Dimensional dual hyperovals associated with quadratic APN functions

Satoshi Yoshiara

Abstract

From each quadratic APN function f on $\mathsf{GF}(2^{d+1})$ with $f(0) = 0$, we construct a d-dimensional dual hyperoval $\mathcal{S}^{d+1}[f]$ over $\mathsf{GF}(2)$. This provides many new examples of d-dual hyperovals over $\mathsf{GF}(2)$ with ambient spaces of dimension $2d + 2$. The automorphism group of $\mathcal{S}^{d+1}[f]$ is a semidirect product of a normal subgroup acting regularly on the members of $\mathcal{S}^{d+1}[f]$ with the stabilizer of a member. Some methods are provided to analyse the structure of the stabilizer. Based on them, $\mathrm{Aut}(\mathcal{S}^{10}[f])$ for an APN function f on $\mathsf{GF}(2^{10})$ found in [3] is determined.

Keywords: dimensional dual hyperoval, APN function

MSC 2000: 51E, 11T, 20B

1. Introduction

Let U be a vector space over a finite field $\mathsf{GF}(r)$ with r elements. A family $\mathcal{A}$ of $(d+1)$-dimensional subspaces of U is called a *d-dimensional dual arc* (abbreviated to *d-dual arc*) over $\mathsf{GF}(r)$ if it satisfies the following conditions.

(1) $\dim(X \cap Y) = 1$ for every distinct members X and Y of $\mathcal{A}$.

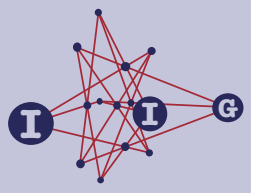
(2) $X \cap Y \cap Z = \{0\}$ for mutually distinct members X, Y, Z of $\mathcal{A}$.

The subspace V of U spanned by the members of $\mathcal{A}$ is called the *ambient space* of $\mathcal{A}$. An automorphism of the projective space $\mathsf{PG}(V)$ associated with V is called an *automorphism* of $\mathcal{A}$, if it sends each member of $\mathcal{A}$ to a member of $\mathcal{A}$. The group of all automorphisms of $\mathcal{A}$ is denoted $\mathrm{Aut}(\mathcal{A})$.

It is easy to see that a d-dual arc has at most $((r^{d+1} - 1)/(r - 1)) + 1$ members. If the upper bound is attained, $\mathcal{A}$ is called a *d-dimensional dual hyperoval*

ACADEMIA PRESS

UNIVERSITEIT GENT



(abbreviated to *d-dual hyperoval*). If $d = 1$, the notion of 1-dual arcs coincides with the classical notion of dual arcs in the projective plane over $\mathsf{GF}(r)$.

Let $q = 2^{d+1}$, a power of 2 with $d \geq 1$. Recall that a map f from $\mathsf{GF}(q)$ to itself is called *APN* (*almost perfect nonlinear*) if the following property holds:

$$\left|\{f(x+a)+f(x) \mid x \in \mathsf{GF}(2^{d+1})\}\right| = q/2 \text{ for every } a \in \mathsf{GF}(q)^\times .$$

It is called *quadratic* if

$$f(x+y+z)+f(x+y)+f(y+z)+f(z+x)+f(x)+f(y)+f(z) = f(0)$$
$$\text{for all } x, y, z \in \mathsf{GF}(q) .$$

In this paper, every quadratic map f is assumed to satisfy $f(0) = 0$.

APN maps (functions) are important for applications in cryptography so that many researches have been done on this subject. As for quadratic APN maps, until recently the only known examples are functions equivalent to the power map $f(x) = x^{2^m+1}$ with m coprime to $d+1$. Two new examples were found in 2005 [3] and then an infinite family of quadratic APN maps which are not equivalent to power mappings were constructed in [1].

In this paper, we construct a d-dimensional dual hyperoval over $\mathsf{GF}(2)$ from each quadratic APN map f on $\mathsf{GF}(2^{d+1})$, which is denoted $\mathcal{S}^{d+1}[f]$. It is observed that $\mathrm{Aut}(\mathcal{S}^{d+1}[f])$ has the group T of translations, so that it is transitive on the members of $\mathcal{S}^{d+1}[f]$ for every quadratic APN map f (Theorem 2.1). In section 3, it is shown that $\mathcal{S}^{d+1}[f]$ is covered by the Huybrechts dual hyperoval, but $\mathcal{S}^{d+1}[f]$ is not isomorphic to any known d-dual hyperoval over $\mathsf{GF}(2)$ with ambient space of dimension $2d+2$, except possibly $\mathcal{S}^{d+1}_{\sigma,\sigma}$ [8].

Section 4 provides some results on the structure of $\mathrm{Aut}(\mathcal{S}^{d+1}[f])$ for an arbitrary quadratic APN map f. We can show that $\mathrm{Aut}(\mathcal{S}^{d+1}[f])$ is a semidirect product of T with the stabilizer A of a member $X(0)$ (Corollary 4.7). Several methods to analize the structure of A are provided. Based on them, in section 5 we determine $\mathrm{Aut}(\mathcal{S}^{10}[f])$ for the APN function $f(x) = x^3 + ux^{36}$ ($u \in \mathsf{GF}(2^{10}) \setminus \mathsf{GF}(2^5)$) found in [3] (Proposition 5.1). This explicitly shows that the dual hyperoval $\mathcal{S}^{10}[f]$ is not isomorphic to any 10-dual hyperoval in $\mathsf{PG}(19,2)$ known before. In principle, many arguments there can be applied to examine $\mathrm{Aut}(\mathcal{S}^{d+1}[f])$ for every APN function f, if the explicit shape of f is given.

ACADEMIA PRESS

UNIVERSITEIT GENT

2. Construction

Let d be a positive integer and set $q = 2^{d+1}$. We regard $\mathsf{GF}(q)$ as a vector space of dimension $d+1$ over $\mathsf{GF}(2)$. Then

$$V := \mathsf{GF}(q) \oplus \mathsf{GF}(q) = \{(x, y) \mid x, y \in \mathsf{GF}(q)\} \tag{1}$$

is a vector space of dimension $2(d+1)$ over $\mathsf{GF}(2)$.

Take a quadratic APN map f on $\mathsf{GF}(q)$. Then the map b_f from $\mathsf{GF}(q) \times \mathsf{GF}(q)$ to $\mathsf{GF}(q)$ given by

$$b_f(x, y) := f(x + y) + f(x) + f(y) \tag{2}$$

for $x, y \in \mathsf{GF}(q)$ is a symmetric $\mathsf{GF}(2)$-bilinear map. In particular, we have $b_f(x, 0) = b_f(0, x) = 0$ for all $x \in \mathsf{GF}(q)$. Thus $f(0) = f(0 + 0) + f(0) + f(0) = b_f(0, 0) = 0$. Furthermore, for all $x \in \mathsf{GF}(q)$ we have

$$b_f(x, x) = f(0) + f(x) + f(x) = 0\,. \tag{3}$$

For each each $t \in \mathsf{GF}(q)^\times$, we set

$$H_t := \{b_f(x, t) \mid x \in \mathsf{GF}(q)\}\,. \tag{4}$$

As b_f is bilinear, H_t is a subspace of $\mathsf{GF}(q)$, regarded as a vector space over $\mathsf{GF}(2)$. It follows from equation (3) that the map β_t sending x of $\mathsf{GF}(q)$ to $b_f(x, t) \in H_t$ is a $\mathsf{GF}(2)$-linear surjection satisfying $\beta_t(x + t) = b_f(x + t, t) = b_f(x, t) + b_f(t, t) = b_f(x, t) = \beta_t(x)$ for all $x \in \mathsf{GF}(q)$. From the defining property of an APN function, the subset $\{f(x+t)+f(x) \mid x \in \mathsf{GF}(q)\}$ has cardinality $q/2$, whence the cardinality of $H_t = \{f(x + t) + f(x) + f(t) \mid x \in \mathsf{GF}(q)\}$ is $q/2 = 2^d$ as well. Thus H_t is a hyperplane of $\mathsf{GF}(q)$ for each $t \in \mathsf{GF}(q)^\times$. This also implies that the kernel of the $\mathsf{GF}(2)$-linear map β_t coincides with $\{0, t\}$. That is, for every $t \in \mathsf{GF}(q)^\times$ we have

$$b_f(x, t) = 0 \iff x = 0 \text{ or } x = t\,. \tag{5}$$

For each $t \in \mathsf{GF}(q)$, we now define a subspace $X(t)$ of V as follows.

$$X(t) := \{(x, b_f(x, t)) \mid x \in \mathsf{GF}(q)\}\,. \tag{6}$$

As b_f is bilinear, $X(t)$ is a subspace of V. Since $(x, b_f(t, x)) \neq (y, b_f(t, y))$ for distinct $x, y \in \mathsf{GF}(q)$, the subspace $X(t)$ is of dimension $d + 1$ over $\mathsf{GF}(2)$. We denote the collection of these subspaces by $\mathcal{S}^{d+1}[f]$:

$$\mathcal{S}^{d+1}[f] := \{X(t) \mid t \in \mathsf{GF}(q)\}\,. \tag{7}$$

Notice that $X(0) = \{(x, 0) \mid x \in \mathsf{GF}(q)\}$.

Theorem 2.1. *Let f be a quadratic APN function on $\mathsf{GF}(q)$, $q = 2^{d+1}$. With the notation above, the following statements hold.*

(1) *The family $\mathcal{S}^{d+1}[f]$ is a d-dimensional dual hyperoval over $\mathsf{GF}(2)$.*

(2) *The ambient space of $\mathcal{S}^{d+1}[f]$ is either V or the hyperplane $\mathsf{GF}(q) \oplus H_1$ of V. The latter case holds if and only if $H_t = H_1$ for all $t \in \mathsf{GF}(q)^\times$.*

(3) *For each $a \in \mathsf{GF}(q)$, define a map t_a on V by*

$$(x, y)^{t_a} := (x, y + b_f(x, a)) \tag{8}$$

for $x, y \in \mathsf{GF}(q)$. Then $t_a \in \mathrm{Aut}(\mathcal{S}^{d+1}[f])$ and $X(t)^{t_a} = X(t + a)$ for $t \in \mathsf{GF}(q)$. The group $T := \{t_a \mid a \in \mathsf{GF}(q)\}$ is an elementary abelian 2-group of order 2^{d+1} which acts regularly on the members of $\mathcal{S}^{d+1}[f]$.

