J Algebr Comb (2012) 35:461–475
DOI 10.1007/s10801-011-0309-1

Equivalences of quadratic APN functions

Satoshi Yoshiara

Received: 24 March 2011 / Accepted: 8 August 2011 / Published online: 13 September 2011

Abstract The following conjecture due to Y. Edel is affirmatively solved: two quadratic APN (almost perfect nonlinear) functions are CCZ-equivalent if and only if they are extended affine equivalent.

Keywords APN functions · Quadratic functions · CCZ-equivalence · Extended affine equivalence

1 Introduction

In this paper, we will show the following statement, which was first conjectured by Edel (see Definition 2 and Definition 1 for the exact definitions of notions such as quadratic APN functions and CCZ- and EA-equivalences):

Theorem 1 *Let f and g be quadratic APN functions on a finite field $F \cong \mathbf{F}_{2^n}$ with $n \geq 2$. Then f is CCZ-equivalent to g if and only if f is EA-equivalent to g.*

In the recent paper [1], this statement is shown to be true under the assumption that the group of translations is the unique regular elementary abelian 2-subgroup of the automorphism group of a certain code [1, Corollary 4].

In this paper, Theorem 1 is established without any additional assumption. The only use of group theory here is the Sylow theorem and a typical argument on the centralizer of a regular permutation group. Some information, prepared in Sect. 2, about the actions of translations and the description of some graphs is

S. Yoshiara (✉)
Department of Mathematics, Tokyo Woman's Christian University, Suginami-ku, Tokyo 167-8585, Japan
e-mail: yoshiara@lab.twcu.ac.jp

used. The proof is given in Sect. 3. This paper is self-contained except quotations from [2].

Let us mention one possible contribution of Theorem 1 to the current activities in constructing new APN functions. One may use Theorem 1 to simplify the task of showing that an APN function he or she found is new, namely, that it is CCZ-equivalent neither to any power mapping nor to any member of currently known infinite families, because so far the latter families consist of quadratic functions only.

Now we give an outline of the proof of Theorem 1 with some details. Assume that f and g are quadratic APN functions on a finite field $F \cong \mathbf{F}_{2^n}$ with $n \geq 2$, which are CCZ-equivalent. By [2, Proposition 3], this assumption is equivalent to the existence of a graph isomorphism between the graphs Γ_f and Γ_g defined on $\mathbf{F}_2 \oplus F \oplus F$ constructed from these functions (see Definition 3). The existence of certain automorphisms of Γ_g, called "translations" (see (12)) allows us to assume that such an isomorphism, say ρ, fixes a point $(0; 0, 0)$ and a block $(1; 0, 0)$. For the function $h = f$ or g, we denote by M_h the stabilizer of $(0; 0, 0)$ in the automorphism group of the graph Γ_h, and by T_h the group of translations of Γ_h (which is contained in M_h). Applying the Sylow theorem and [2, Lemma 3], we may choose ρ as a linear map on $\mathbf{F}_2 \oplus F \oplus F$ so that a Sylow 2-subgroup S_f of M_f containing T_f is sent to a Sylow 2-subgroup S_g of M_g containing T_g (see Lemma 10).

We will show that ρ with these properties (called condition (a) in Sect. 3) preserves a subspace $Y = \{(0; 0, y) \mid y \in F\}$ of $\mathbf{F}_2 \oplus F \oplus F$, which is equivalent to the claim that ρ induces an EA-equivalence of f with g (see Lemma 12). We will derive a contradiction assuming that f is not EA-equivalent to g, namely, that ρ does not preserve Y (condition (b) in Sect. 3). Based on an observation that the center $Z(S_h)$ of the Sylow subgroup S_h lies in T_h for both $h = f$ and g (see Lemma 9), we can calculate the centralizer of $Z(S_h)$ on the set of points of Γ_h (see Lemma 6(3)). If $|Z(S_f)| \geq 4$, they are equal to the subspace Y, whence Y is stabilized by ρ. Therefore, we may assume that $|Z(S_h)| = 2$ $(h = f, g)$ (Lemma 13(1)) because a nontrivial 2-group has a nontrivial center. In this case, the image of Y under ρ is one of the two possible subspaces containing the subspace consisting of $(0; 0, y')$, where y' ranges over a hyperplane of F (Lemma 7). As we assumed that ρ does not preserve Y, the image of Y under ρ is uniquely determined (see Lemma 14). In particular, the values $(x + y)^\pi + x^\pi + y^\pi$ for $x, y \in F$ lie in a one-dimensional subspace spanned by a specific nonzero element a' of F (see Lemma 15), where π is a permutation on F such that the image of a block $(1; x, f(x) + f(0))$ is mapped by ρ to $(1; x^\pi, g(x^\pi) + g(0))$ for every $x \in F$ (see the paragraph after Lemma 10). Then we may introduce a form κ on F which vanishes at (x, y) exactly when $B_f(x, y) = f(x + y) + f(x) + f(y) + f(0)$ lies in a certain hyperplane H_a of F (see (30)). Using (31), we investigate this form to conclude that it is almost the zero form (see Lemma 17). This gives a final contradiction.

The arguments in this proof do not give much information on the structure of automorphism groups of Γ_f for a quadratic APN function f. For example, it seems that they cannot be used to establish the normality of the group of translations in the stabilizer of a point.

2 Preliminaries

In this section, we review some results in [3] on the graph Γ_f associated with an APN function f on a finite field $\mathbf{F}_{2^n}$ with additional remarks in the case where f is quadratic.

Throughout this paper, F denotes a finite field of size 2^n with $n \geq 2$, unless otherwise stated. We regard F as a vector space of dimension n over $\mathbf{F}_2$. Moreover, the following sets $F \oplus F$ and $\mathbf{F}_2 \oplus F \oplus F$ are regarded as vector spaces of dimensions $2n$ and $2n+1$ over $\mathbf{F}_2$, respectively:

$$F \oplus F := \{(x, y) \mid x, y \in F\},$$
$$\mathbf{F}_2 \oplus F \oplus F := \{(\varepsilon; x, y) \mid \varepsilon \in \mathbf{F}_2, x, y \in F\}.$$

Let X be one of the following sets: F, $F \oplus F$, and $\mathbf{F}_2 \oplus F \oplus F$. For a map σ on X, we usually denote the image of an element x of X under σ by x^σ. Thus, the composition $\sigma\tau$ for maps σ and τ on X is defined to be the map on X sending each $x \in X$ to $(x^\sigma)^\tau$. If $X = F$ and σ is an APN function (see Definition 2 (APN)), we denote by $\sigma(x)$ the image of $x \in X = F$ under σ, to stress on the fact that σ is an APN function. Since we do not consider the composition of APN functions, this exceptional notation may not cause any confusion.

