} \mod n$;
4) $i = n - 1$.

Proof. First, observe that all elements of the half-field $\mathbb{F}_{2^m}$ are cubes in $\mathbb{F}_{2^n}$. If some $a \neq 0$ and $x \notin \mathbb{F}_2$ satisfy system (2), then $a^3(x^2 + x) = \alpha_1\beta$ and $a^{2^i+1}(x^{2^i} + x) = \alpha_2\beta$ for some $\alpha_1, \alpha_2 \in \mathbb{F}_{2^m}$ with $\alpha_1 \neq 0$. We can write $\alpha_1 = c^3$ for some $c \in \mathbb{F}_{2^n}^*$. Dividing both sides of the first equation by c^3, we obtain $(a/c)^3(x^2 + x) = \beta$. Dividing both sides of the second equation by c^{2^i+1}, we obtain $(a/c)^{2^i+1}(x^{2^i} + x) = \alpha_2\beta c^{-(2^i+1)}$. Since $3 \mid 2^i + 1$ for odd i, $c^{-(2^i+1)}$ is in $\mathbb{F}_{2^m}$. Thus, system (2) has a non-trivial solution $x \notin \mathbb{F}_2$ if and only of the system

$$\begin{cases} a^3(x^2 + x) = \beta \\ a^{2^i+1}(x^{2^i} + x) = \alpha\beta \end{cases} \tag{6}$$

has a solution for some $\alpha \in \mathbb{F}_{2^m}$. In the following, we show that for each of the values of i given in the statement of the theorem, this reduced system (6) has no solutions.

Case 1 In the case of $i = m - 2$, we have the system

$$\begin{cases} a^3(x^2 + x) = \beta \\ a^{2^{m-2}+1}(x^{2^{m-2}} + x) = \beta \cdot \mathbb{F}_{2^m} \end{cases}$$

for some $\alpha \in \mathbb{F}_{2^m}$. Raising the second equation to the fourth power, we have $a^{2^m+4}(\overline{x} + x^4) = \alpha^4\beta$. From the first equation, we can write $a^3 = \beta/(x^2 + x)$. Substituting this into the previous equation, we obtain $a^{2^m+1}\frac{\overline{x}+x^4}{x^2+x} \in \mathbb{F}_{2^m}$. Since $a^{2^m+1} \in \mathbb{F}_{2^m}$, this simply means $(\overline{x} + x^4)/(x^2 + x) \in \mathbb{F}_{2^m}$. Thus

$$\frac{\overline{x} + x^4}{x^2 + x} = \frac{x + \overline{x}^4}{\overline{x}^2 + \overline{x}}$$

and hence $(x^2 + x)(x + \overline{x}^4) \in \mathbb{F}_{2^m}$. Denoting $c = x^2 + x$, we can express $x + \overline{x}^4 = x + x^{2^{m+2}}$ as $c + c^2 + c^4 + \cdots + c^{2^{m+1}}$. We now have $\mathrm{Tr}_1^n(c) = 0$ and $c(c + c^2 + \cdots + c^{2^{m+1}}) \in \mathbb{F}_{2^m}$, so according to Lemma 1, $c = x^2 + x$ must be a cube. But then $a^3(x^2 + x) \in \beta \cdot \mathbb{F}_{2^m}$ implies that β is a cube which is impossible when $3 \nmid m$.

Case 2 The case $i = m$ trivially has no solutions since if $a^{2^m+1}(x^{2^m} + x) = \alpha\beta$ for some $\alpha \in \mathbb{F}_{2^m}$, then conjugating both sides yields $a^{2^m+1}(x^{2^m} + x) = \alpha\beta^2$, implying $\beta = \beta^2$.

