Constructing new APN functions from known ones

Lilya Budaghyan [a], Claude Carlet [b], and Gregor Leander [c]

[a] *Department of Mathematics*
University of Trento
ITALY

[b] *Department of Mathematics*
University of Paris 8 (MAATICAH)
also with INRIA, Projet CODES
FRANCE

[c] *GRIM, University of Toulon*
FRANCE

Abstract

We present a method for constructing new quadratic APN functions from known ones. Applying this method to the Gold power functions we construct an APN function $x^3 + \mathrm{tr}(x^9)$ over $\mathbb{F}_{2^n}$. It is proven that in general this function is CCZ-inequivalent to the Gold functions (and therefore EA-inequivalent to power functions), to the inverse and Dobbertin mappings, and in the case $n = 7$ it is CCZ-inequivalent to all power mappings.

Key words: Affine equivalence, Almost bent, Almost perfect nonlinear, CCZ-equivalence, Differential uniformity, Nonlinearity, S-box, Vectorial Boolean function

1 Introduction

A function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is called *almost perfect nonlinear* (APN) if, for every $a \neq 0$ and every b in $\mathbb{F}_2^n$, the equation $F(x) + F(x + a) = b$ admits at most two solutions (it is also called *differentially* 2*-uniform*). Vectorial Boolean functions

Email addresses: `lilia.b@mail.ru` (Lilya Budaghyan),
`claude.carlet@inria.fr` (Claude Carlet),
`Gregor.Leander@rub.de` (Gregor Leander).

used as S-boxes in block ciphers must have a low differential uniformity to allow a high resistance to the differential cryptanalysis (see [3,34]). In this sense APN functions are optimal. The notion of the APN function is closely connected to the notion of the almost bent (AB) function. A function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is called AB if the minimum Hamming distance between all the Boolean functions $v \cdot F$, $v \in \mathbb{F}_2^n \setminus \{0\}$ (called the *component* functions of F), and all affine Boolean functions on $\mathbb{F}_2^n$ is maximal. Here, "$\cdot$" denotes the usual inner product in $\mathbb{F}_2^n$. Any other choice of an inner product would lead to the same notion. For instance, the vector space $\mathbb{F}_2^n$ can be identified to the field $\mathbb{F}_{2^n}$ and we can then take for inner product $x \cdot y = \mathrm{tr}(xy)$ where tr is the absolute trace function. The minimum Hamming distance between all component functions of F and all affine Boolean functions on $\mathbb{F}_2^n$ is called the *nonlinearity* of F and its maximum equals $2^{n-1} - 2^{\frac{n-1}{2}}$ (see [18]). AB functions exist for n odd only and oppose an optimum resistance to the linear cryptanalysis (see [32,18]). Besides, every AB function is APN [18], and in the n odd case, any quadratic function is APN if and only if it is AB [17].

The APN and AB properties are preserved by some transformations of functions [17,34]. If F is an APN function, A_1, A_2 are affine permutations and A is affine then the function $F' = A_1 \circ F \circ A_2 + A$ is also APN (the functions F and F' are called extended affine equivalent (*EA-equivalent*)). Besides, the inverse of any APN permutation is APN too. Until recently, the only known constructions of APN and AB functions were EA-equivalent to power functions $F(x) = x^d$ over finite fields ($\mathbb{F}_{2^n}$ being identified with $\mathbb{F}_2^n$). Table 1 gives all known values of exponents d (up to multiplication by a power of 2 modulo $2^n - 1$, and up to taking the inverse when a function is a permutation) such that the power function x^d over $\mathbb{F}_{2^n}$ is APN. For n odd the Gold, Kasami, Welch and Niho APN functions from Table 1 are also AB (for the proofs of AB property see [14,15,27,28,30,34]).

Table 1

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

Functions	Exponents d	Conditions	References
Gold	$2^i + 1$	$\gcd(i, n) = 1$	[27,34]
Kasami	$2^{2i} - 2^i + 1$	$\gcd(i, n) = 1$	[29,30]
Welch	$2^t + 3$	$n = 2t + 1$	[24]
Niho	$2^t + 2^{\frac{t}{2}} - 1$, t even $2^t + 2^{\frac{3t+1}{2}} - 1$, t odd	$n = 2t + 1$	[23]
Inverse	$2^{2t} - 1$	$n = 2t + 1$	[2,34]
Dobbertin	$2^{4t} + 2^{3t} + 2^{2t} + 2^t - 1$	$n = 5t$	[25]

In [17], Carlet, Charpin and Zinoviev introduced an equivalence relation of functions, more recently called CCZ-equivalence, which corresponds to the affine equivalence of the graphs of functions and preserves APN and AB properties. EA-equivalence is a particular case of CCZ-equivalence and any permutation is CCZ-equivalent to its inverse [17]. In [11,12], it is proven that CCZ-equivalence is more general, and applying CCZ-equivalence to the Gold mappings classes of APN functions EA-inequivalent to power functions are constructed in [5,11,12]. These classes are presented in Table 2. When n is odd, these functions are also AB. Besides, for $n = 5$ the first of these AB functions is EA-inequivalent to any permutation and disproves the conjecture from [17] about nonexistence of such AB mappings (see [11,12]).

Table 2

Known APN functions EA-inequivalent to power functions on $\mathbb{F}_{2^n}$.

Functions	Conditions	$d^\circ(F)$
$x^{2^i+1} + (x^{2^i} + x + \mathrm{tr}(1) + 1)\,\mathrm{tr}(x^{2^i+1} + x\,\mathrm{tr}(1))$	$n \geq 4$ $\gcd(i,n) = 1$	3
$\left(x + \mathrm{tr}_{n/3}(x^{2(2^i+1)} + x^{4(2^i+1)}) + \mathrm{tr}(x)\,\mathrm{tr}_{n/3}(x^{2^i+1} + x^{2^{2i}(2^i+1)})\right)^{2^i+1}$	n divisible by 6 $\gcd(i,n) = 1$	4
$\left(x^{\frac{1}{2^i+1}} + \mathrm{tr}_{m/3}(x + x^{2^{2i}})\right)^{-1}$	n divisible by 3 $\gcd(2i,n) = 1$	4
$x^{2^i+1} + \mathrm{tr}_{n/m}(x^{2^i+1}) + x^{2^i}\,\mathrm{tr}_{n/m}(x) + x\ \mathrm{tr}_{n/m}(x)^{2^i}$ $+ \left(\mathrm{tr}_{n/m}(x)^{2^i+1} + \mathrm{tr}_{n/m}(x^{2^i+1}) + \mathrm{tr}_{n/m}(x)\right)^{\frac{1}{2^i+1}} (x^{2^i} + \mathrm{tr}_{n/m}(x)^{2^i} + 1)$ $+ \left(\mathrm{tr}_{n/m}(x)^{2^i+1} + \mathrm{tr}_{n/m}(x^{2^i+1}) + \mathrm{tr}_{n/m}(x)\right)^{\frac{2^i}{2^i+1}} (x + \mathrm{tr}_{n/m}(x))$	$m \neq n$ n odd n divisible by m $\gcd(i,n) = 1$	$m+2$