Proof. (1) As we already saw above, $X(t)$ is a $(d+1)$-dimensional subspace of V for all $t \in \mathsf{GF}(q)$. Take any two distinct $s, t \in \mathsf{GF}(q)$. Then (x, y) belongs to $X(s) \cap X(t)$ if and only if $y = b_f(x, s) = b_f(x, t)$. As b_f is bilinear, this is equivalent to the equation $b_f(x, s + t) = 0$. Thus it follows from equation (5) that we have either $x = 0$ and $y = b_f(s, 0) = 0$ or $x = s + t$ and $y = b_f(s, s + t) = b_f(t, s + t) = b_f(s, t)$. Hence we have

$$X(s) \cap X(t) = \{(0, 0), (s + t, b_f(s, t))\} \tag{9}$$

for each $s \neq t \in \mathsf{GF}(q)$. This shows that $X(s) \cap X(t) \cap X(u) = \{(0, 0)\}$ for any mutually distinct elements s, t, u of $\mathsf{GF}(q)$. Thus $\mathcal{S}^{d+1}[f]$ is a d-dual arc over $\mathsf{GF}(2)$. As $\mathcal{S}^{d+1}[f]$ consists of $q = 2^{d+1} = ((2^{d+1} - 1)/(2 - 1)) + 1$ members, it is a d-dual hyperoval over $\mathsf{GF}(2)$.

(2) For $t \in \mathsf{GF}(q)^\times$, the subspace $\langle X(0), X(t)\rangle$ of V spanned by $X(0)$ and $X(t)$ is

$$\{(y, b_f(t, x)) \mid x, y \in \mathsf{GF}(q)\} = \{(a, b) \mid a \in \mathsf{GF}(q), b \in H_t\}, \tag{10}$$

which is isomorphic to the hyperplane $\mathsf{GF}(q) \oplus H_t$ of V. Thus if there are $s, t \in \mathsf{GF}(q)^\times$ with $H_s \neq H_t$, then the ambient space of $\mathcal{S}^{d+1}[f]$ contains both $\langle X(0), X(s)\rangle = \mathsf{GF}(q) \oplus H_s$ and $\langle X(0), X(t)\rangle = \mathsf{GF}(q) \oplus H_s$, whence it coincides with $V = \mathsf{GF}(q) \oplus \mathsf{GF}(q)$. Otherwise, we have $H_t = H_1$ for all $t \in \mathsf{GF}(q)^\times$. In this case, the ambient space is the hyperplane $\mathsf{GF}(q) \oplus H_1$ of V.

(3) The bilinearity of b_f shows that

$$\begin{aligned}(x_1 + x_2, y_1 + y_2)^{t_a} &= (x_1 + x_2, y_1 + y_2 + b_f(a, x_1 + x_2)) \\ &= (x_1 + x_2, y_1 + y_2 + b_f(a, x_1) + b_f(a, x_2)) \\ &= (x_1, y_1 + b_f(a, x_1)) + (x_2, y_2 + b_f(a, x_2)) \\ &= (x_1, y_1)^{t_a} + (x_2, y_2)^{t_a}\end{aligned}$$

for all $x_i, y_i \in \mathrm{GF}(q)$ $(i = 1, 2)$. Thus t_a is $\mathrm{GF}(2)$-linear. From definition (8), we have

$$\begin{aligned}(x, y)^{t_a t_b} &= (x, y + b_f(a, x))^{t_b} = (x, y + b_f(a, x) + b_f(b, x)) \\ &= (x, y + b_f(a + b, x)) = (x, y)^{t_{a+b}}\end{aligned}$$

for all $x, y \in \mathrm{GF}(q)$ and $a, b \in \mathrm{GF}(q)$. Thus

$$t_a t_b = t_{a+b} \tag{11}$$

for $a, b \in \mathrm{GF}(q)$. In particular, $t_a^{-1} = t_a$ is a bijection, as t_0 is the identity map on V. Equation (11) also shows that the group T is an elementary abelian group of order $q = 2^{d+1}$ via the isomorphism sending $a \in \mathrm{GF}(q)$ to $t_a \in T$.

For each typical vector $(x, b_f(t, x))$ of $X(t)$, we have

$$(x, b_f(t, x))^{t_a} = (x, b_f(t, x) + b_f(a, x)) = (x, b_f(t + a, x)) \tag{12}$$

by the bilinearity of b_f. This shows that

$$X(t)^{t_a} = X(t + a) \tag{13}$$

for all $t, a \in \mathrm{GF}(q)$. Thus t_a sends each member $X(t)$ of $\mathcal{S}^{d+1}[f]$ to a member $X(t + a)$ of $\mathcal{S}^{d+1}[f]$. Hence $t_a \in \mathrm{Aut}(\mathcal{S}^{d+1}[f])$ for each $a \in \mathrm{GF}(q)$. The regularity of the group T on $\mathcal{S}^{d+1}[f]$ follows from equation (13). □

Proposition 2.2. *If $d \geq 2$, then the ambient space of $\mathcal{S}^{d+1}[f]$ coincides with V.*

Proof. We denote by tr the trace function for the field extension $\mathrm{GF}(q)/\mathrm{GF}(2)$: $\mathrm{tr}(y) = \sum_{i=0}^{d} y^{2^i}$ $(y \in \mathrm{GF}(q))$. For each $a \in \mathrm{GF}(q)$, we denote by T_a the $\mathrm{GF}(2)$-linear map from $\mathrm{GF}(q)$ to $\mathrm{GF}(2)$ sending $x \in \mathrm{GF}(q)$ to $\mathrm{tr}(ax)$. Recall that every $\mathrm{GF}(2)$-linear map from $\mathrm{GF}(q)$ to $\mathrm{GF}(2)$ is of the form T_b for some $b \in \mathrm{GF}(q)$, and that every hyperplane of $\mathrm{GF}(q)$ is the kernel of T_a for some $a \in \mathrm{GF}(q)^\times$.

Assume that the ambient space of $\mathcal{S}^{d+1}[f]$ is not V. We shall first show that there are elements $a \in \mathrm{GF}(q)^\times$ and $b \in \mathrm{GF}(q)$ such that the function g defined by $g(x) = af(x) + bx$ $(x \in \mathrm{GF}(q))$ satisfies $\mathrm{tr}(g(x)) = 0$ for all $x \in \mathrm{GF}(q)$.

From Theorem 2.1(2), we have $H_1 = H_t$ for all $t \in \mathrm{GF}(q)$. As H_1 is a hyperplane of $\mathrm{GF}(q)$, the second remark in the first paragraph of the proof implies that there exists $a \in \mathrm{GF}(q)^\times$ such that H_t is the kernel of T_a for all $t \in \mathrm{GF}(q)$. Thus $\mathrm{tr}\big(a(b_f(x, t))\big) = \mathrm{tr}\big(af(x + t) + af(x) + af(t)\big) = 0$ for every $x, t \in \mathrm{GF}(q)$. This implies that the map h sending $x \in \mathrm{GF}(q)$ to $\mathrm{tr}(af(x))$ is a $\mathrm{GF}(2)$-linear map onto $\mathrm{GF}(2)$. Hence there exists some $b \in \mathrm{GF}(q)$ such that $h = T_b$ from the

first remark in the above paragraph. Thus $0 = h(x) + T_b(x) = \mathrm{tr}(af(x) + bx)$ for all $x \in \mathsf{GF}(q)$.

Hence the above claim is verified. It is straightforward to verify that the function g in the claim is a (quadratic) APN function as well (this is a special case of [2, Proposition 2]).

It now suffices to show that there is no APN function g on $\mathsf{GF}(2^{d+1})$ such that $\mathrm{tr}(g(x)) = 0$ for al $x \in \mathsf{GF}(2^{d+1})$, if $d \geq 2$. To this end, we adopt the coding theoretic approach to APN functions introduced in [2, section 3]. I thank the referee of the previous version of the paper for his/her suggestion to use [2, Corollary 1(i)].

We review the definition of code C_g associated with the APN function g on $\mathsf{GF}(q)$, $q = 2^{d+1}$ (see [2, Theorem 5]). Let $n = 2^{d+1} - 1$, and let α be a generator of the cyclic group $\mathsf{GF}(q)^\times$. Fix a basis $(b_0, \ldots, b_d)$ of $\mathsf{GF}(q)$, regarded as a vector space over $\mathsf{GF}(2)$. We associate each element $x = \sum_{i=0}^{d} x_i b_i$ of $\mathsf{GF}(q)$ with the column vector $\rho(x) := {}^t(x_0, \ldots, x_d)$ over $\mathsf{GF}(2)$. Let H_g be the 2 by n matrix over $\mathsf{GF}(q)$ defined by

$$H_g := \begin{pmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \\ g(1) & g(\alpha) & g(\alpha^2) & \cdots & g(\alpha^{n-1}) \end{pmatrix},$$

and let $\rho(H_g)$ be the $2(d+1)$ by n matrix over $\mathsf{GF}(2)$ obtained from H_g by replacing each entry x of H_g by $\rho(x)$. Now C_g is defined to be the $\mathsf{GF}(2)$-subspace of $\mathsf{GF}(2)^n$ consisting of vectors $\mathbf{c} = (c_0, \ldots, c_{n-1})$ ($c_j \in \mathsf{GF}(2)$, $j = 0, \ldots, n$) satisfying $\rho(H_g)^t \mathbf{c} = \mathbf{0}$. (Note that C_g does not depend on the choice of a basis for $\mathsf{GF}(q)$, because the condition $\rho(H_g)^t \mathbf{c} = \mathbf{0}$ holds if and only if $\sum_{j=0}^{n-1} c_j \alpha^j = 0$ and $\sum_{j=0}^{n-1} c_j g(\alpha)^j = 0$.) In particular, $\dim_{\mathsf{GF}(2)}(C_g) = n - r$, where r denotes the rank of the matrix $\rho(H_g)$ over $\mathsf{GF}(2)$.

From [2, Corollary 1(i)], the dimension over $\mathsf{GF}(2)$ of C_g is $n - 2(d+1)$, if $d \geq 2$. (Notice that the restriction on d is not explicitly stated there, but [2, Theorem 5] states that C_g has the minimum weight 5. As the minimum weight 5 should not exceed the length $n = 2^{d+1} - 1$, the result holds only when $d \geq 2$.) Thus the rank of $\rho(H_g)$ is $2(d+1)$, the number of rows. In particular, the $d+1$ row vectors of the submatrix $(\rho(g(1)), \rho(g(\alpha)), \ldots, \rho(\alpha^{n-1}))$ of $\rho(H_g)$ are linearly independent.

On the other hand, take a normal basis $(b_0, \ldots, b_d)$ of $\mathsf{GF}(q)$ over $\mathsf{GF}(2)$ and set $g(\alpha^j) = \sum_{i=0}^{d} x_{ij} b_i$, or equivalently $\rho(g(\alpha^j)) = {}^t(x_{0j}, x_{1j}, \ldots, x_{dj})$ (with $j = 0, \ldots, n-1$). As $\mathrm{tr}(b_i) = 1$ for all $i = 0, \ldots, d$, we have

$$0 = \mathrm{tr}(g(\alpha^j)) = \sum_{i=0}^{d} x_{ij} \,\mathrm{tr}(b_i) = \sum_{i=0}^{d} x_{ij}$$

for all $j = 0, \ldots, n-1$. This implies that the sum of all rows of the matrix $(\rho(g(1)), \ldots, \rho(g(\alpha^{n-1}))$ coincides with the zero vector, which contradicts the conclusion in the above paragraph. Hence there is no APN function g over $\mathsf{GF}(d+1)$ with $\mathrm{tr}(g(x)) = 0$ for all $x \in \mathsf{GF}(q)$, if $d \geq 2$. □

Remark 2.3. If $d = 1$, $\mathcal{S}^2[f]$ is a dual hyperoval in the classical sense, so that its ambient space has dimension 3, whence it is a proper subspace of V.

