A new almost perfect nonlinear function which is not quadratic

Yves Edel[*] Alexander Pott[†]

July 18, 2008

Abstract

Following an example in [13], we show how to change one coordinate function of an almost perfect nonlinear (APN) function in order to obtain new examples. It turns out that this is a very powerful method to construct new APN functions. In particular, we show that the approach can be used to construct "non-quadratic" APN functions. This new example is in remarkable contrast to all recently constructed functions which have all been quadratic.[1]

1 Preliminaries

In this paper, we consider functions $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ with "good" differential and linear properties. Motivated by applications in cryptography, a lot of research has been done to construct functions which are "as nonlinear as possible". We discuss two possibilities to define nonlinearity: One approach uses differential properties of linear functions, the other measures the "distance" to linear functions.

Let us begin with the differential properties. Given $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$, we define

$$\Delta_F(a,b) := |\{x \ : \ F(x+a) - F(x) = b\}|.$$

We have $\Delta_F(0,0) = 2^n$, and $\Delta_F(0,b) = 0$ if $b \neq 0$. Since we are working in fields of characteristic 2, we may replace the "$-$" by $+$ and write $F(x+a)+F(x)$ instead of $F(x-a)-F(x)$. We say that F is **almost perfect nonlinear (APN)** if $\Delta_F(a,b) \in \{0,2\}$ for all $a,b \in \mathbb{F}_2^n$, $a \neq 0$. Note that $\Delta_F(a,b) \in \{0,2^n\}$ if F is linear, hence the condition $\Delta_F(a,b) \in \{0,2\}$ identifies functions which are quite different from linear mappings. Since we are working in characteristic 2, it is impossible that $\Delta_F(a,b) = 1$ for some a,b, since the values $\Delta_F(a,b)$ must be even: If x is a solution of $F(x+a) - F(x) = b$, then $x+a$, too. In the case of odd characteristic, functions $F : \mathbb{F}_q^n \to \mathbb{F}_q^n$ with $\Delta_F(a,b) = 1$ for all $a \neq 0$ do exist, and they are called **perfect nonlinear** or **planar**. In the last few years, many new APN functions have been constructed. The first example of a non-power mapping has been described in [26]. Infinite series are contained in [5, 10, 11, 12, 13, 16, 17]. Also some new planar functions have been found, see [15, 22, 36].

There may be a possibility for a unified treatment of (some of) these constructions in the even and odd characteristic case. In particular, we suggest to look more carefully at the underlying *design* of an APN function, similar to the designs corresponding to planar functions, which are projective planes, see [29].

[*] Department of Pure Mathematics and Computer Algebra, Ghent University, Krijgslaan 281, S22, B-9000 Ghent, Belgium. The research is supported by the Interuniversitary Attraction Poles Programme-Belgian State-Belgian Science Policy: project P6/26-Bcrypt.

[†] Department of Mathematics, Otto-von-Guericke-University Magdeburg, D-39016 Magdeburg, Germany

[1] An equivalent function has been found independently by Brinkmann and Leander [7]. However, they claimed that their function is CCZ equivalent to a quadratic one. In this paper we give several reasons why this new function is not equivalent to a quadratic one

Another approach is to measure the *distance* between linear functions $h : \mathbb{F}_2^n \to \mathbb{F}_2$ and the coordinate functions $F_g : \mathbb{F}_2^n \to \mathbb{F}_2$: They are defined via $F_g(x) := g(F(x))$ where g is a nonzero linear function $\mathbb{F}_2^n \to \mathbb{F}_2$. We denote the set of all linear functions $f : \mathbb{F}_2^n \to \mathbb{F}_2$ by $\widehat{\mathbb{F}_2^n}$. The **Hamming distance** $d_H(f,g)$ between two Boolean functions $f, g : \mathbb{F}_2^n \to \mathbb{F}_2$ is simply the number of x such that $f(x) \neq g(x)$.

We say that a function F is *highly nonlinear* if

$$\min_{f,g \in \widehat{\mathbb{F}_2^n}\, g \neq 0} (d_H(f, F_g), d_H(f+1, F_g)) \tag{1}$$

is large, i.e. the coordinate functions $g \circ F = F_g$ of F are as different as possible from all *affine linear functions* f and $f+1$, where $f \in \widehat{\mathbb{F}_2^n}$.

Instead of investigating $d_H(f, F_g)$ and $d_H(f+1, F_g)$, we may equivalently investigate

$$\mathcal{W}_F(f,g) = \sum_{x \in \mathbb{F}_2^n} (-1)^{(g \circ F)(x) + f(x)}.$$

We have

$$2^n - 2d_H(f, F_g) = \mathcal{W}_F(f,g) \quad \text{and} \quad 2^n - 2d_H(f+1, F_g) = -\mathcal{W}_F(f,g).$$

This shows that the distances come in pairs d_1 and d_2 with $d_1 + d_2 = 2^n$. Instead of maximizing the minimum of the $d_H(f, F_g)$, $d_H(f+1, F_g)$ with $g \neq 0$, we may equivalently minimize the maximum of $|\mathcal{W}(f,g)|$, $g \neq 0$.

The Walsh coefficients are basically the weights of the following code of length 2^n: Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be any function. Define a matrix $C_F \in \mathbb{F}_2^{(2n, 2^n)}$ as follows: The columns are the vectors $\begin{pmatrix} x \\ F(x) \end{pmatrix}$, $x \in \mathbb{F}_2^n$. Then the rows of the matrix

$$C_F = \begin{pmatrix} \cdots & x & \cdots \\ \cdots & F(x) & \cdots \end{pmatrix}_{x \in \mathbb{F}_2^n}$$

generate a code $\mathcal{C}_F$ whose codewords are the vectors

$$v(f,g) = (f(x) + (g \circ F)(x))_{x \in \mathbb{F}_2^n},$$

where f and g are linear functions $\mathbb{F}_2^n \to \mathbb{F}_2$. It is easy to see that the Hamming weight $d_H(v(f,g))$ of this codeword is related to the Walsh coefficient $\mathcal{W}(f,g)$ as follows:

$$2^n - 2d_H(v(f,g)) = \mathcal{W}(f,g).$$

If the code $\mathcal{C}_F$ does not contain the vector $(1, \ldots, 1)$, we may add this vector as a row to C_F. The vector space generated by the rows of this extended matrix is called the **extended code** $\mathcal{C}_F^{\text{ext}}$ associated with the function F. This construction means that we add the vectors $w := v(f+1, g)$ to the code $\mathcal{C}_F$. If $u := v(f,g)$, we have $d_H(u) + d_H(w) = 2^n$ and therefore

$$2^n - 2d_H(u) = -(2^n - 2d_H(w)),$$

which gives rise to the Walsh coefficients $\pm\mathcal{W}(f,g)$. We note that the vector $(1, \ldots 1)$ is not contained in C_F if F is APN, see [9, 19], for instance.

The multiset of values $\mathcal{W}_F(f,g)$ for all linear functions f, g is called the **Walsh spectrum** of F.

Usually, the Walsh spectrum is defined in terms of the trace function of a finite field. This "finite field definition" is completely equivalent to ours. We have used the vector space definition in order to emphasize that the Walsh spectrum (or the Walsh transformation) is just a property of the additive group of $\mathbb{F}_2^n$. If we identify $\mathbb{F}_2^n$ with the additive group of the finite field $\mathbb{F}_{2^n}$, then the linear mappings $f : \mathbb{F}_2^n \to \mathbb{F}_2$ are just the mappings f_α defined via $x \mapsto \mathsf{tr}(\alpha x)$, where tr is the usual trace function $\mathsf{tr}(x) := \sum_{i=0}^{n-1} x^{2^i}$. We have $f_\alpha \neq f_\beta$ for $\alpha \neq \beta$, and we put

$$\mathcal{W}_F(f_\alpha, f_\beta) =: \mathcal{W}_F(\alpha, \beta).$$

We have $\mathcal{W}_F(\alpha, 0) = 0$ if $\alpha \neq 0$ and $\mathcal{W}_F(0,0) = 2^n$.

It is well known that there are $\alpha \in \mathbb{F}_{2^n}$ and $\beta \in \mathbb{F}_{2^n} \setminus \{0\}$ such that

$$|\mathcal{W}_F(\alpha, \beta)| \geq 2^{(n+1)/2},$$

see [28], for instance. If n is odd, there are functions F with

$$|\mathcal{W}_F(\alpha, \beta)| \leq 2^{(n+1)/2}$$

for all $\beta \neq 0$. Functions $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ with $|\mathcal{W}_F(\alpha, \beta)| \leq 2^{(n+1)/2}$ for all $\beta \neq 0$ are called **almost bent (AB)**. Note that AB functions may exist only if n is odd. It is well known that any almost bent function is also APN (see [35]), but not vice versa, see the comments about Table 1. However, any quadratic APN (see Definition 2) in $\mathbb{F}_2^n$ must be AB, see [19]. If a function F with $F(0) = 0$ is AB, its Walsh spectrum is completely known:

$$\{*\quad 2^n\ [1],\ 0\ [(2^{n-1}+1)(2^n-1)],\ \pm 2^{(n+1)/2}\ [(2^n-1)(2^{n-2} \pm 2^{(n-3)/2})]\quad *\} \tag{2}$$

(the values in brackets [ ] denote the multiplicities of the Walsh coefficients, and the notion $\{*\quad *\}$ indicates *multisets*). Similarly, the Walsh spectra of the Gold APN's (see Table 1) with n even are completely known, too, see [20], for instance:

$$\begin{aligned}\{*\quad 2^n\ [1],\ 0\ [(2^n-1)(2^{n-2}+1)],\ \pm 2^{(n+2)/2}\ [\tfrac{1}{3}(2^n-1)(2^{n-3} \pm 2^{(n-4)/2})],\\ \pm 2^{n/2}\ [\tfrac{2}{3}(2^n-1)(2^{n-1} \pm 2^{(n-2)/2})]\quad *\}.\end{aligned} \tag{3}$$

We say that an APN function with spectrum (2) (if n is odd) or (3) (if n is even) has the **classical Walsh spectrum**. We want to stress that just the APN property does not determine the Walsh spectrum. APN functions may have quite different Walsh spectra. The reader can find the classical spectra in [20], for instance. If $F(0) \neq 0$, the distribution of the spectral values may be different, however the distribution of the absolute values will not change, see the comments following Proposition 1.

