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

On the Equivalence of Quadratic APN Functions

Carl Bracken · Eimear Byrne · Gary McGuire · Gabriele Nebe

Received: date / Accepted: date

Abstract Establishing the CCZ-equivalence of a pair of APN functions is generally quite difficult. In some cases, when seeking to show that a putative new infinite family of APN functions is CCZ inequivalent to an already known family, we rely on computer calculation for small values of n. In this paper we present a method to prove the inequivalence of quadratic APN functions with the Gold functions. Our main result is that a quadratic function is CCZ-equivalent to the APN Gold function x^{2^r+1} if and only if it is EA-equivalent to that Gold function. As an application of this result, we prove that a trinomial family of APN functions that exist on finite fields of order 2^n where $n \equiv 2 \bmod 4$ are CCZ inequivalent to the Gold functions. The proof relies on some knowledge of the automorphism group of a code associated with such a function.

Keywords almost perfect nonlinear · APN · automorphism group · CCZ-equivalence · EA-equivalence · Gold function

Research supported by the Claude Shannon Institute, Science Foundation Ireland Grant 06/MI/006 and the Irish Research Council for Science, Engineering and Technology

E. Byrne
School of Mathematical Sciences, University College Dublin, Ireland
E-mail: ebyrne@ucd.ie

C. Bracken
School of Mathematical Sciences, University College Dublin, Ireland
E-mail: carlbracken@yahoo.com

G. McGuire
School of Mathematical Sciences, University College Dublin, Ireland
E-mail: gary.mcguire@ucd.ie

G. Nebe
Lehrstuhl D für Mathematik, RWTH Aachen University, 52056 Aachen, Germany
E-mail: Gabriele.Nebe@rwth-aachen.de

1 Introduction

Let L be a finite field. A function $f : L \longrightarrow L$ is said to be *almost perfect nonlinear* (APN) if the number of solutions in L of the equation

$$f(x+a) - f(x) = b \tag{1}$$

is at most 2, for all $a, b \in L$, $a \neq 0$. If the number of solutions of (1) in L is at most δ, we say f is differentially δ-uniform. Thus APN is the same as differentially 2-uniform. A differentially 1-uniform function is also called a perfect nonlinear function, or a planar function; however, these do not exist in characteristic 2 because in that case if x is a solution of (1), so is $x + a$. In this paper we only consider finite fields of characteristic 2.

The classical example of an APN function is $f(x) = x^3$, which is APN (over any field) because (1) is quadratic. These were generalized to the Gold functions $f(x) = x^{2^r+1}$, which are APN over $\mathbb{F}_{2^n}$ if $(n, r) = 1$.

APN functions were introduced in [7] by Nyberg, who defined them as the mappings with highest resistance to differential cryptanalysis. Since then many papers have been written on APN functions, although not many different families of such functions are known. For some time the list of known (extended affine) inequivalent APN functions comprised only monomial functions and was conjectured to be complete. Since 2006 several new families of non-monomial APN functions have been discovered. Two binomial families are presented in Budaghyan-Carlet-Leander [3]. Two infinite families, one of which generalizes the binomial family, were discovered in [2]. One of these families consists of the trinomials in Equation (2) below, which we will study in Sections 5 and 6.

An important aspect of this problem, after establishing the APN property is to check that the functions are really new, i.e. that they are *inequivalent* to the known APN families. The notions of equivalence most pervasive in the current literature are *extended affine* (EA) and *Carlet-Charpin-Zinoviev* (CCZ) equivalence [4]. EA-equivalence is finer than CCZ-equivalence and is usually somewhat easier to establish.

Two functions $f, g : L \longrightarrow L$ are called EA-equivalent if there exist affine permutations A_1, A_2 and an affine map A such that $g = A_1 \circ f \circ A_2 + A$. The differential uniformity of a function is an invariant of EA-equivalence. However, a bijective function is not necessarily EA-equivalent to its inverse, even though they have the same differential uniformity.

Two functions are called CCZ-equivalent if the graph of one can be obtained from the graph of the other by an affine permutation of the product space. Differential uniformity and resistance to linear and differential attacks are invariants of CCZ-equivalence, and unlike EA-equivalence, any permutation *is* always CCZ-equivalent to its inverse.

In the instance that a function $f : L \longrightarrow L$ is *quadratic*, the map $f(x+y)+f(x)+f(y)$ is bilinear. Therefore, the problem of testing the APN property of f is reduced to obtaining an estimate on the size of the kernel of the linear map $f(x+a)+f(x)+f(a)$. For this reason, most of the known non-monomial APN functions are in fact quadratic.

It turns out that in the case of quadratic functions the problem of establishing CCZ equivalence can sometimes be reduced to checking EA-equivalence. Yves Edel has asked recently in some conference presentations whether any two quadratic APN functions are CCZ-equivalent if and only if they are EA-equivalent. The main result of this paper is a partial answer: we prove that a quadratic APN function is CCZ-equivalent to a Gold function if and only if it is EA-equivalent to that Gold function.