These new results on CCZ-equivalence have raised several interesting questions. One of them is whether the known classes of APN power functions are CCZ-inequivalent. Partly the answer is given in [8]: it is proven that in general the Gold functions are CCZ-inequivalent to the Kasami and Welch functions, and that for different parameters $1 \leq i, j \leq \frac{n-1}{2}$ the Gold functions x^{2^i+1} and x^{2^j+1} are CCZ-inequivalent. Another interesting question is the existence of APN polynomials CCZ-inequivalent to power functions. In [26] it is shown that one of the ways to construct such polynomials is to consider linear combinations of two different Gold power functions. Using this approach they have introduced two quadratic APN binomials on $\mathbb{F}_{2^{10}}$ and $\mathbb{F}_{2^{12}}$ which are CCZ-inequivalent to power maps. After that, two infinite classes of quadratic APN binomials CCZ-inequivalent to power functions have been constructed in [7–9]. These classes are presented in Table 3 (this table gives all known classes of

APN functions CCZ-inequivalent to power functions) by cases 1 and 2. When n is odd these functions are AB permutations and this disproves the conjecture from [17] about nonexistence of AB functions CCZ-inequivalent to the Gold maps [8,9]. Another approach for constructing quadratic APN polynomials CCZ-inequivalent to power functions is introduced in [20]: the idea is to consider quadratic hexanomials of a certain type over $\mathbb{F}_{2^{2m}}$ as good candidates for being differentially 4-uniform [1]. This method has been generalized in [6]. Following the methods from [6,20] classes of APN trinomials and hexanomials (see cases 3 and 4 in Table 3) have been introduced in [6]. This functions are conjectured to be CCZ-inequivalent to power functions and this conjecture was confirmed for $n = 6$ (see [6]).

Table 3

Known APN functions CCZ-inequivalent to power functions on $\mathbb{F}_{2^n}$.

No	Functions	Conditions	References
1	$x^{2^s+1} + wx^{2^{ik}+2^{mk+s}}$	$n = 3k$, $\gcd(k, 3) = \gcd(s, 3k) = 1$ $k \geq 4$, $i = sk \mod 3$, $m = 3 - i$ w has the order $2^{2k} + 2^k + 1$	[8,9]
2	$x^{2^s+1} + wx^{2^{ik}+2^{mk+s}}$	$n = 4k$, $\gcd(k, 2) = \gcd(s, 2k) = 1$ $k \geq 3$, $i = sk \mod 4$, $m = 4 - i$ w has the order $2^{3k} + 2^{2k} + 2^k + 1$	[7]
3	$x^{2^{2i}+2^i} + bx^{q+1} + cx^{q(2^{2i}+2^i)}$	$n = 2m$, $m \geq 3$, $q = 2^m$ $c^{q+1} = 1$, $c \notin \{\lambda^{(2^i+1)(q-1)}, \lambda \in \mathbb{F}_{2^n}\}$ $\gcd(i, m) = 1$, $cb^q + b \neq 0$	[6]
4	$x(x^{2^i} + x^q + cx^{2^i q})$ $+x^{2^i}(c^q x^q + sx^{2^i q}) + x^{(2^i+1)q}$	$n = 2m$, $m \geq 3$, $q = 2^m$ $\gcd(i, m) = 1$, $s \notin \mathbb{F}_q$ $x^{2^i+1} + cx^{2^i} + c^q x + 1$ is irreducible over $\mathbb{F}_{2^n}$	[6]
5	$x^3 + \mathrm{tr}(x^9)$	$n \geq 7$ $n > 2p$ for the smallest possible $p > 1$ such that $p \neq 3$, $\gcd(p, n) = 1$	Corollary 1 of the present paper

All constructions of APN polynomials CCZ-inequivalent to power functions mentioned above have not given new APN polynomials with coefficients in $\mathbb{F}_2$. A natural question is whether all APN polynomials with coefficients in

[1] Similar approach for constructing differentially 4-uniform functions was proposed in [33]: they consider quadratic quadrinomials of a certain type over $\mathbb{F}_{2^{2m}}$.

$\mathbb{F}_2$ are CCZ-equivalent to power functions. In the present paper we show that the answer to this question is negative. We give a new approach for constructing quadratic APN functions and using it we construct a class of quadratic APN polynomials with coefficients in $\mathbb{F}_2$. We prove that the function $F(x) = x^3+\mathrm{tr}(x^9)$ is APN over $\mathbb{F}_{2^n}$ for any n, and that for almost all $n \geq 7$ it is CCZ-inequivalent to the Gold functions (and therefore EA-inequivalent to power functions), to the inverse and Dobbertin functions. Obviously, this function is AB for all odd n. We conjecture that for $n \geq 7$ the function F is CCZ-inequivalent to any power function. This conjecture is confirmed for the case $n = 7$. Further we show that applying CCZ-equivalence to quadratic APN functions, it is possible to construct classes of nonquadratic APN mappings CCZ-inequivalent to power functions. Note that the existence of APN functions CCZ-inequivalent to power functions and to quadratic functions is still an open problem.

2 Preliminaries

Let $\mathbb{F}_2^n$ be the n-dimensional vector space over the field $\mathbb{F}_2$. Any function F from $\mathbb{F}_2^n$ to itself can be uniquely represented as a polynomial on n variables with coefficients in $\mathbb{F}_2^n$, whose degree with respect to each coordinate is at most one:

$$F(x_1, ..., x_n) = \sum_{u \in \mathbb{F}_2^n} c(u) \Big(\prod_{i=1}^{n} x_i^{u_i} \Big), \qquad c(u) \in \mathbb{F}_2^n.$$

This representation is called the *algebraic normal form* of F and its degree $d^\circ(F)$ the *algebraic degree* of the function F.

Besides, the field $\mathbb{F}_{2^n}$ can be identified with $\mathbb{F}_2^n$ as a vector space. Then, viewed as a function from this field to itself, F has a unique representation as a univariate polynomial over $\mathbb{F}_{2^n}$ of degree smaller than 2^n:

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

For any k, $0 \leq k \leq 2^n - 1$, the number $w_2(k)$ of the nonzero coefficients $k_s \in \{0, 1\}$ in the binary expansion $\sum_{s=0}^{n-1} 2^s k_s$ of k is called the 2-*weight* of k. The algebraic degree of F is equal to the maximum 2-weight of the exponents i of the polynomial $F(x)$ such that $c_i \neq 0$, that is, $d^\circ(F) = \max_{0 \leq i \leq n-1, c_i \neq 0} w_2(i)$ (see [17]).

A function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is *linear* if and only if $F(x)$ is a linearized polynomial over $\mathbb{F}_{2^n}$, that is,

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

The sum of a linear function and a constant is called an *affine function.*

Let F be a function from $\mathbb{F}_{2^n}$ to itself and A_1, $A_2 : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ be affine permutations. The functions F and $A_1 \circ F \circ A_2$ are then called *affine equivalent.* Affine equivalent functions have the same algebraic degree (i.e. the algebraic degree is *affine invariant*).

As recalled in the Introduction, we say that the functions F and F' are *extended affine equivalent* if $F' = A_1 \circ F \circ A_2 + A$ for some affine permutations A_1, A_2 and an affine function A. If F is not affine, then F and F' have again the same algebraic degree.