Observe that every $\mathbf{F}_2$-linear map λ on $F \oplus F$, regarded as a $2n$-dimensional vector space over $\mathbf{F}_2$, is expressed uniquely by the quadruple $(\alpha, \beta, \gamma, \delta)$ of $\mathbf{F}_2$-linear maps α, β, γ, and δ on F such that

$$(x, y)^\lambda = \left(x^\alpha + y^\gamma, x^\beta + y^\delta\right) \tag{1}$$

for every $x, y \in F$. We will denote $\lambda = \lambda(\alpha, \beta, \gamma, \delta)$ if λ is expressed in this way. Accordingly, every $\mathbf{F}_2$-affine map $\tilde{\lambda}$ on $F \oplus F$ is uniquely expressed as a composition $\lambda(\alpha, \beta, \gamma, \delta)\tau(c, d)$ for some $\mathbf{F}_2$-linear maps $\alpha, \beta, \gamma, \delta$ on F and some elements c, d of F, where $\tau(c, d)$ is defined by

$$(x, y)^{\tau(c,d)} := (x + c, y + d) \tag{2}$$

for every $x, y \in F$.

With the above convention, we introduce two equivalence relations for functions on F.

Definition 1 For a function f on F, its graph $G(f)$ is defined to be a subset

$$G(f) := \left\{\left(x, x^f\right) \mid x \in F\right\}$$

of $F \oplus F$. Let f and g be two functions on F.

(CCZ) f is called **CCZ-equivalent** to g if there is a bijective affine map on $F \oplus F$ sending $G(f)$ to $G(g)$.

(EA) f is called **extended affine equivalent** (**EA-equivalent** for short) to g if there is a bijective affine map of the shape $\lambda(\alpha, \beta, 0, \delta)\tau(c, d)$ (with $\gamma = 0$) on $F \oplus F$ sending $G(f)$ to $G(g)$.

We note that the definition of EA-equivalence above coincides with the usual definition of EA-equivalence (see, e.g., [1, Introduction]). For $x, y \in F$, we have

$$(x, y)^{\lambda(\alpha,\beta,0,\delta)\tau(c,d)} = \big(x^\alpha + c, x^\beta + y^\delta + d\big).$$

Thus, two functions f and g are EA-equivalent if and only if there are $\mathbf{F}_2$-linear maps α, β, δ with α and δ bijective and elements c, d of F such that

$$g\big(x^\alpha + c\big) = f(x)^\delta + x^\beta + d \tag{3}$$

for all $x, y \in F$. (Here we denote the images of f and g by $f(x)$ and so on, because we usually use this notation for APN functions f and g.) This implies that

$$g(z) = f\big(z^{\alpha^{-1}} + c^{\alpha^{-1}}\big)^\delta + \big(z^{\alpha^{-1}\beta} + c^{\alpha^{-1}\beta} + d\big)$$

for $z \in F$. Thus, g is the sum of an affine map $\alpha^{-1}\beta\tau(c^{\alpha^{-1}\beta} + d)$ on F and the composition $(\alpha^{-1}\tau(c^{\alpha^{-1}}))f\delta$, where $\tau(k)$ for $k \in F$ denotes the affine map on F sending each $z \in F$ to $z + k$. This is the usual form adopted as a definition of EA-equivalence (see, e.g., [1, Introduction]).

We now introduce some classes of functions on F.

Definition 2 Let f be a function on a finite field $F \cong \mathbf{F}_{2^n}$.

(APN) f is called **almost perfect nonlinear** (abbreviated as **APN**) if

$$^{\#}\big\{x \in F \mid f(x + a) + f(x) = b\big\} \leq 2$$

for all $a \in F^\times := F \setminus \{0\}$ and $b \in F$.

(Quad) f is called **quadratic** if

$$\sum_{(x_a,x_b,x_c)\in\mathbf{F}_2^3} f(x_a a + x_b b + x_c c) = 0$$

for any elements a, b, c of F.

We associate with each function f on F a graph Γ_f. We first define, for each function f on F, the function $\overline{f}$ by

$$\overline{f}(x) := f(x) + f(0) \quad (x \in F).$$

Definition 3 [3, Definition 4] The set of vertices of Γ_f is defined to be $\mathbf{F}_2 \oplus F \oplus F$. A vertex $(\varepsilon; x, y)$ of Γ_f ($\varepsilon \in \mathbf{F}_2$, $x, y \in F$) is called a **point** or **block** according to $\varepsilon = 0$ or $\varepsilon = 1$. We denote the set of points and blocks by $\mathcal{P}$ and $\mathcal{B}$, respectively. We sometimes identify $\mathcal{P}$ with $F \oplus F$ via the natural identification map sending $(0; x, y)$ to (x, y).

$$\mathcal{P} := \big\{(0; x, y) \mid x, y \in F\big\}, \quad \mathcal{B} := \big\{(1; x, y) \mid x, y \in F\big\}.$$

Two vertices $(\varepsilon; x, y)$ and $(\varepsilon'; x', y')$ are adjacent in Γ_f whenever

$$\varepsilon + \varepsilon' = 1 \text{ and } y + y' = \overline{f}(x + x'). \tag{4}$$

It is easy to see that the following maps ι and $\tau(a,b)$ $(a,b \in F)$ are graph automorphisms of Γ_f for any function f on F:

$$\iota:\ (\varepsilon; x, y) \mapsto (\varepsilon + 1; x, y), \tag{5}$$

$$\tau(a,b):\ (\varepsilon; x, y) \mapsto (\varepsilon; x + a, y + b). \tag{6}$$

Observe that $\tau(a,b)$ is a bijective affine map on $\mathbf{F}_2 \oplus F \oplus F$ stabilizing the set $\mathcal{P}$ of points. Thus, its restriction on $\mathcal{P}$ is a bijective affine map on $\mathcal{P} = F \oplus F$ which coincides with the map $\tau(a,b)$ on $F \oplus F$ defined in (2). Thus, we also denote this restriction on $\mathcal{P}$ by $\tau(a,b)$.

For a vertex v of Γ_f and a nonnegative integer i, we denote by $(\Gamma_f)_i(v)$ the set of vertices of Γ_f at distance i from v. When a function f on F is clear from the context, we just denote it by $\Gamma_i(v)$, omitting f. We also denote by $\Gamma_{\le i}(v)$ the subset of vertices of Γ_f consisting of vertices at distance at most i from v.

Lemma 1 [3, Proposition 1] *A function f on F is an APN function if and only if the graph Γ_f is the incidence graph of a semibiplane, namely, if it is a connected graph with the following property*:

> *for any distinct points (resp. blocks), there are exactly 0 or 2 blocks (resp. points) adjacent to both of them.*

By the definition of adjacency in Γ_f, the set $\Gamma_1(\mathbf{0})$ of blocks of Γ_f adjacent to $\mathbf{0} = (0; 0, 0)$ consists of the following $2^n = |F|$ blocks:

$$\Gamma_1(\mathbf{0}) = \big\{(1; x, \overline{f}(x)) \mid x \in F\big\}. \tag{7}$$

Furthermore, for an APN function f on F, the set of points at distance two from $\mathbf{0}$ consists of the following $2^{n-1}(2^n - 1)$ points:

$$\Gamma_2(\mathbf{0}) = \big\{(0; x + y, \overline{f}(x) + \overline{f}(y)) \mid x, y \in F, x \ne y\big\}. \tag{8}$$

Lemma 2 [3, Proposition 2] *Two APN functions f and g on F are CCZ-equivalent if and only if the corresponding graphs Γ_f and Γ_g are isomorphic as graphs.*

This result corresponds to [1, Theorem 6], but in terms of the graphs Γ_f and Γ_g. To establish this claim, the following result is important, where a vector $(\varepsilon; x, y)$ of $\mathbf{F}_2 \oplus F \oplus F$ is denoted by $(\varepsilon; x, y)_h$ when it is regarded as a vertex of the graph Γ_h for a function $h = f$ or g on F.