Up to now, proofs that CCZ-equivalence implies EA-equivalence have been by lengthy brute force computations for specific functions; see the proof of Theorem 4 in [3], for example. Our result is more general, holding for any quadratic function, and the proof is by different methods. Our methods will involve a study of the automorphism group of a code determined by a quadratic function. For the Gold functions, this group is known and has been determined by Berger [1]. We combine our main result with a study of the automorphism group to show that a new family of APN functions found by Bracken-Byrne-Markin-McGuire are CCZ inequivalent to any Gold function. This family is a subclass of that given in [2] and has the following description. Let k and s be odd coprime integers, let $b, c \in \mathbb{F}_{2^{2k}}$ with $c \notin \mathbb{F}_{2^k}$, and b a primitive element of $\mathbb{F}_{2^{2k}}$. The polynomials of the form

$$f_s(x) = bx^{2^s+1} + (bx^{2^s+1})^{2^k} + cx^{2^k+1} \tag{2}$$

are APN on $\mathbb{F}_{2^{2k}}$. Previously, these polynomials were demonstrated in [2] to be inequivalent in general to x^{2^r+1} by using a computer to show the result for $k = 3$ and $k = 5$.

This paper is organized as follows. In Section 2 we discuss some general background, including the important connections between an APN function and a certain associated code. Section 3 discusses the particular case of quadratic APN functions, and introduces the property we use in this paper. In Section 4 we present our main result, which proves that any quadratic APN function that is CCZ-equivalent to a Gold function must be EA-equivalent to that Gold function. Section 5 proves some results about automorphisms of family of APN functions in Equation (2), and Section 6 applies the results of the paper to that family.

2 Equivalence of APN functions and codes.

Throughout the paper we fix a finite field $K := \mathbb{F}_{2^n}$ of characteristic 2. Let Tr denote the absolute trace map from K to $\mathbb{F}_2$. We write $\mathbb{F}_2^{2^n} = \mathbb{F}_2^K$, implicitly fixing an ordering of K. To a function $f : K \to K$ we associate a linear code $C_f \leq \mathbb{F}_2^{2^n} = \mathbb{F}_2^K$ as

$$C_f := \{c^f_{\alpha,\beta,\epsilon} \mid \alpha, \beta \in K, \epsilon \in \mathbb{F}_2\}$$

where

$$c^f_{\alpha,\beta,\epsilon} : K \to \mathbb{F}_2, x \mapsto \mathrm{Tr}(\alpha x) + \mathrm{Tr}(\beta f(x)) + \epsilon.$$

It was first observed in [4] that the dual code of C_f has minimum distance 6 if and only if f is APN. Also [2, Thm. 6] (first stated by John Dillon in a talk given at Banff in 2006 and later in [5]) shows that two functions f, g are CCZ-equivalent if and only if the associated linear binary codes C_f and C_g are equivalent. Recall that two codes $C, D \leq \mathbb{F}_2^N$ are *equivalent*, if there is some permutation $\pi \in S_N$ of the coordinate places with $\pi(C) = D$. Explicitly,

$$\pi(C) = \{c^f_{\alpha,\beta,\epsilon}\pi \mid \alpha, \beta \in K, \epsilon \in \mathbb{F}_2\}$$

where

$$c^f_{\alpha,\beta,\epsilon}\pi = x \mapsto \mathrm{Tr}(\alpha x\pi) + \mathrm{Tr}(\beta f(x\pi)) + \epsilon.$$

The *automorphism group* of a code C is defined as

$$\mathrm{Aut}(C) := \{\pi \in S_N \mid \pi(C) = C\}.$$

Remark 1 Identifying the places of the codes with the elements of K, we obtain certain canonical permutation groups:

(a) $E := (K, +)$, the additive group of K, isomorphic to $\mathbb{Z}_2^n$, acting regularly on K by $a : K \to K, x \mapsto a + x$.
(b) $M := K^*$, the multiplicative group of K, isomorphic to $\mathbb{Z}_{2^n-1}$ acting on K by $a : K \to K, x \mapsto ax$. Note that K^* fixes 0 and acts regularly on $K \setminus \{0\}$.
(c) $\Gamma := \mathrm{Gal}(K/\mathbb{F}_2) = \langle\sigma\rangle \cong \mathbb{Z}_n$, the Galois group of K acting on K as the *Frobenius automorphism* $\sigma : K \to K, x \mapsto x^2$.

This paper mainly treats the important class of *quadratic* APN functions $f : K \to K$. Recall that the polynomial $f \in K[x]$ is quadratic if for any non-zero $k \in K$, the function $f(x + k) + f(x) + f(k)$ is a linearized polyomial in x, or equivalently, if it is $\mathbb{F}_2$-linear. The family of trinomials (2) is quadratic, as is x^{2^r+1}.

The following proposition is well known – it states that the additive group of the field is contained in the automorphism group of a quadratic function.

Proposition 1 *Let $f : K \longrightarrow K$ be quadratic. Then $(K, +) \leq \mathrm{Aut}(C_f)$.*

Proof Since f is quadratic, for each $k \in K$ we may write $L(x+k) := f(x+k)+f(x)+f(k) = \sum_i k_i x^{2^i}$ for some $k_i \in K$. Using this and that fact that $\mathrm{Tr}(a) = \mathrm{Tr}(a^2)$ for each $a \in K$ we obtain:

$$\begin{aligned}
\pi_k(c^f_{\alpha,\beta,\epsilon}(x)) &= c^f_{\alpha,\beta,\epsilon}(x + k) \\
&= \mathrm{Tr}(\alpha(x + k)) + \mathrm{Tr}(\beta f(x + k)) + \epsilon \\
&= \mathrm{Tr}(\alpha x) + \mathrm{Tr}(\beta(L(x + k) + f(x) + f(k))) + \mathrm{Tr}(\alpha k) + \epsilon \\
&= \mathrm{Tr}(\alpha x) + \mathrm{Tr}(\beta L(x + k)) + \mathrm{Tr}(\beta f(x)) + \mathrm{Tr}(\beta f(k)) + \mathrm{Tr}(\alpha k) + \epsilon \\
&= \mathrm{Tr}(\alpha x) + \mathrm{Tr}(\sum_i (\beta k_i)^{2^{-i}} x) + \mathrm{Tr}(\beta f(x)) + \mathrm{Tr}(\beta f(k)) + \mathrm{Tr}(\alpha k) + \epsilon \\
&= c^f_{\alpha',\beta,\epsilon'}(x)
\end{aligned}$$