Two mappings F and F' from $\mathbb{F}_{2^n}$ to itself are called Carlet-Charpin-Zinoviev equivalent (*CCZ-equivalent*) if the graphs of F and F', that is, the subsets $G_F = \{(x, F(x)) \mid x \in \mathbb{F}_{2^n}\}$ and $G_{F'} = \{(x, F'(x)) \mid x \in \mathbb{F}_{2^n}\}$ of $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$, are affine equivalent. Hence, F and F' are CCZ-equivalent if and only if there exists an affine automorphism $\mathcal{L} = (L_1, L_2)$ of $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ such that

$$y = F(x) \Leftrightarrow L_2(x, y) = F'(L_1(x, y)).$$

Note that since $\mathcal{L}$ is a permutation then the function $L_1(x, F(x))$ has to be a permutation too (see [8]). As shown in [17], EA-equivalence is a particular case of CCZ-equivalence and any permutation is CCZ-equivalent to its inverse.

For a function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ and any elements $a, b \in \mathbb{F}_{2^n}$ we denote

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

F is called a *differentially δ-uniform* function if $\max_{a \in \mathbb{F}_{2^n}^*, b \in \mathbb{F}_{2^n}} \delta_F(a, b) \leq \delta$. Note that $\delta \geq 2$ for any function over $\mathbb{F}_{2^n}$. Differentially 2-uniform mappings are called *almost perfect nonlinear.*

For any function $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ we denote

$$\lambda_F(a, b) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\mathrm{tr}(bF(x) + ax)}, \qquad a, b \in \mathbb{F}_{2^n},$$

where $\mathrm{tr}(x) = x + x^2 + x^4 + ... + x^{2^{n-1}}$ is the trace function from $\mathbb{F}_{2^n}$ into $\mathbb{F}_2$ (and for any divisor m of n we also denote $\mathrm{tr}_{n/m}(x) = x + x^{2^m} + ... + x^{2^{m(n/m-1)}}$). The set $\Lambda_F = \{\lambda_F(a, b) : a, b \in \mathbb{F}_{2^n}, b \neq 0\}$ is called the *Walsh spectrum* of the function F and the multiset $\{|\lambda_F(a, b)| : a, b \in \mathbb{F}_{2^n}, b \neq 0\}$ is called the *extended Walsh spectrum* of F. The value

$$\mathcal{NL}(F) = 2^{n-1} - \frac{1}{2} \max_{a \in \mathbb{F}_{2^n}, b \in \mathbb{F}_{2^n}^*} |\lambda_F(a, b)|$$

equals the *nonlinearity* of the function F. The nonlinearity of any function F

satisfies the inequality

$$\mathcal{NL}(F) \leq 2^{n-1} - 2^{\frac{n-1}{2}}$$

([18,36]) and in case of equality F is called *almost bent* or *maximum nonlinear.*

Obviously, AB functions exist only for n odd. It is proven in [18] that every AB function is APN and its Walsh spectrum equals $\{0, \pm 2^{\frac{n+1}{2}}\}$. If n is odd, every APN mapping which is quadratic (that is, whose algebraic degree equals 2) is AB [17], but this is not true for nonquadratic cases: the Dobbertin and the inverse APN functions are not AB (see [15,17]). When n is even, the inverse function x^{2^n-2} is a differentially 4-uniform permutation [34] and has the best known nonlinearity [31], that is $2^{n-1} - 2^{\frac{n}{2}}$ (see [15,22]). This function has been chosen as the basic S-box, with $n = 8$, in the Advanced Encryption Standard (AES), see [19]. A comprehensive survey on APN and AB functions can be found in [16].

It is shown in [17] that, if F and G are CCZ-equivalent, then F is APN (resp. AB) if and only if G is APN (resp. AB). More generally, CCZ-equivalent functions have the same differential uniformity and the same extended Walsh spectrum (see [11]). Further invariants for CCZ-equivalence are given in [26] (see also [20]) in terms of group algebras. Let $G = \mathbb{F}_2[\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}]$ be the group algebra of $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ over $\mathbb{F}_2$. It consists of the formal sums

$$\sum_{g \in G} a_g g$$

where $a_g \in \mathbb{F}_2$. If S is a subset of $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ then it can be identified with the element $\sum_{s \in S} s$ of G. For any APN mapping F we denote

$$\Delta_F = \{(a, b) : F(x) + F(x + a) = b \text{ has 2 solutions}\} \subset \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}\,.$$

The dimensions of the ideals of G generated by Δ_F and by the graph G_F of F are called Δ- and Γ-ranks, respectively. According to [26] (and also [20]), Δ- and Γ-ranks of a function are CCZ-invariant.

3 Construction of new quadratic APN functions

In the theorem below we give a general approach for constructing new quadratic APN functions from known ones.

Theorem 1 *Let F be a quadratic APN function from $\mathbb{F}_{2^n}$ to itself, let f be a quadratic Boolean function on $\mathbb{F}_{2^n}$ and*

$$\varphi_F(x, a) = F(x) + F(x + a) + F(a) + F(0),$$

$$\varphi_f(x, a) = f(x) + f(x + a) + f(a) + f(0).$$

Then the function $F(x) + f(x)$ is APN if for every nonzero $a \in \mathbb{F}_{2^n}$ there exists a linear Boolean function ℓ_a satisfying the conditions

1) $\varphi_f(x, a) = \ell_a(\varphi_F(x, a))$,
2) *if* $\varphi_F(x, a) = 1$ *for some* $x \in \mathbb{F}_{2^n}$ *then* $\ell_a(1) = 0$.

Proof. Since the function $F(x)+f(x)$ is quadratic, it is APN if and only if, for every nonzero $a \in \mathbb{F}_{2^n}$, the equation $\varphi_F(x, a)+\varphi_f(x, a) = 0$ admits at most two solutions (see e.g. [16]). According to the hypothesis on ℓ_a, a solution to this equation must be such that $\varphi_f(x, a) = 0$ and therefore such that $\varphi_F(x, a) = 0$. Then, F being quadratic APN, this equation admits at most two solutions.□

The same principle as in Theorem 1 allows generating a large variety of differentially 4-uniform functions from APN functions as it is shown in the proposition below.

Proposition 1 *For any APN function F the following functions are differentially 4-uniform over $\mathbb{F}_{2^n}$*

1) $F(x) + \mathrm{tr}(G(x))$ *for any function G;*
2) $F(x) + x^{2^n-1}$*;*
3) $F \circ A$ *and* $A \circ F$ *for any affine function A which is 2-to-1;*
4) *any function F' such that $\mathcal{L}(G_F) = G_{F'}$ for some affine 2-to-1 mapping $\mathcal{L}$ of $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$.*

Remark 1 Note that, in the situation of Theorem 1, a linear function l_a satisfying $\varphi_f(x, a) = \ell_a(\varphi_F(x, a))$ always exists. This is due to the fact that, by the assumption F is APN and then the kernel of $\varphi_F(x, a)$ equals $\{0, a\}$. This set is always a subset of the kernel of $\varphi_f(x, a)$, which is indeed the necessary and sufficient condition for the existence of l_a. □

A direct consequence of Theorem 1 is that, if F is APN and if ℓ is a linear form such that $\ell(1) = 0$, then the function $F(x)+\ell(F(x))$ is APN. But this function is affine equivalent to F since it is equal to $L \circ F$ where $L(x) = x + \ell(x)$, and the condition that $\ell(1) = 0$ is equivalent to saying that L is a permutation.