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

	Exponents d	Conditions	Proven in
Gold functions	$2^i + 1$	$\gcd(i, n) = 1$	[27, 35]
Kasami functions	$2^{2i} - 2^i + 1$	$\gcd(i, n) = 1$	[30, 31]
Welch function	$2^t + 3$	$n = 2t + 1$	[24]
Niho function	$2^t + 2^{\frac{t}{2}} - 1$, t even $2^t + 2^{\frac{3t+1}{2}} - 1$, t odd	$n = 2t + 1$	[23]
Inverse function	$2^{2t} - 1$	$n = 2t + 1$	[35]
Dobbertin function	$2^{4t} + 2^{3t} + 2^{2t} + 2^t - 1$	$n = 5t$	[25]

In Table 1, we list all known power APN mappings on $\mathbb{F}_{2^n}$ which are known so far: The Welsh and Niho functions are also AB, the Gold and Kasami functions are AB if n is odd. It is known that the inverse function and the Dobbertin function are not AB: The complete Walsh spectrum of the inverse function has been determined in [33], those of the Dobbertin function in [18], and these are not the spectra as defined in (3) and (2).

There are two questions which arise quite naturally:

Question 1. *(1.) Is the list in Table 1 complete?*
(2.) Are all these examples "different"?

We will discuss these questions in the next section.

2 Equivalence of APN mappings

Let us begin with the second part of Question 1. In order to describe whether two functions F and H are equivalent, we introduce group ring notation. This notion is also quite useful to describe the technique of "switching" an APN function. This is a very powerful tool to construct new APN functions, as we will show in this paper.

Let $\mathbb{F}$ be an arbitrary field, and let $(G, +)$ be an additively written abelian group (we are only interested in abelian groups, so we do not care about the general case). The group algebra $\mathbb{F}[G]$ consists of all "formal" sums

$$\sum_{g \in G} a_g\, g, \quad a_g \in \mathbb{F}.$$

We define componentwise addition

$$\sum_{g \in G} a_g\, g \;+\; \sum_{g \in G} b_g\, g \;:=\; \sum_{g \in G} (a_g + b_g) g,$$

and a multiplication

$$\sum_{g \in G} a_g\, g \;\cdot\; \sum_{g \in G} b_g\, g \;:=\; \sum_{g \in G} \left(\sum_{h \in G} a_h \cdot b_{g-h} \right) g.$$

Together with these two operations and the scalar multiplication $\lambda \sum_{g \in G} a_g g := \sum_{g \in G} (\lambda a_g) g$, the set $\mathbb{F}[G]$ becomes an algebra, the so called **group algebra**. The dimension of this algebra as an $\mathbb{F}$-vectorspace is $|G|$. Given a function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$, we associate a group algebra element G_F in $\mathbb{F}[\mathbb{F}_2^n \times \mathbb{F}_2^n]$ with it:

$$G_F := \sum_{v \in \mathbb{F}_2^n} (v, F(v)) \quad \text{in } \mathbb{F}[\mathbb{F}_2^n \times \mathbb{F}_2^n].$$

The coefficients of the group elements in G_F are just 0 or 1 (more generally, any subset T of a group G can be identified with the element $\sum_{g \in T} g$, where the coefficients of all elements in T are 1). We have the following very easy Lemma:

Lemma 1. *A function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is APN if and only if*

$$G_F \cdot G_F = 2^n \cdot (0, 0) + 2 \cdot D_F \text{ in } \mathbb{C}[\mathbb{F}_2^n \times \mathbb{F}_2^n] \tag{4}$$

for some subset $D_F \in \mathbb{F}_2^n \times \mathbb{F}_2^n$.

In (4), we may replace $\mathbb{C}$ by any field of characteristic $\neq 2$ if we say *for some subset $D_F \in \mathbb{F}_2^n \times \mathbb{F}_2^n$ of size $2^{n-1} \cdot (2^n - 1)$.*

We emphasize that G is additively written, but this addition is quite different from the addition in the group algebra $\mathbb{F}[G]$. If, for instance, $A, B \subset G$ and $A \cap B = \emptyset$, then $A \cup B$ is the subset of G corresponding to $A + B$ in $\mathbb{F}[G]$. If $g \in G$, then $A \cdot g$ in $\mathbb{F}[G]$ corresponds to the subset $\{a + g : a \in A\}$. We call $A \cdot g$ a **translate** of A. It looks a bit awkward that the product $A \cdot g$ is the set of *sums* $a + g$ with $a \in A$.

The ideal generated by G_F in $\mathbb{F}_2[\mathbb{F}_2^n \times \mathbb{F}_2^n]$ is a subspace of the 2^{2n}-dimensional vector space of the group algebra $\mathbb{F}_2[\mathbb{F}_2^n \times \mathbb{F}_2^n]$. The dimension is called the **Γ-rank** of the function F. Similarly, the dimension of the ideal generated by D_F in $\mathbb{F}_2[\mathbb{F}_2^n \times \mathbb{F}_2^n]$ is called the **Δ-rank** of F.

The Walsh transform of a function F is nothing else than the Discrete Fourier transform of G_F, which we will describe briefly: If G is a finite abelian group, then there are $|G|$ different homomorphisms $\chi : G \to \mathbb{C}$, and the set of these homomorphisms (called **characters**) form a group under multiplication $\chi_1\chi_2(g) := \chi_1(g) \cdot \chi_2(g)$. This group is isomorphic to G. Characters χ may be extended to homomorphisms $\chi : \mathbb{C}[G] \to \mathbb{C}[G]$ by linearity:

$$\chi(\sum_{g \in G} a_g\, g) := \sum_{g \in G} a_g \chi(g).$$

Let χ be a character of G, and Ψ an automorphism of G. Then the mapping $\chi^{\Psi} : G \to \mathbb{C}$ with $\chi^{\Psi}(g) := \chi(\Psi(g))$ is again a character. Moreover, Ψ may be extended to a group algebra automorphism. This shows that the Walsh spectrum of an element $D \in \mathbb{C}[G]$ is invariant under the application of group automorphisms.

If $G = \mathbb{F}_2^n \times \mathbb{F}_2^n$, the characters are the mappings $\chi_{\alpha,\beta}$ defined by $\chi_{\alpha,\beta}(u,v) := (-1)^{\mathsf{tr}(\alpha u+\beta v)}$, where we identify the vector space $\mathbb{F}_2^n$ with the additive group of the finite field $\mathbb{F}_{2^n}$. Therefore, the Walsh spectrum is just the multi-set of character values of G_F.

Definition 1 (CCZ and EA equivalence, [14])**.** *Two functions $F, H : \mathbb{F}_2^n \to \mathbb{F}_2^n$ are called* **CCZ equivalent** *if there is a group automorphism Ψ of $\mathbb{F}_2^n \times \mathbb{F}_2^n$ and an element $(u,v) \in \mathbb{F}_2^n \times \mathbb{F}_2^n$ such that*

$$\Psi(G_F) = G_H \cdot (u,v),$$

hence $\Psi(G_F)$ is a translate of G_H. If Ψ fixes the subgroup $\{(0,y) : y \in \mathbb{F}_2^n\}$ setwise, we say that the functions are **EA equivalent** *(EA = extended affine equivalent). If, additionally, Ψ fixes the set $\{(x,0) : x \in \mathbb{F}_2^n\}$, then F and G are called* **affine** *equivalent.*

We call this relation *CCZ equivalent* since it has been first introduced (using different notation) by Carlet, Charpin and Zinoviev [19].

Proposition 1. *If F is an APN (resp. AB) function, and if H is CCZ equivalent to F, then H is also an APN (resp. AB) function.*

Proof. Let $G_H = \Psi(G_F) \cdot (u,v)$. If χ is a character of $\mathbb{F}_2^n \times \mathbb{F}_2^n$, then $\chi(G_H) = \chi^{\Psi}(G_F) \cdot \chi(u,v)$, hence the maximum absolute character value is invariant under CCZ equivalence, hence H is AB if F is *AB*. If F is APN, then

$$G_F \cdot G_F = n \cdot (0,0) + 2 \cdot D_F$$

and therefore

$$G_H \cdot G_H = n \cdot (0,0) + 2 \cdot \Psi(D_F) \quad \text{in } \mathbb{C}[\mathbb{F}_2^n \times \mathbb{F}_2^n].$$

□

This Proposition and its proof have some consequences: The Walsh spectrum is *not* invariant under CCZ equivalence: The Walsh coefficients $\chi(G_F)$ and $\chi(G_F) \cdot \chi(u,v)$ differ by the factor $\chi(u,v)$, hence by ±1. The problem comes via the addition of the element (u,v): The Walsh spectrum is invariant under affine equivalence, but not under EA or CCZ equivalence. The set containing the Walsh spectrum and its negative is called the **extended Walsh spectrum**, and this is invariant under CCZ equivalence.

