J Algebr Comb (2016) 44:561–585
DOI 10.1007/s10801-016-0680-z

Equivalences of power APN functions with power or quadratic APN functions

Satoshi Yoshiara[1]

Received: 12 May 2015 / Accepted: 7 March 2016 / Published online: 28 March 2016

Abstract On $F = \mathbb{F}_{2^n}$ $(n \geq 3)$, the power APN function f_d with exponent d is CCZ-equivalent to the power APN function f_e with exponent e if and only if there is an integer a with $0 \leq a \leq n-1$ such that either (A) $e \equiv d2^a \bmod 2^n - 1$ or (B) $de \equiv 2^a \bmod 2^n - 1$, where case (B) occurs only when n is odd (Theorem 1). A quadratic APN function f is CCZ-equivalent to a power APN function if and only if f is EA-equivalent to one of the Gold functions (Theorem 2). Using Theorem 1, a complete answer is given for the question exactly when two known power APN functions are CCZ-equivalent (Proposition 2). The key result to establish Theorem 1 is the conjugacy of some cyclic subgroups in the automorphism group of a power APN function (Corollary 3). Theorem 2 characterizes the Gold functions as unique quadratic APN functions which are CCZ-equivalent to power functions.

Keywords Almost perfect nonlinear (APN) function · Carlet–Charpin–Zinoviev (CCZ) equivalence · Extended affine (EA) equivalence · Quadratic APN function · Power APN function · Dimensional dual hyperoval (DHO)

Mathematics Subject Classification 05E18 · 11T06 · 12E12 · 20B25 · 51E20

This paper is dedicated to Professor Hiramine, who passed away on January, 2016.

✉ Satoshi Yoshiara
yoshiara@lab.twcu.ac.jp

[1] Department of Mathematics, Tokyo Woman’s Christian University, Suginami-ku, Tokyo 167-8585, Japan

1 Introduction

Let n be a natural number with $n \geq 3$, and let F be a finite field of size 2^n. We regard the direct sum $F \oplus F = \{(x, y) \in F\}$ as a vector space over $\mathbb{F}_2$ of dimension $2n$. Two functions f and g are called Carlet–Charpin–Zinoviev equivalent (CCZ-equivalent for short) if there is a bijective $\mathbb{F}_2$-affine map λ on $F \oplus F$ which sends the graph $G(f) := \{(x, f(x)) \mid x \in F\}$ of f to the graph $G(g) = \{(x, g(x)) \mid x \in F\}$ of g. If we may choose such a λ to stabilize the subspace $\{(0, y) \mid y \in F\}$ of $F \oplus F$, we say that f is *extended affine equivalent* (EA-equivalent for short) to g. Needless to say, if f is EA-equivalent to g, then f is CCZ-equivalent to g. The *automorphism group* $\mathrm{Aut}(f)$ of a function f on F is defined to be the group of all $\mathbb{F}_2$-affine bijections on $F \oplus F$ which stabilizes the graph $G(f)$.

A map f on F to itself is called *almost perfect nonlinear* (abbreviated to APN) if there are exactly 0 or 2 solutions in F of the equation $f(x + a) + f(x) = b$ for every choice of elements a, b of F with $a \neq 0$. It can be shown that if a function g on F is CCZ-equivalent to an APN function f on F, then g is APN as well. A map f on F is called *quadratic* if the map B_f defined by $B_f(x, y) := f(x+y)+f(x)+f(y)+f(0)$ is an $\mathbb{F}_2$-bilinear map from $F \oplus F$ to F. With a quadratic APN function f, we can associate a geometric object $\mathcal{S}[f]$, a *dimensional dual hyperoval* associated with a quadratic APN function f. (For the precise definition, see the proof of Theorem 2.) It can be shown that two quadratic APN functions f and g are EA-equivalent if and only if $\mathcal{S}[f]$ and $\mathcal{S}[g]$ are isomorphic as dimensional dual hyperovals [14, Prop 5].

Motivated by applications to cryptography, several infinite series of APN functions are constructed recently; they are divided into two classes: One consists of those CCZ-equivalent to power functions, and the other CCZ-equivalent to quadratic functions. The unique known class of quadratic APN functions CCZ-equivalent to power functions are the EA-equivalence classes of the Gold functions (see Sect. 2). On $\mathbb{F}_{2^n}$ with $n \leq 9$, there are several APN functions CCZ-inequivalent to power and quadratic functions, but as far as the author knows no infinite family of such functions has been found.

In this paper, the author investigates the *CCZ-equivalence problem*, namely, to determine whether or not two given APN functions are CCZ-equivalent. In Sect. 2, we give a review on a current situation for the CCZ-equivalence problem among known power APN functions. For two quadratic functions, a theoretical result in [15] reduces the problem to a much easier problem to examine the EA-equivalence between them.

The aim of this paper is to establish the following two theoretical results on the CCZ-equivalence between a power APN function and a power or quadratic APN function, by comparing their automorphism groups.

Theorem 1 *Let $f_d(x) = x^d$ and $f_e(x) = x^e$ be power APN functions on $F = \mathbb{F}_{2^n}$ with $n \geq 3$. Then f_d and f_e are CCZ-equivalent if and only if either (A) $e \equiv d2^a$ for some integer a in the interval $[0, n-1]$ or (B) n is odd and $ed \equiv 2^a$ modulo $2^n - 1$ for an integer a in $[0, n-1]$.*

In other words, f_d is CCZ-equivalent to f_e if and only if f_e is EA-equivalent to f_d or $f_{1/d}$, where $1/d$ denotes the multiplicative inverse of d modulo $2^n - 1$ when n is odd.

Theorem 2 *Let f be a quadratic APN function and f_d be a power APN function on $F = \mathbb{F}_{2^n}$ with $n \geq 3$. If f and f_d are CCZ-equivalent, then f is EA-equivalent to the Gold function $g_s(x) = x^{1+2^s}$ for some integer s with $1 \leq s < n/2$ coprime to n.*

Theorem 1 reduces the CCZ-problem between power APN functions (involving those may be found in future) to solve some congruence equations. Based on Theorem 1, we shall provide a complete answer for the CCZ-problem among known power APN functions (see Proposition 2). As we shall see in the proof, this sometimes requires straightforward but tedious calculations.

Theorem 2 generalizes [1]. It also characterizes the EA-equivalence classes of Gold functions as unique quadratic APN functions CCZ-equivalent to power functions. Moreover, since any function in the list of infinite families of APN functions known at the present time is CCZ-equivalent to either a quadratic or a power function, Theorem 2 with [15, Thm 1] implies the following reduction: in order to show that a given quadratic function is not known before, it suffices to establish EA-inequivalence to every quadratic APN function known at the present time.

The idea of a proof for Theorem 2 is natural and simple: the automorphism group of a quadratic APN function f is doubly transitive on the graph $G(f)$ if f is CCZ-equivalent to a power function, as it allows the group of translations as well as a certain cyclic group. Then we can exploit classifications of the associated DHOs such as [13, Thm 1], because the automorphism group of f and the automorphism of the associated DHO are isomorphic by [4, Corollary 5.11]. It turns out that a quadratic function is CCZ-equivalent to a power function only when it is EA-equivalent to a Gold function (Theorem 2).

The idea of a proof for Theorem 1 is natural as well (a prototype of the proof appeared in [10, Lemma 9,10]): to compare the proper subspaces of $F \oplus F$ invariant under the automorphisms of power APN functions, assuming that they are CCZ-equivalent. It is not difficult to determine such subspaces (see Corollary 1), which gives a certain restriction on affine bijections on $F \oplus F$ inducing CCZ-equivalence. However, in order to obtain much stronger restrictions between the exponents of power APN functions in question, we need to establish that certain cyclic subgroups of the automorphism group are conjugate (see Corollary 3). The conjugacy follows from Proposition 1 which describes the centralizer of a Sylow p-subgroup of an explicit cyclic group, where p is a 2-primitive prime divisor of $2^n - 1$ (when $n \neq 6$). The proof of this key result is naturally divided into two cases, depending on the minimal polynomials of two $\mathbb{F}_2$-linear bijections on F induced by a generator of a Sylow p-subgroup (see Lemma 5). It is easy to establish the key result when these polynomials are distinct (corresponding to Proposition 1a). On the other hand, when they are identical (corresponding to Proposition 1b), the centralizer in question is naturally identified with a subgroup of the matrix group $GL_2(2^n)$, and we can establish the key result by exploiting a classification of subgroups of $PSL_2(2^n) \cong SL_2(2^n)$ (e.g. [9, Thm 6.25]).

Section 2 is a review on the known list of power APN functions and the results about CCZ-equivalence problem among them. In Sect. 3, fundamental terminologies are given for automorphism groups of APN functions. Section 4 is the core part of the paper, where Proposition 1 and its corollaries are proved, with the notation given in

Table 1 Known APN power functions x^d on GF(2^n)

Name	Exponent d	Conditions	$w_2(d)$
Gold	$2^s + 1$	$(s, n) = 1$	2
Kasami	$2^{2s} - 2^s + 1$	$(s, n) = 1$	$s + 1$
Welch	$2^t + 3$	$n = 2t + 1$	3
Niho	$2^t + 2^{t/2} - 1$, t even	$n = 2t + 1$	$(t + 2)/2$
	$2^t + 2^{(3t+1)/2} - 1$, t odd		$t + 1$
Inverse	$2^n - 2$	$n = 2t + 1$	$n - 1$
Dobbertin	$2^{4t} + 2^{3t} + 2^{2t} + 2^t - 1$	$n = 5t$	$t + 3$

Sect. 4.1. In Sect. 5, the main theorems are established using the results in Sect. 4. As an application of Theorem 1, in Sect. 6 we shall solve the CCZ-equivalence problem among known power APN functions (Proposition 2).

In this paper, we try to give self-contained expositions as possible. The exception lies in the proof of Theorem 2, where we assume some familiarity with DHOs. We adopt this way, because it makes the arguments shorter.

2 Known infinite families of APN functions

In this section, we review results on the CCZ-equivalence problem among the known CCZ power APN functions. For convenience of the reader, we first give a list of known infinite families of CCZ power APN functions on $F \cong \mathbb{F}_{2^n}$, $n \geq 3$. In Table 1, which is essentially same as [2, Table 1], the representatives x^d are given. We only describe the exponent d, where $w_2(d)$ denotes the 2-weight of an integer d; namely, the number of integers i with $0 \leq i \leq n-1$ satisfying $a_i \neq 0$ in the 2-adic expression $d = \sum_{i=0}^{n-1} a_i 2^i$, $a_i \in \{0, 1\}$.

For each integer s with $1 \leq s \leq n-1$ and $(s, n) = 1$, we denote by $\mathcal{G}_s(n)$ and $\mathcal{K}_s(n)$ respectively the sets of functions CCZ-equivalent to the Gold function g_s on F given by $g_s(x) := x^{2^s+1}$ $(x \in F)$ and the Kasami function k_s on F given by $k_s(x) := x^{2^{2s}-2^s+1}$ $(x \in F)$. Clearly $g_1 = k_1$. It is easy to see that if $s + s' = n$ then g_s and $g_{s'}$ (respectively k_s and $k_{s'}$) are EA-equivalent. We denote by $\mathcal{G}(n)$ the union of $\mathcal{G}_s$ for all positive integer s with $1 \leq s < n/2$ and $(s, n) = 1$. Let $\mathcal{K}(n)$ be the union of $\mathcal{K}_s$ for all positive integer r with $2 \leq s < n/2$ and $(s, n) = 1$. Observe that here is no such s for $n = 3, 4$ and 6: $\mathcal{K}(3) = \mathcal{K}(4) = \mathcal{K}(6) = \emptyset$.

For n odd with $n \geq 5$, we denote by $\mathcal{W}(n)$ (resp. $\mathcal{I}(n)$ and $\mathcal{N}(n)$) the set of functions on $F = \mathbb{F}_{2^n}$ CCZ-equivalent to the Welch function $w(x) := x^{2^{(n-1)/2}+3}$ (resp. the inverse function $\iota(x) = x^{2^n-2}$ and the Niho function $\nu(x) := x^d$, where $d := 2^{(n-1)/2} + 2^{(n-1)/4} - 1$ or $d := 2^{(n-1)/2} + 2^{(3n-1)/4} - 1$ according as $n \equiv 1$ or 3 modulo 4). We have $\mathcal{W}(5) = \mathcal{G}_2(5)$ and $\mathcal{W}(7) = \mathcal{K}_3(7)$, because $w(x) = x^7$ on $\mathbb{F}_{2^5}$ is CCZ-equivalent to its inverse function $x^9 = g_3(x)$ and $w(x) = x^{11}$ on $\mathbb{F}_{2^7}$ is CCZ-equivalent to $(w^{-1}(x))^{2^3} = (x^{23})^8 = x^{57} = k_3(x)$. We also have $\mathcal{N}(5) = \mathcal{G}_2(5)$, $\mathcal{N}(7) = \mathcal{K}_3(7)$ and $\mathcal{W}(9) = \mathcal{N}(9)$, because the above formula for the exponent of the

Niho function gives $d = 5, 39$ or 19, respectively for $n = 5, 7$ or 9, but we can verify that $x^5 = g_2(x)$ on $GF(2^5)$, $w(x) = x^{19} = \nu(x)$ on $\mathbb{F}_{2^9}$ and that x^{39} on $GF(2^7)$ is CCZ-equivalent to $\kappa_3(x)$ (as $(-13)2^4 \equiv 57$ for the multiplicative inverse -13 of 39 modulo $2^7 - 1$). Thus we usually assume that n is an odd integer $n \geq 9$ in the definition of the Welch function w, and that n is an odd integer $n \geq 11$ in the definition of the Niho function. This convention is adopted in Table in Sect. 6.

