Some remarks on dimensional dual hyperovals of polar type

Satoshi Yoshiara

Abstract

A notion of dimensional dual polar spaces of polar type is given with a family of new examples. Nonexistence is shown for those of dimension 3, while there are just two isomorphism classes for those of dimension 2.

1 Introduction

A family $\mathcal{S}$ of d-(projective) dimensional subspaces of a Desarguesian projective space $PG(n,q)$ over a finite filed $GF(q)$ is called a *d-dimensional dual hyperoval* (resp. *dimensional dual arc*) if the following conditions (i)–(iv) (resp. (i)–(iii)) are satisfied:

(i) any two distinct members of $\mathcal{S}$ intersect at a projective point.

(ii) any three mutually distinct members of $\mathcal{S}$ intersect trivially.

(iii) the members of $\mathcal{S}$ generate $PG(n,q)$.

(iv) $\mathcal{S}$ consists of $(q^{d+1}-1)/(q-1)+1$ members.

In this paper, $PG(n,q)$ (or sometimes the underlying vector space V of rank $n+1$ over $GF(q)$) is called the *ambient space* of $\mathcal{S}$. We also use the word '*rank*' to refer to 'vector space dimension'.

Let f be one of the following forms on the vector space V underlying $PG(n,q)$: a nondegenerate alternating form, a nondegenerate Hermitian form (in this case we assume that q is a square), a nonsingular quadratic form. The form f is also referred to as a symplectic, unitary or orthogonal form, respectively. A d-dimensional dual

Bull. Belg. Math. Soc. 12 (2005), 925–939

arc $\mathcal{S}$ with ambient space V is said to be *of polar type with respect to* f if each member of $\mathcal{S}$ is a maximal totally isotropic subspace of V with respect to f. We also say that $\mathcal{S}$ is of symplectic, unitary or orthogonal polar type, according as f is a symplectic, unitary or orthogonal form.

The dimension $d+1$ of a maximal totally isotropic space is related to the rank $n+1$ of the ambient space V as follows. If f is a symplectic form, $n+1$ is even and $n+1 = 2(d+1)$. If f is unitary, $d+1$ is the largest integer with $d+1 \leq (n+1)/2$, namely $n+1 = 2(d+1)$ or $n = 2(d+1)$ according as n is odd or even. If f is orthogonal and n is even, then $n = 2(d+1)$. If f is orthogonal and n is odd, there are two cases: $n+1 = 2(d+1)$ or $n+1 = 2(d+2)$. In the former (resp. latter) case, $\mathcal{S}$ is said to be of *plus* (resp. *minus*) orthogonal polar type.

In this paper, we consider the case when $n = 2d+1$, that is, either f is a symplectic form, a unitary form with n odd, or an orthogonal form of plus type. Notice that if q is even, the bilinear form associated with an orthogonal form is symplectic, whence a dual hyperoval of plus orthogonal polar type is automatically of symplectic polar type.

As far as the author knows, there are only two examples known for dimensional dual hyperovals of polar type. One is the remarkable 2-dimensional dual hyperoval $\mathcal{M}$ in $PG(5, 2^2)$ of unitary polar type admitting the Mathieu group M_{22} inside $Aut(\mathcal{M})$. The other example is a 2-dimensional dual hyperoval $\mathcal{D}$ in $PG(5, 2)$ which satisfies Condition (T) of Del Fra [1], namely $\dim(\langle X, Y\rangle \cap Z) = 1$ for all mutually distinct members X, Y, Z of $\mathcal{D}$. This is of orthogonal polar type, though it seems to be less known.

The main aim of this paper is to provide a new family of examples of dimensional dual hyperovals of polar type, which includes $\mathcal{D}$. They are found in a family $\mathcal{S}^{d+1}_{m,h}$ constructed by Yoshiara [7]. It turns out that $\mathcal{S}^{d+1}_{-2h,h}$ is always of plus orthogonal type for each even d (Proposition 7), while the existence of a d-dimensional dual arc of plus orthogonal type implies that d is even (Proposition 3). A similar method is applied to a class of dimensional dual hyperovals constructed by Taniguchi [5], but we found no example there (Proposition 8). The subsidiary aim is to provide preliminary remarks to dimensional dual hyperovals of polar type, from which nonexistence of those of dimension 3 is obtained (Proposition 5). Classification of those of dimension 2 is also given (Proposition 4).