There is one drawback in the concept of CCZ equivalence: If F is APN (or AB), the group algebra element $\Psi(G_F)$ does not necessarily correspond to a function H, see [14], for instance.

It is obvious that the Δ- and Γ-ranks are invariant under CCZ equivalence.

Now we discuss the first part of Question 1: Is the list in Table 1 complete? This has been answered negatively in [26]. One of the examples in [26] has been generalized to an infinite family, and a lot more constructions have been found since. In particular, Dillon [21] presented a list of 12 examples in $\mathbb{F}_2^6$. This list apppears in [8], together with many new examples in the cases $\mathbb{F}_2^7$ and $\mathbb{F}_2^8$.

However, all the new examples that have been constructed so far are "quadratic" in the sense that the *derivatives* $F(x+a) - F(x)$ are linear mappings. Since the property of being "quadratic" is not invariant under CCZ equivalence (see [14]), we modify the definition as follows:

Definition 2. *A function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is* **CCZ quadratic** *if F is CCZ equivalent to a function H with the property that $H(x+a) - H(x)$ is linear for all $a \in \mathbb{F}_2^n$.*

How can we prove that a function is *not* CCZ quadratic? For this purpose, we look at the following *design* or *incidence structure* associated with an APN function. We refer the reader to the encyclopaedic book [2] for background from design theory and difference sets: The designs that we are going to define here may be viewed as the designs developed from a certain type of difference set.

Definition 3 ([29]). *Let $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ be an APN function. Then we define two incidence structures (designs) on the point set $\mathbb{F}_2^n \times \mathbb{F}_2^n$: In the first case, the blocks are the the sets*

$$G_F \cdot (a,b) := \{(x+a, F(x)+b) \ : \ x \in \mathbb{F}_2^n\}$$

for $a, b \in \mathbb{F}_2^n$, i.e. the translates of G_F. We call this design the **development of** *G_F, denoted by dev(G_F). Similarly, the design whose blocks are the translates*

$$D_F \cdot (a,b)$$

of D_F (see Lemma 1) is the **development of** *D_F, denoted by dev(D_F). We call two designs* **isomorphic** *if there is a permutation π on the set of points such that blocks (which are in our situation just subsets $B = \{g_1, \ldots\}$ of the point set) are mapped to blocks (i.e. $\{\pi(g_1, \ldots\}$ is a block).*

Any incidence structure gives rise to an incidence matrix: Rows and columns are indexed by the points and blocks, and the (p, B)-entry is 1 if the point p is incident with the block B; the other entries are 0. The Γ-rank defined earlier is nothing else than the rank of the incidence matrix of dev(G_F), considered as a matrix with entries in $\mathbb{F}_2$; similarly, the Δ-rank is the $\mathbb{F}_2$-rank of an incidence matrix of dev(D_F).

Lemma 2. *If F and H are CCZ equivalent APN functions, then the designs dev(G_F) and dev(G_H) are isomorphic. Moreover, the designs dev(D_F) and dev(D_H) are isomorphic.*

Proof. Straightforward, see also [29]: The group automorphism Ψ with $\Psi(G_F) = G_H \cdot (u,v)$ is the permutation on the point set which maps blocks to blocks. □

Using MAGMA [4] it is quite easy to determine the automorphism groups of these designs for small values of n. There is another group associated with the designs dev(G_F) (resp. dev(D_F)): The sets G_F (resp. D_F) are subsets of $\mathbb{F}_2^{2n}$. Then there may exist automorphisms φ of $\mathbb{F}_2^{2n}$ such that $\varphi(G_F) = G_F \cdot (u,v)$ (resp. $\varphi(D_F) = D_F \cdot (u,v)$) for some $u, v \in \mathbb{F}_2^n$. These automorphisms form a group *contained* in the automorphism group of the designs dev(G_F) (resp. dev(D_F)). Using notion adopted from the theory of difference sets, we call the group of these automorphisms the **multiplier group** $\mathcal{M}(G_F)$ (resp. $\mathcal{M}(D_F)$) of dev(G_F) (resp. dev(D_F)). It turns out that this group is much easier to compute with MAGMA than the full automorphism groups of the designs. We denote the group of translations $\tau_{a,b} : \mathbb{F}_2^n \times \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n \times \mathbb{F}_2^n$ with $\tau_{a,b}(x,y) := (x+a, y+b)$ by $\mathcal{T}$. Obviously, we have $|\mathcal{T}| = 2^{2n}$, and $|\mathcal{M}(G_F) \cap \mathcal{T}| = 1$ as well as $|\mathcal{M}(D_F) \cap \mathcal{T}| = 1$.

Since the multiplier group normalizes $\mathcal{T}$, we have the following Lemma:

Lemma 3. *Let $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ be an APN function. Then*

1. $\langle \mathcal{M}(G_F), \mathcal{T} \rangle \subseteq Aut(dev(G_F))$.
2. $\langle \mathcal{M}(D_F), \mathcal{T} \rangle \subseteq Aut(dev(D_F))$.
3. $|\mathcal{M}(G_F)| \cdot 2^{2n} = |\langle \mathcal{M}(G_F), \mathcal{T} \rangle|$.
4. $|\mathcal{M}(D_F)| \cdot 2^{2n} = |\langle \mathcal{M}(D_F), \mathcal{T} \rangle|$.
5. $\mathcal{M}(G_F) \subseteq \mathcal{M}(D_F)$.

It is possible to show that $\mathcal{M}(G_F)$ is just the automorphism group of the extended code $\mathcal{C}_F^{\text{ext}}$ defined in the Introduction, see [8]. In all cases known to us, the "full" automorphism group of the design dev(G_F) is just the multiplier group "times" the translations $\tau_{a,b}$.

We do not knwo whether this observation that holds for small values is true in general:

Question 2. *Is it possible that the* **full** *automorphism group of dev(G_F) (resp. dev(D_F)) is larger than $|\mathcal{M}(G_F)| \cdot 2^{2n}$ (resp. $|\mathcal{M}(D_F)| \cdot 2^{2n}$)?*

It seems that the automorphism group is a good invariant for CCZ equivalence, in particular to distinguish the quadratic from the non-quadratic case:

Theorem 4. *If $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is an APN mapping such that $F(x+a) - F(x)$ is linear for all $a \in \mathbb{F}_2^n$, then the subgroup of the automorphism group of the development of G_F which is generated by the translations $\tau_{a,b}$ and the multipliers contains an elementary abelian group of order 2^{3n}.*

Proof. The mappings $\tau_{a,b} : \mathbb{F}_2^{2n} \to \mathbb{F}_2^{2n}$ with $\tau_{a,b}(x,y) = (x+a, y+b)$ are automorphisms of $\mathrm{dev}(G_F)$, since $\tau_{a,b}(G_F) = G_F \cdot (a,b)$. If F is quadratic, then we may assume (after replacing F by a CCZ equivalent function, if necessary) that the mappings $L_a(x) = F(x+a)+F(x)+F(a)+F(0)$ are linear. We compute

$$\begin{aligned}(L_a + L_b)(x) &= F(x) + F(x+a) + F(a) + F(0) + F(x) + F(x+b) + F(b) + F(0)\\ &= F(x+a) + F(x+b) + F(a) + F(b).\end{aligned}$$

Now we use

$$L_a(b+x) = F(a+b+x) + F(b+x) + F(a) + F(0)$$

and

$$L_a(b+x) = L_a(b) + L_a(x) = F(b) + F(a+b) + F(x) + F(a+x)$$

to obtain

$$F(a+b+x) = F(b+x) + F(a) + F(0) + F(b) + F(a+b) + F(x) + F(a+x). \tag{5}$$

We get

$$\begin{aligned}L_{a+b}(x) &= F(a+b+x) + F(a+b) + F(x) + F(0)\\ &= F(b+x) + F(a) + F(b) + F(a+x) \quad \text{using (5)}\\ &= L_a(x) + L_b(x).\end{aligned}$$

This shows that the mappings ψ_a defined by $\psi_a(x,y) = (x, y + L_a(x))$ are linear, and

$$\begin{aligned}\psi_a(G_F) &= \{(x, F(x) + L_a(x) \,:\, x \in \mathbb{F}_2^n\}\\ &= \{(x, F(x+a) + F(a) + F(0) \,:\, x \in \mathbb{F}_2^n\}\\ &= \{(x-a, F(x) + F(a) + F(0) \,:\, x \in \mathbb{F}_2^n\}\\ &= G_F \cdot (-a, F(a) + F(0))\end{aligned}$$

is a translate of G_F, hence the mappings ψ_a are automorphisms of $\mathrm{dev}(G_F)$. Moreover, $\psi_{a+b} = \psi_b \circ \psi_a$, hence the ψ_a's form a group of order 2^n. It is not difficult to see that the ψ_c together with the mappings $\tau_{a,b}$ from a group of order 2^{3n}. □

Corollary 5. *Under the assumptions of Theorem 4, the multiplier group $\mathcal{M}(G_F)$ (equivalently the automorphism group of the extended code $\mathcal{C}_F^{ext}$) has size divisible by 2^n, and both the orders of $Aut(dev(G_F))$ and $Aut(dev(D_F))$ are divisible by 2^{3n}.*

Corollary 6 (Göloğlu, Pott [29])**.** *The Kasami power functions x^{13} and x^{57} on $\mathbb{F}_2^7$ are not CCZ quadratic, hence they are not CCZ equivalent to quadratic functions.*

Proof. Using MAGMA, it is easy to compute $|\mathrm{Aut}(\mathrm{dev}(G_F))|$ for $F(x) = x^{13}$ and $F(x) = x^{157}$: The order of the groups is, in both cases, $2^{14} \cdot 7 \cdot (2^7 - 1)$ (Table 6) which is not divisible by 2^{21}. □

Most people conjecture that the examples in Table 1 are all CCZ inequivalent, except for small n where some of the cases coincide, but as far as we know there is no proof, yet. It is known that the Gold power mappings are CCZ inequivalent to the Kasami power mappings, and different Gold exponents are CCZ inequivalent, see [11].