For even n, $\mathcal{W}(n), \mathcal{I}(n)$ and $\mathcal{N}(n)$ are understood to be the empty set. For n divisible by 5, $\mathcal{D}(n)$ denotes the set of functions CCZ-equivalent to the Dobbertine function $\delta(x) := x^d$ with $d = 2^{4n/5} + 2^{3n/5} + 2^{2n/5} + 2^{n/5} - 1$. If n is not divisible by 5, we set $\mathcal{D}(n) = \emptyset$. Notice that both $\mathcal{G}(n)$ and $\mathcal{K}(n)$ may consist of several CCZ-equivalence classes, but each of $\mathcal{W}(n)$, $\mathcal{N}(n)$, $\mathcal{I}(n)$ and $\mathcal{D}(n)$ consists of at most a single CCZ-class. We denote by $\mathcal{KP}(n)$ (standing for the known CCZ power APN functions) the union of $\mathcal{G}(n)$, $\mathcal{K}(n)$, $\mathcal{W}(n)$, $\mathcal{N}(n)$, $\mathcal{I}(n)$ and $\mathcal{D}(n)$.

We review the results on the CCZ-equivalence problem among known CCZ power functions, including those first obtained in this paper.

It is known that two Gold functions g_s and $g_{s'}$ ($1 \leq s, s' \leq n-1$, $(n,s) = (n,s') = 1$) are CCZ-equivalent if and only if $s = s'$ or $s + s' = n$ [2, Thm 2.1]. Thus $\mathcal{G}(n)$ consists of exactly $\phi(n)/2$ CCZ-equivalence classes $\mathcal{G}_s(n)$ for integers s with $1 \leq s < n/2$ and $(s,n) = 1$. As for the CCZ-equivalence between Gold and Kasami functions, it is shown that $\mathcal{K}_s(n) \cap \mathcal{G}(n) = \emptyset$ if $3s \not\equiv \pm 1$ modulo n [2, Thm 2.2] as well as $\mathcal{W}(n) \cap \mathcal{G}(n) = \emptyset$ for $n \geq 9$ in [2, Thm 6], based on complicated calculations. We have $\mathcal{D}(n) \cap (\mathcal{KP}(n) \setminus \mathcal{D}(n)) = \emptyset$, which is verified by comparing the extended Walsh (Fourier) spectrum of $g_s(x)$, $k_s(x)$, $w(x)$, $\nu(x)$, $\iota(x)$ and $\delta(x)$. See [5] for the definition of the extended Walsh spectrum and its invariance under CCZ-equivalence [5, Comment after Prop 1]. The same reasoning shows that $\mathcal{I}(n) \cap (\mathcal{KP}(n) \setminus \mathcal{I}(n)) = \emptyset$.

Thus it remains to examine CCZ-equivalences about the following pairs:

$$(\mathcal{G}_s(n), \mathcal{K}_r(n)), (\mathcal{G}_s(n), \mathcal{N}(n)), (\mathcal{K}_r(n), \mathcal{K}_{r'}(n)), (\mathcal{K}(n), \mathcal{W}(n)), (\mathcal{K}(n), \mathcal{N}(n)), (\mathcal{W}(n), \mathcal{N}(n)).$$

They shall be solved in Proposition 2(ii), (iv), (v), (vi), (vii) and (viii): in fact, $\mathcal{K}_s(n) \cap \mathcal{G}(n) \neq \emptyset$ if and only if $(n,s) = (5,2)$ (in this case $\mathcal{K}_2(5) = \mathcal{G}_1(5)$); $\mathcal{N}(n) \cap \mathcal{G}(n) = \emptyset$ for $n \geq 11$; $\mathcal{K}_r(n) \cap \mathcal{K}_{r'}(n) = \emptyset$ if $r \neq r', 2 \leq r, r' \leq n/2, (r,n) = (r',n) = 1$; $\mathcal{K}(n) \cap \mathcal{W}(n) = \emptyset$ for every $n \geq 9$ and $\mathcal{K}(n) \cap \mathcal{N}(n) = \mathcal{W}(n) \cap \mathcal{N}(n) = \emptyset$ for every $n \geq 11$.

3 The automorphism group of a function on a finite field

In this paper, we use F to denote a finite field of size 2^n. We regard F and $F \oplus F := \{(x,y) \mid x, y \in F\}$ as vector spaces over $\mathbb{F}_2$ of dimension n and $2n$ respectively. We use the symbols $GL(F)$ and $GL(F \oplus F)$ to denote the groups of all $\mathbb{F}_2$-linear bijections on F and $F \oplus F$, respectively. For $\mathbb{F}_2$-linear maps α and β on F, we denote the composition of α by β and the sum of α and β by $\alpha\beta$ and $\alpha + \beta$, respectively:

$$(x)\alpha\beta := ((x)\alpha)\beta, \quad (x)(\alpha + \beta) = (x)\alpha + (x)\beta$$

for $x \in F$, where we denote the image of $x \in F$ under a linear map α by $(x)\alpha$., etc. On the other hand, we usually denote the image of $x \in F$ under a (not necessarily linear) map f by $f(x)$. For a subgroup G of $GL(F) \cong GL_n(2)$ (resp. $GL(F \oplus F) \cong GL_{2n}(2)$), a subspace W of F (resp. $F \oplus F$) is called G-invariant if every element of G stabilizes W. The subspace W is called G-irreducible (or G *acts irreducibly* on W) if there is no G-invariant subspace of W other than $\{0\}$ and W.

For an element λ of $GL(F \oplus F)$, there is a quadruple $(\alpha, \beta, \gamma, \delta)$ of $\mathbb{F}_2$-linear maps α, β, γ and δ on F such that $\alpha\delta + \beta\gamma \neq 0_F$ (the zero map on F) and $(x, y)\lambda = ((x)\alpha + (y)\gamma, (x)\beta + (y)\delta)$ for all $x, y \in F$. In this case, we denote

$$\lambda = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}.$$

The composition $\lambda\lambda'$ of λ by an $\mathbb{F}_2$-linear map $\lambda' = \begin{pmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{pmatrix}$ is equal to

$$\lambda\lambda' = \begin{pmatrix} \alpha\alpha' + \beta\gamma' & \alpha\beta' + \beta\delta' \\ \gamma\alpha' + \delta\gamma' & \gamma\beta' + \delta\delta' \end{pmatrix}.$$

An $\mathbb{F}_2$-affine bijection on $F \oplus F$ is a bijection α on $F \oplus F$ sending $(x, y) \in F \oplus F$ to $((x, y))\lambda + (u, v)$ for an $\mathbb{F}_2$-linear map λ and a vector $(u, v) \in F \oplus F$. Then λ lies in $GL(F \oplus F)$, which is called the *linear part* of α; while (u, v) is called the *vector part* of α. We denote α by $\lambda + (u, v)$. The set of all $\mathbb{F}_2$-affine bijections on $F \oplus F$ forms a group relative to the composition of maps, which is denoted $\mathrm{AGL}(F \oplus F)$:

$$\mathrm{AGL}(F \oplus F) := \{\lambda + (u, v) \mid \lambda \in GL(F \oplus F), (u, v) \in F \oplus F\}.$$

We have $(\lambda+(u, v))(\lambda'+(u, v)) = \lambda\lambda'+((u, v)\lambda'+(u', v'))$. The group $\mathrm{AGL}(F\oplus F)$ acts on $F\oplus F$, in which $T(F\oplus F) := \{\mathrm{id}_{F\oplus F}+(u, v) \mid u, v \in F\}$ is a normal subgroup acting regularly on $F \oplus F$ and the stabilizer of a point $(0, 0)$ is $GL(F \oplus F)$, satisfying $\mathrm{AGL}(F \oplus F) = T(F \oplus F)GL(F \oplus F)$ and $T(F \oplus F) \cap GL(F \oplus F) = \{\mathrm{id}_{F\oplus F}\}$.

For a map f from F to itself (also referred to as f a map on F), the graph $G(f)$ of f is a subset of $F \oplus F$ defined by

$$G(f) := \{(x, f(x)) \mid x \in F\}. \tag{1}$$

The *automorphism group* $\mathrm{Aut}(f)$ of f is defined to be the group of all $\mathbb{F}_2$-affine bijections stabilizing the graph $G(f)$. For an $\mathbb{F}_2$-affine bijection $\lambda + (u, v)$ on $F \oplus F$ with the linear part $\lambda = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$, we have

$$(x, f(x))(\lambda + (u, v)) = ((x)\alpha + (f(x))\gamma + u, (x)\beta + (f(x))\delta + v)$$

for all $x \in F$. Thus $\lambda + (u, v)$ lies in $\mathrm{Aut}(f)$ if and only if the following conditions are satisfied

$$\text{the map} \qquad F \ni x \mapsto (x)\alpha + (f(x))\gamma \in F \text{ is a bijection}, \tag{2}$$

$$f((x)\alpha + (f(x))\gamma + u) = (x)\beta + (f(x))\delta + v \ \text{ for all } x \in F. \tag{3}$$

Lemma 1 *The graph $G(f)$ of an APN function f spans $F \oplus F$. In particular, the action of* $\mathrm{Aut}(f)$ *on the graph $G(f)$ is faithful.*

Proof Let W be the subspace of $F \oplus F$ spanned by $G(f)$. By [3, p. 245, Remark after Prop 9.15], for every $c \in F^{\times}$ there is a triple (x, y, z) of elements of F such that $f(x) + f(y) + f(z) + f(x + y + z) = c$. Thus $(0, c) = (x, f(x)) + (y, f(y)) + (z, f(z)) + (x + y + z, f(x + y + z))$ lies in W, whence $Y := \{(0, c) \mid c \in F\}$ is contained in W. Then $(x, 0) = (x, f(x)) + (0, f(x))$ lies in W for every $x \in W$, as $(x, f(x)) \in G(f)$ and $(0, f(x)) \in Y \subseteq W$. Thus $X := \{(x, 0) \mid x \in F\} \subseteq W$ and $F \oplus F = X + Y = W$. □

For short, we denote a 'diagonal' $\mathbb{F}_2$-linear bijection $\begin{pmatrix} \alpha & 0 \\ 0 & \delta \end{pmatrix}$ by (α, δ):

$$(\alpha, \delta) := \begin{pmatrix} \alpha & 0 \\ 0 & \delta \end{pmatrix}.$$

In this case, both α and δ are $\mathbb{F}_2$-linear bijections on F. An element λ of $GL(F \oplus F)$ is represented as a diagonal matrix exactly when it stabilizes two subspaces

$$X := \{(x, 0) \mid x \in F\} \quad \text{and } Y := \{(0, y) \mid y \in F\}.$$

For a nonzero element $b \in F^{\times}$, we use the symbol m_b to denote the *multiplication* by b:

$$(x)m_b := xb \quad (x \in F),$$

which is an $\mathbb{F}_2$-linear bijection. The group $\{(m_b, m_c) \mid b, c \in F^{\times}\}$ is a subgroup of $GL(F \oplus F)$ of order $(2^n - 1)^2$ consisting of all diagonal $\mathbb{F}_2$-linear bijections.

Recall that an element of $GL(F) \cong GL_n(2)$ of order $2^n - 1$ is called a *Singer cycle* and the cyclic subgroup of $GL(F)$ generated by a Singer cycle is called a *Singer group*. For example, the multiplication m_ζ by a generator ζ of $F^{\times}$ is a Singer cycle and $S = \{m_b \mid b \in F^{\times}\}$ is a Singer group, which acts regularly on $F^{\times}$. In the sequel, we shall use the following standard facts (e.g. [7, Satz II.7.3 a)]):

Lemma 2 *(i) The normalizer $N_{GL(F)}(S)$ of a Singer group $S := \{m_b \mid b \in F^{\times}\}$ in $GL(F)$ coincides with $S\{\phi_a \mid a \in [0, n-1]\}$, where ϕ_a denotes the field automorphism $x \mapsto x^{2^a}$ of F for an integer a in the period* $[0, n-1]$, *regarded as an $\mathbb{F}_2$-linear bijection on F.*

(ii) We have $N_{GL(F)}(T) = N_{GL(F)}(S)$ for a subgroup T of the above Singer group S, if F is T-irreducible.

Observe that F is both S and T-irreducible with notation in Lemma 2. The following lemma is an interpretation of Lemma 2 in terms of linear algebra about an $\mathbb{F}_2$-bijection acting irreducibly on F. (In fact, Lemma 3(ii) implies that $F_\lambda^{\times}$ can be regarded as the standard Singer group S in Lemma 2 via a suitable identification of F with F_λ. Then we obtain Lemma 2(i), because $N_{GL(F)}(S)/S$ induces a group of field automorphisms on F_λ. We have Lemma 2(ii), as $F_\lambda = F_\mu$ for a generator μ of T.) We supply a proof for Lemma 3, because this lemma will be used to verify Lemma 5.

Lemma 3 *If F is $\langle\lambda\rangle$-irreducible for $\lambda \in GL(F)$, the following hold:*

(i) The minimal polynomial m_λ of λ is an irreducible polynomial in $\mathbb{F}_2[x]$ of degree $n = \dim_{\mathbb{F}_2}(F)$.