2 Some general results

In this section, we assume that $\mathcal{S}$ is a d-dimensional dual arc in $PG(2d+1, q)$ which is of polar type with respect to a form f on the underlying space V of $PG(2d+1, q)$. For a subspace U of V, we denote by $U^{\perp}$ the subspace of V consisting of vectors $x \in V$ with $b_f(x, y) = 0$ for all $y \in U$, where $b_f = f$ unless f is of an orthogonal form and b_f denotes the associated bilinear form with f if f is an orthogonal form. Note that b_f is nondegenerate, in the sense that $V^{\perp} = \{0\}$. We frequently use the following properties for subspaces A, B of V without further references, where $\dim(U)$ denotes the projective dimension of $PG(U)$.

$$\dim(A^{\perp}) = 2d - \dim(A),\ \ (A^{\perp})^{\perp} = A,$$
$$\langle A, B\rangle^{\perp} = A^{\perp} \cap B^{\perp},\ \ (A \cap B)^{\perp} = \left\langle A^{\perp}, B^{\perp}\right\rangle,$$

$A \subseteq B$ if and only if $A^\perp \supseteq B^\perp$. In particular,
$A^\perp = A$ if A is a maximal totally isotropic subspace of V.

The first property we note on dimensional dual arc of polar type is as follows.

Lemma 1. *For any mutually distinct members X, Y, Z of $\mathcal{S}$, we have*

$$\dim(\langle X, Y\rangle \cap Z) = d - 1.$$

In particular, a 2-dimensional dual hyperoval in $PG(5, q)$ satisfies Property (T) in [1].

Proof. As $X = X^\perp$ and $Y = Y^\perp$ by the definition of dual arcs of polar type, we have $(X \cap Y)^\perp = \left\langle X^\perp, Y^\perp \right\rangle = \langle X, Y\rangle$. As $X \cap Y$ is a projective point of $PG(2d + 1, q)$, $\langle X, Y\rangle$ is a hyperplane of $PG(2d + 1, q)$, whence $Z \subseteq \langle X, Y\rangle$ or the equality in the lemma holds. In the former case, Z is perpendicular to $X \cap Y$, and hence the maximality of Z as a totally isotropic subspace implies that Z contains $X \cap Y$. However, this contradicts that three distinct members of $\mathcal{S}$ intersect trivially. ∎

The next lemma is also easy to verify, but it turns out to be very helpful.

Lemma 2. *Fix a member X of $\mathcal{S}$ and let π be a $(d - i)$-dimensional subspace of X with $1 \leq i \leq d - 1$. For a member $A \in \mathcal{S} \setminus \{X\}$, we have $X \cap A \in \pi$ (resp. $\notin \pi$) if and only if $\dim(A \cap \pi^\perp) = i$ (resp. $i - 1$). Furthermore, $\left\langle A \cap \pi^\perp, \pi \right\rangle$ is a maximal totally isotropic subspace of $PG(2d + 1, q)$.*

Proof. The (projective) dimension of $\pi^\perp$ is $2d - (d - i) = d + i$. As A is maximal totally isotropic, we have $\left\langle A, \pi^\perp \right\rangle^\perp = A^\perp \cap \pi = A \cap \pi$, whence $\dim(\left\langle A, \pi^\perp \right\rangle) = 2d - \dim(A \cap \pi)$. Thus

$$\begin{aligned}
\dim(A \cap \pi^\perp) &= \dim(A) + \dim(\pi^\perp) - \dim(\left\langle A, \pi^\perp \right\rangle) \\
&= d + (d + i) - (2d - \dim(A \cap \pi)) \\
&= i + \dim(A \cap \pi).
\end{aligned}$$

As $A \cap \pi$ is a subspace of a projective point $A \cap X$, we have $\dim(A \cap \pi) = 0$ or -1 according as $A \cap X \in \pi$ or not. Thus the former part of Lemma follows.

As π and A are totally isotropic, the subspace $\left\langle A \cap \pi^\perp, \pi \right\rangle$ is a totally isotropic subspace and $\pi \subseteq \pi^\perp$. Then $A \cap \pi^\perp \cap \pi = A \cap \pi$, and the dimension of $\left\langle A \cap \pi^\perp, \pi \right\rangle$ is $\dim(A \cap \pi^\perp) + \dim(\pi) - \dim(A \cap \pi) = i + \dim(A \cap \pi) + \dim(\pi) - \dim(A \cap \pi) = d$. This shows the latter part of Lemma. ∎

We state an easy consequence of the existence of dimensional dual arcs of plus orthogonal type.