In fact, every quadratic APN fucntion on $\mathsf{GF}(2^2)$ is of the form $f(x) = a_1x + a_2x^2 + a_3x^3$ ($x \in \mathsf{GF}(4)$) with $a_1, a_2 \in \mathsf{GF}(4)$ and $a_3 \in \mathsf{GF}(4)^\times$. Then $H_t = \{b_f(x,t) \mid x \in \mathsf{GF}(4)\} = \{0, a_3\} = H_1$ for every $t \in \mathsf{GF}(4)^\times$. For $a := a_3^{-1}$ and $b := a_3^{-1}a_1 + a_3a_2^2$, the map g on $\mathsf{GF}(4)$ defined by $g(x) := af(x) + bx$ ($x \in \mathsf{GF}(4)$) satisfies that $\mathrm{tr}(g(x)) = 0$ for all $x \in \mathsf{GF}(4)$.

3. Relations with known examples

The d-dual hyperoval $\mathcal{S}^{d+1}[f]$ constructed for a quadratic APN function f on $\mathsf{GF}(2^{d+1})$ is not new, in the sense that it is covered by the known d-dual hyperoval over $\mathsf{GF}(2)$ with ambient space of dimension $(d+1)(d+2)/2$. See [9, subsection 2.5] for the notion of covers. For the Huybrechts dual hyperoval, see [9, subsection 5.3] or [5, subsection 6.2].

Proposition 3.1. *For any quadratic APN function f, the d-dual hyperoval $\mathcal{S}^{d+1}[f]$ constructed in Theorem 2.1 is covered by the Huybrechts dual hyperoval.*

Proof. The proof is exactly the same as one given for [5, Proposition 6.8]. The letters n and e there are $d+2$ and $d+1$, respectively, with our notation. There we showed that a map (denoted f) gives a cover of dual hyperoval $\mathcal{S}^{d+1}_{m,m}$ by the Huybrechts dual hyperoval (denoted $\mathcal{S}$ there, but we use the letter $\mathcal{H}$ in this paper). To define a covering map from $\mathcal{H}$ onto $\mathcal{S}^{d+1}[g]$ for a quadratic APN map g on $\mathsf{GF}(2^{d+1})$, just replace the definition of this map f (in the latter part of equation (1)) by

$$f((0, e_i \wedge e_j)) := (0, b_g(f_i, f_j))$$

for $1 \leq i < j \leq d+1$. Then, verbatim repetition of the arguments there shows that this modified map gives a cover of $\mathcal{S}^{d+1}[g]$ by the Huybrechts dual hyperoval $\mathcal{H}$. □

However, $\mathcal{S}^{d+1}[f]$ is new, in general, among d-dual hyperovals over $\mathsf{GF}(2)$ with ambient space of dimension $2d+2$. Notice that the known examples of such dual hyperovals are the Yoshiara dual hyperovals $\mathcal{S}^{d+1}_{\sigma,\phi}$ (see [9, subsection 5.5]) and the Taniguchi dual hyperovals $\mathcal{T}_\sigma$ over $\mathsf{GF}(2)$ with ambient space

of dimension $2d+2$ (see [9, subsection 5.6] and [6]), where σ are generators of the Galois group of the field extension $\mathrm{GF}(2^{d+1})/\mathrm{GF}(2)$ and ϕ are bijections on $\mathrm{GF}(2^{d+1})$ induced by o-polynomials.

Proposition 3.2. *Let σ be a generator of the Galois group of $\mathrm{GF}(2^{d+1})/\mathrm{GF}(2)$, and let ϕ be a bijection on $\mathrm{GF}(2^{d+1})$ induced by an o-polynomial.*

(1) *The dual hyperoval $\mathcal{T}_\sigma$ over $\mathrm{GF}(2)$ with ambient space of dimension $2d+2$ is not isomorphic to $\mathcal{S}^{d+1}[f]$ for every quadratic APN function f on $\mathrm{GF}(2^{d+1})$.*

(2) *The dual hyperoval $\mathcal{S}^{d+1}_{\sigma,\phi}$ is isomorphic to $\mathcal{S}^{d+1}[f]$ for a quadratic APN function f on $\mathrm{GF}(2^{d+1})$ if and only if $\sigma(x)=\phi(x)=x^{2^m}$ $(x\in\mathrm{GF}(2^{d+1}))$ for an integer m with $1\le m\le d$ coprime with $d+1$. In this case, $\mathcal{S}^{d+1}_{\sigma,\phi}$ coincides with $\mathcal{S}^{d+1}[f]$ for the Gold function $f(x)=x^{2^m+1}$ $(x\in\mathrm{GF}(q))$.*

Proof. Recall that for any d-dual hyperoval $\mathcal{S}$ over $\mathrm{GF}(2)$ we can construct an incidence geometry $\mathrm{Af}(\mathcal{S})$, the affine expansion of $\mathcal{S}$, which is a semibiplane. Then we can define an integer $w(\mathcal{S})$, called the wrapping number of $\mathcal{S}$, to be the wrapping number of the $c.c^*$-geometry associated with $\mathrm{Af}(\mathcal{S})$. See [5, subsection 1.1]. Notice that if $\mathcal{S}$ is covered by a d-dual hyperoval $\mathcal{S}'$ over $\mathrm{GF}(2)$, then $w(\mathcal{S})=w(\mathcal{S}')$ (see e.g. [5, Proposition 1.2]).

The wrapping numbers of $\mathcal{S}^{d+1}_{\sigma,\tau}$ for generators σ and τ of the Galois group of $\mathrm{GF}(2^{d+1})/\mathrm{GF}(2)$ are calculated in [5]. From Proposition 1.3 and Theorem 1.11 of [5], we have $w(\mathcal{S}^{d+1}_{\sigma,\tau})=1$ if and only if $\sigma=\tau$. As $\sigma(x)=x^{2^m}$ $(x\in\mathrm{GF}(2^{d+1}))$ for some m coprime with $d+1$, we verify that $\mathcal{S}^{d+1}_{\sigma,\sigma}$ coincides with $\mathcal{S}^{d+1}[g]$ for the Gold function $g(x)=x^{2^m+1}$, which is a classical example of quadratic APN functions. Since the latter dual hyperoval is covered by the Huybrechts dual hyperoval $\mathcal{H}$ by Proposition 3.1, we have $w(\mathcal{H})=w(\mathcal{S}^{d+1}[g])=1$. Then, applying Proposition 3.1 again, we have $1=w(\mathcal{H})=w(\mathcal{S}^{d+1}[f])$ for every quadratic APN function f.

Now we will establish claim (1). By [10, Proposition 1], $\mathcal{T}_\sigma$ is coverd by the Veronesean dual hyperoval. Further, the wapping number of the latter, which is equal to $w(\mathcal{T}_\sigma)$, is calculated to be 2 [10, Corollary 4]. Hence $\mathcal{T}_\sigma$ is never isomorphic to $\mathcal{S}^{d+1}[f]$ for every quadratic APN map f on $\mathrm{GF}(2^{d+1})$. (Claim (1) is also established by comparing the automorphism groups, because we can show that $\mathrm{Aut}(\mathcal{T}_\sigma)$ fixes a special member, while $\mathrm{Aut}(\mathcal{S}^{d+1}[f])$ is transitive by Theorem 2.1(3).)

Next we establish claim (2). Assume that $\mathcal{S}^{d+1}_{\sigma,\phi}$ is isomorphic to $\mathcal{S}^{d+1}[f]$ for a quadratic APN function f on $\mathrm{GF}(2^{d+1})$. If ϕ is not a generator of the Galois group of $\mathrm{GF}(2^{d+1})/\mathrm{GF}(2)$, then it follows from [7] that $\mathrm{Aut}(\mathcal{S}^{d+1}_{\sigma,\phi})$ fixes a special member. As $\mathcal{S}^{d+1}[f]$ admits the group of translations (Theorem 2.1(3)), in this case $\mathcal{S}^{d+1}_{\sigma,\phi}$ is never isomorphic to $\mathcal{S}^{d+1}[f]$. Thus we may assume that

ϕ is also a generator τ of $\mathrm{Gal}(\mathsf{GF}(2^{d+1})/\mathsf{GF}(2))$. However, as $w(\mathcal{S}^{d+1}[f]) = 1$, the d-dual hyperoval $\mathcal{S}^{d+1}_{\sigma,\tau}$ isomorphic to $\mathcal{S}^{d+1}[f]$ has the wrapping number 1 as well. As we remarked above, this is possible only when $\sigma = \tau$. Conversely, $\mathcal{S}^{d+1}_{\sigma,\sigma} = \mathcal{S}^{d+1}[g]$ for the Gold function $g(x) = x^{2^m+1}$, where $\sigma(x) = x^{2^m}$. □

We conclude this section with two open problems.

The first one is the isomorphism problem among d-dual hyperovals $\mathcal{S}^{d+1}[f]$: given quadratic APN functions f and g on $\mathsf{GF}(2^{d+1})$, find a necessary and sufficient condition for $\mathcal{S}^{d+1}[f]$ to be isomorphic to $\mathcal{S}^{d+1}[g]$, in terms of f and g.

Here is an easy observation. Recall that two APN functions f and g on $\mathsf{GF}(q)$, $q = 2^{d+1}$, are called *affinely equivalent* if there are $\mathsf{GF}(2)$-linear bijections σ and τ on $\mathsf{GF}(q)$ and elements c and c' of $\mathsf{GF}(q)$ such that $g(x) = f(x^\sigma + c)^\tau + c'$ for all $x \in \mathsf{GF}(q)$. Notice that if f and g are quadratic, then $c' = f(c)^\tau$, because we assume that $f(0) = g(0) = 0$.