(ii) The subring $F_\lambda := \{f(\lambda) \mid f \in \mathbb{F}_2[x]\}$ of the endomorphism ring $\mathrm{End}_{\mathbb{F}_2}(F)$ is a field isomorphic to F, and $F_\lambda^\times = F_\lambda \setminus \{0\}$ is a Singer group of $GL(F)$. Moreover, the centralizer $C_{GL(F)}(F_\lambda^\times)$ of $F_\lambda^\times$ in $GL(F)$ coincides with $F_\lambda^\times$.

Proof (i) As $\lambda \neq 0$, there is $v \in Z$ with $(v)\lambda \neq 0$. Then the subspace of F spanned by $(v)\lambda^i$ for all $0 \leq i \leq \deg(m_\lambda) - 1$ is $\langle\lambda\rangle$-invariant. As F is $\langle\lambda\rangle$-irreducible, this subspace coincides with F, and hence $\deg(m_\lambda) \geq n$. As m_λ divides the characteristic polynomial of λ, which is of degree n, we have $\deg(m_\lambda) = n$.

Suppose m_λ is reducible over $\mathbb{F}_2$: $m_\lambda = fg$ for some non-constant polynomials $f, g \in \mathbb{F}_2[x]$ of degrees less than n. Then there is $v \in F$ with $w := (v)f(\lambda) \neq 0$ and the subspace spanned by $(w)\lambda^i$ for $0 \leq i \leq \deg(g) - 1$ is a $\langle\lambda\rangle$-invariant proper nonzero subspace of F, which contradicts the irreducibility of $\langle\lambda\rangle$ on F.

(ii) The ring homomorphism from $\mathbb{F}_2[x]$ into $\mathrm{End}_{\mathbb{F}_2}(F)$ sending g to $g(\lambda)$ has the image F_λ and the kernel (m_λ). As m_λ is an irreducible polynomial in $\mathbb{F}_2[x]$ of degree n by Claim (i), the quotient ring $\mathbb{F}_2[x]/(m_\lambda)$ is a field of size 2^n. Thus we have $F_\lambda \cong \mathbb{F}_2[x]/(m_\lambda) \cong \mathbb{F}_{2^n} \cong F$. In particular, $S_0 := F_\lambda^\times$ is a Singer group of $GL(F)$.

As S_0 is an abelian group acting regularly on $F^\times$, we have $C_{GL(F)}(S_0) = S_0 C_1$ with the stabilizer C_1 of $1 \in F^\times$ in $C_{GL(F)}(S_0)$. However, C_1 fixes all elements in $F^\times$, whence C_1 is the trivial subgroup. □

4 Subgroups of the automorphism group of a power APN function

4.1 Settings

Throughout the paper, unless otherwise stated, we use the letter d (or e) to denote the exponent of a *power APN function* f_d on $F \cong \mathbb{F}_{2^n}$, $n \geq 3$, defined by

$$f_d(x) := x^d \quad (x \in F).$$

Recall that, by definition, f_d is an APN function if the number of solutions x in F for equation $(x + a)^d + x^d = b$ is 0 or 2 for every $a \in F^\times$ and every $b \in F$. The graph $G(f_d)$ of f_d is

$$G(f_d) = \{(x, x^d) \mid x \in F\}, \tag{4}$$

in particular, $G(f_d)$ contains $(0, 0)$. In the action of $\mathrm{Aut}(f_d)$ on the graph $G(f_d)$, the stabilizer of $(0, 0)$ consists of all $\mathbb{F}_2$-linear bijections λ on $F \oplus F$ satisfying the following conditions:

$$\text{the map} \quad F \ni x \mapsto (x)\alpha + (x^d)\gamma \in F \text{ is a bijection,} \tag{5}$$

$$((x)\alpha + (x^d)\gamma)^d = (x)\beta + (x^d)\delta \text{ for all } x \in F. \tag{6}$$

We denote the stabilizer of (0, 0) in $\mathrm{Aut}(f_d)$ by $GL(f_d)$:

$$GL(f_d) := \left\{ \lambda = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in GL(F \oplus F) \mid \lambda \text{ satisfies (5) and (6)} \right\}. \tag{7}$$

For the exponent d, we use the symbol $Z^{(d)}$ to denote a cyclic subgroup of order $2^n - 1$ of $GL(F \oplus F)$ consisting of diagonal bijections (m_b, m_{b^d}) for all $b \in F^\times$:

$$Z^{(d)} := \{(m_b, m_{b^d}) \mid b \in F^\times\}. \tag{8}$$

As $x \mapsto (x)m_b = bx$ is bijective on F and $((x)m_b)^d = (x^d)m_{b^d}$ for all $x \in F$ and $b \in F^\times$, the group $Z^{(d)}$ lies in $GL(f_d)$. Recall that $GL(F)$ contains a field automorphism ϕ_a on F for every integer a in the period $[0, n-1]$, defined by $(x)\phi_a := x^{2^a}$ (see Lemma 2(i)). Then it is immediate to see the following subgroup $\mathrm{Aut}(F)$ of $GL(F \oplus F)$ lies in $GL(f_d)$.

$$\mathrm{Aut}(F) := \{(\phi_a, \phi_a) : (x, y) \mapsto (x^{2^a}, y^{2^a}) \mid a \in \mathbb{Z}, a \in [0, n-1]\}. \tag{9}$$

The group $\mathrm{Aut}(F)$ normalizes $Z^{(d)}$, because $(\phi_a, \phi_a)^{-1}(m_b, m_{b^d})(\phi_a, \phi_a) = (m_{b^{2^a}}, m_{b^{2^a d}})$ for $b \in F^\times$ and $a \in [0, n-1]$.

If $n \neq 6$, it is known that there is a 2-*primitive prime divisor* of $2^n - 1$, namely, a prime p which divides $2^n - 1$ but does not divide $2^i - 1$ for all integer i in the interval $[0, n-1]$. In the sequel of the paper, for $F \cong \mathbb{F}_{2^n}$ with $n \neq 6$, we use the symbols p, P and $Z_P^{(d)}$ defined as follows:

p denotes a 2-primitive prime divisor of $2^n - 1$, (10)

P denotes a unique Sylow p-subgroup of a cyclic group $F^\times$, (11)

$$Z_P^{(d)} := \{(m_b, m_{b^d}) \mid b \in P\}. \tag{12}$$

Then $Z_P^{(d)}$ is a unique Sylow p-subgroup (of order $|P|$) of the cyclic group $Z^{(d)}$ defined by (8).

We shall give few elementary observations used later.

Lemma 4 *With the above notation, the following hold.*

(i) $(d, 2^n - 1) = 1$ *or* 3 *according as n is odd or even. In particular, d is coprime to p, and hence* $P = \{b^d \mid b \in P\}$.

(ii) F *is* S_P*-irreducible for* $S_P := \{m_b \mid b \in P\}$.

Proof (i) Notice that $p \neq 3$, as we assume that $n \geq 3$. On the other hand, as d is the exponent of a power APN function, we have $(d, 2^n - 1) = 1$ or 3 according as n is odd or even (see [3, Prop 9.19]). Then the prime divisor p of $2^n - 1$, which is distinct from 3, is coprime to d.

(ii) Let K be a nonzero S_P-invariant subspace of F of dimension, say i $(1 \leq i \leq n)$. Then every S_P-orbit in $K^\times$ is of length $|P|$, whence p divides $|K| - 1 = 2^i - 1$. As p is a 2-primitive divisor of $2^n - 1$, this implies that $i = n$, that is, $K = F$. Hence F is S_P-irreducible. □

4.2 Key properties

In this subsection, d denotes the exponent of a power APN function $f_d(x) = x^d$ defined on $F \cong \mathbb{F}_{2^n}$. For $n \neq 6$, we use the symbols $Z^{(d)}$, p, P and $Z_P^{(d)}$ following definitions (8), (10), (11) and (12) in Sect. 4.1.

We shall first state a lemma describing the centralizer of a 'diagonal' element of $GL(F \oplus F)$ in the affine group $AGL(F \oplus F)$. Although it can be verified by elementary arguments, Lemma 5 makes clear the dichotomy of Proposition 1. In the proof, we frequently use the following fundamental property of the minimal polynomial m_λ of an $\mathbb{F}_2$-linear map λ: for a polynomial $g \in \mathbb{F}_2[x]$, we have $g(\lambda) = 0$ if and only if m_λ divides g.

Lemma 5 *With the notation above, let* $\lambda = (\lambda_X, \lambda_Y)$ *be a 'diagonal' element of* $GL(F \oplus F)$ *such that* λ_Z *acts irreducibly on* Z *for both* $Z \in \{X, Y\}$. *Via identifications* $(x, 0) \mapsto x$ *and* $(0, x) \mapsto x$ $(x \in F)$, *we identify* X *and* Y *with* F, *and regard* λ_X *and* λ_Y *as elements in* $GL(F)$. *We denote by* m_{λ_Z} *the minimal polynomial of* λ_Z $(Z \in \{X, Y\})$, *and denote* $F_Z := \{f(\lambda_Z) \mid f \in \mathbb{F}_2[x]\}$. *Set* $C_0 := C_{\mathrm{AGL}(F \oplus F)}(\lambda)$, *the centralizer of* λ *in* $\mathrm{AGL}(F \oplus F)$.

Then C_0 *coincides with the centralizer of* λ *in* $GL(F \oplus F)$, *and exactly one of the following holds.*

(*a*) *If* $m_{\lambda_X} \neq m_{\lambda_Y}$, X *and* Y *are the only proper nonzero* $\langle \lambda \rangle$*-invariant subspaces of* $F \oplus F$ *and*

$$C_0 = \{(\alpha, \delta) \mid \alpha \in F_X^\times, \delta \in F_Y^\times\}.$$

(*b*) *If* $m_{\lambda_X} = m_{\lambda_Y}$, *we can identify* λ_X *with* λ_Y *and* F_X *with* F_Y *such that*

$$C_0 = \left\{ \begin{pmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{pmatrix} \in GL(F \oplus F) \mid \alpha_{ij} \in F_X \right\} \cong GL_2(2^n).$$

Proof Let $v = (v_X, v_Y)$ be a vector of $F \oplus F$ fixed by λ. Then v_Z spans a $\langle \lambda_Z \rangle$-invariant subspace of Z of $\mathbb{F}_2$-dimension at most 1 $(Z \in \{X, Y\})$. As λ_Z acts irreducibly on Z and $\dim_{\mathbb{F}_2}(Z) = n \geq 2$ $(Z \in \{X, Y\})$, this implies that $v_X = v_Y = 0$, whence $v = (0, 0)$ is the unique vector in $F \oplus F$ fixed by λ. As $\mathrm{AGL}(F \oplus F)$ acts on $F \oplus F$, this vector is fixed by the centralizer C_0 of λ in $\mathrm{AGL}(F \oplus F)$, whence $C_0 \leq GL(F \oplus F)$.

By Lemma 3(i), (ii), the minimal polynomials m_{λ_Z} are irreducible of degree n, $F_Z^\times = F_Z \setminus \{0\}$ are Singer groups of $GL(F)$, and $C_{GL(F)}(\lambda_Z) = C_{GL(F)}(F_Z^\times) = F_Z^\times$ $(Z \in \{X, Y\})$.

Notice that we have $g(\lambda) = (g(\lambda_X), g(\lambda_Y))$ for every $g \in \mathbb{F}_2[x]$. For $g = m_\lambda$, the minimal polynomial of λ, we have $(0, 0) = m_\lambda(\lambda) = (m_\lambda(\lambda_X), m_\lambda(\lambda_X))$, which implies that m_λ is divisible by m_{λ_X} and m_{λ_Y}. For $g = m_{\lambda_X}$, we have $m_{\lambda_X}(\lambda) = (0, m_{\lambda_X}(\lambda_Y))$, whence $X \subseteq \mathrm{Ker}(m_{\lambda_X}(\lambda))$. Similarly, $Y \subseteq \mathrm{Ker}(m_{\lambda_Y}(\lambda))$. As $F \oplus F = X + Y$, this implies that $m_{\lambda_X} m_{\lambda_Y}(\lambda)$ is the zero map on $F \oplus F$, whence m_λ divides $m_{\lambda_X} m_{\lambda_Y}$.

Now assume that $m_{\lambda_X} \neq m_{\lambda_Y}$. Then m_{λ_X} and m_{λ_Y} are all irreducible divisors of m_λ by the conclusion in the above paragraph, whence $m_\lambda = m_{\lambda_X} m_{\lambda_Y}$. Furthermore, as

m_{λ_X} and m_{λ_Y} are coprime, the constant 1 is expressed as $1 = bm_{\lambda_X} + cm_{\lambda_Y}$ for some polynomial $b, c \in \mathbb{F}_2[x]$. Thus the identity map takes the value 0 at $\mathrm{Ker}(m_{\lambda_X}(\lambda)) \cap \mathrm{Ker}(m_{\lambda_Y}(\lambda))$, which implies that $\mathrm{Ker}(m_{\lambda_X}(\lambda)) \cap \mathrm{Ker}(m_{\lambda_Y}(\lambda)) = \{(0,0)\}$. As $X \oplus Y = F \oplus F$ and $Z \subseteq \mathrm{Ker}(m_{\lambda_Z}(\lambda))$ for $Z \in \{X, Y\}$, this implies $Z = \mathrm{Ker}(m_{\lambda_Z}(\lambda))$ for $Z \in \{X, Y\}$.