There is another concept related to quadratic APN functions: If F is quadratic, then $F(x+a)-F(x)$ is linear, hence

$$H_a := \{b \,:\, F(x+a)-F(x)=b \quad \text{for some } x \in \mathbb{F}_2^n\} \tag{6}$$

is an affine subspace. If $a \neq 0$, this subspace has 2^{n-1} elements (since F is APN), hence its is an (affine) hyperplane. We say that a function is *crooked* if the sets in (6) are (affine) hyperplanes for all a. This concept is due to Bending and Fon-der-Flaas [1]. "Crooked" is not invariant under CCZ equivalence, hence it would be better to say that a function F is crooked if it is CCZ equivalent to a function for which all the sets H_a are hyperplanes:

Definition 4. *An APN function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is called* **CCZ crooked** *if F is CCZ equivalent to a function G such that the sets*

$$\{b \,:\, G(x+a)-G(x)=b \textit{ for some } x \in \mathbb{F}_2^n\}$$

are affine hyperplanes in $\mathbb{F}_2^n$.

It is obvious that any (CCZ) quadratic function is (CCZ) crooked, and it is conjectured that the converse is also true, see [3, 32] for partial results in this direction. However, as long as we do not know whether non-quadratic crooked functions may exist, we need to find arguments that a function is not CCZ crooked. The following argument gives an interesting necesary condition that a function is crooked:

Theorem 7. *Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be an APN mapping. If F is CCZ crooked, then the dimension of the ideal generated by $D_F \in \mathbb{F}_2[\mathbb{F}_2^n \times \mathbb{F}_2^n]$ is at most 2^{n+1}, hence the Δ-rank is at most 2^{n+1} (see Lemma 1 for the definition of D_F).*

Proof. If F is crooked, there are 2^n-1 (affine) hyperplanes H_a such that

$$D_F = \{(a,x) \,:\, a \in \mathbb{F}_2^n \setminus \{0\}, x \in H_a\}$$

(replace F by a CCZ equivalent function if necessary). We define

$$J_a := \{(a,x) \,:\, x \in \mathbb{F}_2^n\}.$$

As explained above, these subsets may be also interpreted as elements in $\mathbb{F}_2[\mathbb{F}_2^n \times \mathbb{F}_2^n]$. We will show that the ideal generated by D_F is contained in the subspace $\mathcal{I}$ generated (as a vector space) by the 2^{n+1} elements

$$\{D_F \cdot (u,0) \,:\, u \in \mathbb{F}_2^n\} \,\cup\, \{J_a \,:\, a \in \mathbb{F}_2^n\}.$$

It is sufficient to show that $D_F \cdot (u,v) \in \mathcal{I}$ for all $(u,v) \in \mathbb{F}_2^n \times \mathbb{F}_2^n$. The set corresponding to $D_F \cdot (u,v)$ is $\{(a+u, H_a+v) \,:\, a \in \mathbb{F}_2^n\}$, where $H_a + v = \{h+v \,:\, h \in H_a\}$. Here we have used the notation (x,T) to denote the set of elements $\{(x,t) \,:\, t \in T\}$. Since H_a is a hyperplane, we have $H_a + y = H_a$ or $H_a + y$ is the complement of H_a: In group algebra notation, this means for fixed $a \in \mathbb{F}_2^n$

$$(a+u, H_a+v) = (a+u, H_a)\} \quad \text{or} \quad (a+u, H_a+v) = (a+u, H_a) + J_{a+u}$$

in $\mathbb{F}_2[\mathbb{F}_2^n \times \mathbb{F}_2^n]$. In the equation above, we again identify subsets with the corresoponding group algebra elements. Adding the element J_{a+u} has the effect of complementing H_a in $(a+u, H_a)$. □

Corollary 8. *The Kasami power mappings x^{13} and x^{57} on $\mathbb{F}_2^7$ are not CCZ crooked.*

Proof. It is easy to compute the Δ-ranks of x^{13} (resp. x^{57}) using MAGMA: The ranks are 338 (resp. 436), see Table 6. □

It would be very interesting to determine the Δ- and Γ-ranks of APN functions theoretically.

In the next section (Theorem 11), we will construct a new APN function which, at first view, seems to be non-quadratic. In order to prove that the function is indeed non-quadratic, we use Theorem 7 to show that the function cannot be CCZ equivalent to a crooked function, hence it cannot be quadratic. We may also use Theorem 4 to show that the function is non-quadratic, since the automorphism group of $\mathrm{dev}(G_F)$ is too small for the new function F. We have checked that our function is equivalent to the new example given in [7]. However, in that paper the authors erroneously claimed that their new function is CCZ equivalent to a quadratic one. Moreover, our function has been found independently from the search in [7].

3 The switching construction

The following interesting construction of an APN function is contained in [13]:

Proposition 2. *The function $x^3 + tr(x^9)$ is APN in $\mathbb{F}_2^n$.*

This is a special case of what we will call "switching". For this purpose, we consider certain projection homomorphisms on the group algebra $\mathbb{F}[G]$. Let U be a subgroup of G. Then the canonical homomorphism $\varphi_U : G \to G/U$ defined by $\varphi_U(g) := g + U$ can be extended by linearity to a homomorphism $\varphi_U : \mathbb{F}[G] \to \mathbb{F}[G/U]$. Let $D = \sum a_g g$ be an element in $\mathbb{F}[G]$. The coefficient of $g + U$ in $\varphi(D)$ is $\sum_{h \in g+U} a_h$. If D has just coefficients 0 and 1, hence D corresponds to a set $D \subseteq G$, then the coefficient of $g+U$ is $|D \cap (g+U)|$. In particular, if each coset of U meets D in at most one element, then $\varphi_U(D)$ has also just coefficients 0 and 1. This is the case if $U \leq \{0\} \times \mathbb{F}_2^n$.

Definition 5 (switching neighbours)**.** *Let $F, H : \mathbb{F}_2^n \to \mathbb{F}_2^n$ be two functions, and let $U \leq \mathbb{F}_2^n \times \mathbb{F}_2^n$ be a subgroup of $\mathbb{F}_2^n \times \mathbb{F}_2^n$. We say that F and H are* **switching neighbours with respect to** *U if $\varphi_U(G_F) = \varphi_U(G_H)$. We say that they are* **switching neighbours in the narrow sense** *if $U \leq \{0\} \times \mathbb{F}_2^n$ and $dim(U) = 1$.*

If F and H are switching neighbours with respect to U, we may obtain H from F by first *projecting* G_F onto $\varphi_U(G_F)$, and then we *lift* this element to G_H. We may also try to construct new switching neighbours H of F via such a *project and lift* procedure such that (hopefully) F and H are CCZ inequivalent. This is in particular promising if the dimension of U is small. The intuitive idea behind this approach is that $\varphi_U(G_F)$ is *almost* an APN function, and so it may be easy to turn this "almost" APN into an APN function.

We will describe this approach (and applications) in the situation where $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ and $U \leq \{0\} \times \mathbb{F}_2^n$. This has the advantage that the coefficients of $\varphi_U(G_F)$ are just 0 and 1, since the cosets of $\{0\} \times \mathbb{F}_2^n$ (and therefore also the cosets of U) meet G_F no more than once. In this case, $\varphi_U(G_F)$ corresponds to a mapping $F_U : \mathbb{F}_2^n \to \mathbb{F}_2^n/U'$ with $F_U(v) := v + U'$ and

$$U' = \{u \, : \, (0, u) \in U\} \tag{7}$$

(hence U' is basically the same as U).

Proposition 3. *Let $F, H : \mathbb{F}_2^n \to \mathbb{F}_2^n$, and let $U \leq \{0\} \times \mathbb{F}_2^n$. Then*

$$F_U = H_U \quad \textit{if and only if} \quad (0, F(v) - H(v)) \in U \quad \textit{for all } v \in \mathbb{F}_2^n.$$

If $U = \{(0,0), (0,u)\}$, then $F_U = H_U$ if and only if there is a Boolean function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ such that $H(v) = F(v) + f(v) \cdot u$.

Proof. We define U' as in (7). Then $F_U(v) = H_U(v)$ if and only if $F(v) + U' = H(v) + U'$, hence $F_U(v) - H_U(v) \in U'$ for all v. This shows the first part of the proposition.