where $\alpha' = \alpha + \sum_i (\beta k_i)^{2^{-i}}$ and $\epsilon' = \epsilon + \mathrm{Tr}(\beta f(k)) + \mathrm{Tr}(\alpha k)$. It follows that the map

$$\pi_k : C_f \longrightarrow C_f : c^f_{\alpha,\beta,\epsilon}(x) \mapsto c^f_{\alpha,\beta,\epsilon}(x + k)$$

is an automorphism of C_f.

□

We recall some basic definitions from group theory. Further background reading may be read in [8]

Definition 1 Let G be a group and let H, N be subgroups of G, with N normal.

1. The *normalizer* of H in G, denoted $N_G(H)$, is the subgroup of G comprising all $g \in G$ such that $gHg^{-1} = H$.
2. The *centralizer* of H in G, for which we write $C_G(H)$ is the subgroup of G comprising all $g \in G$ such that $ghg^{-1} = h$ for all $h \in H$.
3. If $N \cap H$ is the identity then the group NH is called the *semi-direct product* of N and H and we write $N : H$.

For the remainder, we will write $\mathcal{A} := N_{S_{2^n}}(K,+)$ to denote the normalizer of $(K,+)$ in the symmetric group on 2^n elements.

This normalizer $\mathcal{A}$ plays the key role in establishing EA-equivalence via Theorem 1 below.

Proposition 2 *The normalizer $\mathcal{A}$ of $(K,+)$ in the symmetric group is the full affine group. That is,*

$$\mathcal{A} = (K,+) : \mathrm{GL}_n(\mathbb{F}_2) \cong (\mathbb{Z}_2^n) : \mathrm{GL}_n(\mathbb{F}_2).$$

Proof Since conjugation is a group automorphism, we obtain a group homomorphism from the normalizer into the automorphism group

$$\kappa : \mathcal{A} \to \mathrm{Aut}(K,+) \cong \mathrm{GL}_n(\mathbb{F}_2), \pi \mapsto (e \mapsto \pi e \pi^{-1}).$$

Clearly, the kernel of κ is the centralizer $C_{S_{2^n}}(K,+)$ of $(K,+)$ in S_{2^n} and so $\mathcal{A}/C_{S_{2^n}}(K,+) \cong \mathrm{GL}_n(\mathbb{F}_2)$. Now $(K,+)$ acts regularly on itself via $\pi_k : x \mapsto x+k$. We claim that $C_{S_{2^n}}(K,+) = (K,+)$. It is clear that $(K,+) \subseteq C_{S_{2^n}}(K,+)$, since $(K,+)$ is abelian. To see the converse inclusion let $\theta \in C_{S_{2^n}}(K,+)$. Composing θ with the inverse of the permutation $\pi_{\theta(0)} \in (K,+)$ we may assume that $\pi(0) = 0$. By assumption, $\theta = \pi_k \theta \pi_{-k}$ for all $k \in K$ and hence $\theta(x) = \theta(x-k)+k$ for all $x, k \in K$. In particular this gives $\theta(k) = k$ for all k, so that θ is the identity. We deduce that $C_{S_{2^n}}(K,+) = (K,+)$. The elements in $\mathrm{GL}_n(\mathbb{F}_2)$ stabilize $0 \in K$, hence $(K,+)$ meets $\mathrm{GL}_n(\mathbb{F}_2)$ at the identity and we conclude that the normalizer $\mathcal{A}$ is the semidirect product as given in the proposition.

□

Remark 2 The group $\mathcal{A}$ is also the automorphism group, $\mathcal{A} = \mathrm{Aut}(C_0)$, of the first-order Reed-Muller code (see [6, Ch. 13, Sec. 9])

$$C_0 = \{c_{\alpha,0,\epsilon} \mid \alpha \in K, \epsilon \in \mathbb{F}_2\}.$$

The next 'folklore' result is an important reformulation of EA-equivalence in terms of codes. To our knowledge a proof has not appeared in literature. We include a proof here for completeness.

Theorem 1 *$\mathcal{A}$ acts on $\{C_f \mid f : K \to K\}$. Functions f and g are EA-equivalent functions if and only if the codes C_f and C_g are in the same $\mathcal{A}$-orbit.*

In the proof it will be convenient to work with generator matrices. Let $N := 2^n$ denote the length of the code C_f. By a generator matrix G for C_f we mean a matrix G with row-space C_f. Choosing an $\mathbb{F}_2$-basis $(b_1, \ldots, b_n)$ of K we obtain a generator matrix of the form $G = \begin{pmatrix} \mathbf{1} \\ G_0' \\ G_f \end{pmatrix}$ where $\mathbf{1} \in \{1\}^{1\times N}$ denotes the row consisting of 1 only and $G_0', G_f \in \mathbb{F}_2^{n\times N}$ are defined by indexing the columns with the elements of K as

$$(G_0')_{i,x} := \mathrm{Tr}(b_i x), \quad (G_f)_{i,x} := \mathrm{Tr}(b_i f(x)). \quad (\star)$$

Note that $G_0 := \begin{pmatrix} \mathbf{1} \\ G_0' \end{pmatrix} \in \mathbb{F}_2^{(n+1)\times N}$ is a generator matrix for the first-order Reed-Muller code C_0.