Let W be a $\langle\lambda\rangle$-invariant proper nonzero subspace of $F \oplus F$. The restriction λ_W of λ on W satisfies $m_\lambda(\lambda_W) = m_\lambda(\lambda)_W = 0_W$, whence m_{λ_W} divides $m_\lambda = m_{\lambda_X} m_{\lambda_Y}$. As m_{λ_Z} ($Z \in \{X, Y\}$) are irreducible, we have $m_{\lambda_W} = m_{\lambda_Z}$ for some $Z \in \{X, Y\}$. Then $W \subseteq \mathrm{Ker}(m_{\lambda_W}(\lambda)) = \mathrm{Ker}(m_{\lambda_Z}(\lambda)) = Z$ by the above conclusion. By the irreducibility of λ_Z on Z, this implies that $W = Z$. Hence X and Y are the unique proper nonzero $\langle\lambda\rangle$-invariant subspaces of $F \oplus F$.

For every $\alpha \in C_0$, α commutes with λ and hence with every polynomial of λ, in particular $m_{\lambda_X}(\lambda)$ and $m_{\lambda_Y}(\lambda)$. Thus α stabilizes $X = \mathrm{Ker}(m_{\lambda_X}(\lambda))$ and $Y = \mathrm{Ker}(m_{\lambda_Y}(\lambda))$. Then α is 'diagonal', namely $\alpha = (\alpha_X, \alpha_Y)$ for some $\alpha_Z \in C_{GL(Z)}(\lambda_Z) = F_Z^\times$ ($Z \in \{X, Y\}$). Thus we obtain (a).

Next assume that $m_{\lambda_X} = m_{\lambda_Y}$. Then $m_{\lambda_X}(\lambda) = (m_{\lambda_X}(\lambda_X), m_{\lambda_Y}(\lambda_Y)) = (0, 0)$, whence the minimal polynomial m_λ of λ divides m_{λ_X}. As we saw in the above paragraph, m_{λ_X} divides m_λ, and therefore we have $m_\lambda = m_{\lambda_X} = m_{\lambda_Y}$. We set $F_0 := \{f(\lambda) \mid f \in \mathbb{F}_2[x]\}$. Then $F_0 \cong \mathbb{F}_2[x]/(m_\lambda) = \mathbb{F}_2[x]/(m_{\lambda_X}) \cong F$. Via this ring isomorphism, $F \oplus F$ has a structure of an F_0-space of dimension 2. As C_0 commutes with F_0, every element of C_0 is an F_0-linear bijection on $F \oplus F$. Thus C_0 is a subgroup of the group of all F_0-linear bijections on $F \oplus F$, which is isomorphic to $GL_2(F_0) \cong GL_2(2^n)$.

On the other hand, as $m_{\lambda_X} = m_{\lambda_Y}$ is of degree n, the matrix representing λ_X with respect to the basis λ_X^i ($i = 0, 1, \ldots, n-1$) of F_X is identical to the matrix representing λ_Y with respect to the basis λ_Y^i ($i = 0, 1 \ldots, n-1$). Thus the map $\lambda_X \mapsto \lambda_Y$ is extended to a ring isomorphism of F_X with F_Y. Via this identification, we have $\lambda_0 := \lambda_X = \lambda_Y$ and $F_X = F_Y$. Furthermore, any element $\begin{pmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{pmatrix}$ of $GL(F \oplus F)$ with $\alpha_{ij} \in F_X$ commutes with $\lambda = (\lambda_0, \lambda_0)$. Thus we obtain (b). □

Corollary 1 *With the notation in* Sect. 4.1, *the only nonzero proper $Z^{(d)}$-invariant subspaces of $F \oplus F$ are X and Y.*

Proof Notice that $Z^{(d)}$ is generated by a 'diagonal' element $\lambda = (m_\zeta, m_{\zeta^d})$ of $GL(F \oplus F)$, where ζ is a generator of $F^\times$. Then $\lambda_X := m_\zeta$ acts irreducibly on X, being naturally identified with F via $(x, 0) \mapsto x$. It follows from Lemma 4(i),(ii) that $\lambda_Y = m_{\zeta^d}$ acts irreducibly on Y, identified with F via $(0, y) \mapsto y$. Thus the assumptions of Lemma 5 are satisfied. Then by Lemma 3(i) the minimal polynomial m_{λ_Z} is an irreducible polynomial of degree n for any $Z \in \{X, Y\}$. As $\lambda_X = m_\zeta$ and $\lambda_Y = m_\zeta^d$ lie in the common Singer cycle $S := \langle m_\zeta \rangle$ of $GL(X) = GL(Y) = GL(F)$, we have $F_X = F_Y$ and $F_X^\times = S$ with notation in Lemma 5.

Suppose $m_{\lambda_X} = m_{\lambda_Y}$ of λ_Y. Then λ_X and λ_Y are roots in the field $F_X = F_Y$ ($\cong \mathbb{F}_{2^n}$) of the irreducible polynomial $m_{\lambda_X} = m_{\lambda_Y}$. Thus they are conjugate over $\mathbb{F}_2$, namely there is an integer k in $[0, n-1]$ satisfying $\lambda_Y = \lambda_X^{2^k}$. Then $m_{\zeta^d} = m_{\zeta^{2^k}}$, or equivalently $d \equiv 2^k$ (modulo $2^n - 1$). However, this implies that the power APN map

$f_d(x) = x^d$ is $\mathbb{F}_2$-linear, a contradiction. Hence we have $m_{\lambda_X} \neq m_{\lambda_Y}$. Then the claim follows from Lemma 5. □

Now we shall establish an important property of a cyclic group $Z^{(d)}$ of order $2^n - 1$ of $\mathrm{Aut}(f_d)$ as Proposition 1. We investigate the centralizer of $Z_P^{(d)}$ in $\mathrm{Aut}(f_d)$. We first verify that $Z_P^{(d)}$ is generated by a 'diagonal' element λ of $GL(F \oplus F)$ satisfying the assumption of Lemma 5. As Lemma 5 suggests, then the investigation naturally splits into two cases according as the minimal polynomials of λ_X and λ_Y are distinct or identical. They correspond to the cases (a) and (b) in Proposition 1. In Case (b), the centralizer in question is embedded into a linear group $GL_2(F)$ over F by Lemma 5. We shall exploit a classification of subgroups of $PSL_2(2^n) \cong SL_2(2^n)$ (see e.g. [9, Thm 6.25]).

Proposition 1 *Assume $n \neq 6$. With the notation in* Sect. 4.1, *we denote by C the centralizer of $Z_P^{(d)}$ in* $\mathrm{Aut}(f_d)$. *Then one of the following holds.*

(a) If there is no integer a in the period $[0, n-1]$ *such that $d \equiv 2^a$ (mod $|P|$), then $C = Z^{(d)}$.*

(b) If there is an integer $a \in$ $[0, n-1]$ *such that $d \equiv 2^a$ (mod $|P|$), then C contains $Z^{(d)}$ as a normal subgroup of index at most* 2.

Proof Observe that $Z_P^{(d)} = \{(m_b, m_{b^d}) \mid b \in P\}$ is a cyclic subgroup generated by a 'diagonal' element $\lambda = (m_\eta, m_\eta^d)$ of $GL(F \oplus F)$, where η is a generator of P. Through the identifications of X and Y with F via the maps $(x, 0) \mapsto x$ and $(0, x) \mapsto x$, the $\mathbb{F}_2$-bijections $\lambda_X := m_\eta$ on X and $\lambda_Y := m_\eta^d$ on Y are regarded as elements in $GL(F) \cong GL_n(2)$. In particular, F_X and F_Y with notation in Lemma 5 are subsets of the endomorphism ring $\mathrm{End}(F)$. By Lemma 4(i),(ii), λ_X and λ_Y act irreducibly on F, identified with X and Y. Thus the assumptions of Lemma 5 are satisfied. Then it follows from Lemma 5 that $C = C_{\mathrm{Aut}(f_d)}(Z_P^{(d)}) = C_{GL(f_d)}(Z_P^{(d)})$, as $\mathrm{Aut}(f_d) \cap GL(F \oplus F) = GL(f_d)$. We have $Z^{(d)} \subseteq C$, as $Z^{(d)}$ is an abelian subgroup of $GL(f_d)$ containing $Z_P^{(d)}$.

Let m_{λ_Z} be the minimal polynomial of λ_Z ($Z \in \{X, Y\}$). As $\lambda_Y = \lambda_X^d$ and Lemma 4(i), the field F_X coincides with the field F_Y, and $S = F_X^\times$ is a Singer cycle of $GL(F)$. Then we have $m_{\lambda_X} = m_{\lambda_Y}$ if and only if $\lambda_Y = m_{\eta^d}$ and $\lambda_X = m_\eta$ are conjugate over $\mathbb{F}_2$, namely, there is an integer $a \in [0, n-1]$ such that $m_{\eta^d} = m_\eta^{2^a}$, or equivalently $\eta^d = \eta^{2^a}$. This is equivalent to the requirement that $d \equiv 2^a \pmod{|P|}$. Summarizing, we have $m_{\lambda_X} = m_{\lambda_Y}$ if and only if there is an integer $a \in [0, n-1]$ such that $d \equiv 2^a \pmod{|P|}$.

Proof of (a): If there is no integer a in $[0, n-1]$ with $d \equiv 2^a \pmod{|P|}$, we have $m_{\lambda_X} \neq m_{\lambda_Y}$ by the conclusion in the above paragraph. Then it follows from Lemma 5 that the centralizer $C_{GL(F\oplus F)}(Z_P^{(d)})$ of $Z_P^{(d)}$ in $GL(F \oplus F)$ coincides with the group $\{(m_b, m_c) \mid b, c \in F^\times\}$, as $F_X^\times = F_Y^\times = S = \{m_b \mid b \in F^\times\}$. Now (m_b, m_c) preserves the graph $G(f_d) = \{(x, x^d) \mid x \in F\}$ if and only if $(x, x^d)(m_b, m_c) = (xb, x^d c) \in G(f_d)$ for all $x \in F$, which implies that $c = b^d$. Thus we have $C = C_{GL(F\oplus F)}(Z_P^{(d)}) \cap \mathrm{Aut}(f_d) = \{(m_b, m_b^d) \mid b \in F^\times\} = Z^{(d)}$.

Proof of (b): If there is an integer a in $[0, n-1]$ with $d \equiv 2^a \pmod{|P|}$, we have $m_{\lambda_X} = m_{\lambda_Y}$ by the conclusion in the above paragraph. Then it follows from Lemma 5 that the centralizer $C_{GL(F\oplus F)}(Z_P^{(d)})$ of $Z_P^{(d)}$ in $GL(F\oplus F)$ coincides with the group isomorphic to $GL_2(2^n)$, consisting of $\mathbb{F}_2$-linear bijections of the form

$$g = \begin{pmatrix} m_{a_0} & m_{b_0} \\ m_{c_0} & m_{d_0} \end{pmatrix}$$

for some a_0, b_0, c_0, d_0 of F. (Notice that $S = F_X^{\times}$.) As g is bijective, we have $a_0d_0 + b_0c_0 \neq 0$. Thus the map sending the above g to the following matrix over F

$$\begin{pmatrix} a_0 & b_0 \\ c_0 & d_0 \end{pmatrix}$$

is a group isomorphism of the centralizer $C_{GL(F\oplus F)}(Z_P^{(d)})$ with the matrix group $GL_2(F)$ of degree 2 over F. Furthermore, the action of the element g on $F\oplus F$ is equivalent to the natural action of the corresponding element in $GL_2(F)$ on $F\oplus F$: for every $x, y \in F$,

$$(x, y)g = (xa_0 + yc_0, xb_0 + yd_0).$$

Observe that $GL_2(F) = Z(GL_2(F)) \times SL_2(F)$, where $Z(GL_2(F))$ denotes the center of $GL_2(F)$ and $SL_2(F) \cong PSL_2(F)$ consists of matrices in $GL_2(F)$ of determinant 1. Then C is identified with a subgroup of $GL_2(F)$ containing $Z^{(d)}$, which is identified with a subgroup consisting of the following diagonal matrices for all $b \in F^{\times}$, where we adopt the convention $\mathrm{diag}(a, d)$ to denote the diagonal matrix with (1, 1) and (2, 2) entries a and d respectively:

$$\mathrm{diag}(b, b^d) = \begin{pmatrix} b & 0 \\ 0 & b^d \end{pmatrix}.$$

In the sequel, for simplicity C is identified with a subgroup of the matrix group $GL_2(F)$.

With these preparations, we shall now proceed the proof of the claim (b).

We shall first show that if C is of odd order then $C = Z^{(d)}$. For short, we set $Z := Z(GL_2(F))$, the center of $GL_2(F)$. By the assumption, C is a subgroup of $GL_2(F) = Z \times SL_2(F)$ of odd order. Then the factor group CZ/Z is isomorphic to a subgroup of $SL_2(F) \cong GL_2(F)/Z$ of odd order. By [9, (6.23)], every subgroup of $SL_2(F)$ of odd order is contained in a cyclic group of order $2^n - 1$ or $2^n + 1$. In particular, $C/(C \cap Z) \cong CZ/Z$ is a cyclic group. As $C \subseteq GL_2(F)$, $C \cap Z$ lies in the center of C. Thus it follows from an elementary argument in group theory (e.g. [6, Lemma 3.4 in Chapter 1]) that C is an abelian group. As C acts on $G(f_d)^{\times} := G(f_d) \setminus \{(0, 0)\}$, with a subgroup $Z^{(d)}$ acting regularly on $G(f_d)^{\times}$, we have $C = Z^{(d)}C_{(1,1)}$, where $C_{(1,1)}$ denotes the stabilizer of a point $(1, 1)$ of $G(f_d)^{\times}$ in C. As $C_{(1,1)}$ commutes with $Z^{(d)}$, $C_{(1,1)}$ fixes every point of $G(f_d)^{\times}$, and therefore $C_{(1,1)}$ fixes all vectors in $F \oplus F$ by Lemma 1. Then $C_{(1,1)} = \{\mathrm{id}_F\}$ and $C = Z^{(d)}C_{(1,1)} = Z^{(d)}$, as desired.