We give now an example where Theorem 1 leads to a function which is CCZ-inequivalent to the original function F.

Corollary 1 *Let n be any positive integer. Then the function $x^3 + \mathrm{tr}(x^9)$ is APN on $\mathbb{F}_{2^n}$.*

Proof. We can apply Theorem 1 with $F(x) = x^3$, $\varphi_F(x, a) = a^2x + ax^2$, $f(x) = \mathrm{tr}(x^9)$, $\varphi_f(x, a) = \mathrm{tr}(a^8x + ax^8)$ and $\ell_a(y) = \mathrm{tr}(a^6y + a^3y^2 + a^{-3}y^4)$.

Indeed, we have then

$$\ell_a(\varphi_F(x,a)) = \mathrm{tr}\left(a^6(a^2x+ax^2)+a^3(a^4x^2+a^2x^4)+a^{-3}(a^8x^4+a^4x^8)\right) = \varphi_f(x,a)$$

and if there exists $x \in \mathbb{F}_2^n$ such that $\varphi_F(x,a)=1$ then

$$\ell_a(1) = \mathrm{tr}\left(a^{-3}\right) = \mathrm{tr}\left(\frac{x}{a}+\left(\frac{x}{a}\right)^2\right) = 0.$$

$\square$

Remark 2 The APN property of the function $x^3+\mathrm{tr}(x^9)$ can be proven also with the following arguments due to Dillon [21]. If F is a quadratic function then for any nonzero a and for $\varphi_F(x,y) = F(x+y)+F(x)+F(y)+F(0)$ there exists a linear function L_a such that $\varphi_F(ax,a) = L_a(x+x^2)$. Indeed, if $F(x) = \sum_{i\leq j} c_{i,j}x^{2^i+2^j}$ then $L_a(z) = \sum_{i\leq j} c_{i,j}a^{2^i+2^j}(T_{j-i}(z))^{2^i}$, where $T_k(z) = z+z^2+...+z^{2^{k-1}}$. Thus, F is APN if and only if for any nonzero a and z the equality $L_a(z)=0$ implies $\mathrm{tr}(z)=1$. In the case when $F(x)=x^3+\mathrm{tr}(x^9)$ we have $L_a(z) = a^3z+\mathrm{tr}(a^9T_3(z))$ and if $L_a(z)=0$ for some $z\neq 0$ then $1 = a^3z = \mathrm{tr}(a^9T_3(z))$ which implies $1 = \mathrm{tr}(z^{-3}(z+z^2+z^4)) = \mathrm{tr}(z)$. $\square$

Another class of APN functions, to which the construction of Theorem 1 can be applied, is a class of trinomial APN functions described in [6] (see case 3 in Table 3). However, for this class of functions we were able to construct only functions that are EA-equivalent to the original trinomial. More precisely we have the following proposition.

Proposition 2 *Let m be a positive odd integer, $n=2m$, α a primitive element of $\mathbb{F}_{2^n}$. Then the functions $F,G:\mathbb{F}_{2^n}\to\mathbb{F}_{2^n}$ with*

$$F(x) = x^6+x^{2^m+1}+\alpha^{2^m-1}x^{6\cdot 2^m}$$

and

$$G(x) = F(x)+\mathrm{tr}(\alpha^{2^{m-1}+1}x^3)$$

are EA-equivalent.

Proof. Let

$$t = \frac{\alpha^{2^{m+1}+1}}{\alpha^{2^m-1}+1}$$

and $L(x) = x+\mathrm{tr}(tx)$. We claim that $L(F(x)) = G(x)$.

First note that $t\in\mathbb{F}_{2^m}$, which in particular implies that L is bijective. Furthermore we have

$$
\begin{aligned}
L(F(x)) &= F(x) + \operatorname{tr}(tx^{2^m+1}) + \operatorname{tr}(tx^6) + \operatorname{tr}(t\alpha^{2^m-1}x^{6*2^m}) \\
&= F(x) + 0 + \operatorname{tr}(t^{2^m}x^{3*2^{m+1}}) + \operatorname{tr}(t\alpha^{2^m-1}x^{3*2^{m+1}}) \\
&= F(x) + \operatorname{tr}(t(1+\alpha^{2^m-1})x^{3*2^{m+1}}) \\
&= F(x) + \operatorname{tr}(\alpha^{2^{m+1}+1}x^{3*2^{m+1}}) \\
&= F(x) + \operatorname{tr}\left(\left(\alpha^{2^{m-1}+1}x^3\right)^{2^{m+1}}\right) \\
&= G(x)
\end{aligned}
$$

□

3.1 An algorithmic approach

Below we describe an algorithmic approach to search for functions fulfilling the conditions of Theorem 1 when F is a Gold function. The first step will be to find an explicit description of the linear function l_a used in Theorem 1. Let $F(x) = x^{2^r+1}$ and $f(x) = \operatorname{tr}(x^{2^i+1})$. Then

$$\varphi_F(x,a) = a^{2^r+1}\left(\left(\frac{x}{a}\right) + \left(\frac{x}{a}\right)^{2^r}\right)$$

and

$$\varphi_f(x,a) = \operatorname{tr}\left(a^{2^i+1}\left(\left(\frac{x}{a}\right) + \left(\frac{x}{a}\right)^{2^i}\right)\right).$$

If we define $t = (ir^{-1} - 1) \bmod n$ we get

$$
\begin{aligned}
\varphi_f(x,a) &= \operatorname{tr}\left(a^{2^i+1}\left(\left(\frac{x}{a}\right) + \left(\frac{x}{a}\right)^{2^i}\right)\right) \\
&= \operatorname{tr}\left(a^{2^i+1}\left(\sum_{j=0}^{t}\left[\left(\frac{x}{a}\right) + \left(\frac{x}{a}\right)^{2^r}\right]^{2^{jr}}\right)\right) \\
&= \operatorname{tr}\left(a^{2^i+1}\left(\sum_{j=0}^{t}\left[\frac{\varphi_F(x,a)}{a^{2^r+1}}\right]^{2^{jr}}\right)\right) \\
&= \operatorname{tr}\left(\sum_{j=0}^{t} a^{2^i+1-(2^r+1)2^{jr}}\varphi_F(x,a)^{2^j}\right) \\
&= \operatorname{tr}\left(\left(\sum_{j=0}^{t} a^{2^{i-jr}+2^{-jr}-(2^r+1)}\right)\varphi_F(x)\right).
\end{aligned}
$$

Thus denoting

$$T_i^r(a) = \sum_{j=0}^{t} a^{2^{i-jr}+2^{-jr}-(2^r+1)}$$

we get

$$\varphi_f(x,a) = \operatorname{tr}(T_i^r(a)\varphi_F(x,a)).$$

In general for $g(x) = \sum_i \alpha_i x^{2^i+1}$ we get

$$\varphi_g(x,a) = \operatorname{tr}\left(\left(\sum_i \alpha_i T_i^r(a)\right)\varphi_F(x,a)\right).$$

Following Theorem 1, the condition for $F+g$ to be APN is that, if $\operatorname{tr}(a^{-(2^r+1)}) = 0$ then

$$\operatorname{tr}\left(\sum_i \alpha_i T_i(a)\right) = \sum_i \operatorname{tr}\left(\alpha_i T_i^r(a)\right) = 0.$$

Fixing a base $(b_j)_j$ of $\mathbb{F}_{2^n}$ over $\mathbb{F}_2$ we can consider the set of vectors

$$\left\{\operatorname{tr}(b_j T_i^r(a))_{a\in\mathbb{F}_{2^n},\operatorname{tr}(a^{-3})=0} \mid i,j \in \{0\dots n-1\}\right\}.$$

Given F, finding a quadratic function g such that the conditions of Theorem 1 are fulfilled is equivalent to finding a set of linearly dependent vectors in this set. We computed these vectors and all linear dependent sets up to dimension 15. The only examples in addition to $x^3 + \operatorname{tr}(x^9)$ are listed below.