The following Lemma is of independent interest.

Lemma 1 *Let $f, g : K \to K$. Then $C_f = C_g$ if and only if $g = A_1 \circ f + A$ for some affine permutation A_1 and some affine map A.*

Proof Let $G = \begin{pmatrix} \mathbf{1} \\ G_0' \\ G_f \end{pmatrix}$ and $G' = \begin{pmatrix} \mathbf{1} \\ G_0' \\ G_g \end{pmatrix}$ be generator matrices of C_f resp. C_g as above. Then $C_f = C_g$ if and only if G and G' have the same rowspace, if and only if there are $B_1 \in \mathrm{GL}_n(\mathbb{F}_2)$, $B \in \mathbb{F}_2^{n \times n}$, $t \in \mathbb{F}_2^{n \times 1}$ such that

$$G_g = B_1 G_f + B G_0' + t\mathbf{1}.$$

By $(\star)$ above, this means that for all $x \in K$ and all $1 \leq i \leq n$

$$\mathrm{Tr}(b_i g(x)) = \mathrm{Tr}(B_1 b_i f(x)) + \mathrm{Tr}(B b_i x) + t_i$$

and hence $g = A_1 \circ f + A$ with $A_1 = (B_1^{\mathrm{ad}}, 0)$ and $A = (B^{\mathrm{ad}}, t)$ where a^{ad} denotes the adjoint linear map of a with respect to the trace bilinear form. A similar calculation shows the converse.

□

Proof of Theorem 1: **(1)** We first show that

$$\{C_f \mid f : K \to K\} = \{C \leq \mathbb{F}_2^K \mid C_0 \subseteq C, \dim(C) \leq 2n+1\},$$

and in particular that $\mathcal{A} = \mathrm{Aut}(C_0)$ acts on this set.
The inclusion $\subseteq$ is clear. So let $C \leq \mathbb{F}_2^K$ be a code of dimension $\leq 2n+1$ that contains C_0 and let

$$G = \begin{pmatrix} G_0 \\ G_1 \end{pmatrix} \in \mathbb{F}_2^{(2n+1) \times N}$$

be a generator matrix of C. Let $T \in \mathbb{F}_2^{n \times n}$ denote the Gram matrix of the basis $(b_1, \ldots, b_n)$ of K with respect to the trace bilinear form,

$$T_{i,j} = \mathrm{Tr}(b_i b_j).$$

Then $T \in \mathrm{GL}_n(\mathbb{F}_2)$ by the non degeneracy of the trace. For $x \in K$ let f_x denote the column of index x of $T^{-1}G_1$ and define $f : K \to K$ by $f(x) := \sum_{i=1}^{d} (f_x)_i b_i \in K$ the corresponding element in K. Then $G_1 = G_f$ and hence $C = C_f$.
(2) Now let $f, g : K \to K$ be EA-equivalent, so there are affine permutations A_1, A_2 and an affine mapping A such that $g = (A_1 \circ f \circ A_2) + A$. We have to show that C_g and C_f are in the same orbit under $\mathcal{A}$. By Lemma 1 we may assume that $A_1 = 1$ and $A = 0$ and hence that $g = f \circ A_2$ for some $A_2 \in (K, +) : \mathrm{GL}_{\mathbb{F}_2}(K) \cong \mathcal{A}$. This means that $g(x) = f(A_2(x))$ and A_2 induces a permutation of the places $x \in K$ that are in $\mathcal{A}$.
(3) Finally we prove the converse implication. Assume that there is some $\pi \in \mathcal{A}$ such that $C_f = \pi(C_g)$. Let $G = \begin{pmatrix} \mathbf{1} \\ G_0' \\ G_g \end{pmatrix}$ be the generator matrix of C_g as above. Then $\pi(C_g) = C_f$ has a generator matrix

$$G\pi = \begin{pmatrix} \mathbf{1} \\ G_0'\pi \\ G_g\pi \end{pmatrix}$$

obtained by multiplying G with the permutation matrix π from the right. Since π fixes the code C_0, there is $A \in \mathrm{GL}_n(\mathbb{F}_2)$ and $t \in \mathbb{F}_2^{n\times 1}$ such that

$$G_0'\pi = AG_0' + t\mathbf{1}.$$

Therefore there are matrices $t_1 \in \mathbb{F}_2^{n\times 1}, B_1 \in \mathbb{F}_2^{n\times n}, A_1 \in \mathrm{GL}_n(\mathbb{F}_2)$ s.t.

$$\left(\begin{array}{c|c|c} 1 & 0 & 0 \\ \hline t & A & 0 \\ \hline t_1 & B_1 & A_1 \end{array}\right)\left(\begin{array}{c} \mathbf{1} \\ \hline G_0'\pi \\ \hline G_g\pi \end{array}\right) = \left(\begin{array}{c} \mathbf{1} \\ \hline G_0' \\ \hline G_f \end{array}\right)$$

reading as

$$G_f = A_1G_g\pi + B_1G_0' + t_1\mathbf{1} = G_{A_1\circ g\circ\pi+(B_1,t_1)}.$$

Since π is an affine permutation, and (B_1, t_1) is an affine mapping this yields that $f = A_1 \circ g \circ \pi + (B_1, t_1)$ is EA-equivalent to g. □

3 Quadratic APN functions

We now consider quadratic APN functions h satisfying the property that all regular elementary abelian subgroups of $\mathrm{Aut}(C_h)$ are conjugate to $(K, +)$. We will show that such functions satisfy Edel's conjecture, i.e., that CCZ-equivalence for this family implies EA-equivalence. In fact the APN property is not required in what follows. However, our interest in CCZ-equivalence is usually restricted to the class of APN functions.