Thus we may assume that a Sylow 2-subgroup of C is non-trivial. As C is a subgroup of $GL_2(F) = Z \times SL_2(F)$ with Z of odd order, every Sylow 2-subgroup of C is contained in $C \cap SL_2(F)$. As $C \cap SL_2(F)$ is a normal subgroup of C, $Z^{(d)}$ acts on the set $\mathrm{Syl}_2(C \cap SL_2(F))$ of Sylow 2-subgroups of $C \cap SL_2(F)$. Notice that $\mathrm{Syl}_2(C \cap SL_2(F)) = \mathrm{Syl}_2(\mathrm{C})$, the set of all Sylow 2-subgroups of C. We shall show that the action of $Z^{(d)}$ on $\mathrm{Syl}_2(C)$ is transitive and that $|\mathrm{Syl}_2(C)| = (2^n - 1)/(2^n - 1, d - 1)$.

We shall refer to a 1-dimensional subspace over F of $F \oplus F$ as a *projective point*. We first review some properties of 2-subgroups in $SL_2(F)$. Every non-trivial 2-subgroup T of $SL_2(F)$ acts on the set of $2^n + 1$ projective points, and hence T fixes a projective point. If T fixes more than one projective points, then up to the conjugacy in $SL_2(F)$ T lies in the diagonal subgroup of order $2^n - 1$, a contradiction. Thus there is a unique projective point fixed by T. In particular, for every projective point v, there is a unique Sylow 2-subgroup of $SL_2(F)$ fixing v but does not fix any projective point other than v. We denote such a Sylow 2-subgroup by U_v. Thus if T is a nontrivial 2-subgroup fixing a projective point v then T is contained in U_v.

Applying this remark to a Sylow 2-subgroup T of C (which lies in $C \cap SL_2(F)$), we have $T = C \cap U_v$, where v is the unique projective point fixed by T. As T lies in C, acting on $G(f_d)^\times$ of length $2^n - 1$, T fixes a vector (x, x^d) in $G(f_d)^\times$. Thus we have $v = F(x, x^d)$. Hence for every two subgroups T_i in $\mathrm{Syl}_2(C)$ $(i = 1, 2)$ we have $T_i = C \cap U_{v_i}$ with $v_i = F(x_i, x_i^d)$ for some $x_i \in F^\times$ $(i = 1, 2)$. As $Z^{(d)}$ is transitive on $G(f_d)^\times$, there is $g \in Z^{(d)}$ such that $(v_1)g = v_2$. Then we have $g^{-1}U_{v_1}g = U_{v_2}$ and $g^{-1}T_1 g = g^{-1}(C \cap U_{v_1})g = C \cap g^{-1}U_{v_1}g = C \cap U_{v_2} = T_2$. This verifies the transitivity of $Z^{(d)}$ on $\mathrm{Syl}_2(C)$. Assume that $g = \mathrm{diag}(b, b^d)$ normalizes $T = C \cap U_v$ for $v = F(x, x^d)$ with $x \in F^\times$. Then g stabilizes the unique projective point $v = F(x, x^d)$ fixed by T, and therefore $(x, x^d)g = (xb, x^d b^d) = c(x, x^d)$ for some $c \in F^\times$. This implies that $b = c = b^d$, whence $b^{d-1} = 1$. Thus the normalizer of $T \in \mathrm{Syl}_2(C)$ in $Z^{(d)}$ is $\{\mathrm{diag}(b, b^d) \mid b \in F^\times, b^{d-1} = 1\}$, which has order $(2^n - 1, d - 1)$. Thus we conclude that $|\mathrm{Syl}_2(C)| = (2^n - 1)/(2^n - 1, d - 1)$.

In view of the list of subgroups of $SL_2(F) \cong PSL_2(2^n)$ [9, Thm 6.25], $C \cap SL_2(F)$ is isomorphic to one of the following groups:

(a) The dihedral groups of order $2(2^n \pm 1)$ and their subgroups.
(b) A subgroup H of order $2^n(2^n - 1)$ and their subgroups. H has a unique Sylow 2-subgroup T on which a cyclic subgroup of order $2^n - 1$ acts fixed point freely. H is the stabilizer of a projective point.
(c) A_4 or A_5 (the possibility S_4 does not occur by [9, Thm 6.26(iii)]).
(d) A subgroup of $GL_2(2^m)$ containing $SL_2(2^m)$ for a positive divisor m of n.

Accordingly, $|\mathrm{Syl}_2(C \cap SL_2(F))| = (2^n - 1)/(2^n - 1, d - 1)$ is given as follows:

$$\begin{array}{ll} (1/2)|C \cap SL_2(F)| & \text{for (a),} \\ 1 & \text{for (b) and the first case of (c),} \\ 2^m + 1 & \text{for (d) and the second case of (c) (with } m = 2). \end{array}$$

If (b) or the first case of (c) occurs, we have $2^n - 1 = (2^n - 1, d - 1)$. Then $d - 1$ is a multiple of $2^n - 1$, and thus $x^{d-1} = 1$ for all $x \in F^\times$. This implies that $f_d(x) = x^d = x$ for all $x \in F$, contradicting that f_d is APN. If (d) or the second case of (c) occurs, we conclude that $2^m - 1$ divides $(2^n - 1, d - 1)$ and hence $d - 1$, because $2^m - 1$ is a divisor of $2^n - 1$ which is coprime to $2^m + 1 = (2^n - 1)/(2^n - 1, d - 1)$. This implies that we have $y^{d-1} = 1$ for any nonzero element y in the subfield $K \cong \mathbb{F}_{2^m}$ of F. Thus $y^d = y$ for every $y \in K$. Fixing $a \in K^\times$, we have $(y + a)^d + y^d = y + a + y = a$, as $y + a \in K$ as well. However, this implies that every $y \in K$ is a solution for equation $(x + a)^d + x^d = a$. As $f_d(x) = x^d$ is APN, this equation has at most 2 solutions. Hence we have $2^m = |K| \leq 2$. This happens only when $m = 1$. Notice that in this case $C \cap SL_2(F) \cong PSL_2(2) \cong PGL_2(3) \cong S_3$, the symmetric group of order 3, and that $3 = 2^1 + 1$ divides $2^n - 1$. Thus this is contained in case (a). Summarizing, the only remaining case is (a). In both cases, we have $|C \cap SL_2(F)| = 2k$ for an odd number $k := (2^n - 1)/(2^n - 1, d - 1)$ dividing $2^n - 1$. We have $k \neq 1$, as we saw above.

Then the 2-part of $|C|$ is 2, because $C/(C \cap SL_2(F)) \cong CSL_2(F)/SL_2(F)$ is isomorphic to a subgroup of $GL_2(F)/SL_2(F) \cong Z(GL_2(F))$, which is a cyclic group of order $2^n - 1$, and thus $|C| = |C \cap SL_2(F)|k_1 = 2kk_1$ for a divisor k_1 of $2^n - 1$. Considering the action of C on C via the right multiplication, we can verify that there is a normal subgroup of order kk_1 of C (e.g. [9, Chapter 5,(1.8)]). This is a unique maximal subgroup of odd order in C, denoted $O(C)$. Thus $O(C) \cap SL_2(F)$ (of order k) and $Z^{(d)}$ are subgroups of C of odd order, whence they are contained in $O(C)$. Observe that $O(C) \cap SL_2(F)$ is a subgroup of order k, dividing $2^n - 1$, and that it acts on the set of $2^n + 1$ projective points (in $F \oplus F$). Let R be a Sylow r-subgroup R of $O(C) \cap SL_2(F)$ for a prime divisor r of k. Notice that R fixes at least two projective points, because $|R|$ divides $2^n - 1$ and R acts on the $2^n + 1$ projective points. As R is a nontrivial group, it fixes exactly two projective points, say X_i $(i = 1, 2)$. By [8,(6.23)], $O(C) \cap SL_2(F)$ is cyclic. Thus R is the unique Sylow r-subgroup of $O(C) \cap SL_2(F)$, whence R is a normal subgroup of $O(C)$. Then $O(C)$ is a nontrivial group of odd order permuting X_i $(i = 1, 2)$, and hence fixing X_i $(i = 1, 2)$. In particular, X_i $(i = 1, 2)$ are the only projective points fixed by $O(C)$. On the other hand, we know that a subgroup $Z^{(d)}$ of $O(C)$ stabilizes two projective points $X = \{(x, 0) \mid x \in F\}$ and $Y = \{(0, y) \mid y \in F\}$. Hence we should have $\{X_1, X_2\} = \{X, Y\}$, and $O(C)$ stabilizes X and Y. Thus $O(C)$ consists of diagonal matrices $\mathrm{diag}(a, b)$ $(a, b \in F^\times)$. As $O(C)$ acts on the graph $G(f_d)$, we should have $(ax, bx^d) \in G(f_d)$ for all $x \in F$, which implies that $b = a^d$. Hence $O(C)$ lies in $Z^{(d)} = \{\mathrm{diag}(a, a^d) \mid a \in F^\times\}$. We have verified that C contains $O(C) = Z^{(d)}$ as a subgroup of index 2. □

We close this section with two corollaries of Proposition 1.

Corollary 2 *Assume* $n \neq 6$. *With the notation in Sect. 4.1,* $Z_P^{(d)}$ *is a Sylow* p*-subgroup of* $\mathrm{Aut}(f_d)$.

Proof We first show that $Q := \{(m_b, m_c) \mid b, c \in P\}$, an abelian group of order $|P|^2$, is a Sylow p-subgroup of $GL(F \oplus F)$. We have $|GL(F \oplus F)| = |GL_{2n}(2)| = 2^{n(2n-1)}\Pi_{i=1}^{2n}(2^i - 1)$, where $2^{n+i} - 1 \equiv 2^i - 1 \pmod{2^n - 1}$ for all $i \in [1, n]$. As p is a 2-primitive prime divisor of $2^n - 1$, integers $2^j - 1$ for $j \in [1, 2n]$ are coprime with p, unless $j = n$ or $2n$. Thus the p-part of $|GL(F \oplus F)|$ is $|P|^2$, whence the above subgroup Q of $GL(F \oplus F)$ is a Sylow p-subgroup of $GL(F \oplus F)$.

Then Q is a Sylow p-subgroup of $\mathrm{AGL}(F \oplus F)$ as well, because $[\mathrm{AGL}(F \oplus F) : GL(F \oplus F)] = 2^n$. In particular, every Sylow p-subgroup of $\mathrm{AGL}(F \oplus F)$ is abelian, and thus the same holds for every Sylow p-subgroup of $\mathrm{Aut}(f_d)$. Let R be a Sylow p-subgroup of $\mathrm{Aut}(f_d)$ containing $Z_P^{(d)} = \{(m_b, m_{b^d}) \mid b \in P\}$. As R is abelian, R is a subgroup of the centralizer C of $Z_P^{(d)}$ in $\mathrm{Aut}(f_d)$. By Proposition 1(a)(b), $Z^{(d)}$ is the unique maximal subgroup of C of odd order, and thus $R \subseteq Z^{(d)}$, as p is odd. Then R coincides with the unique Sylow p-subgroup $Z_P^{(d)}$ of a cyclic group $Z^{(d)}$ of order $2^n - 1$. Thus $R = Z_P^{(d)}$ is a Sylow p-subgroup of $\mathrm{Aut}(f_d)$, as desired. □

Corollary 3 *Let d be the exponent of a power APN function $f_d(x) = x^d$ defined on $F \cong \mathbb{F}_{2^n}$ ($n \geq 3$, $n \neq 6$). Then every cyclic subgroup of* $\mathrm{Aut}(f_d)$ *of order* $2^n - 1$ *is conjugate to $Z^{(d)}$.*

Proof Let Z be a cyclic subgroup of $\mathrm{Aut}(f_d)$ of order $2^n - 1$, and let Q be a Sylow p-subgroup of Z. Then $|Q| = |Z_P^{(d)}| = |P|$. As $Z_P^{(d)}$ is a Sylow p-subgroup of $\mathrm{Aut}(f_d)$ by Corollary 2, Q is also a Sylow p-subgroup of $\mathrm{Aut}(f_d)$, and therefore, there is an element $g \in \mathrm{Aut}(f_d)$ such that $g^{-1}Qg = Z_P^{(d)}$ by Sylow's theorem. As $g^{-1}Zg$ is an abelian group containing $g^{-1}Qg = Z_P^{(d)}$, we see that $g^{-1}Zg$ is a subgroup of C of odd order. Thus $g^{-1}Zg \subseteq Z^{(d)}$ by Proposition 1(a)(b). Then we have $g^{-1}Zg = Z^{(d)}$ by comparing the orders. □

Remark Corollary 3 holds even when $n = 6$. Power APN functions on $F \cong \mathbb{F}_{2^6}$ are EA-equivalent to the Gold function $f_3(x) = x^3$, as we will see in the proof of Theorem 1. By the remark (2) after Theorem 2, we have $\mathrm{Aut}(f_3) \cong A\Gamma L(1, 2^6)$, which has a normal subgroup T of order 2^6 with factor group $\mathrm{Aut}(f_3)/T$ of order $(2^6 - 1) \cdot 6$. The subgroup $Z^{(3)}\mathrm{Aut}(F)$ (defined as (8) and (9)) corresponds to a normal subgroup of $\mathrm{Aut}(f_3)/T$. For the subfield K of F of size 2^3, $Q := \{(m_b, m_{b^3}) \mid b \in K^\times\}$ is a Sylow 7-subgroup of $\mathrm{Aut}(f_3)$. The centralizer of Q in $\mathrm{Aut}(f_3)$ is $Z^{(3)}\{\phi_a \mid a \in \{0, 3\}\}$ of order $63 \cdot 2$. Thus Sylow's theorem for the prime 7 implies that every cyclic subgroup of $\mathrm{Aut}(f_3)$ of order 63 is conjugate to $Z^{(3)}$.