Lemma 3 [3, Lemma 3] *Assume that λ is a graph isomorphism from Γ_f to Γ_g sending $(0; 0, 0)_f$ to $(0; 0, 0)_g$. Then λ is an* $\mathbf{F}_2$**-linear** *map on $\mathbf{F}_2 \oplus F \oplus F$.*

Observe that the map λ in Lemma 3 sends a point $(0; 0, 0)_f$ of Γ_f to a point $(0; 0, 0)_g$ of Γ_g, whence λ sends the set $\mathcal{P}_f$ of points of Γ_f to the set $\mathcal{P}_g$ of points of Γ_g. Since $\mathcal{P}_f$ and $\mathcal{P}_g$ are identical to $\mathcal{P}$, the map λ preserves both $\mathcal{P}$ and $\mathcal{B} = (\mathbf{F}_2 \oplus F \oplus F) \setminus \mathcal{P}$.

The semidirect product $N\langle\iota\rangle$ of $N := \{\tau(a,b) \mid a,b \in F\}$ with $\langle\iota\rangle$ (see (5) and (6)) is a subgroup of the automorphism group $\mathrm{Aut}(\Gamma_f)$ of graph Γ_f which acts regularly on the set $\mathbf{F}_2 \oplus F \oplus F = \mathcal{P} \cup \mathcal{B}$ of vertices. In fact, $\mathrm{Aut}(\Gamma_f)$ has the following structure:

Lemma 4 [3, Proposition 3] *The automorphism group* $\mathrm{Aut}(\Gamma_f)$ *of the graph* Γ_f *for an APN function* f *on* F *has the subgroup* $\mathrm{Aut}(\Gamma_f)_+$ *of automorphisms preserving both* $\mathcal{P}$ *and* $\mathcal{B}$ *as a normal subgroup of index* 2. *The subgroup* $\mathrm{Aut}(\Gamma_f)_+$ *is a semidirect product of a normal subgroup* $N = \{\tau(a,b) \mid a,b \in F\}$ *with the stabilizer* M *of a point* $(0;0,0)$. *The subgroup* M *consists of* $\mathbf{F}_2$*-linear bijections on* $\mathbf{F}_2 \oplus F \oplus F$ *preserving* $\mathcal{P}$ *and* $\mathcal{B}$ *together with the adjacency of* Γ_f.

Observe that the stabilizer M in Lemma 4 acts on $\Gamma_i(\mathbf{0})$ for each nonnegative integer i, as M fixes the point $\mathbf{0}$ and preserves the distance on Γ_f.

Now we assume that f is a quadratic APN function on F. Then the map B_f on $F \times F$ defined by

$$B_f(x,y) := \overline{f}(x+y) + \overline{f}(x) + \overline{f}(y) \tag{9}$$

for $x, y \in F$ is an $\mathbf{F}_2$-bilinear form on F. Moreover, as f is an APN function, the kernel of the linear map sending $x \in F$ to $B_f(a,x)$ coincides with $\{0,a\}$ for each $a \in F^\times$. Thus, for each $a \in F^\times$,

$$H_a := \big\{B_f(a,x) \mid x \in F\big\} \tag{10}$$

is a hyperplane of F.

Recall that for every hyperplane H of F, there is a unique element α of $F^\times$ such that H is the kernel of the linear form sending $x \in F$ to $\mathrm{Tr}(\alpha x)$, where Tr denotes the trace function for extension $F/\mathbf{F}_2$: $\mathrm{Tr}(x) = \sum_{i=0}^{n-1} x^{2^i}$ $(x \in F)$. Thus, we may introduce a map α on $F^\times$ by

$$H_a = \big\{y \in F \mid \mathrm{Tr}(\alpha(a)y) = 0\big\}. \tag{11}$$

Next we state a result on hyperplanes H_a $(a \in F^*)$ above, which is used in the last part of the proof of Theorem 1. This result is shown, e.g., in [2, Proposition 2.2]. There, the ambient space of the dual hyperoval $\mathcal{S}^n[f]$ associated with a quadratic APN function f is shown to be $F \oplus F$. By definition, this subspace consists of vectors (x,y) where x ranges over F and y ranges over the subspace of F spanned by all hyperplanes H_b for $b \in F^\times$. Thus, this implies that:

Lemma 5 *For a quadratic APN function* f *on* F, *the hyperplanes* $H_b = \{B_f(b,x) \mid x \in F\}$ *of* F *for all* $b \in F^\times$ *span* F.

For a quadratic APN function f on F, we can verify that the following $\mathbf{F}_2$-linear map t_a for every $a \in F$ is an automorphism of Γ_f belonging to the stabilizer M of $(0;0,0)$ (and so preserving both $\mathcal{P}$ and $\mathcal{B}$):

$$(\varepsilon;x,y)^{t_a} := \varepsilon\big(1;a,\overline{f}(a)\big) + \big(0;x,y+B_f(a,x)\big) \tag{12}$$

for $\varepsilon \in \mathbf{F}_2$ and $x, y \in F$. We call t_a the **translation** with respect to $a \in F$. We define T to be the subgroup of M consisting of all translations,

$$T := \{t_a \mid a \in F\}. \tag{13}$$

Since $t_a t_b = t_{a+b}$ for $a, b \in F$, T is an elementary abelian group of order $2^n = |F|$.

We collect information on the actions of translations on the vertices of Γ_f.

Lemma 6 *If f is a quadratic APN function on F, the following statements hold for every nonidentity translation t_a ($a \in F^\times$):*

(1) *The translation t_a does not fix any block of Γ_f. In particular, the group T of translations acts regularly on the set $\Gamma_1(\mathbf{0})$ of blocks adjacent to $\mathbf{0}$.*
(2) *The commutator space $[\mathcal{P}, t_a] := \{\mathbf{x} + \mathbf{x}^{t_a} \mid \mathbf{x} \in \mathcal{P}\}$ of t_a on $\mathcal{P}$ is given as*

$$[\mathcal{P}, t_a] = \{(0; 0, B_f(a, x)) \mid x \in F\} = \{(0; 0, y) \mid y \in H_a\}. \tag{14}$$

(3) *The centralizer $C_{\mathcal{P}}(t_a) := \{\mathbf{x} \in \mathcal{P} \mid \mathbf{x}^{t_a} = \mathbf{x}\}$ of t_a on $\mathcal{P}$ is given as*

$$C_{\mathcal{P}}(t_a) = \{(0; a, y), (0; 0, y) \mid y \in F\}, \tag{15}$$

which intersects $\Gamma_2(\mathbf{0})$ at

$$C_{\mathcal{P}}(t_a) \cap \Gamma_2(\mathbf{0}) = \{(0; a, \overline{f}(a) + y) \mid y \in H_a\}. \tag{16}$$

Proof (1) From (12) we have

$$\begin{aligned}(1; x, y)^{t_a} &= (1; x + a, y + \overline{f}(a) + B_f(a, x)) \\ &= (1; x + a, \overline{f}(x + a) + \overline{f}(x) + y)\end{aligned} \tag{17}$$

for $x, y \in F$, as $B_f(a, x) = \overline{f}(a + x) + \overline{f}(a) + \overline{f}(x)$. Thus, t_a ($a \in F^\times$) does not fix any block of Γ_f, and T acts regularly on $\Gamma_1(\mathbf{0}) = \{(1; x, \overline{f}(x)) \mid x \in F\}$ (see (7)).