Theorem 2 *Let h be a quadratic function such that $E := (K, +) \leq \mathrm{Aut}(C_h) =: H \leq S_{2^n}$. Assume that for all $\pi \in S_{2^n}$*

$$\pi E\pi^{-1} \leq H \Rightarrow \text{ there is some } h_\pi \in H \text{ such that } \pi E\pi^{-1} = h_\pi E h_\pi^{-1}.$$

If a quadratic function f is CCZ-equivalent to h then it is also EA-equivalent to h.

Proof Since f and h are CCZ-equivalent, there is $\pi \in S_{2^n}$ such that $\pi(C_f) = C_h$. The subgroup $E \leq \mathrm{Aut}(C_f)$ is hence conjugated to $\pi E\pi^{-1} \leq \mathrm{Aut}(C_h)$. By assumption this implies that $h_\pi^{-1}\pi$ normalizes E, and hence $h_\pi^{-1}\pi \in N_{S_{2^n}}(E) = \mathcal{A}$ and $h_\pi^{-1}\pi(C_f) = h_\pi^{-1}(C_h) = C_h$. By Theorem 1 this means that the two functions are EA-equivalent. □

Since all regular elementary abelian subgroups are conjugate in S_{2^n}, the following corollary is a reformulation of the theorem above and suggests one strategy to prove Edel's conjecture for arbitrary quadratic APN functions.

Corollary 1 *Let h be a quadratic function such that all regular elementary abelian subgroups of $\mathrm{Aut}(C_h)$ are conjugate to $(K, +)$. Then all quadratic functions f that are CCZ-equivalent to h are indeed EA-equivalent to h.*

Thus Edel's conjecture for APN functions is proved under the stated hypothesis of Corollary 1. We do not know any quadratic APN functions h for which the above property does not hold, i.e., for which $\mathrm{Aut}(C_h)$ contains more than one conjugacy class of regular elementary abelian subgroups. We checked that it holds for all known APN functions of degree up to 7. Note that this is not true for arbitrary functions, for example, linear functions f have $\mathrm{Aut}(C_f)$ equal to the affine linear group, which usually has several different conjugacy classes of elementary abelian subgroups of order 2^n.

4 Quadratic functions equivalent to the Gold function

Well understood examples of quadratic APN functions are the Gold functions

$$g : K \to K,\ x \mapsto x^{2^r+1}$$

for a fixed positive integer r satisfying $(r, n) = 1$. The automorphism group $\mathcal{G}$ of C_g contains some obvious automorphisms: the additive group of the field, the multiplicative group of the field, and the Galois automorphisms. Results of Berger [1] show that this is the full automorphism group, i.e.,

$$\mathcal{G} := \mathrm{Aut}(C_g) \cong (K, +) : K^* : \mathrm{Gal}(K/\mathbb{F}_2) = EM\Gamma$$

(in the notation of Remark 1) of order $|\mathcal{G}| = |E| \cdot |M| \cdot |\Gamma| = 2^n(2^n - 1)n$. The proof uses the classification of finite simple groups.

We recall some basic definitions.

Definition 2 Let G be a finite group and let H be a subgroup of G. We say that H is a p-subgroup of G if H has order p^r for some positive integer r. H is called a Sylow p-subgroup of G if r is the greatest positive integer such that p^r divides $|G|$.

The well-known second Sylow theorem states that all Sylow p-subgroups of a group G are conjugate in G. Since any subgroup that is normal in G forms its own conjugacy class, as a direct consequence of this Sylow theorem we have that if H is a normal Sylow p-subgroup of G then it is the unique subgroup of G of that order.

Lemma 2 *$(K, +)$ is the unique subgroup of $\mathcal{G}$ that is isomorphic to $\mathbb{Z}_2^n$.*

Proof This is clear, if n is odd, since then 2^n is the largest 2-power in $|\mathcal{G}|$ and $(K, +)$ is a Sylow 2-subgroup of $\mathcal{G}$, which must be unique since $(K, +)$ is normal in $\mathcal{G}$ and all such Sylow 2-subgroups are conjugate.
Assume now that $n = 2k$ is even and let $T \cong \mathbb{Z}_2^n$ be an elementary abelian subgroup of $\mathcal{G}$. Then any $x \in T$ satisfies $x^2 = 1$ so in particular $x^2 \in (K, +)$. Therefore T is a subgroup of $S := (K, +) : \langle\tau\rangle = \{x \in \mathcal{G} \mid x^2 \in (K, +)\}$, where $\tau = \sigma^k : z \mapsto z^{2^k} \in \mathrm{Gal}(K/\mathbb{F}_2)$ is the Galois automorphism of order 2. It is easy to check that the centralizer of τ in S is isomorphic to $(\mathbb{F}_{2^k}, +) \times \langle\tau\rangle$, which has order 2^{k+1}. Now consider the natural epimorphism $S \to S/(K, +) \cong \langle\tau\rangle$ and assume that the elementary abelian subgroup $T \leq S$ is not contained in the kernel of this map (i.e. assume that T is not equal to K). Then there exists some $s \in (K, +)$ such that $s\tau \in T$. Now T is abelian and is generated by $s\tau$ and $T \cap K$. Therefore $T \cap K$ has index 2 in T and so has order $|T|/2 = 2^{2k-1}$. Let $\theta \in T \cap K$. Then $s\tau\theta = \theta s\tau = s\theta\tau$, and hence θ commutes with τ. This shows that $T \cap K \subset C_S(\tau)$. But then $2^{2k-1} = |T \cap K| \leq |C_S(\tau)| = 2^{k+1} < 2^{2k-1}$, giving a contradiction. We deduce that $T = (K, +)$, and hence $(K, +)$ is the unique elementary abelian subgroup of order 2^{2k} of $\mathcal{G}$.