5 Proof of the main theorems

In this section, we shall provide proofs for the main Theorems 1 and 2 given in the introduction.

Proof of Theorem 1 We first treat the case $n = 6$. In this case, Lemma 4(i) implies that the exponent d of a power APN function is of the form $d = 3f$ for some integer f in $[0, 21]$ coprime to 3 and 7, as $2^n - 1 = 63$. There are $21 - (21/3) - (21/7) + (21/21) = 12$ such integers f. Thus the corresponding d's split into two 2-cyclotomic classes $\{3 \cdot 2^a \mid a \in [0, 5]\}$ and $\{(-3) \cdot 2^a \mid a \in [0, 5]\}$ modulo 63. The former class yields power APN functions EA-equivalent to the Gold function $f_3(x) = x^3$. The latter class yields a power function EA-equivalent to $f_{-3}(x)$ ($= x^{-3}$ or 0 according as $x \neq 0$ or $x = 0$), which is not APN: because, for the subfield $K \cong \mathbb{F}_{2^3}$ of F all elements x in

$K \setminus \mathbb{F}_2$ satisfy $0 = (x^7+1)/(x+1) = \sum_{i=0}^{6} x^i$, and thus

$$(x+1)^{-3} + x^{-3} = \frac{x^3 + (x^3+x^2+x+1)}{x^3(x+1)^3} = \frac{\sum_{i=0}^{2} x^i}{\sum_{i=3}^{6} x^i} = 1.$$

Thus the case (A) holds for exponents d and e for power APN functions on $F = \mathbb{F}_{2^6}$.

Hence we shall assume $n \neq 6$ in the sequel.

Assume first that f_d is CCZ-equivalent to f_e. Let α' be an $\mathbb{F}_2$-affine bijection on $F \oplus F$ sending the graph $G(f_d)$ to the graph $G(f_e)$. Then $\alpha' Z^{(e)} \alpha'^{-1}$ and $Z^{(d)}$ are cyclic subgroups of $\mathrm{Aut}(f_d)$ of order $2^n - 1$. By Corollary 3, there is an element g in $\mathrm{Aut}(f_d)$ such that $g^{-1}\alpha' Z^{(e)} \alpha'^{-1} g = Z^{(d)}$. Then $\lambda := g^{-1}\alpha'$ is an $\mathbb{F}_2$-linear affine bijection on $F \oplus F$ sending $G(f_d)$ to $G(f_e)$ and

$$Z^{(e)} = \lambda^{-1} Z^{(d)} \lambda. \tag{13}$$

Remark that $\lambda \in GL(F \oplus F)$, because λ sends the unique point $(0,0)$ on $G(f_e)$ fixed by $Z^{(e)}$ to the unique point $(0,0)$ on $G(f_d)$ fixed by $Z^{(d)}$, and hence λ fixes $(0,0)$.

By Corollary 1 applied to $Z^{(d)}$, the only nonzero proper $Z^{(d)}$-invariant subspaces of $F \oplus F$ are X and Y, which are sent by λ to nonzero proper $Z^{(e)}$-invariant subspaces of $F \oplus F$. The latter subspaces are X and Y as well by Corollary 1 applied to $Z^{(e)}$. Thus we have

either (a) $(X)\lambda = X$ and $(Y)\lambda = Y$ or (b) $(X)\lambda = Y$ and $(Y)\lambda = X$.

In case (a), λ is an element in $GL(F \oplus F)$ of the diagonal form (α, δ) for some $\mathbb{F}_2$-linear bijections α and δ on F. Then the condition (13) implies that for every $b \in F^\times$ there is some $c \in F$ such that

$$(\alpha^{-1}, \delta^{-1})(m_b, m_{b^d})(\alpha, \delta) = (m_c, m_{c^e}).$$

Then $m_c = \alpha^{-1} m_b \alpha$ and $m_{c^e} = \delta^{-1} m_{b^d} \delta$. As $m_{c^e} = m_c^e = (\alpha^{-1} m_b \alpha)^e = \alpha^{-1} m_{b^e} \alpha$, we conclude that

$$(\delta\alpha^{-1})^{-1} m_{b^d} \delta\alpha^{-1} = m_{b^e} \tag{14}$$

for all $b \in F^\times$. Now $S^{(e)} := \{m_{b^e} \mid b \in F^\times\}$ and $S^{(d)} := \{m_{b^d} \mid b \in F^\times\}$ are subgroups of the Singer group $S = \{m_b \mid b \in F\}$ of index 1 or 3 according as n is odd or even (see Lemma 4(i)). Thus $S^{(e)} = S^{(d)}$ and $\delta\alpha^{-1}$ normalizes $S^{(d)}$. As F is $S^{(d)}$-irreducible by Lemma 4(ii), we have $\delta\alpha^{-1} \in N_{GL(F)}(S) = S\{\phi_a \mid a \in [0, n-1]\}$ by Lemma 2(ii). Then $\delta\alpha^{-1} = m_c \phi_a$ for some $c \in F^\times$ and $a \in [0, n-1]$. As m_c commutes with S, Eq. (14) for $\delta\alpha^{-1} = m_c\phi_a$ reads $\phi_a^{-1} m_{b^d} \phi_a = m_{b^{d2^a}} = m_{b^e}$ for all $b \in F^\times$. Thus we have $b^{d2^a} = b^e$ for all $b \in F^\times$, and therefore $e \equiv d2^a \pmod{2^n - 1}$.

In case (b), λ is an element in $GL(F \oplus F)$ of the anti-diagonal form $\begin{pmatrix} 0 & \beta \\ \gamma & 0 \end{pmatrix}$ for some $\mathbb{F}_2$-linear bijections β and γ on F. Then the condition (13) implies that for every

$b \in F^{\times}$ there is some $c \in F$ with

$$\begin{pmatrix} 0 & \gamma^{-1} \\ \beta^{-1} & 0 \end{pmatrix} (m_b, m_{b^e}) \begin{pmatrix} 0 & \beta \\ \gamma & 0 \end{pmatrix} = (m_c, m_{c^d}).$$

Then $m_c = \gamma^{-1} m_{b^e} \gamma$ and $m_{c^d} = \beta^{-1} m_b \beta$. As $m_{c^d} = (m_c)^d = \gamma^{-1}(m_{b^e})^d \gamma = \gamma^{-1} m_{b^{de}} \gamma$, we have

$$(\beta\gamma^{-1})^{-1} m_b \beta\gamma^{-1} = m_{b^{de}} \tag{15}$$

for all $b \in F^{\times}$. Then the conjugation by $\beta\gamma^{-1} \in GL(F)$ sends a Singer group S to its subgroup $\{m_{b^{de}} \mid b \in F^{\times}\}$ of index $(de, 2^n - 1)$. In particular, we should have $(de, 2^n - 1) = 1$. As $(d, 2^n - 1) = (e, 2^n - 1) = 1$ or 3 according as n is odd or even, this happens only when n is odd. In the case when n is odd, $\beta\gamma^{-1}$ normalizes S, and therefore the arguments in the case (a) show that $2^a \equiv de \pmod{2^n - 1}$ for some integer a in $[0, n-1]$.

Conversely, assume that $d \equiv 2^a e$ or $de \equiv 2^a \pmod{2^n - 1}$ for some integer $a \in [0, n-1]$ with n odd in the latter case. In the former case, the linear bijection $(x, y) \mapsto (x, y^{2^a})$ on $F \oplus F$ induces an EA-equivalence of f_d with f_e. In the latter case, the linear map $(x, y) \mapsto (y, x^{2^a})$ on $F \oplus F$ maps $G(f_d)$ to $G(f_e)$, whence it induces a CCZ-equivalence of f_d with f_e. □

Proof of Theorem 2 As an $\mathbb{F}_2$-affine bijection $(x, y) \mapsto (x, y + (0)f)$ $(x, y \in F)$ induces an EA-equivalence of f with $\bar{f}$ (defined by $(x)\bar{f} = (x)f + (0)f$), we may assume that $(0)f = f$ by replacing f with $\bar{f}$. We define B_f by $B_f(x, y) := f(x + y) + f(x) + f(y)$ for $x, y \in F$. Then B_f is an $\mathbb{F}_2$-bilinear map from $F \oplus F$ to F, as f is quadratic. Observe that the following map t_a for each $a \in F$ is an $\mathbb{F}_2$-affine map which sends $(x, f(x)) \in G(f)$ to $(x + a, f(x + a)) \in G(f)$ for all $x \in F$:

$$t_a : (x, y) \mapsto (x, B_f(x, a) + y) + (a, f(a)).$$

As $t_{a+b} = t_a t_b$ for $a, b \in F$, we see that $T := \{t_a \mid a \in F\}$ is a subgroup of $\mathrm{Aut}(f)$, called the *standard translation group*. Observe that T acts regularly on $G(f)$, as $(0, 0)t_a = (a, f(a))$. We recall an important result [4, Corollary 5.11], which in particular says that the standard translation group T is normal in $\mathrm{Aut}(f)$.

On the other hand, recall that $\mathrm{Aut}(f_d)$ of a power APN function f_d contains the cyclic group $Z^{(d)}$ (see 8) which fixes $(0, 0)$ but acts regularly on $G(f_d) \setminus \{(0, 0)\}$. Then it follows from the assumption that f is CCZ-equivalent to f_d, the automorphism group $\mathrm{Aut}(f) \cong \mathrm{Aut}(f_d)$ contains a cyclic group Z of order $2^n - 1$, which fixes a point v and is transitive on the remaining points $G(f) \setminus \{v\}$ in the graph $G(f)$. Thus $\mathrm{Aut}(f)$ is doubly transitive on the graph $G(f)$.

In order to have exact shape of $\mathrm{Aut}(f)$ and f, we shall exploit results about a *dimensional dual hyperoval* (abbreviated to DHO) and the associated incidence geometry. The former concept is defined to be a collection of some subspaces of constant dimension in a finite-dimensional vector space with some intersection properties, and the latter is obtained as the incidence graph of its "affine expansion." For their formal definitions and fundamental properties, see e.g. [11] as for DHOs, and [14] as for the associated *semibiplanes*. The explicit DHO we consider here is just the following object:

$$\mathcal{S}[f] := \{X(t) \mid t \in F\}, \text{ where } X(t) := \{(x, B_f(x,t)) \mid x \in F\} \text{ for } t \in F.$$

Observe that $X(t)$ for each $t \in F$ is a subspace of $F \oplus F$ of dimension n. The collection $\mathcal{S}[f]$ of such subspaces is a DHO associated with a quadratic APN function f. The semibiplane Γ_f associated with $\mathcal{S}[f]$ is isomorphic to the incidence graph of the affine expansion of $\mathcal{S}[f]$ [14, Prop 6].

There is a close relation between the automorphisms of a quadratic APN function and a DHO associated with a quadratic APN function. By [4, Thm 3.10], the automorphism group of the DHO $\mathcal{S}[f]$ is isomorphic to the normalizer of the standard translation group T in $\mathrm{Aut}(f)$. In our situation, this implies that $\mathrm{Aut}(\mathcal{S}[f])$ is isomorphic to $\mathrm{Aut}(f)$, as T is normal in $\mathrm{Aut}(f)$.

As $\mathrm{Aut}(f)$ is doubly transitive on $G(f)$, $\mathrm{Aut}(\mathcal{S}[f])$ is doubly transitive on $\mathcal{S}$. Furthermore, $\mathrm{Aut}(\mathcal{S}[f])$ contains a cyclic subgroup Z of order $2^n - 1$ which fixes a member X but transitive on the remaining members in $\mathcal{S}[f]$. As $\mathrm{Aut}(\mathcal{S}[f])$ contains a normal subgroup acting regularly on $\mathcal{S}[f]$, we may assume that $X = X(0) = \{(x, 0) \mid x \in F\}$. Then Z acts regularly on $\mathcal{S}[f] \setminus \{X(0)\}$. We note that Z acts regularly on the nonzero vectors of $X(0)$, because the map sending a member $X(t)$ of $\mathcal{S}[f] \setminus \{X(0)\}$ to the unique nonzero vector $X(t) \cap X(0)$ is a bijection. Now we verified that the assumption of [13, Thm 10] is satisfied, unless $n = 6$.

When $n = 6$, the power APN functions on $F \cong \mathbb{F}_{2^6}$ are f_d for $d = 3 \cdot 2^a$ for $a \in [0, 5]$, as we saw at the beginning in the proof of Theorem 1. They are quadratic as well, because they are EA-equivalent to the Gold function g_1. Thus the theorem holds if $n = 6$. Thus in the following we assume $n \neq 6$.