(2), (3) Fix $a \in F^\times$. From (12) we have

$$(0; x, y)^{t_a} = (0; x, y + B_f(a, x)) \tag{18}$$

for $x, y \in F$. Claim (2) follows. We also have $(0; x, y)^{t_a} = (0; x, y)$ if and only if $B_f(a, x) = 0$, which is equivalent to the condition that $x = 0$ or $x = a$. This implies (15). Then Claim (3) follows from the description of $\Gamma_2(\mathbf{0})$ (see (8)). □

Lemma 7 *For a nonidentity translation t_a ($a \in F^\times$), there are exactly two subspaces X of $\mathcal{P}$ of dimension n with the following properties*:

(i) $[\mathcal{P}, t_a] \subset X \subset C_{\mathcal{P}}(t_a)$, *and*
(ii) $X \cap \Gamma_2(\mathbf{0}) = \emptyset$.

In fact, X is one of the following subspaces Y and $Y(a)$, where c is a fixed element of F not contained in the hyperplane H_a (see (10)) of F and $\varepsilon = \mathrm{Tr}(\alpha(a)\overline{f}(a))$, which is equal to 0 or 1 according as $\overline{f}(a) \in H_a$ or not (see (11) for the definition of $\alpha(a)$):

$$Y := \{(0; 0, y) \mid y \in F\},$$

and

$$Y(a) := \big\{(0; a, (\varepsilon+1)c + y), (0; 0, y) \mid y \in H_a\big\}.$$

Proof From Lemma 6(2)(3) we have $C_{\mathcal{P}}(t_a) = \{(0; a, y), (0; 0, y) \mid y \in F\}$ and $[\mathcal{P}, t_a] = \{(0; 0, y) \mid y \in H_a\}$. Fix an element c in $F \setminus H_a$. Then the factor group $C_{\mathcal{P}}(t_a)/[\mathcal{P}, t_a]$ consists of $(0; 0, c) + [\mathcal{P}, t_a]$, $(0; a, 0) + [\mathcal{P}, t_a]$, $(0; a, c) + [\mathcal{P}, t_a]$ together with the trivial coset. Since $X/[\mathcal{P}, t_a]$ is a one-dimensional subspace of $C_{\mathcal{P}}(t_a)/[\mathcal{P}, t_a]$, the subspace X coincides with $Y := \langle (0; 0, c), [\mathcal{P}, t_a]\rangle$, $Y_1 := \langle (0; a, 0), [\mathcal{P}, t_a]\rangle$, or $Y_2 := \langle (0; a, c), [\mathcal{P}, t_a]\rangle$.

Observe that $Y = \langle (0; 0, c), [\mathcal{P}, t_a]\rangle = \{(0; 0, y) \mid y \in F\}$ does not contain any point of $\Gamma_2(\mathbf{0})$ by (8). Thus, Y is one of the candidates for X.

Since $Y_1 \setminus [\mathcal{P}, t_a] = \{(0; a, y) \mid y \in H_a\}$ and $Y_2 \setminus [\mathcal{P}, t_a] = \{(0; a, y') \mid y' \in F \setminus H_a\}$, any point of $(Y_1 \cup Y_2) \setminus [\mathcal{P}, t_a]$ is of the shape $(0; a, y)$ for some $y \in F$. It is contained in $\Gamma_2(\mathbf{0})$ if and only if $y = \overline{f}(x + a) + \overline{f}(x) = \overline{f}(a) + B_f(x, a)$ for some $x \in F$ from (8). Thus, $Y_1 \cap \Gamma_2(\mathbf{0}) \neq \emptyset$ (resp. $Y_2 \cap \Gamma_2(\mathbf{0}) \neq \emptyset$) if and only if Y_1 (resp. Y_2) contains a point $(0; a, \overline{f}(a))$, which is equivalent to $\overline{f}(a) \in H_a$ (resp. $\overline{f}(a) \notin H_a$). Furthermore, in this case, $Y_2 \cap \Gamma_2(\mathbf{0}) = \emptyset$ (resp. $Y_1 \cap \Gamma_2(\mathbf{0}) = \emptyset$). Thus, the second candidate for X is either Y_2 or Y_1 according as $\overline{f}(a) \in H_a$ or not. Summarizing, the second candidate for X is given as $Y(a) := \{(0; a, (1+\varepsilon)c + y), (0; 0, y) \mid y \in H_a\}$, where $\varepsilon = \mathrm{Tr}(\alpha(a)\overline{f}(a))$. □

We give a remark on the action of M, the stabilizer of a point $\mathbf{0} = (0; 0, 0)$ in $\mathrm{Aut}(\Gamma_f)$ (see Lemma 4), on the set $\Gamma_1(\mathbf{0})$ of blocks adjacent to $\mathbf{0}$.

Lemma 8 *M acts faithfully on the set $\Gamma_1(\mathbf{0})$ of blocks adjacent to $\mathbf{0} = (0; 0, 0)$.*

Proof Let K be a subgroup of M acting trivially on $\Gamma_1(\mathbf{0})$. Take any positive integer i with $i \geq 2$, and let v be any vertex of $\Gamma_i(\mathbf{0})$. Since Γ_f is connected, there is a vertex w of $\Gamma_{i-2}(\mathbf{0})$ at distance 2 from v. Then there are exactly two vertices B and B' of $\Gamma_{i-1}(\mathbf{0})$ adjacent to both v and w, because Γ_f is the incidence graph of a semibiplane. Observe that v is the unique vertex in $\Gamma_i(\mathbf{0})$ adjacent to both B and B' (which are both in $\Gamma_{i-1}(\mathbf{0}) \cap \Gamma_1(w)$). Thus, if K fixes all vertices in $\Gamma_{\leq i-1}(\mathbf{0})$, then K fixes v as well. Namely, K fixes all vertices in $\Gamma_{\leq i}(\mathbf{0})$. Thus, starting with the assumption that K fixes all vertices in $\Gamma_{\leq 1}(\mathbf{0})$, we conclude that K fixes all vertices in Γ_f, whence $K = 1$. □

The previous lemma poses some restriction on the center of a Sylow 2-subgroup of M containing T, the group of translations (see Lemma 4).