□

The main result of this paper, stated below, follows now from Lemma 2 and Corollary 1.

Theorem 3 *Let f be a quadratic APN function and g be a Gold function. If f and g are CCZ-equivalent, then they are EA-equivalent.*

Corollary 2 *Let h be a quadratic APN function such that $\mathrm{Aut}(C_h)$ is isomorphic to a subgroup of $\mathcal{G}$. Then all quadratic APN functions f that are CCZ-equivalent to h are indeed EA-equivalent to h.*

Regarding a proof of Edel's conjecture, we may indeed hope that the automorphism group of any quadratic APN function is contained in $\mathcal{G}$. If this were true, proving it would complete a proof of Edel's conjecture, thanks to Corollary 2. However, this is not true:

Example 1 Consider the quadratic functions given in [5] .

$$h_1 := x^3 + x^5 + u^{62}x^9 + u^3x^{10} + x^{18} + u^3x^{20} + u^3x^{34} + x^{40},$$

$$h_2 := x^3 + u^{11}x^5 + u^{13}x^9 + x^{17} + u^{11}x^{33} + x^{48},$$

and

$$h_3 := x^3 + x^{17} + u^{16}(x^{18} + x^{33}) + u^{15}x^{48}.$$

Then h_1 and h_2 are APN on $GF(2^6)$ and $|\mathrm{Aut}(C_{h_1})| = |\mathrm{Aut}(C_{h_2})| = 2^6.5$, which is not a divisor of $2^6(2^6-1)6$. The polynomial h_3 is APN on $GF(2^8)$ and $\mathrm{Aut}(C_{h_3})$ has order $2^{10}.3^2.5$, which does not divide $2^8(2^8-1)8$.

5 Automorphisms of Family (2)

We could now use Theorem 3 directly to establish CCZ-inequivalence of a member of Family (2) (or indeed any other quadratic) to the Gold functions by establishing EA-inequivalence, which can be achieved by a brute-force comparison of coefficients in the equation $g = A_1 \circ f \circ A_2 + A$.

Instead we find that further knowledge of the automorphism group associated with Family (2) allows us to show that for this family, CCZ-equivalence with the Gold functions holds not merely if and only if the corresponding codes are equivalent (EA-equivalence), but if and only if they are equal. Thus in this instance we can avoid applying brute-force.

Let k, s be odd coprime integers, $K = \mathbb{F}_{2^{2k}}$ and $L := \mathbb{F}_{2^k}$ the subfield of K of index 2. We denote by $T_2 : K \to L$ the relative trace of K to L.

We compute a subgroup $\mathcal{U}$ of the automorphism group of the APN functions in Family (2), which is big enough to allow us to prove that if a function f in Family (2) is EA-equivalent to a Gold function g, then $C_f = C_g$. We remark that the particular form of $f = T_2(bx^{2^s+1}) + cx^{2^k+1}$ is helpful in determining some of the automorphisms of C_f. Most other (known) APN functions do not have such a form, and determining their automorphisms seems to be difficult.

It will be helpful to us to parametrize f by s and $c \in K \backslash L$; we write

$$f = f_{c,s} := bx^{2^s+1} + (bx^{2^s+1})^{2^k} + cx^{2^k+1},$$

for any b primitive in K.

Since $f_{c,s}$ is an APN function, $\dim(C_{f_{c,s}}) = 4k+1$ (c.f. [4, Cor. 1]) and

$$C_{f_{c,s}} = \langle \mathbf{1} \rangle \oplus C_0 \oplus C_c = \langle c_{0,0,1} \rangle \oplus \{c_{\alpha,0,0} \mid \alpha \in K\} \oplus \{c^f_{0,\beta,0} \mid \beta \in K\}.$$

We claim the following.

Lemma 3 *Any two $c, d \in K \setminus L$ define the same codes, i.e., $C_c = C_d$.*

Proof For $c \in K \setminus L$ we have

$$f_{c,s}(x) = (bx^{2^s+1}) + (bx^{2^s+1})^{2^k} + cx^{2^k+1} = T_2(bx^{2^s+1}) + cx^{2^k+1}.$$

Note that for any $x \in K$ the element x^{2^k+1} lies in L. We have to show that the set $\{c^f_{0,\beta,0} \mid \beta \in K\}$ is independent of the choice of c. By the transitivity of the trace we obtain $c^f_{0,\beta,0}(x) = \mathrm{Tr}_{L/\mathbb{F}_2}(T_2(\beta f_{c,s}(x)))$ and

$$T_2(\beta f_{c,s}(x)) = T_2(\beta)T_2(bx^{2^s+1}) + T_2(\beta c)x^{2^k+1}.$$

Since the trace T_2 is nondegenerate and $(1, c)$ as well as $(1, d)$ form a basis of K over L, there is for any given pair $(T_2(\beta), T_2(\beta c))$ a unique $\beta' \in K$ such that

$$T_2(\beta') = T_2(\beta) \text{ and } T_2(\beta' d) = T_2(\beta c).$$

So the code C_c is independent of the choice of $c \in K \setminus L$.