The function f is defined via

$$f(v) := \begin{cases} 0 & \text{if } F(v) = H(v) \\ 1 & \text{if } F(v) \neq H(v) \end{cases}$$

which finishes the proof. □

The two functions $F(x) = x^3$ and $H(x) = x^3 + \mathsf{tr}(x^9)$ are switching neighbours in the narrow sense: Take the 1-dimensional subspace U generated by $(0,1) \in \mathbb{F}_2^n \times \mathbb{F}_2^n$. Then $\varphi_U(G_F) = \varphi_U(G_F)$.

Proposition 3 shows that we may obtain all switching neighbours of F in the narrow sense (with respect to a one-dimensional subspace) by adding a Boolean function f times a vector $u \neq 0$. Let F be an APN function. The following Theorem gives a necessary and sufficient condition for f to produce another (not necessarily equivalent) APN function:

Theorem 9. *Assume that $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is an APN function. Let $u \in \mathbb{F}_2^n$, $u \neq 0$, and let $f : \mathbb{F}_2^n \to \mathbb{F}_2$ be a Boolean function. Then $F(v) + f(v) \cdot u$ is an APN function if and only if*

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

for all $x, y, a \in \mathbb{F}_2^n$ with

$$F(x) + F(x+a) + F(y) + F(y+a) = u.$$

Proof. Since F is APN, the equation

$$F(x+a) + F(x) + (f(x+a) + f(x))u = b$$

hat at most 4 solutions for x, namely those x for which $F(x+a) + F(x) \in \{b, b+u\}$. If there are 4 different solutions $x, y, x+a, y+a$, then

$$\begin{aligned} F(x+a) + F(x) + (f(x+a) + f(x))u &= b \\ F(y+a) + F(y) + (f(y+a) + f(y))u &= b. \end{aligned}$$

But this is possible if and only if

$$\begin{aligned} F(x) + F(x+a) + F(y) + F(y+a) &= u \qquad (8) \\ f(x) + f(x+a) + f(y) + f(y+a) &= 1. \end{aligned}$$

□

Remark 1.

1. *The Boolean function f depends on u, i.e. for different choices of u we may get different f's.*
2. *It seems to be difficult to find a theoretical criteria that the function $F(v) + f(v)u$ is CCZ equivalent to $F(v)$.*
3. *The functions $F(v)$ and $F(v) + f(v)u$ are switching neighbours in the narrow sense with respect to $\{(0,0), (0,u)\}$.*

Theorem 9 immediately suggests a strategy to find Boolean functions f such that $F(v) + f(v)u$ is APN: Determine all 4-tuples $x, y, x+y, y+a$ such that (8) holds. These 4-tuples give rise to constraints

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

We may view f as a vector of length 2^n (coordinates are indexed by elements v in $\mathbb{F}_2^n$, and the entries of the vector are $f(v)$). Thus the constraints are linear conditions, and we may find f's by solving a system of linear equations.

Here is another interpretation: Write $\mathbb{F}_2^n$ as direct sum $U \oplus \overline{U}$. The function F is uniquely determined by its function values. Consider the n-dimensional subspace V of $\mathbb{F}_2^{2^n}$ spanned by $\{F(x) : x \in \mathbb{F}_2^n\}$. Write $\mathbb{F}_2^n$ as direct sum $U \oplus \overline{U}$, this lifts to a decomposition of $V = V' \oplus \overline{V}$. So the evaluation of $f(v)u$ will be in the 1-dimensional space V'.

All 4-tuples $x, y, x+y, y+a$ such that the condition of Theorem 9 holds thus are the vectors of weight 4 in $\overline{V}^{\perp}$ (these are automaticly in $\overline{V}^{\perp} - V^{\perp}$ as F is APN). Let $\tilde{V}$ be the vector space generated by these words of weight 4. An evaluation vector of $f(v)u$ (satisfying Theorem 9) is just an element of $\tilde{V}^\perp$. Moreover the functions $f(x)u$ in $\tilde{V}^\perp$ in the same coset modulo $\overline{V} \subseteq \tilde{V}^\perp$ are CCZ equivalent (the difference is some AF, A being a linear map $\mathbb{F}_2^n \mapsto \mathbb{F}_2$). So it is sufficient to test one $f(x)u$ from each coset.

So we know in particular that in the case that $\tilde{V}^\perp$ has dimension $n-1$ there is no candidate for a CCZ inequivalent switching function.

Definition 6. *The finest equivalence relation on the set of APN functions such that all switching neighbours in the narrow sense and all EA-equivalent functions are equivalent, is called the* **EA switching** *equivalence relation. In the same way, we define* **CCC switching equivalence**.

This "switching idea" is closely related to a comment of John F. Dillon (which was motivated by [13]). Using the notion in Proposition 3, he considered just the case $u = 1$.

In the next section, we determine the EA switching equivalence classes of all known CCZ inequivalent APN functions on $\mathbb{F}_2^n$, $n \leq 8$. Several of the new constructions in the literature are switching equivalent. It seems that the switching idea is quite powerful to construct new APN functions, since many of the new APN functions listed by Dillon in [8] are within just one switching class. In the case $n = 8$, the switching class of the Gold function x^3 contains 17 CCZ inequivalent functions!

A more appropriate search would be to find all CCZ switching classes, which seems to be much harder than determining the EA switching classes.

4 Computational results and open problems

There is, up to equivalence, just one APN mapping $\mathbb{F}_2^n \to \mathbb{F}_2^n$ for $n \leq 4$, hence no interesting things happen in these cases. In the case $n = 5$, a complete classification of APN functions (up to CCZ equivalence) is contained in [6]. We summarize our computational results in the following tables. We also include some interesting CCZ invariants:

- Δ- and Γ-Rank.
- Orders of automorphism groups of $\mathrm{dev}(D_F)$, $\mathrm{dev}(G_F)$ and $\mathcal{M}(G_F)$.
- extended Walsh spectrum.

If all these invariants are the same, we used a direct test to check that the examples are CCZ inequivalent, hence the reader can be sure that all the examples in the following tables are CCZ inequivalent. However, we do not claim that our tables are complete in the sense that they contain all possible CCZ equivalence classes of APN functions with $n = 6, 7$ and 8.

We list the Walsh spectrum just if it is different from the Walsh spectrum of x^3. The Walsh spectrum of x^3 is called **classical**.

We number the examples as 1.1, 1.2, ..., 2.1, 2.2, ... etc. The first number describes the switching class, and the second number the CCZ inequivalent examples within this class. Our search was complete in the sense that, starting from the known APN functions, we searched through the entire switching class. Hence any new APN function must be a member of a new switching class. We used the examples in [21] and [8] as the starting cases.

Some comments about the sizes of the automorphism groups are in order: The automorphism groups contain the translations $\tau_{a,b}$, see Theorem 4, therefore we divided the group sizes in our tables by 2^{2n}. We were not able to determine the sizes of these groups if $n = 8$. However, it was possible to determine the multiplier group $\mathcal{M}(G_F)$ of $\mathrm{dev}(G_F)$: Using MAGMA, we determined the automorphism groups of the associated extended codes $\mathcal{C}_F^{\mathrm{ext}}$. In the cases $n \leq 7$, the automorphism groups of $\mathrm{dev}(G_F)$ have been always the groups generated by the multipliers plus the translations; therefore, it may be possible that the the group sizes in Table 10 desribe actually the sizes of the full automorphism groups.

We did not determine the multiplier groups $\mathcal{M}(D_F)$. In a forthcoming paper, we will continue the investigation of the relations between the different groups associated with APN functions

It is quite interesting to look at the automorphism groups of the designs $\mathrm{dev}(G_F)$, since they give some information about F:

Theorem 10. *Let $F(x)$ be an APN function on $\mathbb{F}_{2^n}$. Let $v = |\mathcal{M}(G_F)|$. Then the following holds:*

(1.) If $F(x)$ is quadratic, then 2^n divides v.

(2.) If F is CCZ equivalent to a power mapping, then $n \cdot (2^n - 1)$ divides v.

(3.) If F is CCZ equivalent to a polynomial in $\mathbb{F}_2[x]$, then n divides v.

Proof. The first statement is simply Theorem 4. If $F(x) \in \mathbb{F}_2[x]$, then the mapping $\mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ defined by $(x, y) \mapsto (x^2, y^2)$ has order n, and it fixes the set G_F. This shows (3). If $F(x) = \gamma \cdot x^d$, then the $2^n - 1$ mappings defined by $(x, y) \mapsto (\alpha x, \alpha^d \cdot y)$, $\alpha \in \mathbb{F}_{2^n}$, fix the set G_F. Moreover, we may assume that $\gamma = 1$, otherwise we replace F by the CCZ equivalent function $\frac{1}{\gamma}F$, which shows (2). □

We did mention already that quadratic functions are crooked. The following question is of interest:

Question 3. *Are all crooked functions quadratic?*

A function defined by $\sum_{i,j} \alpha_{i,j} x^{2^i+2^j}$ is quadratic. Therefore, Theorems 10 and 7 show the following:

Remark 2. *The only non-quadratic functions in Tables 3, 5 and 7 are the function no. 2.12 in Table 3 and the functions no. 5.1,6.1 and 7.1 in 7. Moreover, none of these functions is crooked.*

We note that our new function 14.3 in Table 7 is inequivalent to a polynomial with coefficients in $\mathbb{F}_2$ (Theorem 10).