Lemma 3.3. *Let f and g be quadratic APN functions on $\mathsf{GF}(q)$, $q = 2^{d+1}$, which are affinely equivalent to each other. Then $\mathcal{S}^{d+1}[f]$ is isomorphic to $\mathcal{S}^{d+1}[g]$.*

Proof. Choose $\mathsf{GF}(2)$-linear bijections σ and τ on $\mathsf{GF}(q)$ and an element c of $\mathsf{GF}(q)$ such that $g(x) = f(x^\sigma + c)^\tau + f(c)^\tau$ for all $x \in \mathsf{GF}(q)$. Then, for each $t, x \in \mathsf{GF}(q)$, we have

$$\begin{aligned} b_g(t,x) &= g(t+x) + g(t) + g(x) \\ &= f(x^\sigma + t^\sigma + c)^\tau + f(t^\sigma + c)^\tau + f(x^\sigma + c)^\tau + f(c)^\tau \\ &= (f(x^\sigma + t^\sigma) + f(t^\sigma) + f(x^\sigma))^\tau = b_f(t^\sigma, x^\sigma)^\tau , \end{aligned}$$

because f is quadratic. Define a $\mathsf{GF}(2)$-bijection ρ on $V = \mathsf{GF}(q) \oplus \mathsf{GF}(q)$ by $\rho((x,y)) := (x^{\sigma^{-1}}, y^\tau)$ $(x, y \in \mathsf{GF}(q))$. Then a vector $(x^\sigma, b_f(t^\sigma, x^\sigma))$ $(x, t \in \mathsf{GF}(q))$ of a member $X(t^\sigma)$ of $\mathcal{S}^{d+1}[f]$ is sent by ρ to $(x, b_f(t^\sigma, x^\sigma)^\tau)$, which is equal to $(x, b_g(t,x))$ by the above equation. Hence $\rho((x^\sigma, b_f(t^\sigma, x^\sigma)))$ lies in a member $X(t)$ of $\mathcal{S}^{d+1}[g]$. Thus ρ induces an isomorphism of $\mathcal{S}^{d+1}[f]$ with $\mathcal{S}^{d+1}[g]$ sending each member $X(t^\sigma)$ of $\mathcal{S}^{d+1}[f]$ to a member $X(t)$ of $\mathcal{S}^{d+1}[g]$. □

The second open problem is: given a quadratic APN function f on $\mathsf{GF}(q)$, $q = 2^{d+1}$, if $\mathcal{S}^{d+1}[f]$ is isomorphic to $\mathcal{S}^{d+1}_{\sigma,\sigma}$, where σ is a Galois automorphism $\sigma(x) = x^{2^m}$ $(x \in \mathsf{GF}(q))$ for some m coprime with $d+1$, can we conclude that f is affinely equivalent to the Gold function g defined by $g(x) = x^{2^m+1}$ $(x \in \mathsf{GF}(2^{d+1}))$?

We conjecture that the answer is yes, because $\mathrm{Aut}(\mathcal{S}^{d+1}[f])$ are observed to be transitive but not doubly transitive on $\mathcal{S}^{d+1}[f]$ for many explicit quadratic

APN functions f other than those affinely equivalent to the Gold function. (See also the last paragraph in section 5.)

4. Some results on automorphisms

Let $\mathcal{S}^{d+1}[f]$ be the d-dual hyperoval over $\mathsf{GF}(2)$ constructed in section 2. We use the same notation as in section 2. In particular, we write $q = 2^{d+1}$ and $V = \mathsf{GF}(q) \oplus \mathsf{GF}(q)$. We refer to t_a ($a \in \mathsf{GF}(q)$) as *translations* of $\mathcal{S}^{d+1}[f]$. As the group T of translations acts regularly on the members of $\mathcal{S}^{d+1}[f]$, we have

$$\mathrm{Aut}(\mathcal{S}^{d+1}[f]) = TA \text{ and } T \cap A = 1\,, \tag{14}$$

where A denotes the stabilizer of member $X(0) = \{(x,0) \mid x \in \mathsf{GF}(q)\}$ in $\mathrm{Aut}(\mathcal{S}^{d+1}[f])$. Notice that, at the present stage, we do not know whether T is normal in $\mathrm{Aut}(\mathcal{S}^{d+1}[f])$.

In this section, we denote by U the ambient space of $\mathcal{S}^{d+1}[f]$. We also use the letter H to denote the subspace of $\mathsf{GF}(q)$ spanned by $b_f(t,x)$ for all $t, x \in \mathsf{GF}(q)$. We also set

$$Y := \{(0,y) \mid y \in H\}\,.$$

Then it follows from Theorem 2.1(2) that

$$U = \mathsf{GF}(q) \oplus H = \{(x,y) \mid x \in \mathsf{GF}(q), y \in H\} = X(0) \oplus Y\,.$$

Notice that one of the following holds:

- $H = \mathsf{GF}(q)$, $U = V$ and $\dim(U) = 2d+2$; or
- $H = H_t = \{b_f(t,x) \mid x \in \mathsf{GF}(q)\}$ for every $t \in \mathsf{GF}(q)^\times$, $U = \mathsf{GF}(q) \oplus H_1$ and $\dim(U) = 2d+1$.

We shall analyze the structure of the stabilizer A of $X(0)$. Take any element g of $\mathrm{Aut}(\mathcal{S}^{d+1}[f])$. As it is a $\mathsf{GF}(2)$-linear bijection on U, there are four $\mathsf{GF}(2)$-linear maps $\alpha(g)\colon \mathsf{GF}(q) \to \mathsf{GF}(q)$, $\beta(g)\colon H \to H$, $\gamma(g)\colon H \to \mathsf{GF}(q)$ and $\delta(g)\colon \mathsf{GF}(q) \to H$ such that

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

for all $x, y \in \mathsf{GF}(q)$. If g stabilizes $X(0)$, then $(x,0)^g = \left(x^{\alpha(g)}, x^{\delta(g)}\right) \in X(0)$, whence $x^{\delta(g)} = 0$ for all $x \in \mathsf{GF}(q)$. Thus if $g \in A$, we have

$$(x,y)^g = \left(x^{\alpha(g)} + y^{\gamma(g)}, y^{\beta(g)}\right)$$

for all $x, y \in \mathsf{GF}(q)$. Notice that $\alpha(g)$ and $\beta(g)$ are bijections (with inverse maps $\alpha(g^{-1})$ and $\beta(g^{-1})$) on $\mathsf{GF}(q)$ and H respectively. In particular, we have

$$(x,0)^g = (x^{\alpha(g)}, 0)$$

for all $x \in \mathsf{GF}(q)$.

This determines the action of A on $\mathcal{S}^{d+1}[f] \setminus \{X(0)\}$ as follows. From equation (9), we have $X(0) \cap X(t) = \langle (t,0) \rangle$ for each $t \in \mathsf{GF}(q)^\times$. As $\mathcal{S}^{d+1}[f]$ is a d-dual hyperoval, this implies that the unique member of $\mathcal{S}^{d+1}[f] \setminus \{X(0)\}$ intersecting $X(0)$ at $\langle (t,0) \rangle$ is $X(t)$. Thus, with the notation above, we have

$$X(t)^g = X\left(t^{\alpha(g)}\right). \tag{15}$$

The map α sending an element g of A to $\alpha(g)$ is a homomorphism from A into $\mathsf{GL}(X(0)) \cong \mathsf{GL}_{d+1}(2)$. Identifying $X(0)$ with $\mathsf{GF}(q)$ via the map sending $(x,0)$ to x, α gives a representation of A on $\mathsf{GF}(q)$.

We claim that A acts faithfully on $\mathsf{GF}(q)$ via α. In particular, A is isomorphic to a subgroup $\alpha(A)$ of $\mathsf{GL}(\mathsf{GF}(q)) \cong \mathsf{GL}_{d+1}(2)$. If an element $g \in A$ satisfies $\alpha(g) = \mathrm{id}_{\mathsf{GF}(q)}$, g stabilizes all members of $\mathcal{S}^{d+1}[f]$ by equation (15) and hence it fixes all 1-subspaces of each member $X(t)$, as they are intersections $X(t) \cap X(s)$ for $s \in \mathsf{GF}(q) \setminus \{t\}$. As $\mathcal{S}^{d+1}[f]$ is defined over $\mathsf{GF}(2)$, g fixes all vectors of each $X(t)$, and hence fixes each vector of the ambient space U.

Proposition 4.1. *The stabilizer A acts on Y.*

Proof. Fix any element $g \in A$, and use the notation in the paragraphs previous to the proof. We shall show that $\gamma(g)$ is the zero map on H. We abbreviate $\alpha(g)$, $\beta(g)$ and $\gamma(g)$ by α, β and γ respectively.

Take a typical vector $(x, b_f(x,t))$ of a member $X(t)$ of $\mathcal{S}^{d+1}[f]$. As $X(t)^g = X(t^\alpha)$ by equation (15), the image $\left(x, b_f(x,t)\right)^g = \left(x^\alpha + b_f(x,t)^\gamma, b_f(x,t)^\beta\right)$ lies in $X(t^\alpha)$. Hence we have

$$b_f(x,t)^\beta = b_f\left(x^\alpha + b_f(x,t)^\gamma, t^\alpha\right) \tag{16}$$

for every $x, t \in \mathsf{GF}(q)$. Take any two elements s and t in $\mathsf{GF}(q)$. Applying equation (16) to x and $s+t$, we have

$$b_f(x,s+t)^\beta = b_f\left(x^\alpha + b_f(x,s+t)^\gamma, (s+t)^\alpha\right). \tag{17}$$

By the bilinearity of b_f and the linearity of α and γ, the right hand side of equation (17) is rewritten as

$$\begin{aligned} &b_f\left(x^\alpha + b_f(x,s)^\gamma + b_f(x,t)^\gamma, s^\alpha + t^\alpha\right) \\ &\qquad = b_f\left(x^\alpha + b_f(x,s)^\gamma, s^\alpha\right) + b_f\left(x^\alpha + b_f(x,t)^\gamma, t^\alpha\right) \\ &\qquad\qquad + b_f\left(b_f(x,s)^\gamma, t^\alpha\right) + b_f\left(b_f(x,t)^\gamma, s^\alpha\right). \end{aligned}$$

On the other hand, the left hand side of equality (17) is $b_f(x,s)^\beta + b_f(x,t)^\beta$, which is equal to $b_f\left(x^\alpha + b_f(x,s)^\gamma, s^\alpha\right) + b_f\left(x^\alpha + b_f(x,t)^\gamma, t^\alpha\right)$ by equation (16)

applied to (x,s) and (x,t). Hence we have the following equality for all $x,s,t \in \mathsf{GF}(q)$:

$$b_f\big(b_f(x,s)^\gamma, t^\alpha\big) = b_f\big(b_f(x,t)^\gamma, s^\alpha\big)\,.$$

In particular, for $x = s$, we have

$$0 = b_f(0,t^\alpha) = b_f\big(b_f(s,s)^\gamma, t^\alpha\big) = b_f\big(b_f(s,t)^\gamma, s^\alpha\big)\,.$$

By equation (5), this occurs only when $b_f(s,t)^\gamma = 0$ or $b_f(s,t)^\gamma = s^\alpha$. In the latter case, from equation (16) applied to $x = s$ and t, we have

$$b_f(s,t)^\beta = b_f\big(s^\alpha + b_f(s,t)^\gamma, t^\alpha\big) = b_f(0,t^\alpha) = 0\,.$$

As β is a bijection, this implies that $b_f(s,t) = 0$ for all $s,t \in \mathsf{GF}(q)$, which is impossible. Thus we have $b_f(s,t)^\gamma = 0$ for all $s,t \in \mathsf{GF}(q)$.