Case 3 In the case of $i = (m - 2)^{-1} \mod n$, we have the equation system

$$\begin{cases} a^{i(m-2)+1}(x^{2^{i(m-2)}} + x) = \beta \\ a^{2^i+1}(x^{2^i} + x) = \alpha\beta \end{cases} \tag{7}$$

for some $\alpha \in \mathbb{F}_{2^m}$. Raising the first equation to the power 2^{2i}, we obtain

$$a^{2^{im}+2^{2i}}(x^{2^{im}} + x^{2^{2i}}) = \beta, \tag{8}$$

and raising the second equation to the power $2^i - 1$ yields

$$a^{2^{2i}-1}(x^{2^i} + x)^{2^i-1} = \alpha^{2^i-1}\beta. \tag{9}$$

From (8) and (9) we obtain the identity

$$\frac{\alpha^{2^i-1}\beta a^{2^{im}+2^{2i}}}{\beta a^{2^{2i}-1}} = \frac{(x^{2^i}+x)^{2^i-1}}{x^{2^{im}} + x^{2^{2i}}}. \tag{10}$$

The left-hand side of (10) simplifies to $\alpha^{2^i-1}a^{2^{im}+1}$. Since $a^{2^{im}+1} = a^{2^m+1}$ is in $\mathbb{F}_{2^m}$ for any $a \in \mathbb{F}_{2^n}$, we have that $(x^{2^{im}} + x^{2^{2i}})/(x^{2^i} + x)^{2^i-1} \in \mathbb{F}_{2^m}$, i.e.,

$$\frac{(\overline{x} + x^{2^{2i}})(x^{2^i} + x)}{(x^{2^i} + x)^{2^i}} = \frac{(x + \overline{x}^{2^{2i}})(\overline{x}^{2^i} + \overline{x})}{(\overline{x}^{2^i} + \overline{x})^{2^i}}$$

and hence

$$(\overline{x}+x^{2^{2i}})(x^{2^i}+x)(\overline{x}^{2^{2i}}+\overline{x}^{2^i}) = (x+\overline{x}^{2^{2i}})(\overline{x}^{2^i}+\overline{x})(x^{2^{2i}}+x^{2^i}). \tag{11}$$

The left-hand side of (11) takes the form

$$\begin{aligned} A(x) = x^{2^i}\overline{x}^{2^{2i}+1} + x^{2^i}\overline{x}^{2^i+1} + x^{2^{2i}+2^i}\overline{x}^{2^{2i}} + x^{2^{2i}+2^i}\overline{x}^{2^i} + \\ x\overline{x}^{2^{2i}+1} + x\overline{x}^{2^i+1} + x^{2^{2i}+1}\overline{x}^{2^{2i}} + x^{2^{2i}+1}\overline{x}^{2^i}. \end{aligned}$$

Denoting $S = x + \overline{x}$ and $N = x\overline{x}$, and observing that $A(x) + A(\overline{x}) = 0$, we can write

$$\begin{aligned} A(x) + A(\overline{x}) = \\ (S^{2^i} + S)N^{2^{2i}} + (S^{2^{2i}} + S)N^{2^i} + (S^{2^{2i}} + S^{2^i})N = 0. \end{aligned} \tag{12}$$

We now consider the expression on the right-hand side of (12) as a polynomial in S and N and determine its possible roots by Lemma 3. Before doing so, we need to rule out the cases when $N = 0$ and $S \in \{0, 1\}$. Unless $x = 0$, we must clearly have $N \neq 0$. If $S = x + \overline{x} = 0$, then we must have $x \in \mathbb{F}_{2^m}$ so that $(x^2 + x)$ is in $\mathbb{F}_{2^m}$ and is hence a cube. But then the equation $a^3(x^2 + x) = \beta$ from (7) implies that β is a cube, which is impossible under the assumption $3 \nmid m$. If $S = x + \overline{x} = 1$, then from the identity $x^2 + (x + \overline{x})x = x\overline{x}$ we get $x^2 + x = x\overline{x} = N$ and we once again infer that $x^2 + x$ must be a cube, which is impossible.

We can now apply Lemma 3 to see that only $N = 1$, $N = S$, and $N = S + 1$ are solutions to (12). We can additionally assume $N \neq S + 1$, since otherwise we have $x\overline{x} = x + \overline{x} + 1$; multiplying both sides by x and adding this to the original expression then gives us $(x^2 + 1)(\overline{x} + 1) = 0$, which implies $x = 1$. We thus only need to consider the cases $N = 1$ and $N = S$.