(1) If n is even, then the function $\operatorname{tr} \circ T_{n/2}^r$ is constant zero. Thus in this case we can always add $\operatorname{tr}(x^{2^{n/2}+1})$. However this function is constant zero.
(2) For $n = 5$ the function $x^5 + \operatorname{tr}(x^3)$ is APN.
(3) For $n = 8$ the function $x^9 + \operatorname{tr}(x^3)$ is APN.

4 CCZ-inequivalence of the new APN function to power mappings

Theorem 2 *The function of Corollary 1 is CCZ-inequivalent to any Gold function on $\mathbb{F}_{2^n}$ if $n \geq 7$ and $n > 2p$ where p is the smallest positive integer different from 1 and 3 and coprime with n.*

Proof. Let $F(x) = x^3 + \operatorname{tr}(x^9)$ and $G(x) = x^{2^r+1}$ be APN functions on $\mathbb{F}_{2^n}$, $n \geq 7$, $r \leq (n-1)/2$.

Suppose the functions F and G are EA-equivalent. Then, there exist affine permutations L_1, L_2 and an affine function L' such that

$$L_1(x^3) + L_1(\operatorname{tr}(x^9)) = (L_2(x))^{2^t+1} + L'(x).$$

That is,

$$L_1(x^3) + L_1(1)\operatorname{tr}(x^9) = (L_2(x))^{2^t+1} + L'(x).$$

Since the functions are quadratic, we can assume without loss of generality that L_1 and L_2 are linear: $L_1(x) = \sum_{m\in\mathbb{Z}/n\mathbb{Z}} b_m x^{2^m}$, $L_2(x) = \sum_{p\in\mathbb{Z}/n\mathbb{Z}} c_p x^{2^p}$.

Then we get

$$\sum_{m\in\mathbb{Z}/n\mathbb{Z}} b_m x^{3\cdot 2^m} + \mathrm{tr}(x^9)\sum_{m\in\mathbb{Z}/n\mathbb{Z}} b_m = \sum_{l,p\in\mathbb{Z}/n\mathbb{Z}} c_p c_l^{2^t} x^{2^{l+t}+2^p} + L'(x). \tag{1}$$

On the left hand side of the identity (1) we have only items of the type $x^{3\cdot 2^m}$, $x^{9\cdot 2^m}$, with some coefficients. Therefore this must be true also for the right hand side of the identity.

Let p be the smallest positive integer different from 1 and 3 such that $\gcd(n,p) = 1$ (for example, if n is odd then $p=2$, if n is even and not divisible by 5 then $p=5$). If $n>2p$ then 2^p+1 is not in the same cyclotomic coset with 3 or 9. Therefore, the items of the type $x^{2^k(2^p+1)}$ must cancel. That is, for any k

$$c_k c_{k-t+p}^{2^t} = c_{k+p} c_{k-t}^{2^t}. \tag{2}$$

Since $n \geq 7$ then 3 and 9 are in different cyclotomic cosets and we have for any k

$$L_1(1) = c_k c_{k-t+3}^{2^t} + c_{k+3} c_{k-t}^{2^t}.$$

If $L_1(1) \neq 0$ then

$$c_k c_{k-t+3}^{2^t} \neq c_{k+3} c_{k-t}^{2^t}. \tag{3}$$

If $c_k \neq 0$ for all k then from (2) and (3) we get

$$c_k c_{k-t}^{-2^t} = c_{k+p} c_{k-t+p}^{-2^t}, \tag{4}$$

$$c_k c_{k-t}^{-2^t} \neq c_{k+3} c_{k-t+3}^{-2^t}. \tag{5}$$

Since $\gcd(n,p)=1$ and from (4)

$$c_k c_{k-t}^{-2^t} = c_m c_{m-t}^{-2^t}$$

for any m. It contradicts (5). Thus, $c_k = 0$ for some k. Then from (2) and (3) we get that $c_{k+p} = 0$. Repeating this step for $c_{k+p}, c_{k+2p}, \ldots$ we get $c_{k+ps} = 0$ and since $\gcd(n,p) = 1$ then $c_k = 0$ for all k. A contradiction. If $L_1(1) = 0$ then the equation $L(x) = 0$ has at least 2 solutions $0,1$ and therefore L_1 is not a permutation. Thus, F and G are EA-inequivalent.

Suppose that $F(x)$ and $G(x)$ are CCZ-equivalent, that is, there exists an affine automorphism $L = (L_1, L_2)$ of $\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ such that $y = F(x) \Leftrightarrow L_2(x,y) = G(L_1(x,y))$ and $L_1(x, F(x))$ is a permutation. This implies then $L_2(x,F(x)) = G(L_1(x,F(x)))$. Writing $L_1(x,y) = L(x) + L'(y)$ and $L_2(x,y) = L''(x) + L'''(y)$ gives

$$L''(x) + L'''(F(x)) = G\left(L(x) + L'(F(x))\right). \tag{6}$$

We can write

$$
\begin{aligned}
L(x) &= b + \sum_{m\in\mathbb{Z}/n\mathbb{Z}} b_m x^{2^m},\\
L'(x) &= b' + \sum_{m\in\mathbb{Z}/n\mathbb{Z}} b'_m x^{2^m},\\
L''(x) &= b'' + \sum_{m\in\mathbb{Z}/n\mathbb{Z}} b''_m x^{2^m},\\
L'''(x) &= b''' + \sum_{m\in\mathbb{Z}/n\mathbb{Z}} b'''_m x^{2^m},\\
b + b' &= c.
\end{aligned}
$$