As H is generated by $b_f(s,t)$ ($s,t \in \mathsf{GF}(q)$), the above conclusion implies that $\gamma = \gamma(g)$ is the zero map on H. Then $(x,y)^g = \big(x^{\alpha(g)}, y^{\beta(g)}\big)$ for any $x \in \mathsf{GF}(q)$ and $y \in H$, whence an arbitrary element g of A acts on $Y = \{(0,y) \mid y \in H\}$. □

Proposition 4.1 shows that the map β sending $g \in A$ to $\beta(g)$ is a homomorphism from A to $\mathsf{GL}(Y)$ ($\cong \mathsf{GL}_{d+1}(2)$ or $\mathsf{GL}_d(2)$, according as $U = V$ or $U = \mathsf{GF}(q) \oplus H_1$; see Theorem 2.1(2)). Identifying Y with H via the map $(0,y) \mapsto y$, via β we obtain a representation of A on H (which is $\mathsf{GF}(q)$ or H_t for all $t \in \mathsf{GF}(q)^\times$ according as $U = V$ or $\mathsf{GF}(q) \oplus H_1$). While α is injective, β may not be injective, as we shall see below.

In the remainder of this section, the letters α and β denote these representations of A, namely, for $g \in A$, $\alpha(g)$ and $\beta(g)$ are the $\mathsf{GF}(2)$-linear bijections on $\mathsf{GF}(q)$ given by

$$(x,y)^g = \big(x^{\alpha(g)}, y^{\beta(g)}\big)$$

for $(x,y) \in U$.

In view of equation (8), we find that the group T of translations fixes each vector of Y. In particular, T acts on Y. By Proposition 4.1, the stabilizer A acts on Y as well. As $\mathrm{Aut}(\mathcal{S}^{d+1}[f]) = TA$ by equation (14), the automorphism group $\mathrm{Aut}(\mathcal{S}^{d+1}[f])$ acts on Y. If we denote the kernel of this action by K_Y, we have $K_Y = T(A \cap K_Y)$, as $T \le K_Y$. Hence we obtained the following.

Corollary 4.2. *The automorphism group $\mathrm{Aut}(\mathcal{S}^{d+1}[f])$ acts on Y. The kernel K_Y of the action contains T, whence $K_Y = T(A \cap K_Y)$.*

We next determine the kernel $Z := A \cap K_Y$ of the action of A on Y. To this end, we make some observations.

Let g be an element of A. Then it acts on both $X(0)$ and Y by Proposition 4.1.

Lemma 4.3. *Let g be any element of A. For every $x, s \in \mathsf{GF}(q)$ we have*

$$b_f(x,s)^{\beta(g)} = b_f\big(x^{\alpha(g)}, s^{\alpha(g)}\big)\,. \tag{18}$$

Proof. A vector $(x, b_f(x,s))$ of $X(s)$ ($x \in \mathsf{GF}(q)$) is sent by g to $(x, b_f(x,s))^g = \big(x^{\alpha(g)}, (b_f(x,s))^{\beta(g)}\big)$. On the other hand, as $g \in \mathrm{Aut}(\mathcal{S}^{d+1}[f])$, the last vector is contained in $X(s)^g = X(s^{\alpha(g)})$ by equation (15). Thus it coincides with $\big(x^{\alpha(g)}, b_f(x^{\alpha(g)}, s^{\alpha(g)})\big)$. This gives equation (18). □

Lemma 4.4. *The group T acts trivially on the factor space U/Y. In particular, for any $t \in T$, $g \in A$ and $(x,y) \in U$ we have*

$$\big((x,y)+Y\big)^{tg} = \big(x^{\alpha(g)}, y^{\beta(g)}\big) + Y\,. \tag{19}$$

Proof. As T and A act on Y, they act on the factor space U/Y. Let $t = t_a$ be any element of T ($a \in \mathsf{GF}(q)$). From (8), each vector $(x,y)+Y = (x,0)+Y$ of U/Y is sent by t_a to $(x, y+b_f(x,a))+Y = (x,0)+Y$. Thus $(x,y)+Y$ is fixed by t_a. Then $((x,y)+Y)^{t_a g} = ((x,y)+Y)^g = \big(x^{\alpha(g)}, y^{\beta(g)}\big)+Y$ for each $g \in A$. □

Proposition 4.5. *Assume that $d \geq 2$. Let $Z = K_Y \cap A$ be the kernel of the action of A on Y. Then $|Z| = 1$ or 3. Furthermore, if $|Z| = 3$, then Z acts fixed point freely on $X(0)$.*

Proof. Choose any $1 \neq z \in Z$ and write $\alpha = \alpha(z)$ for simplicity. We have $(x,y)^z = (x^\alpha, y)$ for all $x \in \mathsf{GF}(q)$ and $y \in H$, as $\beta(z) = \mathrm{id}_H$. Then it follows from equation (18) that for $x, t \in \mathsf{GF}(q)$ we have

$$b_f(x,t) = b_f(x,t)^{\beta(z)} = b_f(x^\alpha, t^\alpha).$$

Assume that z fixes distinct nonzero vectors $(t,0)$ and $(s,0)$ of $X(0)$. Then $t^\alpha = t$ and $s^\alpha = s$. Choose any $x \in \mathsf{GF}(q)$. Then the above equation applied to t and x yields $b_f(x,t) = b_f(x^\alpha, t)$, or equivalently $b_f(x+x^\alpha, t) = 0$ by the bilinearity of b_f. From equation (5), we have $x + x^\alpha = 0$ or t. By a similar argument applied to s and x, we have $x + x^\alpha = 0$ or s. Thus we should have $x = x^\alpha$, because s and t are distinct nonzero elements of $\mathsf{GF}(q)$. As this holds for every $x \in \mathsf{GF}(q)$, we conclude that z acts trivially on $X(0)$, and so on U. This contradicts that $z \neq 1$. Hence z fixes at most one nonzero vector of $X(0)$.

As $(d+1)/2 = \dim X(0)/2 > 1$, this shows that z is not of order 2, because in general an involution w acting on an elementary abelian 2-group W satisfies $W/C_W(w) \cong [W,w] \leq C_W(w)$, and so $\dim(C_W(w)) \geq \dim(W)/2$. As z is any nontrivial element of Z, we conclude that Z is of odd order.

We next show that z does not fix any nonzero vector of $X(0)$. On the contrary, suppose $(t,0)$, $t \in \mathsf{GF}(q)^\times$, is fixed by z. Then it follows from the argument in

the above paragraph that $x + x^\alpha = 0$ or $x + x^\alpha = t$. Applying this conclusion to x^α, we have $x^\alpha + x^{\alpha^2} = 0$ or $x^\alpha + x^{\alpha^2} = t$. As we have $x^\alpha = x^{\alpha^2}$ if and only if $x = x^\alpha$, we have $x + x^\alpha = t$ if and only if $x^\alpha + x^{\alpha^2} = t$. Thus if $x + x^\alpha = t$, then we have $x + x^{\alpha^2} = t + t = 0$, namely x is fixed by α^2. However, $\alpha = \alpha(z)$ is a nontrivial automorphism of $\mathsf{GL}(\mathsf{GF}(q))$ of odd order, as we remarked in the above paragraph. Thus $\langle\alpha\rangle = \langle\alpha^2\rangle$ and x is fixed by α as well. This contradiction shows that $x = x^\alpha$ for all $x \in \mathsf{GF}(q)$. However, this implies that $\alpha = \mathrm{id}_{\mathsf{GF}(q)}$ and $z = 1$, a contradiction. Hence we conclude that every nontrivial element z of Z does not fix any nonzero vector of $X(0)$. That is, Z acts fixed point freely on $X(0)$. In particular, every Sylow p-subgroup for each prime divisor p of $|Z|$ is a cyclic group (e.g. [4, Theorem 18.1(iv)]).

Next we shall show that z is of order at most 3. Take any $x \in \mathsf{GF}(q)^\times$. Then

$$b_f(x, x^\alpha) = b_f(x, x^\alpha)^{\beta(z)} = b_f\left(x^\alpha, x^{\alpha^2}\right)$$

by equation (18). As b_f is symmetric and bilinear, we have $b_f\left(x^\alpha, x + x^{\alpha^2}\right) = 0$. Notice that $x^\alpha \neq 0$ and $x + x^{\alpha^2} \neq 0$, because Z acts fixed point freely on $X(0)$ and $\alpha^2 \neq 1$. It then follows from equation (5) that $x^\alpha = x + x^{\alpha^2}$. Thus $x^{\alpha^2} = x + x^\alpha$ and $x^{\alpha^3} = (x + x^\alpha)^\alpha = x^\alpha + x^{\alpha^2} = x$. As x is an arbitrary element of $\mathsf{GF}(q)^\times$, this shows that $\alpha^3 = \alpha(z^3)$ is trivial on $X(0)$, whence $z^3 = 1$ on U.

Since z is any nontrivial element of Z, the above conclusion first shows that Z is a 3-group. The above conclusion also shows that there is no element of order 9 in Z. As we already showed that Z is cyclic, it follows that Z is of order 1 or 3. This completes the proof of the proposition. □

Remark 4.6. Proposition 4.5 does not hold if $d = 1$.

In this case, as we saw in the last remark in section 2, the ambient space of $\mathcal{S}^2[f]$ is $X(0) \oplus Y$ for a 1-dimensional space Y. Thus A acts trivially on Y, whence $Z = A$. If we take $f(x) = x^3$ ($x \in \mathsf{GF}(4)$), $\mathcal{S}^2[f]$ coincides with $\mathcal{S}^2_{\sigma,\sigma}$, where $x^\sigma = x^2$ ($x \in \mathsf{GF}(4)$), whence $Z = A \cong \mathsf{GL}_2(2) \cong S_3$.

Corollary 4.7. *The automorphism group* $\mathrm{Aut}(\mathcal{S}^{d+1}[f]) = T : A$ *is a semidirect product of the normal subgroup* T *of translations with the stabilizer* A *of* $X(0)$.

Proof. If $d = 1$, $\mathrm{Aut}(\mathcal{S}^2[f])$ is a subgroup of the symmetric group S_4 acting on the four members of $\mathcal{S}^2[f]$. As T acts regularly on $\mathcal{S}^2[f]$, T corresponds to the Klein four subgroup $O_2(S_4)$, whence T is normal in $\mathrm{Aut}(\mathcal{S}^2[f])$ and $\mathrm{Aut}(\mathcal{S}^2[f]) = T : A$. Thus we may assume that $d \geq 2$.

As $K_Y = TZ$ by Corollary 4.2, if $Z = 1$ then $K_Y = T$ is a normal subgroup of $\mathrm{Aut}(\mathcal{S}^{d+1}[f])$. Assume that $Z \neq 1$, whence $|Z| = 3$ by Proposition 4.5. Let

z be an element of order 3 in Z. Then $Z = \{1, z, z^2\}$, whence $K_Y = TZ = T \cup Tz \cup Tz^2$.