By adding $a^3(x^2 + x) = \beta$ and $x^2 + Sx + N = 0$ together, we obtain $(S + 1)x + N = \beta/a^3$ and hence

$$x = (N + \beta/a^3)/(S + 1). \tag{13}$$

Since $N = x\overline{x}$ and thus $x = N/\overline{x}$, we obtain

$$\frac{N + \beta/a^3}{S + 1} = \frac{N(S + 1)}{N + \overline{(\beta/a^3)}}$$

leading to

$$\begin{aligned} N(S + 1)^2 = (N + \beta/a^3)(N + \overline{\beta/a^3}) = \\ N^2 + (\beta/a^3 + \overline{\beta/a^3})N + \beta/a^3\overline{\beta/a^3}. \end{aligned} \tag{14}$$

From (13), we get $S = x + \overline{x} = \frac{N+\beta/a^3+N+\overline{\beta/a^3}}{S+1} = \frac{\beta/a^3+\overline{\beta/a^3}}{S+1}$ so that

$$S^2 + S = \beta/a^3 + \overline{\beta/a^3}. \tag{15}$$

Substituting this into (14), we obtain $N(S + 1)^2 = N^2 + (S^2 + S)N + \beta/a^3\overline{\beta/a^3}$, which implies

$$N^2 + (S + 1)N + \beta/a^3\overline{\beta/a^3} = 0.$$

When $N \in \{1, S\}$, this implies $S = a^{-3}\overline{a^{-3}}$. Hence $S^2 + S = a^{-6}\overline{a^{-6}} + a^{-3}\overline{a^{-3}}$. Combining this with (15), we see that $\beta/a^3 + \overline{\beta/a^3} = a^{-6}\overline{a^{-6}} + a^{-3}\overline{a^{-3}}$ and hence $t_1 = \beta/a^3$ and $t_2 = \overline{\beta/a^3}$ are roots of the polynomial $t^2 + (a^{-6}\overline{a^{-6}} + a^{-3}\overline{a^{-3}})t + a^{-3}\overline{a^{-3}}$.

If we denote $c_1 = (a\overline{a})^{-1}$, $c_2 = c_1^6 + c_1^3$, we can write it more succinctly as $t^2 + c_2 t + c_1^3$. Dividing both sides by c_2^2 and denoting $y = t/c_2$, this becomes $y^2 + y + (c_1^3)/(c_2^2)$.

Since a quadratic equation $y^2 + y = v$ for $v \in \mathbb{F}_{2^k}$ has solutions in $\mathbb{F}_{2^k}$ if and only if $\mathrm{Tr}_1^k(v) = 0$ [1], we have that $\mathrm{Tr}_1^m(\frac{c_1^3}{c_2^2}) = 1$, and hence $\mathrm{Tr}_1^m(\frac{c_1^3}{c_2^2} + 1) = 0$ due to m being odd.

Letting $f(y) = y^3 + c_1 y + c_1^6 + c_1^3$, by Theorem 1, f has either three roots, or none at all. However, c_1^2 can easily be seen to be a root, so that f must have three roots. Again by Theorem 1, this implies that t_1 and t_2 have to be cubes, which is impossible for $3 \nmid m$.

Case 4 When $i = n - 1$, we have the system

$$\begin{cases} a^3(x^2 + x) = \beta \\ a^{2^{n-1}+1}(x^{2^{n-1}} + x) = \alpha\beta \end{cases}$$

for $\alpha \in \mathbb{F}_{2^m}$.

Raising the second equation to the second power yields $a^3(x^2 + x) = \alpha^2\beta^2$ so that we have $\alpha^2\beta^2 = \beta$, implying that β lies in $\mathbb{F}_{2^m}$. □

According to our experimental results up to dimension $n = 46$, the values of i given in Theorem 2 are the only ones for which $C_i(x) = x^3 + \beta x^{2^i+1} + x^{3\cdot 2^m} + x^{2^{i+m}+2^m}$ is APN. We can generalize C_i to the form $C_i'(x) = x^3 + \beta(x^{2^i+1})^{2^k} + \beta^2\overline{x^3} + \overline{(x^{2^i+1})^{2^k}}$ for some non-negative integer k. The APN-ness of such a function can be characterized by the solvability of the system

$$\begin{cases} a^3(x^2 + x) \in \beta \cdot \mathbb{F}_{2^m} \\ (a^{2^i+1}(x^{2^i} + x))^{2^k} \in \beta \cdot \mathbb{F}_{2^m}. \end{cases} \tag{16}$$

Note that raising β to an even power of two leaves it unchanged. Thus, for even values of k, system (16) has non-trivial solutions if and only if (2) does. Therefore, for $i \in \{m-2, m, n-1, (m-2)^{-1} \mod n\}$ and even k the generalized quadrinomial $C_i'(x)$ is APN.