□

Lemma 4 *We have $\mathbb{F}_4^* \subseteq \mathrm{Aut}(C_{f_{c,s}})$.*

Proof Let ω be a generator for $\mathbb{F}_4^*$. Since s and k are odd, the exponents $2^s + 1$ and $2^k + 1$ are both multiples of 3 and hence $f_{c,s}(\omega x) = f_{c,s}(x)$.

□

Lemma 5 *We have $L^* \subseteq \mathrm{Aut}(C_{f_{c,s}})$.*

Proof If $z \in L^*$ it is easy to check that $f_{c,s}(zx) = z^{2^s+1} f_{cz^{1-2^s}}(x)$. All transformations involved do not change the code $C_{f_{c,s}}$, using Lemma 3. So multiplication by a primitive element of L is an automorphism.

□

Hence we obtain the following result:

Theorem 4 $\mathrm{Aut}(C_{f_{c,s}})$ *contains a subgroup $\mathcal{U} \cong (K, +) : (\mathbb{F}_4^* \times L^*)$ of order $2^{2k} \cdot 3(2^k - 1)$.*

Note that $\mathrm{Aut}(C_{f_{c,s}})$ is not abelian, since the subgroup $\mathcal{U}$ we know about is not abelian.

For $s = 1$ we obtain one more automorphism giving rise to a subgroup of order $2^{2k} \cdot 3k \cdot (2^k - 1)$ of $\mathrm{Aut}(C_{f_{c,1}})$. We conjecture that this is the actual order. This has been verified by computer for $k = 3$ and $k = 5$.

Lemma 6 $\mathrm{Aut}(C_{f_{c,1}})$ *has an element δ of order $3k$, such that $\delta^k = \omega$ from Lemma 4.*

Proof Choose $c = b^{(2^k+1)/3}$. Then $c \in K \setminus L$ and by Lemma 3 we may assume without loss of generality that $f = f_{c,1}$. It is easily checked that $f_{c,1}(bx)$ is equal to $\sigma^2(f(x))$, where σ is the Frobenius automorphism of K over $\mathbb{F}_2$. Letting $T_b(f(x)) = f(bx)$, the map $\delta := \sigma^{-2} \circ T_b$ is hence an automorphism of C_{f_c}, and its order can be checked to be $3k$.

□

The automorphism groups of other families of APN functions do not appear to be as easy to work with as for Family (2). Therefore we have not been able to prove similar results for other families.

6 Inequivalence.

We apply the results of the previous sections to give a proof that Family (2) functions are not CCZ-equivalent to Gold functions.

Theorem 5 *Let $g : K \to K$ be a Gold-function and $f : K \to K$ be an APN function in Family (2). If f and g are EA-equivalent, then the associated codes C_f and C_g are equal.*

For the proof of the theorem we need two lemmas, the first one is surely well-known. Recall that if a group G acts on a set X and $a \in X$ then the *stabilizer subgroup* of a, denoted $\mathrm{Stab}_G(a)$ is the set of elements of G that fix a.

Lemma 7 $N_{\mathrm{GL}_n(\mathbb{F}_2)}(K^*) = K^* : \mathrm{Gal}(K/\mathbb{F}_2)$.

Proof Let $G = N_{\mathrm{GL}_n(\mathbb{F}_2)}(K^*)$. Clearly $K^* \leq G = K^*\mathrm{Stab}_G(1)$. So it is enough to show that the elements $\pi \in G$ with $\pi(1) = 1$ are indeed field automorphisms of K and therefore contained in $\mathrm{Gal}(K/\mathbb{F}_2)$. Choose $\pi \in G$ such that $\pi(1) = 1$. Since $\pi \in \mathrm{GL}_n(\mathbb{F}_2)$, the mapping π acts linearly on the set K and hence respects the addition. We now show that

$$\pi(ab) = \pi(a)\pi(b) \text{ for all } a, b \in K.$$

To see this let $\alpha, \beta \in K^* \subset S_n$ be such that $\alpha(1) = a, \beta(1) = b$. Since π normalizes K^*, also

$$\tilde{\alpha} := \pi\alpha\pi^{-1} \text{ and } \tilde{\beta} := \pi\beta\pi^{-1} \in K^*.$$

We calculate $\pi(a) = \pi(\alpha(1)) = (\pi\alpha\pi^{-1})(1) = \tilde{\alpha}(1)$ and similarly $\pi(b) = \tilde{\beta}(1)$. Clearly $ab = \alpha(\beta(1))$ and

$$\pi(ab) = (\pi\alpha\beta\pi^{-1})(1) = \tilde{\alpha}(\tilde{\beta}(1)) = \pi(a)\pi(b).$$

□

Lemma 8 *The group G from Lemma 7 contains a unique cyclic subgroup of order $3(2^k - 1)$.*

Proof All elements of G are of the form $a\gamma$ where $a \in K^*$ and $\gamma \in \mathrm{Gal}(K, \mathbb{F}_2)$. Assume that such an element $a\gamma$ has order $3(2^k - 1)$. Let ℓ be the order of γ. Then ℓ divides $2k = \ell m$ and also the order of $a\gamma$. We calculate

$$(a\gamma)^\ell = N_{K/\mathbb{F}_{2^m}}(a) \in \mathbb{F}_{2^m}^* \cong \mathbb{Z}_{2^m-1}.$$

So $a\gamma$ has order dividing $\ell(2^m - 1)$ and we conclude that

$$3(2^k - 1) \text{ divides } \ell(2^{2k/\ell} - 1)$$

from which we obtain that $\ell = 1$.