We note that Table 3 contains, up to CCZ-equivalence, **all** APN functions on $\mathbb{F}_2^5$. In the tables (5), (7) and (9), we only claim that we did apply the switching construction recursively to all known APN functions, in particular to those given by Dillon. In Table (5), the Example 2.12 is new (see Theorem 11), and in Table (7), the Example 14.3 is new. However, we did not apply the switching construction to all the memebers of the CCZ equivalence classes. In other words, we started with the functions listed in the tables below, and we determined the EA switching classes, **not** the CCZ switching classes.

In our opinion, the most interesting function is the following non-quadratic example, see also [7]:

Theorem 11. *Let $\mathbb{F}_{2^6}$ be the finite field which is constructed as the splitting field of $x^6 + x^4 + x^3 + x + 1 \in \mathbb{F}_2[x]$. Let u be a root of this polynomial in $\mathbb{F}_{2^6}$. Then the function $F : \mathbb{F}_{2^6} \to \mathbb{F}_{2^6}$ with*

$$\begin{aligned} F(x) &= x^3 + u^{17}(x^{17} + x^{18} + x^{20} + x^{24}) + u^{18}x^9 + u^{36}x^{18} + u^9x^{36} + x^{21} + x^{42} + \\ &\quad + \mathsf{tr}(u^{27}x + u^{52}x^3 + u^6x^5 + u^{19}x^7 + u^{28}x^{11} + u^2x^{13}) \end{aligned} \tag{9}$$

is an APN function which is a switching neighbour of Function 2.4 in Table 5.Hier habe ich auch noch mal wg. des primitiven Elementes umgeschrieben This function cannot be CCZ equivalent to a crooked function.

Proof. One may quite easily check that the function is APN. One may also show that it is a switching neighbour of $x^3 + u^{17}(x^{17} + x^{18} + x^{20} + x^{24})$. Note that the Δ-rank $152 > 2^7$ of this function is too big for a crooked function, see Theorem 7. □

Remark 3. *The function $F(x)$ in (9) may be also written*

$$\begin{aligned} F(x) &= x^3 + u^{17}(x^{17} + x^{18} + x^{20} + x^{24}) + \\ &\quad u^{14}(tr(u^{52}x^3 + u^6x^5 + u^{19}x^7 + u^{28}x^{11} + u^2x^{13}) + tr_{8/2}((u^2x)^9) + tr_{4/2}(x^{21})) \end{aligned}$$

where $\mathsf{tr}_{8/2}$ and $\mathsf{tr}_{4/2}$ denote the relative trace $\mathbb{F}_8 \to \mathbb{F}_2$ and $\mathbb{F}_4 \to \mathbb{F}_2$. Note that $(u^2x)^9 \in \mathbb{F}_8$ and $x^{21} \in \mathbb{F}_4$, so this re-writing of F is feasible.

Two APN functions which are switching equivalent in the narrow sense are quite "similar", they are "almost" equal (see Proposition 3). Therefore, the following question seems natural:

Question 4. *Is there some property which distinguishes switching equivalent functions from those which are not switching equivalent?*

Our computational results are quite pessimistic regarding this question. It seems that there is no property of an APN function which is preserved under switching. Also the sizes of the equivalence classes seem to behave "strange": In the $n = 8$ case, there is one large switching class, but in the case $n = 7$ there are only small classes.

It seems that many inequivalent APN functions exist. So, in our opinion, the main question about APN functions is to determine at least a lower bound for the number of inequivalent ones. Let APN(n) denote the number of CCZ inequivalent APN functions $\mathbb{F}_2^n \to \mathbb{F}_2^n$. Then we ask:

Question 5. *Does the function APN(n) grows exponentially?*

This paper contains a new non-quadratic APN function. We think that it is worth to search for more examples:

Problem 1. *Find more nonquadratic APN functions.*

We described the switching construction in quite a general form, and then we specialized to the case of 1-dimensional subspaces $U \leq \{0\} \times \mathbb{F}_2^n$. In this case, it was (rather) easy to find switching neighbours. But of course one may also use higher-dimensional subspaces, or one may use subspaces not contained in $\{0\} \times \mathbb{F}_2^n$. It will be more difficult to handle these cases, but we do not think that it is hopeless. If U becomes larger, the projections are further away from being APN, therefore the "lifting" will become more difficult. On the other hand, if we are using higher-dimensional subspaces U, we obtain more freedom for the lifting. But if U is too big, the approach will most likely become useless: If, in the extremal case, $U = \{0\} \times \mathbb{F}_2^n$, then all APN functions F project onto the same set $\varphi_U(G_F)$.

A generalization of the switching idea to functions between fields of odd characteristic is obvious. Therefore, one may also apply this approach to PN functions:

Problem 2. *Try to use the switching idea for other subspaces U or for PN functions.*

Finally, we come back to the original motivation for studying APN functions: APN's are used in cryptography because they are highly nonlinear. Moreover, functions used in cryptography should quite often have large algebraic degree. Therefore, quadratic functions are usually "weak" regarding applications. But our paper shows that functions of large degree can be quite similar to quadratic (i.e. weak) functions via our projection idea. Therefore, it may be worth to see whether "switching" can be used for cryptanalysis.

In the following tables, it is important to know the primitive element that we have used to construct the finite fields. In Table 2, we list these polynomials $p(x)$. The primitive element u used later in the tables is a root of $p(x)$ in $\mathbb{F}_2[x]/(p(x))$, see [34] for more information about finite field extensions.

Table 2: Used primitive polynomials $p(x)$

n	$p(x)$
6	$x^6 + x^4 + x^3 + x + 1$
7	$x^7 + x + 1$
8	$x^8 + x^4 + x^3 + x^2 + 1$

Table 3: All switching classes of APN's in $\mathbb{F}_2^5$

$n = 5$	
No.	$F(x)$
1.1	x^3
1.2	x^5
2.1	x^{-1}

Table 4: Invariants of switching classes in Table 3

$n = 5$					
No.	Γ-rank	Δ-rank	$\lvert\mathrm{Aut}(\mathrm{dev}(G_F))\rvert/2^{10}$	$\lvert\mathrm{Aut}(\mathrm{dev}(D_F))\rvert/2^{10}$	Walsh spectrum
1.1	330	42	$2^5 \cdot 5 \cdot 31$	$2^5 \cdot 5 \cdot 31$	classical
1.2	330	42	$2^5 \cdot 5 \cdot 31$	$2^{10} \cdot 5 \cdot 31$	classical
2.1	496	232	$2 \cdot 5 \cdot 31$	$2 \cdot 5 \cdot 31$	non-classical, see [33]

Table 5: Known switching classes of APN's in $\mathbb{F}_2^6$

$n = 6$		
No.	No. in [8]	F(x)
1.1	1	x^3
1.2	2	$x^3 + u^{11}x^6 + ux^9$
2.1	3	$ux^5 + x^9 + u^4x^{17} + ux^{18} + u^4x^{20} + ux^{24} + u^4x^{34} + ux^{40}$
2.2	4	$u^7x^3 + x^5 + u^3x^9 + u^4x^{10} + x^{17} + u^6x^{18}$
2.3	5	$x^3 + ux^{24} + x^{10}$
2.4	6	$x^3 + u^{17}(x^{17} + x^{18} + x^{20} + x^{24})$
2.5	7	$x^3 + u^{11}x^5 + u^{13}x^9 + x^{17} + u^{11}x^{33} + x^{48}$
2.6	8	$u^{25}x^5 + x^9 + u^{38}x^{12} + u^{25}x^{18} + u^{25}x^{36}$
2.7	9	$u^{40}x^5 + u^{10}x^6 + u^{62}x^{20} + u^{35}x^{33} + u^{15}x^{34} + u^{29}x^{48}$
2.8	10	$u^{34}x^6 + u^{52}x^9 + u^{48}x^{12} + u^6x^{20} + u^9x^{33} + u^{23}x^{34} + u^{25}x^{40}$
2.9	11	$x^9 + u^4(x^{10} + x^{18}) + u^9(x^{12} + x^{20} + x^{40})$
2.10	12	$u^{52}x^3 + u^{47}x^5 + ux^6 + u^9x^9 + u^{44}x^{12} + u^{47}x^{33} + u^{10}x^{34} + u^{33}x^{40}$
2.11	13	$u(x^6 + x^{10} + x^{24} + x^{33}) + x^9 + u^4x^{17}$
2.12	new	Theorem 11

Table 6: Known switching classes of APN's in $\mathbb{F}_2^6$: Invariants

$n=6$					
No.	Γ-rank	Δ-rank	$\lvert\mathrm{Aut}(\mathrm{dev}(G_F))\rvert/2^{12}$	$\lvert\mathrm{Aut}(\mathrm{dev}(D_F))\rvert/2^{12}$	Walsh spectrum
1.1	1102	94	$2^7 \cdot 3^3 \cdot 7$	$2^8 \cdot 3^3 \cdot 7$	classical
1.2	1146	94	$2^6 \cdot 3^2 \cdot 7$	$2^7 \cdot 3^2 \cdot 7$	classical
2.1	1158	96	$2^6 \cdot 5$	$2^6 \cdot 5$	classical
2.2	1166	94	$2^6 \cdot 7$	$2^7 \cdot 7$	classical
2.3	1166	96	$2^7 \cdot 7$	$2^7 \cdot 7$	classical
2.4	1168	96	2^6	2^6	classical
2.5	1170	96	$2^6 \cdot 5$	$2^6 \cdot 5$	$\{\ 0(1),\ -8(1176),\ 8(1512),\ 0(1071),\ 16(210),\ -16(126),\ 64(1)\ \}$
2.6	1170	96	2^6	2^6	classical
2.7	1170	96	2^6	2^6	classical
2.8	1170	96	2^6	2^6	classical
2.9	1172	96	2^6	2^6	classical
2.10	1172	96	2^6	2^6	classical
2.11	1174	96	2^6	2^6	classical
2.12	1300	152	2^3	2^3	classical