Proposition 3. *Assume that there is a d-dimensional dual arc of plus orthogonal type in $PG(2d + 1, q)$. Then d is even.*

Proof. Let V be the underlying vector space of $PG(2d+1,q)$ equipped with an orthogonal form f with respect to which $\mathcal{S}$ is of polar type. Note that $|\mathcal{S}| \geq 3$, as two distinct members of $\mathcal{S}$ span a hyperplane of $PG(2d+1,q)$. Recall that the set of maximal totally isotropic subspaces of V with respect to f fall into two classes with the property that two subspaces belong to the same class if and only if their intersection has even codimension in each. Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be these two classes. We may assume that $\mathcal{C}_1$ contains a member X of $\mathcal{S}$. Now suppose d is odd. Then every member Y in $\mathcal{S} \setminus \{X\}$ belongs to $\mathcal{C}_2$, as the codimension of a point $X \cap Y$ in X is an odd number d. However, then two distinct members Y, Z of $\mathcal{S} \setminus \{X\}$ lie in the same class $\mathcal{C}_2$, whence the codimension d of $Y \cap Z$ in Y would be even. This contradiction shows that d should be even. ∎

Note that later we show the existence of d-dimensional dual hyperovals of plus orthogonal type for every even integer $d \geq 2$ (Proposition 6). Now we change to examine d-dimensional dual hyperovals of polar type for small d.

Consider the case $d = 2$. Then it follows from Lemma 1 that $\mathcal{S}$ satisfies Property (T) in [1, Subsection 1.1]. As is remarked in [1, Subsection 2.5], we can afford a structure of a Steiner triple system on the members of $\mathcal{S}$ with block size $q+2$, from which we have $q = 2$ or 4. For each possibility of q, there is a unique 2-dimensional dual hyperoval in $PG(5,q)$ with Property (T) up to isomorphism [1, Theorem 2, Theorem 4]. The resulting list of members of $\mathcal{S}$ are given in [1, Subsections 4.3,4.6]. It is not difficult to see that it is of polar type with respect to a plus orthogonal (resp. unitary) form if $q = 2$ (resp. 4). Thus classification of 2-dimensional dual hyperovals of polar type has already been done in [1]. We state the result here for convenience.

Proposition 4. *There are exactly two isomorphism classes of 2-dimensional dual hyperovals of polar type in $PG(5,q)$. One is of plus orthogonal type for $q = 2$, and the other is of unitary type for $q = 4$.*

It is worth mentioning that, instead of quoting the results by Del Fra, we can provide more explicit and constructive proof (at least in the case of unitary polar type), by exploiting (weak) o-polynomials which determine 1-dimensional dual hyperovals on the isotropic planes constructed via Lemma 2. Based on the resulting presentation of $\mathcal{S}$, we can also explicitly see the action of M_{22} on the members. See [4] for details.

Now we consider the case $d = 3$. In contrast with the case $d = 2$, there is no example.

Proposition 5. *There is no 3-dimensional dual hyperoval of polar type in $PG(7,q)$.*

Proof. For a while, we proceed with general dimension d. Let $\mathcal{S}$ be a d-dimensional dual hyperoval in $PG(2d+1,q)$, which is of polar type with respect to a symplectic, unitary or orthogonal form f on the underlying vector space of $PG(2d+1,q)$. Fix a member X of $\mathcal{S}$ and set $\overline{\mathcal{S}} := \mathcal{S} \setminus \{X\}$. Choose a hyperplane π of X and define

$$\overline{\mathcal{S}}(\pi) := \{A \in \overline{\mathcal{S}} \mid A \cap X \in \pi\},$$
$$L(A) := A \cap \pi^{\perp}, \text{ and } T(A) := \langle L(A), \pi \rangle \text{ for } A \in \overline{\mathcal{S}}(\pi).$$

From Lemma 2, $L(A)$ and $T(A)$ are isotropic 1 and d-subspaces respectively for every $A \in \overline{\mathcal{S}}(\pi)$. In particular, $L(A) \nsubseteq X$ and hence $T(A) = \langle L(A), \pi \rangle$ is a totally isotropic d-subspace distinct from X.

There are exactly $(q^d - 1)/(q - 1)$ members of $\overline{\mathcal{S}}(\pi)$, as π consists of $(q^d - 1)/(q - 1)$ points, each of which is uniquely realized as $A \cap X$ for $A \in \overline{\mathcal{S}}(\pi)$. If $A \neq B \in \overline{\mathcal{S}}(\pi)$, then $A \cap X \neq B \cap X$. Then $L(A) \neq L(B)$, as $L(A) \cap \pi = A \cap X$ and $L(B) \cap \pi = B \cap X$.