Then we get

$$
\begin{aligned}
&G(L(x)+L'(F(x))) = \Big(L(x)+L'(x^3+\mathrm{tr}(x^9)\Big)\Big(L(x)+L'(x^3+\mathrm{tr}(x^9)\Big)^{2^r}\\
&= \left(c + \sum_{m\in\mathbb{Z}/n\mathbb{Z}} b_m x^{2^m} + \sum_{m\in\mathbb{Z}/n\mathbb{Z}} b'_m x^{2^m(2+1)} + \mathrm{tr}(x^9)\sum_{m\in\mathbb{Z}/n\mathbb{Z}} b'_m\right)\\
&\times\left(c^{2^r} + \sum_{m\in\mathbb{Z}/n\mathbb{Z}} b_m^{2^r} x^{2^{m+r}} + \sum_{m\in\mathbb{Z}/n\mathbb{Z}} b'^{2^r}_m x^{2^{m+r}(2+1)} + \mathrm{tr}(x^9)\sum_{m\in\mathbb{Z}/n\mathbb{Z}} b'^{2^r}_m\right)\\
&= Q(x) + [\sum_{m,k\in\mathbb{Z}/n\mathbb{Z}} b_m b'^{2^r}_k x^{2^m+2^{k+r}+2^{k+r+1}}\\
&+ L'(1)^{2^r}\sum_{m,k\in\mathbb{Z}/n\mathbb{Z}} b_m x^{2^m+2^{k+3}+2^k} + \sum_{m,k\in\mathbb{Z}/n\mathbb{Z}} b'_m b^{2^r}_k x^{2^{m+1}+2^m+2^{k+r}}\\
&+ L'(1)\sum_{m,k\in\mathbb{Z}/n\mathbb{Z}} b^{2^r}_m x^{2^{m+r}+2^{k+3}+2^k)}]\\
&+ [\sum_{m,k\in\mathbb{Z}/n\mathbb{Z}} b'_m b'^{2^r}_k x^{2^{m+1}+2^m+2^{k+r+1}+2^{k+r}}\\
&+ L'(1)^{2^r}\sum_{m,k\in\mathbb{Z}/n\mathbb{Z}} b'_m x^{2^{m+1}+2^m+2^{k+3}+2^k}\\
&+ L'(1)\sum_{m,k\in\mathbb{Z}/n\mathbb{Z}} b'^{2^r}_m x^{2^{m+r+1}+2^{m+r}+2^{k+3}+2^k}],
\end{aligned}
$$

where $Q(x)$ is a quadratic polynomial. Obviously, all terms in the expression above whose exponents have 2-weight strictly greater than 2 must cancel. Since F and G are EA-inequivalent then L' is not a constant. Then there exists $m \in \mathbb{Z}/n\mathbb{Z}$ such that $b'_m \neq 0$.

Let $L'(1) \neq 0$. Since the items with the exponet $2^{m+1} + 2^m + 2^{m+2} + 2^{m+5}$ have to vanish then we get $L'(1)^{2^r} b'_m = L'(1)b'^{2^r}_{m-r}$ and since $L'(1) \neq 0, b'_m \neq 0$ and r is coprime with n then $b'_k \neq 0$ and $b'_k b'^{-2^r}_{k-r} = L'(1)^{1-2^r}$ for all k. Now we can deduce that $b'_{k+r} = L'(1)^{1-2^r} b'^{2^r}_k$ for all k. Then, introducing μ such that $L'(1)^{1-2^r} = \mu^{2^r-1}$, we deduce that $\mu b'_{k+r} = (\mu b'_k)^{2^r}$ for all k and then that $\mu b'_{k+1} = (\mu b'_k)^2$ (using that $\gcd(r, n) = 1$) and then $\mu b'_k = (\mu b'_0)^{2^k}$. This means

that $\mu L'(x) = \mu b' + \mathrm{tr}(\mu b'_0 x)$. It implies that all nonquadratic items in the last bracket vanish and $L'(x) = d + \mathrm{tr}(d'x)$ for some d, d'.
The function L is not 0 because L' is not a permutation, then $b_m \neq 0$ for some m. Since the items with the exponent $2^m + 2^{m+2} + 2^{m+5}$ have to vanish then $L'(1)^{2^r} b_m = L'(1) b_{m-r}^{2^r}$. Like above we get $L(x) = d + \mathrm{tr}(d'x)$. Thus, $L_1(x, F(x)) = d'' + \mathrm{tr}(F'(x))$ for some d'' and $F'(x)$ and $L_1(x, F(x))$ is not a permutation. A contradiction.

Let $L'(1) = 0$ and $r \neq 1$. Then $2^{m+1} + 2^m + 2^{m+r+1} + 2^{m+r}$ has 2-weight 4 and since the items with this exponent should cancel then we get $b'^{2^r+1}_m = b'_{m+r} b'^{2^r}_{m-r}$. Since $b'_m \neq 0$ then $b'_{m+r}, b'_{m-r} \neq 0$ and $b'_m b'^{-2^r}_{m-r} = b'_{m+r} b'^{-2^r}_m$. Since $\gcd(n, r) = 1$ then $b'_k \neq 0$, $b'_k b'^{-2^r}_{k-r} = b'_m b'^{-2^r}_{m-r}$ for all k and this implies $L'(x) = d + \mathrm{tr}(d'x)$ for some d, d'. Since $L_1(x, F(x))$ is a permutation then $L \neq 0$ and $b_m \neq 0$ for some m. The items with the exponent $2^m + 2^{m+r} + 2^{m+r+1}$ should vanish. Therefore, $b_m b'^{2^r}_m = b'_{m+r} b^{2^r}_{m-r}$ and $b_m b^{-2^r}_{m-r} = b'_{m+r} b'^{-2^r}_m$. As above it leads to the equality $L(x) = d + \mathrm{tr}(d'x)$ which is in contradiction with $L_1(x, F(x))$ being a permutation.

Let $L'(1) = 0$ and $r = 1$. Since $L'(1) = 0$ and $b'_m \neq 0$ then there exists t such that $b'_{m+t} \neq 0$. If $t \neq -1, -2$ then $2^{m+1} + 2^m + 2^{m+t+2} + 2^{m+t+1}$ has 2-weight 4 and we get $b'_m b'^{2^r}_{m+t} = b'_{m+t+1} b'^{2^r}_{m-1}$ and $b'_m b'^{-2^r}_{m-1} = b'_{m+t+1} b'^{-2^r}_{m+t}$. Therefore, $L'(x) = d + \mathrm{tr}(d'x)$ for some d, d'. If $t \neq 1, 2$ then $2^{m+t+1} + 2^{m+t} + 2^{m+2} + 2^{m+1}$ has 2-weight 4 and we get $b'_{m+t} b'^{2^r}_m = b'_{m+1} b'^{2^r}_{m+t-1}$ and again $L'(x) = d + \mathrm{tr}(d'x)$ for some d, d'. Thus, $L \neq 0$ and then $b_m \neq 0$ for some m. Since the items with the exponent $2^m + 2^{m+2} + 2^{m+3}$ cancel then $b_m b'^{2^r}_{m+1} = b'_{m+2} b^{2^r}_{m-1}$ and $b_m b^{-2^r}_{m-1} = b'_{m+2} b'^{-2^r}_{m+1}$. This implies $L(x) = d + \mathrm{tr}(d'x)$ and, thus, $L_1(x, F(x))$ is not a permutation. Therefore, F and G are not CCZ-equivalent. □

Corollary 2 *The function of Corollary 1 is EA-inequivalent to any power function on* $\mathbb{F}_{2^n}$ *if* $n \geq 7$ *and* $n > 2p$*, where* p *is the smallest positive integer different from* 1 *and* 3 *and coprime with* n*.*

Proof. The function $F(x) = x^3 + \mathrm{tr}(x^9)$ is quadratic APN and by Theorem 2 it is EA-inequivalent to any quadratic power function. Since the algebraic degree is EA-invariant then F is EA-inequivalent to any power mapping. □

Dobbertin and inverse APN functions have unique Walsh spectra (except the case $n = 3$ when the inverse function is EA-equivalent to x^3) which are different from the Walsh spectra of quadratic APN functions (see [14,17,35]). Since the extended Walsh spectrum of a function is invariant under CCZ-equivalence then we can make the following conclusion.