□

Proof (of Theorem 5) Assume that there is some $\pi \in \mathcal{A}$ with $\pi(C_f) = C_g$. We identify the places of the code with K. Since $\mathrm{Aut}(C_g)$ is 2-transitive on K (cf. [6]), we may assume without loss of generality that

$$\pi(0) = 0 \text{ and } \pi(1) = 1 \text{ so } \pi \in \mathrm{GL}_n(\mathbb{F}_2) = \mathrm{Stab}_{\mathcal{A}}(0).$$

Moreover π conjugates $\mathcal{U} \leq \mathrm{Aut}(C_f)$ into $\mathcal{G} = \mathrm{Aut}(C_g)$, and since π fixes 0, also

$$\mathbb{Z}_{3(2^k-1)} \cong \pi \mathrm{Stab}_{\mathcal{U}}(0)\pi^{-1} = \pi(L^* \times \mathbb{F}_4^*)\pi^{-1} \leq \mathrm{Stab}_{\mathcal{G}}(0) = K^* : \mathrm{Gal}(K, \mathbb{F}_2).$$

By Lemma 8 this implies that π normalizes $L^* \times \mathbb{F}_4^* \leq K^*$. Since L^* and $\mathbb{F}_4^*$ generate K as an $\mathbb{F}_2$-algebra, the linear span of the matrices in $L^* \times \mathbb{F}_4^*$ is equal to $K = K^* \cup \{0\} \subset \mathbb{F}_2^{n \times n}$. Therefore π also normalizes K and hence K^*, so $\pi \in \mathrm{Gal}(K, \mathbb{F}_2) \leq \mathcal{G}$ by Lemma 7. This proves the theorem since we have shown that any equivalence π between the codes C_f and C_g is indeed already contained in $\mathrm{Aut}(C_g)$.

□

Theorem 6 *$C_f \neq C_g$.*

Proof Suppose that $C_f = C_g$. Then given any $\epsilon \in \mathbb{F}_2$, $\alpha, \beta \in K$ there exist $\epsilon' \in \mathbb{F}_2$, $\alpha', \beta' \in K$ satisfying

$$\epsilon + \mathrm{Tr}(\alpha x) + \mathrm{Tr}(\beta(T_2(bx^{2^s+1}) + cx^{2^k+1})) = \epsilon' + \mathrm{Tr}(\alpha' x) + \mathrm{Tr}(\beta' x^{2^r+1}))$$

for all $x \in K$, so in particular we must have $\epsilon = \epsilon'$. Choose $\beta \in L$. Then we have $\mathrm{Tr}(\beta(T_2(bx^{2^s+1}))) = \mathrm{Tr}(T_2(\beta b x^{2^s+1})) = 0$ and so

$$\mathrm{Tr}((\alpha + \alpha')x) = \mathrm{Tr}(\beta c x^{2^k+1}) + \mathrm{Tr}(\beta' x^{2^r+1}),$$

for all $x \in K$. Using the linearity of the LHS we obtain

$$\mathrm{Tr}(\beta c(x^{2^k}a + xa^{2^k}) + \beta'(x^{2^r}a + xa^{2^r})) = \mathrm{Tr}((\beta x^{2^k}(c + c^{2^k}) + (\beta')^{2^{-r}} x^{2^{-r}} + \beta' x^{2^r})a) = 0,$$

for all $x, a \in K$. This implies that $\beta x(c + c^{2^k}) + (\beta')^{2^{k-r}} x^{2^{k-r}} + (\beta')^{2^k} x^{2^{k+r}} \in K[x]$ is identically zero, which, observing the degree of this polynomial and the fact that $(r, 2k) = 1$, we see is impossible unless $\beta = \beta' = 0$.

□

Remark 3 In fact this can also be readily seen by Lemma 1 by a simple comparison of coefficients.

We now combine the results of Theorems 5, 6 and Corollary 3 in the following statement.

Corollary 3 *The functions of Family 2 are not CCZ-equivalent to the Gold functions.*

Acknowledgements We thank the referees whose comments led to a much better presentation of this paper.

References

1. Berger, T.: On the automorphism groups of affine-invariant codes, Des. Codes Cryptogr., 7, 215–221 (1996) .
2. Bracken, C., Byrne, E., Markin, N., McGuire, G.: New Families of Quadratic Almost Perfect Nonlinear Trinomials and Multinomials, Finite Fields Appl., 14, 703–714 (2008) .
3. Budaghyan, L., Carlet, C., Leander, G.: Two classes of quadratic APN binomials inequivalent to power functions, IEEE Trans. Inform. Theory, 54, (9) 4218-4229 (2008).

4. Carlet, C., Charpin, P., Zinoviev, V.: Codes, bent functions and permutations suitable for DES-like cryptosystems, Des. Codes and Cryptogr., 15, (2) 125–156 (1998).
5. Browning, K., Dillon, J. F., Kibler, R. E., McQuistan, M.: APN polynomials and related codes, J. Comb. Inf. Syst. Sci., 34, 135-159 (2009).
6. MacWilliams, F.J., Sloane, N.J.: The Theory of Error-Correcting Codes, North Holland, Amsterdam, New York, Oxford, 1977.
7. Nyberg, K., Differentially uniform mappings for cryptography, Advances in Cryptology-EUROCRYPT 93, Lecture Notes in Comput. Sci., 765, 55-64 (1994).
8. Robinson, D.: A course in the theory of groups, Springer GTM 80 (1982).