Then it follows from [13, Thm 1] that $\mathcal{S}[f]$ is isomorphic to the DHO $\mathcal{S}^n_{\sigma,\tau}$ for some generators σ and τ of $\mathrm{Gal}(F/\mathbb{F}_2)$ (for the explicit construction of the DHO $\mathcal{S}^n_{\sigma,\tau}$, see e.g. [10]). Furthermore we have $\sigma = \tau$. The exposition after [14, Prop1] claims that the map denoted σ_f there induces a covering map of the semibiplane Γ_f by the truncated Coxeter complex of type D_{2^n} (called the hypercube in [8]). By [8, Thm 1.11], $\mathcal{S}^n_{\sigma,\tau}$ has this property (that is, the associated semibiplane is covered by the hypercube) if and only if $\sigma = \tau$.

Writing $x^\sigma = x^{2^s}$ $(x \in F)$, we have $(s, n) = 1$ and then $\mathcal{S}^n_{\sigma,\sigma}$ is identical to the DHO $\mathcal{S}[g_s]$ for the Gold function g_s defined by $g_s(x) = x^{2^s+1}$. As $\mathcal{S}[f]$ is isomorphic to $\mathcal{S}^n_{\sigma,\sigma} = \mathcal{S}[g_s]$, it follows from [14, Prop 5] that f is EA-equivalent to g_s. □

Remarks (1) To obtain the conclusion $\sigma = \tau$ at the second last paragraph in the proof, I exploited some facts obtained in the language of incidence geometry. Instead, there are several accounts for this conclusion starting with one of the following interpretations for the fact that the semibiplane associated with the DHO $\mathcal{S}[f]$ is covered by the truncated Coxeter complex of type D_{2^n}: the DHO $\mathcal{S}[f]$ is *alternating* in the sense of [4, Definition a) before Example 2.2], or the DHO $\mathcal{S}[f]$ is covered by the Huybrechts DHO.

(2) The automorphism group of the DHO $\mathcal{S}^n_{\sigma,\sigma} = \mathcal{S}[g_s]$ is calculated in [10] (including when $n = 6$): $\mathrm{Aut}(g_s) \cong \mathrm{Aut}(\mathcal{S}[g_s]) \cong 2^n : A\Gamma L(1, F)$ if $n \geq 4$.

6 Applications

We shall give a complete solution for the CCZ-equivalence problems among known power APN functions, as applications of Theorem 1. We adopt the following convention to denote the known power APN functions: defined on $F = \mathbb{F}_{2^n}$, $n \geq 3$. Here we do not include the inverse functions and the Dobbertine functions, as they are CCZ-inequivalent to any power APN functions in this list (this fact is verified e.g. by comparing their Walsh coefficients).

Name	Symbol	Exponents d	Conditions
Gold	g_s	$1+2^s$	$1 \leq s < n/2$, $(s, n) = 1$
Kasami	κ_r	$1-2^r+2^{2r}$	$2 \leq r < n/2$, $(2, r) = 1$
Welch	w	$3+2^t$	$n = 2t+1$: odd, $n \geq 9$
Niho	ν	$-1+2^u+2^{2u}$	$n = 2t+1 = 4u+1$: odd, $t = 2u$, $u \geq 3$ (so $n \geq 13$);
	ν	$-1+2^{2u+1}+2^{3u+2}$	$n = 2t+1 = 4u+3$: odd, $t = 2u+1$, $u \geq 2$ (so $n \geq 11$)

Proposition 2 *(i) The Gold functions g_s and g_t defined on $F = \mathbb{F}_{2^n}$ are CCZ-equivalent if and only if $s = t$.*

(ii) The Gold function g_s and the Kasami function κ_r defined on $F = \mathbb{F}_{2^n}$ are CCZ-equivalent if and only if either $s = r$ or $(n, s, r) = (5, 1, 2)$.

(iii) On $F = \mathbb{F}_{2^n}$ with n odd and $n \geq 9$, the Gold function g_s and the Welch function w are always CCZ-inequivalent.

(iv) On $F = \mathbb{F}_{2^n}$ with n odd and $n \geq 9$, the Gold function g_s and the Niho function ν are always CCZ-inequivalent.

(v) The Kasami functions κ_r and κ_s defined on $F = \mathbb{F}_{2^n}$ are CCZ-equivalent if and only if $r = s$.

(vi) On $F = \mathbb{F}_{2^n}$ with n odd and $n \geq 9$, the Kasami function κ_r and the Welch function w are always CCZ-inequivalent.

(vii) On $F = \mathbb{F}_{2^n}$ with n odd and $n \geq 9$, the Kasami function κ_r and the Niho function ν are always CCZ-inequivalent.

(viii) On $F = \mathbb{F}_{2^n}$ with n odd and $n \geq 11$, the Welch function w and the Niho function ν are always CCZ-inequivalent.

Proof Theorem 1 reduces the CCZ-problem between power APN functions to problems for solving congruence equations modulo $2^n - 1$. The latter are usually settled by straightforward but tedious calculations. Thus we just give such calculations in the cases (i) and (ii), but they are briefly sketched in the remaining cases. The details are left as exercises for the reader.

(i) By Theorem 1, g_s is CCZ-equivalent to g_t if and only if there is $a \in [0, n-1]$ such that (A) $1+2^t \equiv (1+2^s)2^a$ or (B) $(1+2^t)(1+2^s) \equiv 2^a$ modulo $2^n - 1$. In case (A), we have $\{0, t\} \equiv \{a, a+s\} \pmod{n}$ by comparing the 2-adic expansions of both sides of the congruence equation. In particular, $\pm t \equiv (a+s) - a \pmod{n}$, whence

$s \equiv \pm t \pmod n$. If $s \equiv t \pmod n$, we have $s = t$, as $1 \le s, t < n/2$. If $s \equiv -t$ (mod n), $s + t$ is a multiple of n, which contradicts $s + t < 2(n/2) = n$. In case (B), the 2-weight of the left-hand side $1 + 2^s + 2^t + 2^{s+t}$ of the congruence relation should be 1. In particular, 0 should be equal to one of $\{s, t, s+t\}$ modulo n, which is impossible, as $0 < s, t, s + t < n$. This verified the claim.

(ii) By Theorem 1, g_s is CCZ-equivalent to κ_r if and only if there is $a \in [0, n-1]$ such that (A) $e \equiv d2^a$ or (B) $de \equiv 2^a$ modulo $2^n - 1$ for $d := 1 - 2^r + 2^{2r}$ and $e := 1 + 2^s$. In case (A), comparing the 2-weight of both sides of the congruence relation, we have $w_2(1 + 2^s) = w_2(1 - 2^r + 2^{2r})$; namely $2 = r + 1$, which is impossible, as $r \ge 2$. Thus the only possibility is case (B). In this case, we have

$$1 + 2^s + 2^{3r} + 2^{3r+s} = (1 + 2^s)(1 + 2^{3r}) \equiv (1 + 2^r)2^a \pmod{2^n - 1} \quad (16)$$

by multiplying $(1 + 2^r)$ both sides of the congruence equation. As the right-hand side has 2-weight 2, the set $\{0, s, 3r, 3r + s\}$ of the monomial terms in the left-hand side is of size at most 3. Thus one of the following holds modulo n: $0 \equiv s, 0 \equiv 3r, 0 \equiv 3r + s$, $s \equiv 3r$, $s \equiv 3r + s$ or $3r \equiv 3r + s$. As $(n, s) = 1$, we have $0 \not\equiv s \pmod n$. Remark $3r \not\equiv 0 \pmod n$, for otherwise we have $3 \equiv 0 \pmod n$, as $(r, n) = 1$, but this implies that 3 is a multiple of n, whence $n = 3$. However, the Kasami function is not defined on $\mathbb{F}_{2^3}$. Thus we have $3r + s \equiv 0$ or $s \equiv 3r \pmod n$.

If $s \equiv -3r \pmod n$, Eq. (16) reads $2 + 2^{1-3r} \equiv 2^a + 2^{a+r} \pmod{2^n - 1}$, and thus $\{1, 1 - 3r\} \equiv \{a, a + r\}$ by comparing the exponents appearing the 2-adic expansions of both sides. Then we have $(a + r) - a \equiv \pm\{1 - (1 - 3r)\} \pmod n$, or equivalently $4r \equiv 0$ or $2r \equiv 0 \pmod n$. As $(r, n) = 1$, this implies that $4 \equiv 0$ or $2 \equiv 0 \pmod n$, which is impossible because the Kasami function is not defined on $\mathbb{F}_{2^n}$ for $i = 2, 4$.

Thus we have $s \equiv 3r \pmod n$. As the exponents in the left-hand side of Eq. (16) are 0, $s + 1$ and $2s$ in this case, we have $0 \equiv s + 1$ or $s + 1 \equiv 2s \pmod n$ (the case $0 \equiv 2s$ does not happen, for otherwise $0 \equiv 2$ as $(n, s) = 1$). If $s + 1 \equiv 0$ (mod n), we have $s + 1 \ge n$, but this contradicts $s < n/2$. Hence the only remaining case is $3r \equiv s \equiv 1 \pmod n$. In this case, $s = 1$ as $1 \le s < n/2$, and Eq. (16) reads $1 + 2^3 \equiv 2^a + 2^{a+r} \pmod{2^n - 1}$. Thus we have either $r \equiv 3$ or $r \equiv -3 \pmod n$. If $r \equiv 3 \pmod n$, we have $3r = 9 \equiv s = 1 \pmod n$. Thus we have $n = 8$ (as the Kasami function cannot be defined on $\mathbb{F}_{2^4}$). However, in this case $r = 3$ and the exponents $d = 1 + 2^s = 3$ and $e = 1 - 2^r + 2^{2r} = 57$ do not satisfy $de = 171 \equiv 2^a$ (mod $2^n - 1 = 255$) for any integer a in $[0, 7]$. Hence we have $r \equiv -3 \pmod n$. In this case, we have $-3r \equiv -9 \equiv 1 \pmod n$, whence n divides 10. If $n = 10$, then $r \equiv -3$ (mod n) implies $r = 7$, but this contradicts $r < n/2 = 5$. Thus we have $n = 5$. In this unique remaining case $(n, s, r) = (5, 1, 5 - 3 = 2)$, the exponents $d = 1 + 2^s = 3$ and $e = 1 - 2^r + 2^{2r} = 13$ in fact satisfy $de = 39 \equiv 2^3 \bmod 2^n - 1 = 31$.

(iii) We shall omit the details, because the arguments are similar but simpler to those in (iv). Notice that this claim was already shown in [2, Prop 6].

(iv) We just give a verification in the case when $(n - 1)/2 = t = 2u$ is even. The case $t = 2u + 1$ odd can be settled by similar calculations.

By Theorem 1, g_s is CCZ-equivalent to ν if and only if there is $a \in [0, n-1]$ such that (A) $e := -1 + 2^u + 2^{2u} \equiv d2^a$ for $d := 1 + 2^s$, or (B) $de \equiv 2^a$ modulo $2^n - 1$. In case (A), we have $u + 1 = 2$ by comparing the 2-weights of both sides. This contradicts the assumption $u \geq 3$. Thus case (B) remains. The congruence equation is written as

$$2^u + 2^{u+s} + 2^{2u} + 2^{2u+s} \equiv 1 + 2^a + 2^s \pmod{2^n - 1}. \tag{17}$$

As the 2-weight of the right-hand side of Eq. (17) is at most 3, the set $\{u, u+s, 2u, 2u+s\}$ of exponents of the monomial terms appearing in the left-hand side is of size at most 3. Thus one of the following occurs modulo n: $u \equiv u+s$, $u \equiv 2u$, $u \equiv 2u+s$, $u+s \equiv 2u$, $u+s \equiv 2u+s$ or $2u \equiv 2u+s$. As $(n, s) = 1$ and $n = 4u+1$, we have $0 \not\equiv s$ and $0 \not\equiv u$. Hence we have $u \equiv \pm s \pmod{n}$. If $s \equiv -u \pmod{n}$, we have $s = n - u = 3u + 1$, because $n \leq s + u < (n/2) + n < 2n$ and n divides $s + u$. However, $s = 3u + 1$ does not satisfy $s < n/2 = 2u + (1/2)$. Thus the unique remaining possibility is $s \equiv u \pmod{n}$. In this case, Eq. (17) reads

$$2^{2u+1} + 2^{3u} \equiv 1 + 2^a.$$

As $0 < 2u + 1 < 3u < n - 1$, the left-hand side of this equation is of 2-exponent 2. Then the right-hand side is of 2-exponent 2 as well, and therefore these expressions should be the 2-adic expression of an identical integer mod $2^n - 1$. However, the exponent 0 in the right-hand side does not appear in the exponents $2u + 1$, $3u$ in the left-hand side. This contradiction eliminates the unique remaining possibility. Thus on $F = \mathbb{F}_{2^n}$, $n = 4u+1$ for $u \geq 3$, the Gold function g_s for every s with $1 \leq s \leq n/2$, $(s, n) = 1$ is not CCZ-equivalent to the Niho function ν.