We shall show that T is the unique Sylow 2-subgroup of K_Y. Suppose not. Then the subset $Tz \cup Tz^2$ contains an involution tg ($t \in T$, $g = z^i$, $i = 1, 2$) which is a conjugate of an involution in T. Then it follows from equation (19) that we have

$$(x, 0) + Y = ((x, 0) + Y)^{(tg)^2} = \left((x^{\alpha(g)}, 0) + Y\right)^{tg} = \left(x^{\alpha(g^2)}, 0\right) + Y\,.$$

As $X(0) \cap Y = \{(0, 0)\}$, this implies that $(x, 0) = \left(x^{\alpha(g^2)}, 0\right)$. However, as α is a faithful representation, $\alpha(g)$ is an element of $\mathsf{GL}(\mathsf{GF}(q)) \cong \mathsf{GL}_{d+1}(2)$ of order 3. Moreover, it acts fixed point freely on $\mathsf{GF}(q)$ by Proposition 4.5. Thus $x \neq x^{\alpha(g)^2} = x^{\alpha(g^2)}$ for $x \in \mathsf{GF}(q)^\times$, which is a contradiction. Hence T is the unique Sylow 2-subgroup of $TZ = K_Y$. As the kernel K_Y is normal in $\mathrm{Aut}(\mathcal{S}^{d+1}[f])$, this implies that T is normal in $\mathrm{Aut}(\mathcal{S}^{d+1}[f])$ as well. By equation (14), $\mathrm{Aut}(\mathcal{S}^{d+1}[f])$ is a semidirect product of T with A. □

We examine the subspace of U fixed by an involution of A.

Lemma 4.8. *Let $q = 2^{d+1}$, and let g be an involution of A. We use the abbreviations $\alpha := \alpha(g)$ and $\beta := \beta(g)$ so that $(x, y)^g = (x^\alpha, y^\beta)$ for $(x, y) \in V$.*

Then we have $\dim C_U(g) = \dim C_{\mathsf{GF}(q)}(\alpha) + \dim C_H(\beta)$ and exactly one of the following holds, where case (2) or (3) occurs only when $U = V$ (whence $H = \mathsf{GF}(q)$):

(1) *$d + 1$ is even, $\dim C_{\mathsf{GF}(q)}(\alpha) = \dim C_H(\beta) = (d + 1)/2$;*

(2) *$d + 1$ is even, $\dim C_{\mathsf{GF}(q)}(\alpha) = (d + 1)/2$ and $\dim C_{\mathsf{GF}(q)}(\beta) = (d + 3)/2$;*

(3) *d is even, $\dim C_{\mathsf{GF}(q)}(\alpha) = \dim C_{\mathsf{GF}(q)}(\beta) = (d + 2)/2$.*

Proof. As $(x, y)^g = (x^\alpha, y^\beta)$ ($x \in \mathsf{GF}(q)$, $y \in H$), the centralizer $C_U(g)$ is the direct sum of centralizers $C_{\mathsf{GF}(q)}(\alpha)$ and $C_H(\beta)$. Thus we have $\dim C_U(g) = \dim C_{\mathsf{GF}(q)}(\alpha) + \dim C_H(\beta)$.

As g is an involution of the stabilizer A and A acts faithfully on $X(0)$, there exists $t \in \mathsf{GF}(q)$ such that $(t, 0) \neq (t, 0)^g = (t^\alpha, 0)$. Then $s := t + t^\alpha \neq 0$. Consider the hyperplane $H_s = \{b_f(s, x) \mid x \in \mathsf{GF}(q)\}$ of $\mathsf{GF}(q)$, which is a subspace of H. We examine the centralizer $C_{H_s}(\beta)$ of β in H_s. From equation (18), $b_f(x, s) \in H_s$ lies in $C_{H_s}(\beta)$ if and only if $b_f(x^\alpha, s^\alpha) = b_f(x, s)$. Remark that $\alpha^2 = 1$ as g is an involution, and hence α fixes $s = t + t^\alpha$. Thus we have $b_f(x^\alpha, s) = b_f(x, s)$ from the above equation. Then $b_f(x + x^\alpha, s) = 0$ by the bilinearity of b_f. It follows from equation (5) that $x + x^\alpha = 0$ or $x + x^\alpha = s = t + t^\alpha$. Thus x lies in $C_{\mathsf{GF}(q)}(\alpha)$ or the coset $t + C_{\mathsf{GF}(q)}(\alpha)$. Observe that

$\langle C_{\mathsf{GF}(q)}(\alpha), t\rangle = C_{\mathsf{GF}(q)}(\alpha) \cup (t + C_{\mathsf{GF}(q)}(\alpha))$ is a subspace of $\mathsf{GF}(q)$ of dimension $\dim(C_{\mathsf{GF}(q)}(\alpha)) + 1$. Summarizing, we have

$$C_{H_s}(\beta) = \left\{ b_f(x, s) \mid x \in \langle C_{\mathsf{GF}(q)}(\alpha), t\rangle \right\}.$$

Thus the map ζ sending x of $\langle C_{\mathsf{GF}(q)}(\alpha), t\rangle$ to $b_f(x, s) \in C_{H_s}(\beta)$ is a linear surjection. By equation (5), the kernel of ζ coincides with $\{0, s\}$ (Observe that $s \in C_{\mathsf{GF}(q)}(\alpha)$). Thus

$$\dim(C_{H_s}(\beta)) = \dim(C_{\mathsf{GF}(q)}(\alpha)) + 1 - 1 = \dim(C_{\mathsf{GF}(q)}(\alpha)). \tag{20}$$

In particular, since H contains H_s,

$$\dim(C_H(\beta)) \geq \dim(C_{H_s}(\beta)) = \dim(C_{\mathsf{GF}(q)}(\alpha)). \tag{21}$$

Here we make standard remarks. For an automorphism γ of an elementary abelian 2-group W of order at most 2, we have

$$\begin{aligned} 2\dim([W, \gamma]) &\leq \dim(W) = \dim(C_W(\gamma)) + \dim([W, \gamma]) \\ &\leq 2\dim(C_W(\gamma)). \end{aligned} \tag{22}$$

Applying the latter part of inequality (22) to $W = \mathsf{GF}(q)$ and $\gamma = \alpha$, it follows from equation (21) that

$$\begin{aligned} \dim(C_U(g)) &= \dim(C_{\mathsf{GF}(q)}(\alpha)) + \dim(C_H(\beta)) \\ &\geq 2\dim(C_{\mathsf{GF}(q)}(\alpha)) \geq d + 1. \end{aligned} \tag{23}$$

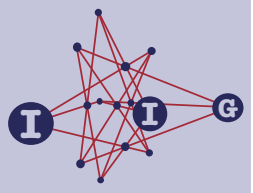
On the other hand, note that $[X(t), g] = \{(x, y)+(x, y)^g \mid (x, y) \in X(t)\}$ is the image of $X(t)$ by the linear map sending (x, y) of U to $(x, y) + (x, y)^g \in [U, g]$. The kernel of this map is $C_{X(t)}(g) = X(t) \cap X(t)^g$, which is 1-dimensional over $\mathsf{GF}(2)$, as $\mathcal{S}^{d+1}[f]$ is a d-dual hyperoval. Then we have

$$\dim[X(t), g] = \dim(X(t)) - 1 = d \leq \dim([U, g]) \leq \dim(U)/2 \leq d + 1,$$

by applying the former part of inequality (22) to $W = U$ and $\gamma = g$. Thus we have either $\big(\dim([U, g]), \dim(C_U(g))\big) = (d, d + 1)$, $(d, d + 2)$ or $(d + 1, d + 1)$, because $\dim U = \dim [U, g] + \dim C_U(g) = 2d + 1$ or $2d + 2$.

In the first and third cases, we have equality in inequality (23), and hence in inequality (21). Thus $d + 1$ is even and $\dim(C_{\mathsf{GF}(q)}(\alpha)) = \dim(C_H(\beta)) = (d + 1)/2$. This is case (1) in the claim.

In the second case, we have $U = V$, $H = \mathsf{GF}(q)$ and $\dim(C_{\mathsf{GF}(q)}(\beta)) = \dim(C_{\mathsf{GF}(q)}(\alpha)) + \delta$ for some nonnegative integer δ by equation (21). Then it follows from the first part of inequality (23) that $d+2 = 2\dim(C_{\mathsf{GF}(q)}(\alpha))+\delta$. As $2\dim(C_{\mathsf{GF}(q)}(\alpha)) \geq d+1$, applying the above standard inequality to $W = \mathsf{GF}(q)$ and $\gamma = \alpha$, we have $d+2 \geq d+1+\delta$. Hence $\delta = 0$ or 1. We have case (2) or (3), according to $\delta = 1$ or $\delta = 0$. □



Corollary 4.9. *Assume that the kernel Z of A on Y is a subgroup of order 3. If $d+1 \equiv 2 \pmod 4$, then $C_A(Z)$ is a normal subgroup of A of odd order with index at most 2.*

Proof. As A acts on Y by Proposition 4.1, Z and $C_A(Z)$ are normal subgroups of A. Then $A/C_A(Z)$, being isomorphic to a subgroup of $\mathrm{Aut}(Z)$, has order at most 2.

Suppose that $C_A(Z)$ contains an involution g. Then we may apply Lemma 4.8. As $d+1$ is even, we have case (1) or (2) in Lemma 4.8. In particular, we have $\dim\big(C_{\mathsf{GF}(q)}(\alpha(g))\big) = (d+1)/2$. As $Z = \langle z\rangle$ commutes with g, the automorphism $\alpha(z)$ on $\mathsf{GF}(q)$ induced by z preserves $C_{\mathsf{GF}(q)}(\alpha(g))$. Notice that $\alpha(z)$ is an element of order 3 acting fixed point freely on $\mathsf{GF}(q)^\times$ by Proposition 4.5. Then we conclude that $\dim\big(C_{\mathsf{GF}(q)}(\alpha(g))\big) = (d+1)/2$ is even. This contradicts the assumption that $d+1 \equiv 2 \pmod 4$. Thus $C_A(z)$ does not contain any involution. □

5. Automorphisms of $\mathcal{S}^{10}[f]$ for $f(x) = x^3 + ux^{36}$

In this section, we determine the automorphism group $\mathrm{Aut}(\mathcal{S}^{10}[f])$ for the APN function $f(x) = x^3 + ux^{36}$ on $\mathsf{GF}(2^{10})$ found in [3, Theorem 2], where u is an element of $\mathsf{GF}(2^{10})^\times$ not belonging to subfield $\mathsf{GF}(2^5)$. We have $\mathsf{GF}(2^{10})^\times = \langle\omega\rangle \times \langle\eta\rangle \times \langle\zeta\rangle$, where ω and η are elements of order 3 and 11 respectively, and ζ is a generator of $\mathsf{GF}(2^5)^\times$. Since $3 = 1+2$ and $36 = 2^2 + 2^5$, for $x, y \in \mathsf{GF}(q)$ we have $(x+y)^3 = (x+y)^{1+2} = (x+y)(x^2+y^2)$ and $(x+y)^{36} = (x^{2^2}+y^{2^2})(x^{2^5}+y^{2^5})$, whence

$$\begin{aligned} b_f(x,y) &= (x+y)^{1+2} + u(x+y)^{2^2+2^5} + x^{1+2} + ux^{2^2+2^5} + y^{1+2} + uy^{2^2+2^5} \\ &= xy^2 + x^2y + u(x^{2^2}y^{2^5} + x^{2^5}y^{2^2})\,. \end{aligned}$$

Proposition 5.1. *Let f be the quadratic APN function on $\mathsf{GF}(2^{10})$ given by $f(x) = x^3 + ux^{36}$ for some $u \in \mathsf{GF}(2^{10}) \setminus \mathsf{GF}(2^5)$. Then*[1] *$\mathrm{Aut}(\mathcal{S}^{10}[f])$ is isomorphic to $2^{10} : ((Z_3 \times Z_{11}) : Z_5)$ or $2^{10} : (Z_3 \times Z_{11})$, according as $u = \omega^{\pm 1}$ or $u \notin \langle\omega\rangle$, where 2^{10}, $Z_3 \times Z_{11}$ and Z_5 correspond respectively to the group of translations, the group of multiplications m_b for $b \in \mathsf{GF}(2^{10})^\times$ with $b^{33} = 1$ and the group of field automorphisms generated by $x \mapsto x^4$ $(x \in \mathsf{GF}(2^{10}))$.*

We set $d+1 = 10$ and $q = 2^{d+1} = 2^{10}$. The notation in section 2 will be used without further reference. We divide the proof into several steps.