Lemma 9 *Let S be a Sylow 2-subgroup of M containing T. Then the centralizer $C_S(T)$ of T in S coincides with T. In particular, the center $Z(S)$ of S is a subgroup of T.*

Proof Since S fixes the point $\mathbf{0} = (0; 0, 0)$, it acts on the set $\Gamma_1(\mathbf{0})$ of blocks adjacent to $\mathbf{0}$. By Lemma 6(1), the group T of translations acts regularly on $\Gamma_1(\mathbf{0}) = \{(1; x, \overline{f}(x)) \mid x \in F\}$ (see (7)). Thus, we have $S = TS_B$, where S_B denotes the

stabilizer of a block $B = (1; 0, 0)$ in $\Gamma_1(\mathbf{0})$. Since T is an abelian group, we have $C_S(T) = TC_{S_B}(T)$, where $C_{S_B}(T)$ is the centralizer of T in S_B. Take any element σ of $C_{S_B}(T)$. Since $\sigma t_a = t_a \sigma$ for any $a \in F$, we have

$$\big(1; a, \overline{f}(a)\big) = B^{t_a} = B^{\sigma t_a} = B^{t_a \sigma} = \big(1; a, \overline{f}(a)\big)^{\sigma}$$

for all $a \in F$, by (17). Thus, σ fixes all the blocks in $\Gamma_1(\mathbf{0})$. Hence, σ is the identity on Γ_f by Lemma 8. Then $C_{S_B}(T) = 1$ and $C_S(T) = T$. □

3 Proof of Theorem 1

Let f and g be quadratic APN functions on a field $F \cong \mathbf{F}_{2^n}$. Assume that f is CCZ-equivalent to g. Then there is a graph isomorphism ρ from Γ_f to Γ_g, that is, ρ is a bijective map from the set $\mathbf{F}_2 \oplus F \oplus F$ of vertices of Γ_f to the set $\mathbf{F}_2 \oplus F \oplus F$ of vertices of Γ_g such that vertices $(\varepsilon; x, y)$ and $(\varepsilon'; x', y')$ ($\varepsilon \in \mathbf{F}_2$, $x, y \in F$) of Γ_f are adjacent in Γ_f if and only if $(\varepsilon; x, y)^{\rho}$ and $(\varepsilon'; x', y')^{\rho}$ are adjacent in Γ_g. To distinguish the points and blocks of Γ_f from those of Γ_g, we put suffixes h ($h = f$ or g) to the corresponding vectors or subsets of $\mathbf{F}_2 \oplus F \oplus F$, when we regard them as vertices or subsets of vertices of Γ_h; for example,

$$(\varepsilon; x, y) = (\varepsilon; x, y)_f = (\varepsilon; x, y)_g \quad (\varepsilon \in \mathbf{F}_2, x, y \in F),$$
$$\mathcal{P}_f = \mathcal{P}_g = \big\{(0; x, y) \mid x, y \in F\big\} \quad \text{and} \quad \mathcal{B}_f = \mathcal{B}_g = \big\{(1; x, y) \mid x, y \in F\big\}.$$

Observe that ρ is a map on $\mathbf{F}_2 \oplus F \oplus F = \mathcal{P}_f \cup \mathcal{B}_f = \mathcal{P}_g \cup \mathcal{B}_g$.

We may assume that ρ sends a point $(0; 0, 0)_f$ of Γ_f to a point $(0; 0, 0)_g$ of Γ_g because $\mathrm{Aut}(\Gamma_g)$ contains a group $\{\tau(a, b) \mid a, b \in F\}\langle\iota\rangle$ acting regularly on $\mathcal{P}_g \cup \mathcal{B}_g$ (see Lemma 4). Then ρ is a map on $\mathbf{F}_2 \oplus F \oplus F$ which sends the set $\mathcal{P}_f = \{(0; x, y)_f \mid x, y \in F\}$ (resp. $\mathcal{B}_f = \{(1; t, z)_f \mid t, z \in F\}$) of points (resp. blocks) of Γ_f to the set $\mathcal{P}_g = \{(0; x, y)_g \mid x, y \in F\}$ (resp. $\mathcal{B}_g = \{(1; t, z)_g \mid t, z \in F\}$) of points (resp. blocks) of Γ_g. By Lemma 3, ρ is $\mathbf{F}_2$-linear as a map on $\mathbf{F}_2 \oplus F \oplus F$, regarded as a vector space over $\mathbf{F}_2$.

We use the letter M_f (resp. M_g) to denote the stabilizer in $\mathrm{Aut}(\Gamma_f)$ (resp. $\mathrm{Aut}(\Gamma_g)$) of a point $(0; 0, 0)_f$ (resp. $(0; 0, 0)_g$) (see Lemma 4). Since ρ sends $(0; 0, 0)_f$ to $(0; 0, 0)_g$, we have $M_g = \rho^{-1} M_f \rho$. For a subgroup G of M_f, we use the symbol G^{ρ} to denote a subgroup $\rho^{-1} G \rho$ of M_g; namely, G^{ρ} is the conjugate of G under ρ.

The letters T_f are T_g are used to denote the groups of translations for Γ_f and Γ_g, respectively (see (12) and (13)); namely, $T_f = \{t_a \mid a \in F\}$, where

$$(0; x, y)_f^{t_a} = \big(0; x, y + B_f(x, a)\big)_f, \tag{19}$$

and

$$(1; t, z)_f^{t_a} = \big(1; t + a, z + B_f(t, a) + \overline{f}(a)\big)_f, \tag{20}$$

for all $x, y \in F$. To distinguish the translations for Γ_g from those for Γ_f, we use the letter $t'_{a'}$ to denote the translation for Γ_g with respect to $a' \in F$:

$$(0; x, y)_g^{t'_{a'}} = \big(0; x, y + B_g(x, a')\big)_g, \tag{21}$$

and

$$(1; t, z)_g^{t'_{a'}} = \big(1; t + a', z + B_g(t, a') + \overline{g}(a')\big)_g, \tag{22}$$

for all $x, y \in F$. Remark that, in general, T_f^ρ may not coincide with T_g.

Let S_f be a Sylow 2-subgroup of the stabilizer M_f containing the group T_f of translations for Γ_f. Then $\rho^{-1} S_f \rho = S_f^\rho$ is a Sylow 2-subgroup of M_g. By the Sylow theorem, there is an element σ of M_g such that $(S_f^\rho)^\sigma$ contains T_g, the group of translations for Γ_g. Replacing ρ by $\rho\sigma$, we may assume that S_f^ρ contains T_g.

The image $(1; 0, 0)_f^\rho$ of a block $(1; 0, 0)_f$ of Γ_f under ρ is a block of Γ_g adjacent to $(0; 0, 0)_f^\rho = (0; 0, 0)_g$. Since T_g acts regularly on $\{(1; x, \overline{g}(x))_g \mid x \in F\}$ (see (22)), which is the set of blocks of Γ_g adjacent to $(0; 0, 0)_g$, we may assume that $(1; 0, 0)^\rho = (1; 0, 0)_g$, replacing ρ by $\rho t'_{a'}$ for some $a' \in F$.