Table 7: Known switching classes of APN's in $\mathbb{F}_2^7$

$n=7$		
No.	No. in [8]	F(x)
1.1	1	x^3
1.2	7	$x^3 + \mathsf{tr}(x^9)$
2.1	8	$x^{34} + x^{18} + x^5$
2.2	11	$x^3 + x^{17} + x^{33} + x^{34}$
3.1	3	x^5
4.1	2	x^9
5.1	4	x^{13}
6.1	5	x^{57}
7.1	6	x^{-1}
8.1	9	$x^{65} + x^{10} + x^3$
9.1	13	$x^3 + x^9 + x^{18} + x^{66}$
10.1	14	$x^3 + x^{12} + x^{17} + x^{33}$
10.2	10	$x^3 + x^{17} + x^{20} + x^{34} + x^{66}$
11.1	15	$x^3 + x^{20} + x^{34} + x^{66}$
12.1	16	$x^3 + x^{12} + x^{40} + x^{72}$
13.1	12	$x^3 + x^5 + x^{10} + x^{33} + x^{34}$
14.1	17	$x^3 + x^6 + x^{34} + x^{40} + x^{72}$
14.2	18	$x^3 + x^5 + x^6 + x^{12} + x^{33} + x^{34}$
14.3	*new*	$u^2x^{96} + u^{78}x^{80} + u^{121}x^{72} + u^{49}x^{68} + u^{77}x^{66} + u^{29}x^{65} + u^{119}x^{48} + u^{117}x^{40} + u^{28}x^{36} + u^{107}x^{34} + u^{62}x^{33} + u^{125}x^{24} + u^{76}x^{20} + u^{84}x^{18} + u^{110}x^{17} + u^{49}x^{12} + u^{102}x^{10} + u^{69}x^9 + u^{14}x^6 + x^5 + x^3$

Table 8: Known switching classes of APN's in $\mathbb{F}_2^7$: Invariants

$n = 7$					
No.	Γ-rank	Δ-rank	$\lvert\mathrm{Aut}(\mathrm{dev}(G_F))\rvert/2^{14}$	$\lvert\mathrm{Aut}(\mathrm{dev}(D_F))\rvert/2^{14}$	Walsh spectrum
1.1	3610	198	$2^7 \cdot 7 \cdot 127$	$2^7 \cdot 7 \cdot 127$	classical
1.2	4026	212	$2^7 \cdot 7$	$2^7 \cdot 7$	classical
2.1	4034	210	$2^7 \cdot 7$	$2^7 \cdot 7$	classical
2.2	4040	212	$2^7 \cdot 7$	$2^7 \cdot 7$	classical
3.1	3708	198	$2^7 \cdot 7 \cdot 127$	$2^7 \cdot 7 \cdot 127$	classical
4.1	3610	198	$2^7 \cdot 7 \cdot 127$	$2^{14} \cdot 7 \cdot 127$	classical
5.1	4270	338	$7 \cdot 127$	$7 \cdot 127$	classical
6.1	4704	436	$7 \cdot 127$	$7 \cdot 127$	classical
7.1	8128	4928	$2 \cdot 7 \cdot 127$	$2 \cdot 7 \cdot 127$	non-classical, see [33]
8.1	4038	212	$2^7 \cdot 7$	$2^7 \cdot 7$	classical
9.1	4044	212	$2^7 \cdot 7$	$2^7 \cdot 7$	classical
10.1	4048	210	$2^7 \cdot 7$	$2^7 \cdot 7$	classical
10.2	4040	210	$2^7 \cdot 7$	$2^7 \cdot 7$	classical
11.1	4048	210	$2^7 \cdot 7$	$2^7 \cdot 7$	classical
12.1	4048	210	$2^7 \cdot 7$	$2^7 \cdot 7$	classical
13.1	4040	212	$2^7 \cdot 7$	$2^7 \cdot 7$	classical
14.1	4048	212	$2^7 \cdot 7$	$2^7 \cdot 7$	classical
14.2	4050	210	$2^7 \cdot 7$	$2^7 \cdot 7$	classical
14.3	4046	212	2^7	2^7	classical

Table 9: Known switching classes of APN's in $\mathbb{F}_2^8$

$n = 8$		
No.	No. in [8]	F(x)
1.1	1	x^3
1.2	2	x^9
1.3	5	$x^3 + \mathsf{tr} x^9$
1.4	6	$x^9 + \mathsf{tr} x^3$
1.5	7	$x^3 + u^{245}x^{33} + u^{183}x^{66} + u^{21}x^{144}$
1.6	8	$x^3 + u^{65}x^{18} + u^{120}x^{66} + u^{135}x^{144}$
1.7	new	$u^{188}x^{192} + u^{129}x^{144} + u^{172}x^{132} + u^{138}x^{129} + u^{74}x^{96} + u^{244}x^{72} + u^{22}x^{66} + u^{178}x^{48} + u^{150}x^{36} + u^{146}x^{33} + u^{6}x^{24} + u^{60}x^{18} + u^{80}x^{12} + u^{140}x^{9} + u^{221}x^{6} + u^{19}x^{3}$
1.8	new	$u^{37}x^{192} + u^{110}x^{144} + u^{40}x^{132} + u^{53}x^{129} + u^{239}x^{96} + u^{235}x^{72} + u^{126}x^{66} + u^{215}x^{48} + u^{96}x^{36} + u^{29}x^{33} + u^{19}x^{24} + u^{14}x^{18} + u^{139}x^{12} + u^{230}x^{9} + u^{234}x^{6} + u^{228}x^{3}$
1.9	new	$u^{242}x^{192} + u^{100}x^{144} + u^{66}x^{132} + u^{230}x^{129} + u^{202}x^{96} + u^{156}x^{72} + u^{254}x^{66} + u^{18}x^{48} + u^{44}x^{36} + u^{95}x^{33} + u^{100}x^{24} + u^{245}x^{18} + u^{174}x^{12} + u^{175}x^{9} + u^{247}x^{6} + u^{166}x^{3}$
1.10	new	$u^{100}x^{192} + u^{83}x^{144} + u^{153}x^{132} + u^{65}x^{129} + u^{174}x^{96} + u^{136}x^{72} + u^{46}x^{66} + u^{55}x^{48} + u^{224}x^{36} + u^{180}x^{33} + u^{179}x^{24} + u^{226}x^{18} + u^{54}x^{12} + u^{168}x^{9} + u^{89}x^{6} + u^{56}x^{3}$
1.11	new	$u^{77}x^{192} + u^{133}x^{144} + u^{47}x^{132} + u^{229}x^{129} + u^{23}x^{96} + u^{242}x^{72} + u^{242}x^{66} + u^{245}x^{48} + u^{212}x^{36} + u^{231}x^{33} + u^{174}x^{24} + u^{216}x^{18} + u^{96}x^{12} + u^{253}x^{9} + u^{154}x^{6} + u^{71}x^{3}$
1.12	new	$u^{220}x^{192} + u^{94}x^{144} + u^{70}x^{132} + u^{159}x^{129} + u^{145}x^{96} + u^{160}x^{72} + u^{74}x^{66} + u^{184}x^{48} + u^{119}x^{36} + u^{106}x^{33} + u^{253}x^{24} + ax^{18} + u^{90}x^{12} + u^{169}x^{9} + u^{118}x^{6} + +u^{187}x^{3}$
1.13	new	$u^{98}x^{192} + u^{225}x^{144} + u^{111}x^{132} + u^{238}x^{129} + u^{182}x^{96} + u^{125}x^{72} + u^{196}x^{66} + u^{219}x^{48} + u^{189}x^{36} + u^{199}x^{33} + u^{181}x^{24} + u^{110}x^{18} + u^{19}x^{12} + u^{175}x^{9} + u^{133}x^{6} + u^{47}x^{3}$
1.14	new	$u^{236}x^{192} + u^{212}x^{160} + u^{153}x^{144} + u^{185}x^{136} + u^{3}x^{132} + u^{89}x^{130} + u^{189}x^{129} + u^{182}x^{96} + u^{105}x^{80} + u^{232}x^{72} + u^{219}x^{68} + u^{145}x^{66} + u^{171}x^{65} + u^{107}x^{48} + u^{179}x^{40} + u^{227}x^{36} + u^{236}x^{34} + u^{189}x^{33} + u^{162}x^{24} + u^{216}x^{20} + u^{162}x^{18} + u^{117}x^{17} + u^{56}x^{12} + u^{107}x^{10} + u^{236}x^{9} + u^{253}x^{6} + u^{180}x^{5} + u^{18}x^{3}$
1.15	new	$u^{27}x^{192} + u^{167}x^{144} + u^{26}x^{132} + u^{231}x^{129} + u^{139}x^{96} + u^{30}x^{72} + u^{139}x^{66} + u^{203}x^{48} + u^{36}x^{36} + u^{210}x^{33} + u^{195}x^{24} + u^{12}x^{18} + u^{43}x^{12} + u^{97}x^{9} + u^{61}x^{6} + u^{39}x^{3}$
1.16	new	$u^{6}x^{192} + u^{85}x^{144} + u^{251}x^{132} + u^{215}x^{129} + u^{229}x^{96} + u^{195}x^{72} + u^{152}x^{66} + u^{173}x^{48} + u^{209}x^{36} + u^{165}x^{33} + u^{213}x^{24} + u^{214}x^{18} + u^{158}x^{12} + u^{146}x^{9} + x^{6} + u^{50}x^{3}$
1.17	new	$u^{164}x^{192} + u^{224}x^{144} + u^{59}x^{132} + u^{124}x^{129} + u^{207}x^{96} + u^{211}x^{72} + u^{5}x^{66} + u^{26}x^{48} + u^{20}x^{36} + u^{101}x^{33} + u^{175}x^{24} + u^{241}x^{18} + x^{12} + u^{15}x^{9} + u^{217}x^{6} + u^{212}x^{3}$
2.1	4	$x^3 + x^{17} + u^{16}(x^{18} + x^{33}) + u^{15}x^{48}$
3.1	9	$x^3 + u^{24}x^6 + u^{182}x^{132} + u^{67}x^{192}$
4.1	10	$x^3 + x^6 + x^{68} + x^{80} + x^{132} + x^{160}$
5.1	11	$x^3 + x^5 + x^{18} + x^{40} + x^{66}$
6.1	12	$x^3 + x^{12} + x^{40} + x^{66} + x^{130}$
7.1	3	x^{57}