Proposition 3 *The function of Corollary 1 is CCZ-inequivalent to the inverse and Dobbertin APN functions for* $n \geq 7$*.*

For $n = 7$ the Δ-rank of the function $F(x) = x^3 + \mathrm{tr}(x^9)$ equals 212 and differs from the Δ-ranks of the Kasami functions x^{13} and x^{23} (which equal 338 and 436, respectively). Thus, for $n = 7$ the function F is CCZ-inequivalent to Kasami functions, and by Theorem 2 to the Gold functions. Since in this field the Welch and Niho cases coincide with the Kasami cases then F is CCZ-inequivalent to all power maps on $\mathbb{F}_{2^7}$.

Corollary 3 *The function $F(x) = x^3 + \mathrm{tr}(x^9)$ is CCZ-inequivalent to power functions on $\mathbb{F}_{2^7}$.*

Conjecture 1 *The function $F(x) = x^3 + \mathrm{tr}(x^9)$ is CCZ-inequivalent to any power function on $\mathbb{F}_{2^n}$ if $n \geq 7$ and $n > 2p$, where p is the smallest positive integer different from 1 and 3 and coprime with n.*

Applying CCZ-equivalence to the quadratic APN function $F(x) = x^3+\mathrm{tr}(x^9)$, it is possible to construct classes of *nonquadratic* APN mappings which are CCZ-inequivalent to power functions.

Proposition 4 *Let $F : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, $F(x) = x^3 + \mathrm{tr}(x^9)$ then the following functions are CCZ-equivalent to F*

1) *for n odd the function with algebraic degree 3*

$$x^3 + \mathrm{tr}(x^9) + (x^2 + x)\,\mathrm{tr}(x^3 + x^9);$$

2) *for n even the function with algebraic degree 3*

$$x^3 + \mathrm{tr}(x^9) + (x^2 + x + 1)\,\mathrm{tr}(x^3);$$

3) *for n divisible by 6 the function with algebraic degree 4*

$$\begin{aligned}&\left(x + \mathrm{tr}_{n/3}(x^6 + x^{12}) + \mathrm{tr}(x)\,\mathrm{tr}_{n/3}(x^3 + x^{12})\right)^3 \\ &+ \mathrm{tr}\left(\left(x + \mathrm{tr}_{n/3}(x^6 + x^{12}) + \mathrm{tr}(x)\,\mathrm{tr}_{n/3}(x^3 + x^{12})\right)^9\right);\end{aligned}$$

4) *for n odd and divisible by 3 the function with algebraic degree 4*

$$\left(x^{\frac{1}{3}} + tr_{n/3}(x + x^4)\right)^{-1} + \mathrm{tr}\left(\left(\left(x^{\frac{1}{3}} + tr_{n/3}(x + x^4)\right)^{-1}\right)^3\right).$$

Proof. The proof is the same as for the cases from [5,11,12] (use the affine permutation $\mathcal{L}(x, y) = (x + \mathrm{tr}(y), y)$ for the first two cases, $\mathcal{L}(x, y) = (x + \mathrm{tr}_{n/3}(y^2 + y^4), y)$ for the third case and $\mathcal{L}(x, y) = (x + \mathrm{tr}_{n/3}(y + y^4), y)$ for the fourth case). □

Remark 3 Note that the second, the third and the fourth APN functions in Proposition 4 can be obtained from respectively the first, the second and the third functions of Table 2 by adding $\mathrm{tr}(G(x))$ for some G. It means that the construction $F(x) + \mathrm{tr}(G(x))$, where F is APN and G is arbitrary, actually gives new APN functions even if F and G are not quadratic. $\square$

5 Further quadratic APN constructions?

There is a straightforward generalization of Theorem 1:

Theorem 3 *Let F be a quadratic APN function from $\mathbb{F}_{2^n}$ to itself, let f be a quadratic function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$ where m is a divisor of n, and*

$$\varphi_F(x,a) = F(x) + F(x+a) + F(a) + F(0),$$

$$\varphi_f(x,a) = f(x) + f(x+a) + f(a) + f(0).$$

Then the function $F(x) + f(x)$ is APN if for every nonzero $a \in \mathbb{F}_{2^n}$ there exists a linear function ℓ_a from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$ which satisfies the conditions

1) $\varphi_f(x,a) = \ell_a(\varphi_F(x,a))$,
2) *for every $u \in \mathbb{F}_{2^m}^*$, if $\varphi_F(x,a) = u$ for some $x \in \mathbb{F}_{2^n}$ then $\ell_a(u) \neq u$.*

We could find an application of Theorem 3:

Corollary 4 *Let $n = 2m$ where m is an even positive integer. Let us denote by $\mathrm{tr}_{n/m}$ the trace function from $\mathbb{F}_{2^n}$ to $\mathbb{F}_{2^m}$: $\mathrm{tr}_{n/m}(x) = x + x^{2^m}$. The functions $F(x) = x^3 + \mathrm{tr}_{n/m}(x^{2^m+2}) = x^3 + x^{2^m+2} + x^{2^{m+1}+1}$ and $F'(x) = x^3 + (\mathrm{tr}_{n/m}(x))^3$ are APN.*

But unfortunately, these functions are EA-equivalent to power functions. Indeed, let G be the Gold function $G(x) = x^{2^{m-1}+1}$. Let γ be any element of $\mathbb{F}_4 \setminus \mathbb{F}_2$ and L_1, L_2 be the linear mappings $L_1(x) = \gamma^2 x^{2^{m+1}} + \gamma\, x^2$, $L_2(x) = \gamma\, x^{2^m} + \gamma^2 x$. Then $\mathcal{L} = (L_1, L_2)$ is an isomorphism since the system

$$\begin{cases} \gamma^2 x^{2^{m+1}} + \gamma\, x^2 = 0 \\ \gamma\, x^{2^m} + \gamma^2 x = 0 \end{cases}$$

clearly admits 0 as the only solution. And since $\gamma^{2^m} = \gamma$, $\gamma^{2^{m-1}} = \gamma^2$ and $\gamma + \gamma^2 = 1$, we have

$$\begin{aligned} G \circ L_1(x) &= \left(\gamma^2 x^{2^{m+1}} + \gamma\, x^2\right)^{2^{m-1}+1} = \left(\gamma\, x + \gamma^2 x^{2^m}\right)\left(\gamma^2 x^{2^{m+1}} + \gamma\, x^2\right) \\ &= \gamma\, \left(x^3 + x^{2^m+2} + x^{2^{m+1}+1}\right)^{2^m} + \gamma^2 \left(x^3 + x^{2^m+2} + x^{2^{m+1}+1}\right) \\ &= L_2 \circ F(x). \end{aligned}$$

Acknowledgments

We would like to thank John Dillon for nice observations, and Willem De Graaf and Nobuo Nakagawa for useful discussions. The research of the first author was partly supported by a postdoctoral fellowship of MIUR-Italy via PRIN 2006, also by Lavoro eseguito con il contributo della Provincia autonoma di Trento. The research of the third author was supported by a DAAD postdoctoral fellowship.