If k is odd, we obtain a slightly different system.

Lemma 4. *Let k be odd. Then the system*

$$\begin{cases} a^3(x^2+x) \in \beta \cdot \mathbb{F}_{2^m} \\ (a^{2^i+1}(x^{2^i}+x))^{2^k} \in \beta \cdot \mathbb{F}_{2^m}. \end{cases} \tag{17}$$

has only trivial solutions for $i \in \{m+2, m, (m+2)^{-1} \mod n\}$.

Proof. Suppose $i = m+2$. Since raising β to an odd power of two yields β^2, raising the second equation of system (17) to the power 2^{n-k} leaves us with $a^{2^{m+2}+1}(x^{2^m+2}+x) = \alpha'\beta^2$ for $\alpha' = \alpha^{2^{n-k}}$. Raising it again to the power (2^{m-2}) and, noting that $m-2$ is odd, we obtain $a^{2^{m-2}}+1(x^{2^{m-2}}+x) = \alpha''\beta$ with $\alpha'' = \alpha'^{2^{m-2}}$, which is the same as system (2). Similarly, when $i = (m+2)^{-1}$, we first raise the second equation to the power 2^{n-k}, and then to the power $2^{(m-2)^{-1} \mod n}$; again, $(m-2)^{-1} \mod n$ is odd, so that we come back to system (7). In the case of $i = m$, it suffices to conjugate the equation $a^{2^m+1}(x^{2^m}+x) = \alpha'\beta^2$ in order to derive a contradiction in the same way as in the proof of Theorem 2. □

When k is odd, the case of $i = n-1$ does allow non-trivial solutions, which can easily be seen by taking $\alpha = 1$ and any $a \in \mathbb{F}_{2^n}^*$ for which $x^2+x = \beta/a^3$ is solvable. According to our data for dimension $n = 10$ (which is the highest dimension for which we can computationally test CCZ-equivalence by our current means), the polynomials C_i' for odd values of k are equivalent to some C_i, so that we may assume $k = 0$. Furthermore, for $i = m$ and $i = n-1$, the polynomial C_i over $\mathbb{F}_{2^{10}}$ is CCZ-equivalent to one of the known CCZ-equivalence classes: in the case of $i = n-1$, C_i is equivalent to the Gold function x^3, and in the case of $i = m$ it is equivalent to family F3 from Table II.

The remaining two values of i, viz. $m-2$ and $(m-2)^{-1} \mod n$ yield for dimension $n = 10$ the two CCZ-inequivalent APN quadrinomials from Observation 1, C_3 and C_7, which are, in addition, CCZ-inequivalent to any currently known APN function over $\mathbb{F}_{2^{10}}$. We have verified this computationally in two ways. First, we used the code isomorphism test described in Section II to compare C_3 and C_7 against representatives from the known infinite families, against the sporadic binomials $B(x)$ and $B'(x)$, and, finally, against themselves. These tests typically take less than half a minute for any given pair of functions, and show that C_3 and C_7 are indeed CCZ-inequivalent to any other known APN function over $\mathbb{F}_{2^{10}}$. Second, we have computed the Γ-ranks of C_3 and C_7, B, and representatives from the equivalence classes of the known APN functions. The results are summarized in Table III below and further confirm these results.

Family F12 in Table II gives six CCZ-inequivalent representatives over $\mathbb{F}_{2^{10}}$. Since their polynomial form is quite complicated, we omit it in Table III, and only list their Γ-ranks; we note that only five values are given, since two of these six CCZ-inequivalent representatives have the same Γ-rank.

In any case, by inspecting the Γ-ranks of the known APN functions in the table, it is evident that C_3 and C_7 are inequivalent to any of them. As a consequence, we collect all the above results in the following corollary and construct a new family of APN functions.