(v) By Theorem 1, κ_s is CCZ-equivalent to κ_r if and only if there is $a \in [0, n-1]$ such that (A) $1 - 2^s + 2^{2s} \equiv (1 - 2^r + 2^{2r})2^a$ or (B) $(1 - 2^r + 2^{2r})(1 - 2^s + 2^{2s}) \equiv 2^a$ modulo $2^n - 1$. In case (A), we have $s = r$ by comparing the 2-weights of both sides. Assume (B) holds. Multiplying $1 + 2^s$ both sides, we obtain

$$1 + 2^{2r} + 2^{3s} + 2^{2r+3s} = (1 + 2^{2r})(1 + 2^{3s}) \equiv 2^a + 2^{a+s} + 2^r + 2^{r+3s}. \tag{18}$$

If both sides of (18) has 2-weight 4, then we have

$$\{0, 2r, 3s, 2r + 3s\} \equiv \{a, a + s, r, r + 3s\} \pmod{n}. \tag{19}$$

In particular, r is congruent to one of $0, 2r, 3s, 2r+3s$. Then $r \equiv 3s$ or $r \equiv -3s \pmod{n}$. If $r \equiv 3s \pmod{n}$, Eq. (19) reads $\{0, 3r\} \equiv \{a, a+s\}$, whence $s \equiv \pm 3r \pmod{n}$. Then $s \equiv \pm 3r = \pm 9s \pmod{n}$, which implies that $n = 8$, 10 or 5. As $2 \leq r, s < n/2$ and $(r, n) = (s, n) = 1$, we have $(r, s, n) = (3, 3, 8)$, $(3, 3, 10)$ or $(2, 2, 5)$, none of these possibilities satisfies $r \equiv 3s \bmod n$. Similarly, if $r \equiv -3s$, we can show that $n = 7$ or 5, and $\{r, s\} \subseteq \{2, 3\}$ if $n = 7$, and $r = s = 2$ if $n = 5$. But none of them satisfies $r \equiv -3s$.

Hence $|\{0, 2r, 3s, 2r + 3s\}| \leq 3$ and $|\{a, a + s, r, r + 3s\}| \leq 3$. As $n \geq 3$ and $(r, n) = 1$, we have $0 \not\equiv 2r \pmod{n}$. We have $3s \not\equiv 0 \pmod{n}$, for otherwise we have $3 \equiv 0 \pmod{n}$, as $(s, n) = 1$, which implies that $n = 3$ and s lies in the empty set $[2, n/2]$, a contradiction. We have $3r \equiv \pm 2s \pmod{n}$ from the former condition. Accordingly the left-hand side of Eq. (18) reads $1 + 2^{2r+1} + 2^{4r}$ or $2 + 2^{2r} + 2^{-2r}$

according as $3s \equiv 2r$ or $3s \equiv -2r \pmod{n}$. We have $a \in \{r, r-s, r+2s, r+3s\}$ from the latter condition. According as $a \equiv r, r-s, r+2s$ or $r+3s \pmod{n}$, the right-hand side of Eq. (18) reads $2^{r+1}+2^{r+s}+2^{r+3s}$, $2^{r+1}+2^{r-s}+2^{r+3s}$, $2^r+2^{r+2s}+2^{r+3s+1}$ or $2^r+2^{r+3s+1}+2^{r+4s}$. In each combination of these possibilities for both sides of Eq. (18), we have restrictions for (a, r, s, n) and obtain a contradiction. It is left for the reader to eliminate all these possibilities.

(vi) By Theorem 1, κ_r is CCZ-equivalent to w if and only if there is $a \in [0, n-1]$ such that (A) $e := 1+2+2^t \equiv d2^a$ for $d := 1-2^r+2^{2r}$, $t = (n-1)/2$ or (B) $de \equiv 2^a$ modulo 2^n-1. In case (A), we have $r = 2$, because $w_2(d) = r+1$ and the 2-weight of the left-hand side is 3. Then the congruence equation reads $1+2+2^t \equiv (1+2^2+2^3)2^a \pmod{2^n-1}$, which implies $\{0, 1, t\} = \{2+a, 3+a, a\}$ modulo n. If $a \equiv 0$ or 1, then $(a+2)-a$ or $(a+3)-a$ would be ± 1 or 0 modulo n, which contradicts that $n \geq 9$. Thus $(0, 1, t) = (2+a, 3+a, a)$ modulo n. However, then $t = (n-1)/2 \equiv -a \equiv 1 \pmod{n}$, which holds only when $n = 3$, again contradicting $n \geq 9$. Hence we have case (B). In this case, we have $de \equiv 2^a$, which is equivalent to

$$1+2^{2r}+2+2^{2r+1}+2^t+2^{2r+t} \equiv 2^a+2^r+2^{r+1}+2^{r+t}. \tag{20}$$

Thus the 2-weight of the left-hand side of Eq. (20) is at most 4. Then some of two exponents in $\{0, 2r, 1, 2r+1, t, 2r+t\}$ coincides modulo n. It is easy to see that one of the following 5 possibilities: $0 \equiv 2r+1$, $0 \equiv 2r+t$, $1 \equiv 2r+t$, $2r \equiv t$ and $2r+1 \equiv t$. If $2r+1 \equiv 0 \pmod{n}$, we have $2r+1 = n = 2t+1$, whence $r = t$. Then Eq. (20) reads $2^2+2^{t-1} \equiv 2^a+2^{t+1}$, from which we have $t-1 \equiv 2 \pmod{n}$ or $(2, t-1) = (1, t+1)$ or $(t+1, 1) \pmod{n}$. In the first case, we have $n = 7$ but there is no $a \in [0, 6]$ with $2^a+2^3 \equiv 0 \pmod{7}$. In the last two cases, we have $2 \equiv 0$ or $1 \equiv t \equiv 2 \pmod{n}$, which are contradictions. Similarly, we can delete the remaining possibilities.

(vii) We just give a verification in the case when $(n-1)/2 = t = 2u+1$ is odd. The case when $t = 2u$ is even can be eliminated by similar calculations.

By Theorem 1, κ_r is CCZ-equivalent to ν if and only if there is $a \in [0, n-1]$ such that (A) $e := -1+2^{2u+1}+2^{3u+2} \equiv d2^a$ for $d := 1-2^r+2^{2r}$, or (B) $de \equiv 2^a$ modulo 2^n-1. In case (A), we have $r+1 = 2u+2$ by comparing the 2-weights of both sides. Then $r = 2u+1$ and the equivalence equation reads $2^{2u+1}+2^{3u+2}+2^{2u+1+a} \equiv 2^a+1+2^{a-1} \pmod{2^n-1}$ as $n = 4u+3$. If the 2-weights of both sides of this equation are 3, then $\{2u+1, 3u+2, 2u+1+a\} \equiv \{0, a, a-1\} \pmod{n}$. Then $2u+1+a \equiv 0$, as $2u+1 < 3u+2 < 4u+3 = n$. But then the above equation reads $\{2u+1, 3u+2\} \equiv \{a, a-1\} \pmod{n}$, whence $(3u+2)-(2u+1) \equiv \pm\{a-(a-1)\} = \pm 1$, or equivalently $u \equiv 0$ or $u \equiv -2 \pmod{n}$. Both contradict that $n = 4u+3$. Hence $|\{0, a-1, a\}| \leq 2$, and then $a \equiv 0$ or 1 (mod n). But in this case, we have $2^{2u+2}+2^{3u+2} \equiv 2+2^{4u+2}$ or $2^{2u+1}+2^{3u+2}+2^{2u+2} \equiv 2^2 \pmod{2^n-1}$. It is immediate to derive contradictions in both cases.

Thus we have case (B). In this case, we have

$$2^{2u+1}+2^{3u+2}+2^{2u+1+3r}+2^{3u+2+3r} \equiv 1+2^{3r}+2^a+2^{a+r}, \tag{21}$$

by multiplying both sides of the congruence equation by $1+2^r$. If the 2-weights of both sides of Eq. (21) is 4, then $\{2u+1, 3u+2, 2u+3r+1, 3u+2+3r\} \equiv \{0, 3r, a, a+r\}$ (mod n). Thus $0 \equiv 2u + 3r + 1$ or $0 \equiv 3u + 2 + 3r$ (mod n), as $5 \le 2u + 1 < 3u + 2 < 4u + 3 = n$. If $3r \equiv -2u - 1$, Eq. (21) reads $2^{u+1} + 2^{2u+1} + 2^{3u+2} \equiv 2^{2u+3} + 2^a + 2^{a+r}$, which is a contradiction, because while the left-hand side is a 2-adic expansion ($0 < u + 1 < 2u + 1 < 3u + 2 \le n - 1 = 4u + 2$), but the right-hand side contains the term 2^{2u+3}. If $3r \equiv -3u - 2 \equiv u + 1$, Eq. (21) reads $2^{2u+1} + 2^{3u+3} \equiv 2^{u+1} + 2^a + 2^{a+r}$, as $n = 4u + 3$. Then $|\{u + 1, a, a + r\}| = 2$. Then either $u + 1 \equiv a$ and $2^{2u+1} + 2^{3u+3} \equiv 2^{u+2} + 2^{u+1+r}$, or $u + 1 \equiv a + r$ and $2^{2u+1} + 2^{3u+3} \equiv 2^{u+2} + 2^{u+1-r}$. Both are contradictions, as $4 \le u + 2 < 2u + 1 < 3u + 3 < 4u + 3 = n$.

Thus $|\{0, u + 1, 3r, u + 1 + 3r\}| \le 3$ and $|\{0, 3r, a, a + r\}| \le 3$. Then we have $u+1 \equiv \pm 3r$ (mod n) and $a \in \{0, -r, 2r, 3r\}$ (mod n). It is straightforward to eliminate these possibilities.

(viii) By Theorem 1, on $F = \mathbb{F}_{2^n}$ with $n = 2t + 1$, $t = 2u$ (resp. $t = 2u + 1$), the Welch function $w(x) = x^d$, $d = 1 + 2 + 2^t$ is CCZ-equivalent to the Niho function $\nu(x) = x^e$ with $e := -1 + 2^u + 2^{2u}$ (resp. $e := -1 + 2^{2u+1} + 2^{3u+2}$) if and only if there is $a \in [0, n - 1]$ such that (A) $e \equiv d2^a$ or (B) $de \equiv 2^a$ modulo $2^n - 1$. In case (A), we have $u + 1 = 3$ (resp. $2u + 2 = 3$) if $t = 2u$ (resp. $t = 2u + 1$). Thus we have $u = 2$, but we assumed that $u \ge 3$.

We consider case (B). When $t = 2u$ is even, the congruence equation reads

$$2^a + 1 + 2 \equiv 2^u + 2^{u+1} + 2^{2u+1} + 2^{3u} + 2^{4u}. \tag{22}$$

As $2 \le u < u + 1 < 2u + 1 < 3u < 4u = n - 1$, the right-hand side of equation (22) is a 2-adic expansion, but the left-hand side is of 2-weight at most 3, which is a contradiction. When $t = 2u + 1$, the congruence equation reads

$$2^a + 1 + 2 \equiv 2^u + 2^{u+2} + 2^{3u+2} + 2^{3u+3} + 2^{4u+2}, \tag{23}$$

as $n = 4u + 3$. As $2 \le u < u + 2 < 3u + 2 < 3u + 3 < 4u + 2 = n - 1$, the right-hand side of Eq. (23) is a 2-adic expansion, but the left-hand side is of 2-weight at most 3, which is a contradiction. □

Acknowledgments The author thanks one of the reviewers to the old version of this paper (where Theorem 2 and only a weaker version of Theorem 1 are shown) for making me aware of the importance to establish the conjugacy of some cyclic subgroups in the automorphism group of a power APN function.

References

1. Bracken, C., Byrne, E., McGuire, G., Nebe, G.: On the equivalence of quadratic APN functions. Des. Codes Cryptogr. **61**, 261–272 (2010)
2. Budaghyan, L., Carlet, C., Leander, G.: On inequivalence between known power APN functions. In: Masnyk-Hansen, O., Michon, J.-F., Valarcher, P., J.-B.Yunes (Eds.) Proceedings of the conference BFCA'08, Copenhagen
3. Carlet, C.: Vectorial boolean functions for cryptography. In: Crema, Y., Hammer, P. (eds.) Chapter 9 in Boolean Methods and Models in Mathematics, Computer Science, and Engineering. Cambridge University Press, Cambridge (2010)

4. Dempwolff, U., Edel, Y.: Dimensional dual hyperovals and APN functions with translation groups. J. Algebraic Combin. **39**, 457–496 (2014)
5. Edel, Y., Pott, A.: A new almost perfect nonlinear function which is not quadratic. Adv. Math. Commun. **3**, 59–81 (2009)
6. Gorenstein, D.: Finite Groups. Harper and Row, New York (1968)
7. Huppert, B.: Endliche Gruppen. Springer, Berlin (1967)
8. Pasini, A., Yoshiara, S.: On a new family of flag-transitive semibiplanes. Eur. J. Combin. **22**, 529–545 (2001)
9. Suzuki, M.: Group Theory, Grundlehren der mathematischen Wissenschaften **247**-**248**, Springer, New York, Berlin, Heidelberg (1982–1986)
10. Yoshiara, S.: A family of d-dimensional dual hyperovals in $PG(2d+1, 2)$. Eur. J. Combin. **20**, 589–603 (1999)
11. Yoshiara, S.: Dimensional dual arcs—a survey. Walter de Gruyter. In: Hulpke, A., Liebler, B., Penttila, T., Seress, A. (eds.) Finite Geometries, Groups, and Computation, pp. 247–266. Berlin, New York (2006)
12. Yoshiara, S.: Dimensional dual hyperovals associated with quadratic APN functions. Innov. Incid. Geom. **8**, 147–169 (2008)
13. Yoshiara, S.: A characterization of a class of dimensional dual hyperovals with doubly transitive automorphism groups and its applications. Eur. J. Combin. **29**, 1521–1534 (2008)
14. Yoshiara, S.: Notes on APN functions, semibiplanes and dimensional dual hyperovals. Des. Codes Cryptogr. **56**, 197–218 (2010)
15. Yoshiara, S.: Equivalences of quadratic APN functions. J. Algebraic Combin. **35**, 461–475 (2012)