Summarizing, we verified the following statement.

Lemma 10 *Assume that f and g are quadratic APN functions on a field $F \cong \mathbf{F}_{2^n}$ with $n \geq 2$ which are CCZ-equivalent. Then there is a graph isomorphism ρ from Γ_f to Γ_g which satisfies the following properties*:

(i) *ρ is an $\mathbf{F}_2$-linear map on $\mathbf{F}_2 \oplus F \oplus F$ preserving the hyperplane $\{(0; x, y) \mid x, y \in F\} = \mathcal{P}_f = \mathcal{P}_g$. In particular, $(0; 0, 0)_f^\rho = (0; 0, 0)_g$.*

(ii) *S_f^ρ is a Sylow 2-subgroup of M_g containing T_g for a Slyow 2-subgroup S_f of M_f containing T_f.*

(iii) *$(1; 0, 0)_f^\rho = (1; 0, 0)_g$.*

In the following, we denote by ρ a graph isomorphism from Γ_f to Γ_g which satisfies properties (i), (ii), and (iii) in Lemma 10.

A permutation π on F. Now we introduce a permutation π on F. Recall that the set $(\Gamma_f)_1((0; 0, 0)_f)$ (resp. $(\Gamma_g)_1((0; 0, 0)_g)$) of blocks of Γ_f (resp. Γ_g) adjacent to $(0; 0, 0)_f$ (resp. $(0; 0, 0)_g$) is given as $\{(1; x, \overline{f}(x))_f \mid x \in F\}$ (resp. $\{(1; x, \overline{g}(x))_g \mid x \in F\}$) by (7). Since ρ maps the set $(\Gamma_f)_1((0; 0, 0)_f)$ onto $(\Gamma_g)_1((0; 0, 0)_g)$, there is a permutation π on F such that

$$\big(1; x, \overline{f}(x)\big)_f^\rho = \big(1; x^\pi, \overline{g}\big(x^\pi\big)\big)_g \quad \text{for all } x \in F. \tag{23}$$

Since $(1; 0, 0)_f^\rho = (1; 0, 0)_g$, we have

$$0^\pi = 0. \tag{24}$$

Since $(0; x, \overline{f}(x))_f = (1; 0, 0)_f + (1; x, \overline{f}(x))_f$, the linearity of ρ and (23) imply

$$\big(0; x, \overline{f}(x)\big)_f^\rho = \big(0; x^\pi, \overline{g}\big(x^\pi\big)\big)_g \quad \text{for all } x \in F. \tag{25}$$

Lemma 11 *For all $x, y \in F$, we have*

$$\big(0; 0, B_f(x, y)\big)_f^\rho = \big(0; (x+y)^\pi + x^\pi + y^\pi, \overline{g}\big((x+y)^\pi\big) + \overline{g}(x^\pi) + \overline{g}(y^\pi)\big)_g. \quad (26)$$

Proof Since

$$\big(0; 0, B_f(x, y)\big)_f = \big(0; x, \overline{f}(x)\big)_f + \big(0; y, \overline{f}(y)\big)_f + \big(0; x+y, \overline{f}(x+y)\big)_f,$$

the linearity of ρ and (25) imply

$$\begin{aligned}
&\big(0; 0, B_f(x, y)\big)_f^\rho \\
&= \big(0; x, \overline{f}(x)\big)_f^\rho + \big(0; y, \overline{f}(y)\big)_f^\rho + \big(0; x+y, \overline{f}(x+y)\big)_f^\rho \\
&= \big(0; x^\pi, \overline{g}\big(x^\pi\big)\big)_g + \big(0; y^\pi, \overline{g}\big(y^\pi\big)\big)_g + \big(0; (x+y)^\pi, \overline{g}\big((x+y)^\pi\big)\big)_g \\
&= \big(0; (x+y)^\pi + x^\pi + y^\pi, \overline{g}((x+y)^\pi) + \overline{g}\big(x^\pi\big) + \overline{g}\big(y^\pi\big)\big)_g.
\end{aligned}$$

Thus, (26) is verified. □

Conditions (a) and (b) In what follows, we consider the following conditions:

(a) ρ is a graph isomorphism from Γ_f to Γ_g satisfying properties (i), (ii), and (iii) in Lemma 10.
(b) ρ does **not** send $\{(0; 0, y)_f \mid y \in F\}$ to $\{(0; 0, y)_g \mid y \in F\}$.
(b′) f is **not** EA-equivalent to g.

As we will see below, to assume (a) and (b) is equivalent to assume (a) and (b′).

Lemma 12 *Under condition* (a), *the map ρ sends $\{(0; 0, y)_f \mid y \in F\}$ to $\{(0; 0, y)_g \mid y \in F\}$ if and only if it induces an EA-equivalence of f with g.*

Proof If ρ sends $\{(0; 0, y)_f \mid y \in F\} = Y$ to $\{(0; 0, y)_g \mid y \in F\} = Y$, ρ is represented by $\mathbf{F}_2$-linear bijective maps α and δ on F and an $\mathbf{F}_2$-linear map β on F such that $(0; x, y)_f^\rho = (0; x^\alpha, x^\beta + y^\delta)_g$. Then we have $(0; x^\pi, \overline{g}(x^\pi))_g = (0; x, \overline{f}(x))_f^\rho = (0; x^\alpha, x^\beta + \overline{f}(x)^\delta)_g$ from (23). Thus, $\pi = \alpha$ is an $\mathbf{F}_2$-linear bijection on F, and $\overline{g}(x^\alpha) = x^\beta + \overline{f}(x)^\delta$. This shows that $g(x^\alpha) = f(x)^\delta + (x^\beta + g(0) + f(0)^\delta)$ for all $x \in F$, whence f is EA-equivalent to g. The converse immediately follows from Definition 1 (EA). □

In the remainder of this paper, we will derive a contradiction, assuming that ρ satisfies conditions (a) and (b) above. This implies that ρ with condition (a) should not satisfy (b′) by Lemma 12; namely, it should induce an EA-equivalence of f with g. This establishes Theorem 1.

Lemma 13 *Under assumptions* (a) *and* (b) *above*, *the following hold.*

(1) *The center $Z(S_f)$ of a Sylow 2-subgroup S_f is of order 2 generated by a non-identity translation t_a ($a \in F^\times$) for Γ_f.*

(2) *The center $Z(S_f)^\rho$ of a Sylow 2-subgroup S_f^ρ is a group of order 2 generated by a nonidentity translation $t'_{a'}$ ($a' \in F^\times$) for Γ_g.*
(3) *We have $t'_{a'} = (t_a)^\rho$ and $a' = a^\pi$.*

Proof Suppose that the center $Z(S_f)$ has order greater than 2. By Lemma 9 applied to S_f, the center $Z(S_f)$ contains at least two distinct nonidentity translations t_a and t_b for some distinct $a, b \in F^\times$. Then from Lemma 6(3) it follows that the centralizer $C_{\mathcal{P}_f}(Z(S_f))$ of $Z(S_f)$ on $\mathcal{P}_f$ coincides with $\{(0;0,y)_f \mid y \in F\} = C_{\mathcal{P}_f}(t_a) \cap C_{\mathcal{P}_f}(t_b)$. (Observe that $(0;0,y)_f$ for any $y \in F$ is fixed by any other translation t_c in $Z(S_f)$.)