Corollary 1. *Let $n = 2m$ with m odd and $3 \nmid m$. Consider the quadrinomial*

$$C(x) = x^3 + a(x^{2^i+1})^{2^k} + bx^{3 \cdot 2^m} + c(x^{2^{i+m}+2^m})^{2^k}.$$

Then $C(x)$ is APN over $\mathbb{F}_{2^n}$ in the following cases:

1) *$n = 10$, $(a,b,c) = (\beta, 0, 0)$, $i = 3$, $k = 2$ (this gives us the binomial $B(x)$);*
2) *$(a,b,c) = (\beta, \beta^2, 1)$, $i = m-2$, k even;*
3) *$(a,b,c) = (\beta, \beta^2, 1)$, $i = (m-2)^{-1}$, k even;*
4) *$(a,b,c) = (\beta, \beta^2, 1)$, $i = m$, k even;*
5) *$(a,b,c) = (\beta, \beta^2, 1)$, $i = n-1$, k even*
6) *$(a,b,c) = (\beta, \beta^2, 1)$, $i = m+2$, k odd;*
7) *$(a,b,c) = (\beta, \beta^2, 1)$, $i = (m+2)^{-1}$, k odd;*
8) *$(a,b,c) = (\beta, \beta^2, 1)$, $i = n-1$, k odd .*

Furthermore, in dimension $n = 10$, the functions in items 2 and 3 lie in distinct classes with respect to CCZ-equivalence and are CCZ-inequivalent to any known APN function over $\mathbb{F}_{2^{10}}$, including $B(x)$.

TABLE III

Γ-RANKS OF ALL KNOWN CCZ-INEQUIVALENT APN FUNCTIONS OVER $\mathbb{F}_{2^{10}}$

Function	Family	Γ-rank
x^3	Gold	125042
x^9	Gold	136492
x^{57}	Kasami	186416
x^{339}	Dobbertin	280604
$x^6 + x^{33} + \alpha^{31}x^{192}$	F3	151216
$x^{33} + x^{72} + \alpha^{31}x^{258}$	F3	153896
$x^3 + \mathrm{Tr}_1^{10}(x^9)$	F4	153896
$x^3 + \alpha^{-1}\mathrm{Tr}_1^{10}(a^3x^9)$	F4	164098
-	F12	162550, 163308, 163398, 163400, 164026
$B(x) = x^3 + \alpha^{341}x^{36}$	[16]	169984
C_3	new	166068
C_7	new	166168

Conclusion

We have constructed a family of quadrinomial functions over finite fields $\mathbb{F}_{2^n}$ with $n = 2m$, m odd and $3 \nmid m$ which contains the previously unclassified binomial $x^3 + \beta x^{36}$ (discovered in 2006 as the first example of an APN function CCZ-inequivalent to a power function) in the sense that $B(x)$ can be obtained by setting two of the coefficients in the quadrinomial construction to zero. We have shown two infinite constructions of APN functions belonging to this family, and demonstrated that their instances over $\mathbb{F}_{2^{10}}$ are CCZ-inequivalent to any known APN function over this field, including the sporadic binomial $B(x)$, and that they are CCZ-inequivalent to each other. We have also characterized the APN-ness of all quadrinomials of the form $x^3 + \beta(x^{2^i+1})^{2^k} + \beta^2 x^{3 \cdot 2^m} + (x^{2^{i+m}+2^m})^{2^k}$ in terms of the solvability of a system of equations.

Acknowledgements

The research presented in this paper was supported by the Trond Mohn Foundation, and by the Research Council of Norway under contract 247742/O70.

References

[1] E. R. Berlekamp, H. Rumsey, and G. Solomon, "On the solution of algebraic equations over finite fields," *Information and control*, vol. 10, no. 6, pp. 553–564, 1967.

[2] T. Beth and C. Ding, "On almost perfect nonlinear permutations," in *Workshop on the Theory and Application of of Cryptographic Techniques*. Springer, 1993, pp. 65–76.

[3] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," *Journal of Cryptology*, vol. 4, no. 1, pp. 3–72, Jan 1991. [Online]. Available: https://doi.org/10.1007/BF00630563

[4] C. Bracken, E. Byrne, N. Markin, and G. McGuire, "New families of quadratic almost perfect nonlinear trinomials and multinomials," *Finite Fields and Their Applications*, vol. 14, no. 3, pp. 703–714, 2008.