References

[1] T. Berger, A. Canteaut, P. Charpin and Y. Laigle-Chapuy. On almost perfect nonlinear functions over F_2^n. *IEEE Trans. Inform. Theory*, vol. 52, no. 9, Sept. 2006.

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

[3] E. Biham and A. Shamir. Differential Cryptanalysis of DES-like Cryptosystems. *Journal of Cryptology*, vol. 4, No.1, pp. 3-72, 1991.

[4] M. Brinkman and G. Leander. On the classification of APN functions up to dimension five. *Proceedings of the International Workshop on Coding and Cryptography, WCC 2007,* dedicated to the memory of Hans Dobbertin, pp. 39-48, Versailles, France, Apr. 2007.

[5] L. Budaghyan. The simplest method for constructing APN polynomials EA-inequivalent to power functions. *Proceedings of the International Workshop on the Arithmetic of Finite Fields, WAIFI 2007*, LNCS 4547, pp. 177-188, Madrid, Spain, June 2007.

[6] L. Budaghyan and C. Carlet. Classes of Quadratic APN Trinomials and Hexanomials and Related Structures. Submitted, available at http://eprint.iacr.org/2007/098

[7] L. Budaghyan, C. Carlet, G. Leander. Another class of quadratic APN binomials over $\mathbb{F}_{2^n}$: the case n divisible by 4. *Proceedings of the International Workshop on Coding and Cryptography, WCC 2007,* dedicated to the memory of Hans Dobbertin, pp. 49-58, Versailles, France, Apr. 2007.

[8] L. Budaghyan, C. Carlet, G. Leander. A class of quadratic APN binomials inequivalent to power functions. Submitted, available at http://eprint.iacr.org/2006/445

[9] L. Budaghyan, C. Carlet, P. Felke, G. Leander. An infinite class of quadratic APN functions which are not equivalent to power mappings. *Proceedings of*

the IEEE International Symposium on Information Theory 2006, Seattle, USA, Jul. 2006.

[10] L. Budaghyan and A. Pott. On Differential Uniformity and Nonlinearity of Functions. Submitted, 2006.

[11] L. Budaghyan, C. Carlet, A. Pott. New Classes of Almost Bent and Almost Perfect Nonlinear Functions. *IEEE Trans. Inform. Theory*, vol. 52, no. 3, pp. 1141-1152, March 2006.

[12] L. Budaghyan, C. Carlet, A. Pott. New Constructions of Almost Bent and Almost Perfect Nonlinear Functions. *Proceedings of the Workshop on Coding and Cryptography 2005*, P. Charpin and Ø. Ytrehus eds, pp. 306-315, 2005.

[13] A. Canteaut, P. Charpin and H. Dobbertin. A new characterization of almost bent functions. *Fast Software Encryption 99, LNCS* 1636, L. Knudsen edt, pp. 186-200. Springer-Verlag, 1999.

[14] A. Canteaut, P. Charpin and H. Dobbertin. Binary m-sequences with three-valued crosscorrelation: A proof of Welch's conjecture. *IEEE Trans. Inform. Theory*, 46 (1), pp. 4-8, 2000.

[15] A. Canteaut, P. Charpin, H. Dobbertin. Weight divisibility of cyclic codes, highly nonlinear functions on $\mathbb{F}_{2^m}$, and crosscorrelation of maximum-length sequences. *SIAM Journal on Discrete Mathematics*, 13(1), pp. 105-138, 2000.

[16] C. Carlet. Vectorial (multi-output) Boolean Functions for Cryptography. Chapter of the monography *Boolean Methods and Models*, Y. Crama and P. Hammer eds, Cambridge University Press, to appear soon. Preliminary version available at http://www-rocq.inria.fr/codes/Claude.Carlet/pubs.html

[17] C. Carlet, P. Charpin and V. Zinoviev. Codes, bent functions and permutations suitable for DES-like cryptosystems. *Designs, Codes and Cryptography*, 15(2), pp. 125-156, 1998.

[18] F. Chabaud and S. Vaudenay. Links between differential and linear cryptanalysis, *Advances in Cryptology -EUROCRYPT'94, LNCS*, Springer-Verlag, New York, 950, pp. 356-365, 1995.

[19] J. Daemen and V. Rijmen. AES proposal: Rijndael. http://csrc.nist.gov/encryption/aes/rijndael/Rijndael.pdf, 1999.

[20] J. F. Dillon. APN Polynomials and Related Codes. *Polynomials over Finite Fields and Applications*, Banff International Research Station, Nov. 2006.

[21] J. F. Dillon. Private communication, Feb. 2007.

[22] H. Dobbertin. One-to-One Highly Nonlinear Power Functions on $GF(2^n)$. *Appl. Algebra Eng. Commun. Comput.* 9 (2), pp. 139-152, 1998.

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

[24] H. Dobbertin. Almost perfect nonlinear power functions over $GF(2^n)$: the Welch case. *IEEE Trans. Inform. Theory*, 45, pp. 1271-1275, 1999.

[25] H. Dobbertin. Almost perfect nonlinear power functions over $GF(2^n)$: a new case for n divisible by 5. D. Jungnickel and H. Niederreiter eds. *Proceedings of Finite Fields and Applications FQ5*, Augsburg, Germany, Springer, pp. 113-121, 2000.

[26] Y. Edel, G. Kyureghyan and A. Pott. A new APN function which is not equivalent to a power mapping. *IEEE Trans. Inform. Theory*, vol. 52, no. 2, pp. 744-747, Feb. 2006.

[27] R. Gold. Maximal recursive sequences with 3-valued recursive crosscorrelation functions. *IEEE Trans. Inform. Theory*, 14, pp. 154-156, 1968.

[28] H. Hollmann and Q. Xiang. A proof of the Welch and Niho conjectures on crosscorrelations of binary m-sequences. *Finite Fields and Their Applications 7*, pp. 253-286, 2001.

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

[30] T. Kasami. The weight enumerators for several classes of subcodes of the second order binary Reed-Muller codes. *Inform. and Control*, 18, pp. 369-394, 1971.

[31] G. Lachaud and J. Wolfmann. The Weights of the Orthogonals of the Extended Quadratic Binary Goppa Codes. *IEEE Trans. Inform. Theory*, vol. 36, pp. 686-692, 1990.

[32] M. Matsui. Linear cryptanalysis method for DES cipher. *Advances in Cryptology-EUROCRYPT'93, LNCS*, Springer-Verlag, pp. 386-397, 1994.

[33] N. Nakagawa and S. Yoshiara. A construction of differentially 4-uniform functions from commutative semifields of characteristic 2. *Proceedings of the International Workshop on the Arithmetic of Finite Fields, WAIFI 2007*, LNCS 4547, pp. 134-146, Madrid, Spain, June 2007.

[34] K. Nyberg. Differentially uniform mappings for cryptography, *Advances in Cryptography, EUROCRYPT'93, LNCS*, Springer-Verlag, New York, 765, pp. 55-64, 1994.

[35] K. Nyberg. S-boxes and Round Functions with Controllable Linearity and Differential Uniformity. *Proceedings of Fast Software Encryption 1994, LNCS* 1008, pp. 111-130, 1995.

[36] V. Sidelnikov. On mutual correlation of sequences. *Soviet Math. Dokl.*, 12, pp. 197-201, 1971.