The conjugate $Z(S_f)^\rho$ of $Z(S_f)$ by ρ is the center $Z(S_f^\rho)$ of a Sylow 2-subgroup S_f^ρ, which contains the group T_g of translations for Γ_g by condition (ii) of Lemma 10. Since $Z(S_f^\rho)$ has the same order as $Z(S_f)$, it follows from Lemma 9 applied to S_f^ρ (a Sylow subgroup of M_g with notation in Lemma 4) that $Z(S_f^\rho)$ contains at least two distinct nonidentity translations $t'_{a'}$ and $t'_{b'}$. Thus, the centralizer $C_{\mathcal{P}_g}(Z(S_f^\rho))$ of $Z(S_f^\rho)$ on $\mathcal{P}_g$ coincides with $\{(0;0,y)_g \mid y \in F\} = C_{\mathcal{P}_g}(t'_{a'}) \cap C_{\mathcal{P}_g}(t'_{b'})$ by Lemma 6(3) applied to Γ_g.

Since ρ sends $C_{\mathcal{P}_f}(Z(S_f))$ to $C_{\mathcal{P}_g}(Z(S_f^\rho))$, this contradicts our assumption that Y is not stabilized by ρ (condition (b)). Hence, we conclude that $Z(S_f)$ has order 2. Since $Z(S_f) \subset T_f$ by Lemma 9, there is a nonzero element a of F such that the translation t_a generates $Z(S_f)$. This proves Claim (1).

Since $Z(S_f^\rho)$ is the conjugate of $Z(S_f)$, it also has order 2. By Lemma 9 applied to S_f^ρ, $Z(S_f^\rho)$ is generated by a nonidentity translation $t'_{a'}$ in T_g. This shows Claim (2).

From Claims (1) and (2) we have $(t_a)^\rho = t'_{a'}$, Then the action of $t'_{a'}$ to the block $(1;0,0)_g$ is calculated as follows, using (20), (22), and (23):

$$\begin{aligned}\big(1;a',\overline{g}(a')\big)_g &= (1;0,0)_g^{t'_{a'}} = (1;0,0)_g^{\rho^{-1}t_a\rho} = \\ &= (1;0,0)_f^{t_a\rho} = \big(1;a,\overline{f}(a)\big)_f^{\rho} = \big(1;a^\pi,\overline{g}(a^\pi)\big).\end{aligned}$$

Thus, we have $a' = a^\pi$. This verifies Claim (3). □

Notation In the following, we use the letters a and a' to denote nonzero elements a and a' of F such that $Z(S_f) = \langle t_a \rangle$ and $Z(S_f^\rho) = \langle t'_{a'} \rangle$ (see Lemma 13).

We also use the letter α to denote $\alpha(a)$ defined in (11); namely, α denotes the specific nonzero element of F for which

$$H_a = \big\{B_f(a,x) \mid x \in F\big\} = \big\{y \in F \mid \mathrm{Tr}(\alpha y) = 0\big\}.$$

We also set

$$H'_{a'} := \big\{B_g(a',x) \mid x \in F\big\},$$

the hyperplane of F determined by a' and a quadratic APN function g.

Lemma 14 *Assuming conditions* (a) *and* (b) *above, we have*:

$$\{(0;0,y)_f \mid y \in H_a\}^\rho = \{(0;0,y')_g \mid y' \in H'_{a'}\}, \tag{27}$$

$$\{(0;0,y)_f \mid y \in F\}^\rho = \{(0;a',(\varepsilon'+1)c'+y'),(0;0,y') \mid y' \in H'_{a'}\}, \tag{28}$$

where c' is a fixed element in $F \setminus H'_{a'}$, and ε' is 0 *or* 1, *according to $\overline{g}(a') \in H'_{a'}$ or not.*

Proof The commutator subspace $[\mathcal{P}_f, Z(S_f)] = [\mathcal{P}_f, t_a] = \{(0;0,y)_f \mid y \in H_a\}$ of $Z(S_f)$ on $\mathcal{P}_f$ (see Lemma 6(2) for t_a) is sent by ρ to the commutator subspace $[\mathcal{P}_g, Z(S)^\rho] = [\mathcal{P}_g, t'_{a'}] = \{(0;0,y')_g \mid y' \in H'_{a'}\}$ of $Z(S_f)^\rho$ on $\mathcal{P}_g$ (see Lemma 6(2) for $t'_{a'}$). This shows the first claim, (27), of the lemma.

Next consider the subspace $Y_f := \{(0;0,y)_f \mid y \in F\}$ of $\mathbf{F}_2 \oplus F \oplus F$. Observe that this is one of the two n-dimensional subspaces of $C_{\mathcal{P}_f}(t_a)$ satisfying conditions in Lemma 7; namely, it contains $[\mathcal{P}_f, t_a] = \{(0;0,y)_f \mid y \in H_a\}$ but does not contain any point at distance two from $(0;0,0)_f$. Remark that the image Y_f^ρ of Y_f under ρ is an n-dimensional subspace of $C_{\mathcal{P}_g}(t'_{a'}) = C_{\mathcal{P}_f}(t_a)^\rho$ containing $[\mathcal{P}_f, t_a]^\rho = \{(0;0,y')_g \mid y' \in H'_{a'}\}$ (see the first claim of the lemma) but having no point at distance two from $(0;0,0)_g = (0;0,0)_f^\rho$. Hence, applying Lemma 7 to $t'_{a'}$ and Y_f^ρ, we have either $Y_f^\rho = Y_g = \{(0;0,y)_g \mid y \in F\}$ or $Y_f^\rho = Y_g(a') = \{(0;a',(\varepsilon'+1)c'+y'),(0;0,y') \mid y' \in H'_{a'}\}$, where c' is a fixed element of $F \setminus H'_{a'}$, and $\varepsilon' = 0$ or 1 according to $\overline{g}(a') \in H'_{a'}$ or not. If the former case holds, the map ρ preserves $\{(0;0,y) \mid y \in F\} = Y_f = Y'_g$, which contradicts condition (b). Hence, the latter holds, which verifies the second claim, (28), of the lemma. □

In view of Lemma 14, a point $(0;0,z)_f$ of Γ_f is mapped by ρ to a point of the form $(0;0,z')_g$ or $(0;a',z'')_g$ according to $z \in H_a$ or $z \notin H_a$. Namely, the second component of $(0;0,z)_f^\rho$ is 0 or a' according to $z \in H_a$ or not.

Using the element α defined in Notation, this observation is rephrased as follows: for any $z \in F$, the second component of $(0;0,z)_f^\rho$ coincides with $\mathrm{Tr}(\alpha z)a'$. Applying this observation to a point $(0;0,z)_f$ with z in the form $B_f(x,y)$ for some $x, y \in F$, we have the following lemma from (26).