[5] ——, "A few more quadratic APN functions," *Cryptography and Communications*, vol. 3, no. 1, pp. 43–53, 2011.

[6] K. Browning, "APN polynomials and related codes," *Special volume of Journal of Combinatorics, Information and System Sciences*, vol. 34, pp. 135–159, 2009.

[7] L. Budaghyan, M. Calderini, C. Carlet, R. S. Coulter, and I. Villa, "Constructing APN functions through isotopic shifts," Cryptology ePrint Archive, Report 2018/769, 2018.

[8] L. Budaghyan and C. Carlet, "Classes of quadratic APN trinomials and hexanomials and related structures," *IEEE Transactions on Information Theory*, vol. 54, no. 5, pp. 2354–2357, 2008.

[9] L. Budaghyan, C. Carlet, and G. Leander, "Two classes of quadratic APN binomials inequivalent to power functions," *IEEE Transactions on Information Theory*, vol. 54, no. 9, pp. 4218–4229, 2008.

[10] ——, "Constructing new APN functions from known ones," *Finite Fields and Their Applications*, vol. 15, no. 2, pp. 150–159, 2009.

[11] ——, "On a construction of quadratic APN functions," in *2009 IEEE Information Theory Workshop*, 2009, pp. 374–378.

[12] H. Dobbertin, "Almost perfect nonlinear power functions on $GF(2^n)$: the Niho case," *Information & Computation*, vol. 151, no. 1, pp. 57–72, 1999.

[13] ——, "Almost perfect nonlinear power functions on $GF(2^n)$: the Welch case," *IEEE Transactions on Information Theory*, vol. 45, no. 4, pp. 1271–1275, 1999.

[14] ——, "Almost perfect nonlinear power functions on $GF(2^n)$: A new case for n divisible by 5," *International Conference on Finite Fields and Applications*, pp. 113–121, 2001.

[15] H. Dobbertin, P. Felke, T. Helleseth, and P. Rosendahl, "Niho type cross-correlation functions via Dickson polynomials and Kloosterman sums," *IEEE Transactions on Information Theory*, vol. 52, no. 2, pp. 613–627, 2006.

[16] Y. Edel, G. Kyureghyan, and A. Pott, "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.

[17] Y. Edel and A. Pott, "A new almost perfect nonlinear function which is not quadratic," *Advances in Mathematics of Communications*, vol. 3, no. 1, pp. 59–81, 2009.

[18] R. Gold, "Maximal recursive sequences with 3-valued recursive cross-correlation functions (corresp.)," *IEEE Transactions on Information Theory*, vol. 14, no. 1, pp. 154–156, 1968.

[19] H. Janwa and R. M. Wilson, "Hyperplane sections of Fermat varieties in P^3 in char. 2 and some applications to cyclic codes," in *International Symposium on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes*. Springer, 1993, pp. 180–194.

[20] T. Kasami, "The weight enumerators for several classes of subcodes of the 2nd order binary reed-muller codes," *Information & Computation*, vol. 18, no. 4, pp. 369–394, 1971.

[21] R. Lidl and H. Niederreiter, *Finite fields*. Cambridge university press, 1997, vol. 20.

[22] K. Nyberg, "Differentially uniform mappings for cryptography," *Lecture Notes in Computer Science*, vol. 765, pp. 55–64, 1994.

[23] H. Taniguchi, "On some quadratic APN functions," *Designs, Codes and Cryptography*, pp. 1–11, 2019.

[24] K. S. Williams, "Note on cubics over $GF(2^n)$ and $GF(3^n)$," *Journal of Number Theory*, vol. 7, no. 4, pp. 361–365, 1975.

[25] Y. Yu, M. Wang, and Y. Li, "A matrix approach for constructing quadratic APN functions," *Designs, codes and cryptography*, vol. 73, no. 2, pp. 587–600, 2014.

[26] Y. Zhou and A. Pott, "A new family of semifields with 2 parameters," *Advances in Mathematics*, vol. 234, pp. 43–60, 2013.