[1] See, however, the correction added in proof on page 22.

Step 1. *For $b, c \in \mathsf{GF}(q)^\times$, the map*

$$\mu\colon U \ni (x, y) \mapsto (bx, cy) \in U \tag{24}$$

is an automorphism of $\mathcal{S}^{10}[f]$ if and only if $b^{33} = 1$ and $c = b^3$.

Proof. Assume that μ is an automorphism of $\mathcal{S}^{10}[f]$ given by equation (24) for some b, c of $\mathsf{GF}(q)^\times$. Take any $t \in \mathsf{GF}(q)^\times$. As $(t, 0)^\mu = (bt, 0)$, we have $X(t)^\mu = X(bt)$ by equation (15). Thus a vector $\big(x, xt^2 + x^2t + u(x^4t^{32} + x^{32}t^4)\big)$ of $X(t)$ for any $x \in \mathsf{GF}(q)$ is sent by μ to a vector of $X(bt)$. As the first component of $\big(x, xt^2 + x^2t + \omega(x^4t^{32} + x^{32}t^4)\big)^\mu$ is bx, we have

$$\begin{aligned} c\big(xt^2 + x^2t + u(x^4t^{32} + x^{32}t^4)\big) \\ = (bx)(bt)^2 + (bx)^2(bt) + u\big((bx)^4(bt)^{32} + (bx)^{32}(bt)^4\big) \end{aligned}$$

by comparing the second components. Rewriting this equality as a polynomial of x, we have

$$(c + b^3)t^2x + (c + b^3)tx^2 + u(c + b^{36})t^{32}x^4 + u(c + b^{36})t^4x^{32} = 0\,.$$

As this holds for all $x \in \mathsf{GF}(q)$, the polynomial

$$P_t(X) = (c + b^3)t^2X + (c + b^3)tX^2 + u(c + b^{36})t^{32}X^4 + u(c + b^{36})t^4X^{32}$$

of degree 32 in $\mathsf{GF}(q)[X]$ has at least $q = 2^{10}$ distinct solutions. Thus all coefficients of $P_t(X)$ are 0, whence

$$(c + b^3)t^2 = (c + b^3)t = (c + b^{36})t^{32} = (c + b^{36})t^4 = 0\,.$$

As this holds for every $t \in \mathsf{GF}(q)^\times$, we have $c = b^3$ and $b^{33} = 1$.

Conversely, the above calculation shows that the map sending each element (x, y) of U to $\big(\omega\eta x, (\omega\eta)^3 y\big)$ is an automorphism of $\mathcal{S}^{10}[f]$ which sends $X(t)$ to $X(\omega\eta t)$ for every $t \in \mathsf{GF}(q)$. Recall here that $\omega\eta$ generates $\langle\omega\rangle \times \langle\eta\rangle$. □

Step 2. *The following map ϕ lies in $\mathrm{Aut}(\mathcal{S}^{10}[f])$ if and only if $u = \omega^{\pm 1}$.*

$$\phi\colon V \ni (x, y) \mapsto (x^4, y^4) \in V\,. \tag{25}$$

Proof. Observe that ϕ stabilizes $X(0)$, and that ϕ sends the unique nonzero vector $(t, 0)$ of $X(0) \cap X(t)$ to the unique nonzero vector $(t^4, 0)$ of $X(0) \cap X(t^4)$. Thus if ϕ lies in $\mathrm{Aut}(\mathcal{S}^{10}[f])$, then we have $X(t)^\phi = X(t)$, whence $\big(x, b_f(x, t)\big)^\phi = \big(x^4, b_f(x, t)^4\big) \in X(t^4)$ for every $x \in \mathsf{GF}(q)$ and every $t \in \mathsf{GF}(q)^\times$. Then

$b_f(x,t)^4 = b_f(x^4,t^4)$ for all $x,t \in \mathsf{GF}(q)$. Conversely, if this condition is satisfied then $X(t)^\phi = X(t)$ for all $t \in \mathsf{GF}(q)$, whence ϕ lies in $\mathrm{Aut}(\mathcal{S}^{10}[f])$. Hence $\phi \in \mathrm{Aut}(\mathcal{S}^{10}[f])$ if and only if $b_f(x,t)^4 = b_f(x^4,t^4)$ for all $x,t \in \mathsf{GF}(q)$.

As $b_f(x,t)^4 = b_f(x^4,t^4)$ is equivalent to $(u^4+u)\left((x+t)^{36}+x^{36}+t^{36}\right) = 0$, this is satisfied for all $x,t \in \mathsf{GF}(q)$ if and only if $u^4 = u$, namely $u = \omega^{\pm 1}$. □

We set $F := \langle\phi\rangle$, which is a group of order 5 acting faithfully on $X(0)$. For elements b of $B := \langle\omega\eta\rangle$, we define m_b to be the following automorphism of $\mathcal{S}^{10}[f]$.

$$m_b \colon U \ni (x,y) \mapsto (bx, b^3y) \in U\,. \tag{26}$$

Then the map sending $b \in B$ to m_b is a homomorphism from B to A. The image $m(B) := \{m_b \mid b \in B\}$ is a cyclic subgroup of order 33 of A. Observe that $z := m_\omega$ acts trivially on Y, so that the kernel Z of the action of A on Y coincides with $\langle z\rangle$ by Proposition 4.5.

Step 3. (1) *The ambient space of $\mathcal{S}^{10}[f]$ is $V = X(0) \oplus Y$. The group $m(B)$ acts irreducibly on both $X(0)$ and Y.*

(2) *The centralizer $C_{\mathrm{Aut}(X(0))}(z)$ of $z = m_\omega$ in $\mathrm{Aut}(X(0))$ is isomorphic to a subgroup of $\mathsf{GL}_5(4)$ of odd order, containing $m(B)F$. Furthermore, $m(B) = C_A(m(B))$.*

Proof. (1) As $m(B)$ acts on Y with kernel Z, the factor group $m(B)/Z$ acts faithfully on Y. From Proposition 2.2, the ambient space of $\mathcal{S}^{10}[f]$ is V, whence $\dim(X(0)) = \dim(Y) = 10$. Furthermore, no nonzero proper subspace of $X(0)$ or Y is invariant under $m(B)$, as 11 divides $2^{10}-1$ but not $2^i - 1$ for any $i = 1,\ldots,9$.

(2) As $m(B)$ is a cyclic group containing $z = m_\omega$, we have $m(B) \le C_A(z)$. From equations (25) and (24), we have $\phi^{-1} m_b \phi = m_{b^4}$. Thus F normalizes $m(B)$ and centralizes $z = m_\omega$. As both $m(B)$ and F act faithfully on $X(0)$, the group $m(B)F \cong Z_{33} : Z_5$ is isomorphic to a subgroup of $\mathrm{Aut}(X(0)) \cong \mathsf{GL}_{10}(2)$ centralizing z. As z corresponds to the scalar matrix $\alpha(z) = \omega I$ in $\mathsf{GL}_5(4)$, $C_{\mathrm{Aut}(X(0))}(z)$ is isomorphic to a subgroup of $\mathsf{GL}_5(4)$.

As $10 \equiv 2$ modulo 4, we can apply corollary 4.9 to conclude that $|C_A(z)|$ is odd. The action of $m(B)$ on $\mathsf{GF}(q)$ via α is the multiplication by some elements of $\mathsf{GF}(q)^\times$. As this action is irreducible on $\mathsf{GF}(q)$ by claim (1), the centralizer of $\alpha(m(B))$ in $\mathsf{GL}(\mathsf{GF}(q)) \cong \mathrm{Aut}(X(0))$ coincides with the group of multiplications of all elements of $\mathsf{GF}(q)^\times$ (see e.g. [4, p.244, Proposition 19.8]). The same argument applied to the action of $m(B)$ on $\mathsf{GF}(q)$ via β shows that the centralizer of $\beta(m(B))$ in $\mathsf{GL}(\mathsf{GF}(q)) \cong \mathsf{GL}(Y)$ is also

given by the multiplications by all elements of $\mathrm{GF}(q)^\times$. In particular, elements of $\alpha(C_A(m(B)))$ and $\beta(C_A(m(B))$ are multiplications by some elements of $\mathrm{GF}(q)^\times$. Thus each element of $C_A(m(B))$ is of the form in equation (24) in Step 1. By the conclusion of Step 1, it lies in $m(B)$. Thus $C_A(m(B)) = m(B)$. □

Step 4. *The proof of Proposition 5.1.*

Proof. It follows from Corollary 4.7 that $\mathrm{Aut}(\mathcal{S}^{10}[f]) = T : A$, where T is an elementary abelian group of order 2^{10}. Thus it remains to determine the stabilizer A of $X(0)$ (and Y). As $\langle z\rangle$ is normal in A, the centralizer $C_A(z)$ is a normal subgroup of A of index at most 2. As $C_A(z)$ is isomorphic to a subgroup of $C_{\mathrm{Aut}(X(0))}(z)$, it follows from Step 2 and Step 3(2) that $C_A(z)$ is isomorphic to a subgroup of $\mathsf{GL}_5(4)$ of odd order which contains $m(B)F$ or $m(B)$ according as $u = \omega^{\pm 1}$ or not.

We will show that $C_A(z)$ coincides with $m(B)F$ or $m(B)$, according as $u = \omega^{\pm 1}$ or not. Let $Q = \langle m_\eta\rangle$ be the subgroup of $m(B)$ of order 11. We claim that $Q = O_{11}(C_A(z))$, where $O_p(X)$ for a prime p denotes the largest normal p-subgroup of a finite group X.