Lemma 15 *Assume conditions* (a) *and* (b) *above. For any $x, y \in F$, we have*

$$(x+y)^\pi + x^\pi + y^\pi = \kappa(x,y)a', \tag{29}$$

where κ is the map from $F \times F$ to $\mathbf{F}_2$ defined by

$$\kappa(x,y) := \mathrm{Tr}\big(\alpha B_f(x,y)\big). \tag{30}$$

We give some remarks on the map κ defined in Lemma 15. Since f is quadratic, B_f is bilinear on F. Hence, κ is a bilinear form on F. Since $B_f(x,x) = 0$, κ is alternating; $\kappa(x,x) = 0$ for all $x \in F$ and hence symmetric: $\kappa(x,y) = \kappa(y,x)$ for all $x, y \in F$. From Definition (30) and Definition (11) we have that $\kappa(x,y) = 0$ if and only if $B_f(x,y)$ lies in the hyperplane H_a of F.

Lemma 16 *Assume conditions* (a) *and* (b) *above. If* $\kappa(x, y) = 0$ *for* $x, y \in F$, *we have*

$$\big(0; 0, B_f(x, y)\big)_f^\rho = \big(0; 0, B_g\big(x^\pi, y^\pi\big)\big)_g. \tag{31}$$

Proof If $\kappa(x, y) = 0$, then we have $(x + y)^\pi = x^\pi + y^\pi$ from (29). Then the third component of $(0; 0, B_f(x, y))_f^\rho$, which is given as $\overline{g}((x + y)^\pi) + \overline{g}(x^\pi) + \overline{g}(y^\pi)$ by (26), coincides with $\overline{g}(x^\pi + y^\pi) + \overline{g}(x^\pi) + \overline{g}(y^\pi) = B_g(x^\pi, y^\pi)$. This verifies the lemma. □

The above lemma imposes a strong restriction on the alternating form κ.

Lemma 17 *Assume conditions* (a) *and* (b) *above. Let* y *be any element in* $F \setminus \{0, a\}$. *Then the subspace* $y^\perp := \{x \in F \mid \kappa(y, x) = 0\}$ *of* F *orthogonal to* y *with respect to* κ *is totally isotropic*; *namely,* $\kappa(x_1, x_2) = 0$ *for any* $x_1, x_2 \in y^\perp$.

Proof Let y be any element in $F \setminus \{0, a\}$. Take any element x_i in $y^\perp$ $(i = 1, 2)$. Since $\kappa(x_i, y) = 0$ for $i = 1, 2$ and κ is bilinear, we have $\kappa(x_1 + x_2, y) = 0$. Then it follows from (31) that

$$\big(0; 0, B_f(x_1 + x_2, y)\big)_f^\rho = \big(0; 0, B_g((x_1 + x_2)^\pi, y^\pi)\big)_g.$$

Since ρ is linear and B_f and B_g are bilinear, the left-hand side of this equation can be written as follows, using (31) and the assumption that $\kappa(x_i, y) = 0$, $i = 1, 2$:

$$\begin{aligned}
&\big(0; 0, B_f(x_1, y)\big)_f^\rho + \big(0; 0, B_f(x_2, y)\big)_f^\rho \\
&= \big(0; 0, B_g\big(x_1^\pi, y^\pi\big)\big)_g + \big(0; 0, B_g\big(x_2^\pi, y^\pi\big)\big)_g \\
&= \big(0; 0, B_g\big(x_1^\pi + x_2^\pi, y^\pi\big)\big)_g.
\end{aligned}$$

Thus, comparing the third components, we have $B_g((x_1 + x_2)^\pi, y^\pi) = B_g(x_1^\pi + x_2^\pi, y^\pi)$. From the bilinearity of B_g we then have

$$B_g\big((x_1 + x_2)^\pi + x_1^\pi + x_2^\pi, y^\pi\big) = 0.$$

Applying (29), this implies that

$$B_g\big(\kappa(x_1, x_2)a', y^\pi\big) = 0.$$

Since $\kappa(x_1, x_2)$ is an element of $\mathbf{F}_2$, we then have

$$\kappa(x_1, x_2) B_g\big(a', y^\pi\big) = 0.$$

Now $B_g(a', y^\pi) = 0$ if and only if $y^\pi = 0$ or $y^\pi = a'$. By (24) and Lemma 13(3), this is equivalent to $y = 0$ or $y = a$. Thus, by our choice of y, we should have $\kappa(x_1, x_2) = 0$. Since this holds for every x_1, x_2 in $y^\perp$, the subspace $y^\perp$ is totally isotropic. □

Proof of Theorem 1 Now we obtain a final contradiction. We assume conditions (a) and (b) above.

Since κ is an alternating form on F, F is decomposed as follows from the standard theory on alternating bilinear forms:

$$F = R \oplus \langle e_1, \ldots, e_r \rangle \oplus \langle f_1, \ldots, f_r \rangle,$$

where $R = \{x \in F \mid \kappa(x, y) = 0 (\forall y \in F)\}$ is the radical, and $\{e_i, f_i\}$ $(i = 1, \ldots, r)$ are parabolic pairs; namely, $\kappa(e_i, e_j) = 0 = \kappa(f_i, f_j)$ and $\kappa(e_i, f_j) = \delta_{i,j}$ for all $i, j \in \{1, \ldots, r\}$.

Assume that $r \geq 2$. Then the subspaces $e_1^{\perp}$ and $f_1^{\perp}$ contain $\langle e_2, f_2 \rangle$, and therefore none of them is totally isotropic. This contradicts Lemma 17, because it states that a is a unique possible nonzero element y in F such that $y^{\perp}$ is not totally isotropic. Thus, we have $r \leq 1$.

Assume that $r = 1$. Then the radical R has codimension 2 in F. As we assume that f and g are CCZ-equivalent but EA-inequivalent APN functions on $F \cong \mathbf{F}_{2^n}$, we must have $n \geq 4$. Then R has dimension at least 2, and hence R contains a nonzero element b distinct from a. However, $b^{\perp} = F$ is not totally isotropic, which contradicts Lemma 17.

Hence, we have $r = 0$, namely, F itself is totally isotropic with respect to κ. However, this implies that $B_f(x, y)$ lies in a hyperplane H_a of F for every $x, y \in F$. This contradicts Lemma 5.

Thus, we have a final contradiction, and Theorem 1 is established. □

References

1. Bracken, C., Byrne, E., McGuire, G., Nebe, G.: On equivalence of quadratic APN-functions. Des. Codes Cryptogr. **61**, 261–272 (2010). doi:10.1007/s10623-010-9475-8
2. Yoshiara, S.: Dimensional dual hyperovals associated with quadratic APN functions. Innov. Incid. Geom. **8**, 147–169 (2008)
3. Yoshiara, S.: Notes on APN functions, semibiplanes and dimensional dual hyperovals. Des. Codes Cryptogr. **56**, 197–218 (2010)