Table 10: Known switching classes of APN's in $\mathbb{F}_2^8$: Invariants

$n = 8$				
No.	Γ-rank	Δ-rank	$\lvert\mathcal{M}(G_F))\rvert$	Walsh spectrum
1.1	11818	420	$2^{11} \cdot 255$	classical
1.2	12370	420	$2^{11} \cdot 255$	classical
1.3	13800	432	$2^{11} \cdot 3$	classical
1.4	13804	434	$2^{11} \cdot 3$	classical
1.5	13842	436	$2^{10} \cdot 3$	classical
1.6	13848	438	$2^{10} \cdot 3$	classical
1.7	14034	438	$2^{8} \cdot 3$	classical
1.8	14032	438	$2^{10} \cdot 3$	classical
1.9	14036	438	$2^{10} \cdot 3$	classical
1.10	14036	438	$2^{9} \cdot 3$	classical
1.11	14032	438	$2^{10} \cdot 3$	classical
1.12	14034	438	$2^{10} \cdot 3$	classical
1.13	14030	438	$2^{9} \cdot 3$	classical
1.14	14046	454	2^{9}	classical
1.15	14036	438	$2^{8} \cdot 3$	classical
1.16	14032	438	$2^{9} \cdot 3$	classical
1.17	14028	438	$2^{9} \cdot 3$	classical
2.1	13200	414	$2^{10} \cdot 3^2 \cdot 5$	classical
3.1	14024	438	$2^{10} \cdot 3$	classical
4.1	14040	454	2^{11}	classical
5.1	14044	446	2^{11}	classical
6.1	14046	438	2^{11}	classical
7.1	15358	960	$2^{3} \cdot 255$	classical

References

[1] T. D. Bending and D. Fon-Der-Flaass, *Crooked functions, bent functions, and distance regular graphs*, Electron. J. Combin., 5 (1998), pp. Research Paper 34, 14 pp. (electronic).

[2] T. Beth, D. Jungnickel, and H. Lenz, *Design Theory*, Cambridge University Press, Cambridge, 2 ed., 1999.

[3] J. Bierbrauer and G. M. Kyureghyan, *Crooked binomials*, Des. Codes Cryptogr., 46 (2008), pp. 269–301.

[4] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language.* J. Symbolic Comput., 24(3-4):235-265, 1997

[5] C. Bracken, E. Byrne, N. Markin, and G. McGuire, *Quadratic almost perfect nonlinear functions with many terms.* IACR Cryptology ePrint Archive: 2007/115, 2007.

[6] M. Brinkmann and G. Leander, *On the classification of APN functions up to dimension five*, in Abstract Book of the Workshop on coding and cryptography, N. S. D. Augo and J.-P. Tillich, eds., INRIA, 2007, pp. 39–48.

[7] ——, *On the classification of apn functions up to dimension five*, Des., Codes, Cryptogr., (2008).

[8] K. Browning, J. Dillon, R. Kibler, and M. McQuistan, *APN polynomials and related codes.* submitted, 2008.

[9] A.E. Brouwer and L.M.G.M. Tolhuizen, *A Sharpening of the Johnson Bound for Binary Linear Codes*, Designs, Codes and Cryptography, Vol. 3, No. 1 (1993) pp. 95-98.

[10] L. Budaghyan and C. Carlet, *Classes of quadratic APN trinomials and hexanomials and related structures.* IACR Cryptology ePrint Archive: 2007/098, 2006.

[11] L. Budaghyan, C. Carlet, and G. Leander, *A class of quadratic APN binomials inequivalent to power functions.* IACR Cryptology ePrint Archive: 2006/445, 2006.

[12] ——, *Another class of quadratic APN binomials over F_{2^n}: the case n divisible by 4*, in Abstract Book of the Workshop on coding and cryptography, N. S. D. Augo and J.-P. Tillich, eds., INRIA, 2007, pp. 49–58.

[13] ——, *Constructing new APN functions from known ones.* `http://eprint.iacr.org/`, 2007.

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

[15] L. Budaghyan and T. Helleseth, *New perfect nonlinear monomials over $\mathbf{f}_{p^{2k}}$ for any odd prime p.* to be presented at SETA '08.

[16] E. Byrne, C. Bracken, N. Markin, and G. McGuire, *New families of quadratic almost perfect nonlinear trinomials and multinomials.* preprint, available online at: `http://mathsci.ucd.ie/~gmg/`, 2007.

[17] E. Byrne and G. McGuire, *Certain new quadratic APN functions are not APN infinitely often*, in Abstract Book of the Workshop on coding and cryptography, N. S. D. Augo and J.-P. Tillich, eds., INRIA, 2007, pp. 59–68.

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

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

[20] J. Dillon and H. Dobbertin, *New cyclic difference sets with Singer parameters.*, Finite Fields Appl., 10 (2004), pp. 342–389.

[21] J. F. Dillon. slides from talk given at "Polynomials over Finite Fields and Appliocations", held at Banff International Research Station, 2006.

[22] C. Ding and J. Yuan, *A new family of skew Paley-Hadamard difference sets*, J. Comb. Theory Ser.A, 113 (2006), pp. 1526–1535.

[23] H. Dobbertin, *Almost perfect nonlinear power functions on GF*(2^n)*: The Niho case*, Information and Computation, 151 (1999), pp. 57–72.

[24] ——, *Almost perfect nonlinear power functions on* $\mathrm{GF}(2^n)$*: the Welch case*, IEEE Trans. Inform. Theory, 45 (1999), pp. 1271–1275.

[25] ——, *Almost perfect nonlinear power functions on GF*(2^n)*: A new case for n divisible by* 5, in Proceedings of the conference on Finite Fields and Applications, Augsburg 1999, D. Jungnickel and H. Niederreiter, eds., Berlin, 2001, Springer-Verlag, pp. 113–121.

[26] Y. Edel, G. Kyureghyan, and A. Pott, *A new APN function which is not equivalent to a power mapping*, IEEE Trans. Inform. Theory, 52 (2006), pp. 744–747.

[27] R. Gold, *Maximal recursive sequences with* 3*-valued recursive cross-correlation function*, IEEE Trans. Inf. Th., 14 (1968), pp. 154–156.

[28] S. W. Golomb and G. Gong, *Signal design for good correlation*, Cambridge University Press, Cambridge, 2005. For wireless communication, cryptography, and radar.

[29] F. Göloğlu and A. Pott, *Almost perfect nonlinear functions: A possible geometric approach (25 pages).* Presented at Academic Contact Forum *Coding Theory and Cryptography*, Brussels, 2008.

[30] H. Janwa and R. M. Wilson, *Hyperplane sections of Fermat varieties in* $\mathbf{P}^3$ *in* char. 2 *and some applications to cyclic codes*, in Applied algebra, algebraic algorithms and error-correcting codes (San Juan, PR, 1993), vol. 673 of Lecture Notes in Comput. Sci., Springer, Berlin, 1993, pp. 180–194.

[31] T. Kasami, *The weight enumerators for several classes of subcodes of the* 2*nd order binary Reed-Muller codes*, Information and Control, 18 (1971), pp. 369–394.

[32] G. M. Kyureghyan, *Crooked maps in* $\mathbb{F}_{2^n}$, Finite Fields Appl., 13 (2007), pp. 713–726.

[33] G. Lachaud and J. Wolfmann, *The weights of the orthogonals of the extended quadratic binary Goppa codes*, IEEE Trans. Inform. Theory, 36 (1990), pp. 686–692.

[34] R. Lidl and H. Niederreiter, *Finite Fields*, vol. 20 of Encyclopedia of Mathematics and its Applications, Cambridge University Press, 2nd ed., 1997.

[35] K. Nyberg, *Differentially uniform mappings for cryptography*, in Advances in Cryptography. EUROCRYPT'93, vol. 765 of Lecture Notes in Computer Science, New York, 1994, Springer-Verlag, pp. 55–64.

[36] Z. Zha, G. M. Kyureghyan, and X. Wang, *A new family of perfect nonlinear binomials.* submitted, 2008.