First, we verify that $O_3(C_A(z)/\langle z\rangle) = 1$. Suppose $O_3(C_A(z)/\langle z\rangle) = H/\langle z\rangle = \overline{H}$ is nontrivial. For a subgroup X of $C_A(z)$, we write $\overline{X} = X\langle z\rangle/\langle z\rangle$. As $\overline{H}$ is normal in $\overline{C_A(z)}$, $\overline{Q}$ acts coprimely on $\overline{H}$. As H is isomorphic to a subgroup of a Sylow 3-subgroup of $\mathsf{GL}_5(4)$, $|\overline{H}|$ is of order at most $3^6/3 = 3^5$. Notice that $\overline{Q}$ does not centralize $\overline{H}$, for otherwise Q centralizes H from a standard property of coprime action, whence $H \le C_A(\langle z\rangle \times Q) = C_A(m(B)) = m(B)$, but this would imply that $H \le \langle z\rangle$. As 11 does not divide $3^i - 1$ for all $i = 1, \dots, 4$, this implies that $\overline{H}$ is an elementary abelian 3-group of order 3^5 on which $\overline{Q}$ acts fixed point freely. Then $|H| = 3^6$, whence H is isomorphic to a Sylow 3-subgroup T of $\mathsf{GL}_5(4)$. We may take T to be a subgroup of $\mathsf{GL}_5(4)$ generated by the diagonal matrices d_i $(i = 1, \dots, 5)$ and a permutation matrix π corresponding to (123), where d_i has diagonal entries ω and four 1's with ω at (i,i)-entry. Notice that $\langle \omega I\rangle$ is a subgroup of T corresponding to $\langle z\rangle$. As $[d_1, \pi] = d_1^{-1}d_2$ does not lie in $\langle \omega I\rangle$, $H/\langle z\rangle = \overline{H}$ is not abelian. This contradiction shows that $O_3(C_A(z)/\langle z\rangle) = 1$.

As $C_A(z)$ is of odd order, we have $O_p(C_A(z)/\langle z\rangle) \ne 1$ for some prime p by the odd order theorem (or more explicit arguments in $\mathsf{GL}_5(4)$). By the above paragraph, $p \ne 3$. Then we have $O_p(C_A(z)) \ne 1$ on which Q acts. Notice that the odd part of $|\mathsf{GL}_5(4)|$ is $3^6 5^2 7 \cdot 11 \cdot 17 \cdot 31$. Thus for each possible odd prime divisor $p \ne 3$, the group Q of order 11 acts trivially on $O_p(C_A(z))$. As $Q\langle z\rangle = m(B) = C_A(m(B))$, this implies that $p = 11$ is the unique possibility. Thus $O_{11}(C_A(z)) = Q$, as we claimed.

Then $C_A(z)$ and F are subgroups of $C_{\mathrm{Aut}(X(0))}(z)$ normalizing Q. Thus $C_A(z)$ and F correspond to subgroups of the normalizer N in $\mathsf{GL}_5(4)$ of a Sylow 11-subgroup (corresponding to Q) by Step 3(2). It is easy to see that N is isomorphic to $(Z_3 \times Z_{11} \times Z_{31}) : Z_5$, which corresponds to $(m(B) \times \langle m_\zeta \rangle)F$. Thus $C_A(z)$ is a subgroup of $(m(B) \times \langle m_\zeta \rangle)F$. By Step 1 and Step 2, we have $C_A(z) = ((m(B) \times \langle m_\zeta \rangle)F) \cap C_A(z) = m(B)F$ or $m(B)$ according as $u = \omega^{\pm 1}$ or not.

Now it remains to show that $A = C_A(z)$, or equivalently there is no involution of A inverting z. Suppose that g is an involution of A inverting z. Then $A = C_A(z)\langle g \rangle$ and g normalizes $m(B) = \langle z \rangle \times Q$. As $d + 1 = 10$ is even, we have case (1) or (2) in Lemma 4.8. In particular, g does not act trivially on Y. By Step 3(1), the group $m(B) : \langle g \rangle$ acting on Y has a normal irreducible cyclic group $m(B)$. As the action of $m(B)$ on Y is given by the multiplication of elements in $\mathsf{GF}(q)^\times$, then it follows from [4, p.244, Proposition 19.8] that there exists an element $\beta \in \mathsf{GF}(q)^\times$ such that $(0, y)^g = (0, \beta y^{2^5})$ for all $y \in \mathsf{GF}(q)$. As $g^2 = 1$, we have $\beta^{33} = 1$. The same argument applied to $X(0)$ shows that $(x, 0)^g = (\alpha x^{2^5}, 0)$ for some $\alpha \in \mathsf{GF}(q)^\times$ with $\alpha^{33} = 1$. Hence $h = gm_\alpha^{-1}$ is an automorphism of $\mathcal{S}^{10}[f]$ such that $(x, y)^h = (x^{2^5}, \gamma y^{2^5})$ for some $\gamma \in \mathsf{GF}(q)^\times$ with $\gamma^{33} = 1$. Then h is an involution with $C_{X(0)}(h) = \{(x, 0) \mid x \in \mathsf{GF}(2^5)\}$.

For $s \neq t \in \mathsf{GF}(2^5)$, it then follows from equation (15) that $X(s)$ and $X(t)$ are stabilized by h. Thus h fixes the unique nonzero vector $\big(s + t, b_f(s, t)\big)$ in $X(s) \cap X(t)$. This implies that $b_f(s, t) = (st^2 + s^2 t) + u\big(s^4 t^{32} + s^{32} t^4\big)$ satisfies $\gamma b_f(s, t)^{2^5} = b_f(s, t)$ for every $s, t \in \mathsf{GF}(2^5)$. Then we have $(\gamma + 1)(st^2 + ts^2) = (\gamma u^2 + u)(s^4 t + st^4)$, as $u^{2^5} = u^2$ and $s^{31} = t^{31} = 1$. Thus we have $\gamma + 1 = (\gamma u^2 + u)(s^2 + st + t^2)$ for all $s \neq t \in \mathsf{GF}(2^5)^\times$. This is impossible. Thus A does not contain any involution, whence $A = C_A(z)$. □

Using Proposition 5.1, we can verify that $\mathcal{S}^{10}[f]$ is not isomorphic to any 9-dual hyperoval in the classes $\mathcal{S}^{10}_{\sigma,\phi}$ and $\mathcal{T}_\sigma$, where σ is a generator of the Galois group of $\mathsf{GF}(2^{10})/\mathsf{GF}(2)$ and ϕ is a bijection on $\mathsf{GF}(2^{10})$ induced by an o-polynomial. In fact, by Proposition 3.2, the only d-dual hyperoval in these classes which could possibly be isomorphic to $\mathcal{S}^{10}[f]$ is $\mathcal{S}^{10}_{\sigma,\sigma}$ for some σ. However, the latter admits the automorphism group acting doubly transitively [8], but $\mathrm{Aut}(\mathcal{S}^{10}[f])$ is not doubly transitive by Proposition 5.1. Hence $\mathcal{S}^{10}[f]$ is, in fact, a new 9-dual hyperoval over $\mathsf{GF}(2)$ with ambient space of dimension 20.

For a quadratic APN fuction f other than the Gold function $f(x) = x^{2^m+1}$ ($x \in \mathsf{GF}(2^{d+1})$), m being coprime with $d+1$ (possibly its equivalents), it is likely that the stabilizer A in $\mathrm{Aut}(\mathcal{S}^{d+1}[f])$ of $X(0)$ is generated by a proper subgroup of a Singer cycle $Z_{2^{d+1}-1}$ and possibly the field automorphisms. In particular, $\mathrm{Aut}(\mathcal{S}^{d+1}[f])$ is not doubly transitive, and hence not isomorphic to $\mathcal{S}^{d+1}_{\sigma,\phi}$ for any

generator σ of $\mathrm{Gal}(\mathsf{GF}(2^{d+1})/\mathsf{GF}(2))$ and any bijection ϕ on $\mathsf{GF}(2^{d+1})$ induced by an o-polynomial. The above observation on the structure of A is verified for some APN functions belonging to the families found in [1]. However, the results obtained so far are partial and do not cover all the members in a family.

Correction added in proof

In Proposition 5.1, the automorphism group $\mathrm{Aut}(\mathcal{S}^{10}[f])$ for an APN map $f(x) = x^3 + ux^{36}$ on $\mathsf{GF}(2^{10})$ with $u \neq \omega^{\pm 1}$ should be $2^{10} : ((Z_3 \times Z_{11}) : Z_5)$, in place of $2^{10} : (Z_3 \times Z_{11})$. In fact, it is shown that the APN maps of form $f(x) = x^3 + ux^{36}$ on $\mathsf{GF}(2^{10})$ for some $u \in \mathsf{GF}(2^{10}) \setminus \mathsf{GF}(2^5)$ are extended affine equivalent to each other, and hence the automorphism groups $\mathrm{Aut}(\mathcal{S}^{10}[f])$ are isomorphic. The claim in the second paragraph of the proof of Step 4 (page 20) is incorrect in the case $u \neq \omega^{\pm 1}$: it is proved in the last line of the first paragraph on page 21 by just referring to Step 1 and Step 2, but this does not work.

I thank Dr. Edel for pointing out the error.

References

[1] **L. Budaghyan**, **C. Carlet**, **P. Felke** and **G. Leander**, An infinite class of quadratic APN functions which are not equivalent to power mappings, *Proceedings of IEEE Intern. Symposium on Information Theory 2006, Seattle, USA, Jul. 2006*.

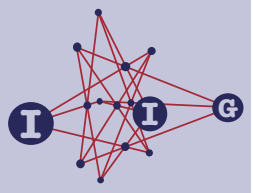
[2] **C. Carlet**, **P. Charpin** and **V. Zinoviev**, Codes, bent functions and permutations suitable for DES-like cryptosystems, *Des. Codes Cryptogr.* **15** (1998), 125–156.

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

[4] **D. S. Passman**, *Permutation Groups*, Benjamin, New York, 1968.

[5] **A. Pasini** and **S. Yoshiara**, On a new family of flag-transitive semibiplanes, *European J. Combin.* **22** (2001), 529–545.

[6] **H. Taniguchi**, A family of dual hyperovals over $\mathsf{GF}(q)$ with q even, *European J. Combin.* **26** (2005), 195–199.



[7] **H. Taniguchi** and **S. Yoshiara**, On dimensional dual hyperovals $\mathcal{S}_{\sigma,\phi}$, *Innov. Incidence Geom.* **1** (2005), 197–219.

[8] **S. Yoshiara**, A family of d-dimensional dual hyperovals in $\mathrm{PG}(2d+1,2)$, *European J. Combin.* **20** (1999), 589–603.

[9] _____, Dimensional dual arcs — a survey, **in** *Finite Geometries, Groups, and Computation*, eds. A. Hulpke, B. Liebler, T. Penttila, and A. Seress, Walter de Gruyter, Berlin-New York, 2006, 247–266.

[10] _____, Note on Taniguchi's dimensional dual hyperovals, *European J. Combin.* **28** (2007), 674–684.

Satoshi Yoshiara

DEPARTMENT OF MATHEMATICS, TOKYO WOMAN'S CHRISTIAN UNIVERSITY, SUGINAMI-KU, TOKYO 167-8585, JAPAN

e-mail: yoshiara@lab.twcu.ac.jp