Let X, Y_1, $\ldots$, $Y_{q'}$ be all the totally isotropic subspaces of $PG(2d + 1, q)$ containing the $(d - 1)$-dimensional totally isotropic subspace π. Then $q' = q$, $\sqrt{q}$ or 1 according as f is symplectic, unitary or orthogonal (of plus type). Notice that $q' \leq q$ in any case. As we saw above, the subspace $T(A)$ for each $A \in \overline{\mathcal{S}}(\pi)$ coincides with Y_j for some $j = 1, \ldots, q'$. Thus we can consider a map sending $A \in \overline{\mathcal{S}}(\pi)$ to $T(A) \in \{Y_1, \ldots, Y_{q'}\}$.

Suppose that $T(A) = T(B)$ but the line $L(A)$ is skew to the line $L(B)$. Then $\langle L(A), L(B) \rangle$ is a 3-subspace in a maximal totally isotropic d-subspace $T := T(A) = T(B)$. Now we assume $d = 3$. Then we have $T = \langle L(A), L(B) \rangle$. This implies that $T \subseteq \langle A, B \rangle = (A \cap B)^{\perp}$ by the maximality of A and B, whence $A \cap B \in T$ by the maximality of T. As π is contained in the totally isotropic subspace T, this impies that $A \cap B \in \pi^{\perp}$, namely $A \cap B = L(A) \cap L(B)$. However, this contradicts our assumption.

Hence if $T(A) = T(B)$, then $L(A)$ and $L(B)$ intersect in $T(A) = T(B)$. We claim that each Y_j $(j = 1, \ldots, q')$ is realized as $T(A)$ for at most $q + 1$ members A of $\overline{\mathcal{S}}(\pi)$. We may assume that $Y_j = T(A)$ for some $A \in \overline{\mathcal{S}}(\pi)$. If $B \in \overline{\mathcal{S}}(\pi) \setminus \{A\}$ with $T(A) = T(B)$ exists, then $L(B)$ intersects $L(A)$ at a point $A \cap B$. Note that $A \cap X \neq A \cap B$, as no three distinct members of $\mathcal{S}$ share a point in common. Hence there are at most q possible $B \in \overline{\mathcal{S}}(\pi)$ other than A with $T(A) = T(B)$.

Therefore we have at most $(q + 1)q'$ members in $\overline{\mathcal{S}}(\pi)$. Then we have

$$|\overline{\mathcal{S}}(\pi)| = (q^3 - 1)/(q - 1) = 1 + q + q^2 \leq (q + 1)q' \leq (q + 1)q,$$

which is impossible. ∎

3 Yoshiara's dimensional dual hyperovals

In the remaining sections of this note, to each d-dimensional dual hyperoval in $PG(2d + 1, q)$ belonging to known classes (constructed by Yoshiara and Taniguchi) we examine whether or not it has a structure of polar type. We first examine the family constructed by Yoshiara [7].

Let d be a positive integer with $d \geq 2$, and let m and h be positive integers coprime with $d + 1$ and $1 \leq m, h \leq d$. We denote respectively by α and β the Galois automorphisms in $Gal(GF(2^{d+1})/GF(2))$ given by $x^{\alpha} = x^{2^m}$ and $x^{\beta} = x^{2^h}$ $(x \in GF(2^{d+1}))$. Observe that both α and β generate $Gal(GF(2^{d+1})/GF(2))$, as $(m, d+1) = (h, d+1) = 1$. Then the map $\alpha - 1$ from $GF(2^{d+1})^{\times}$ to itself defined by $x^{\alpha - 1} = x^{\alpha}/x$ $(x \in GF(2^{d+1}))$ is bijective. We denote its inverse map by $1/(\alpha - 1)$. Similarly we define $1/(1 - \alpha)$, $\beta - 1$, $1 - \beta$ and $1/(\beta - 1)$. The composite of $1/(\alpha - 1)$ and $\beta - 1$ is denoted $(\beta - 1)/(\alpha - 1)$, etc. We regard $U := GF(2^{d+1}) \times GF(2^{d+1})$ as a vector space over $GF(2)$ of rank $2(d + 1)$, underlying $PG(U) \cong PG(2d + 1, 2)$.

With the above setting, Yoshiara constructed a d-dimensional dual hyperoval $\mathcal{S}^{d+1}_{m,h}$ as follows: for $t \in GF(2^{d+1})$, define a rank $(d+1)$-subspace of U by

$$S(t) \quad = \quad \{(x, x^{\alpha}t + xt^{\beta}) \mid x \in GF(2^{d+1})\}. \tag{1}$$

Let A be the subspace of U generated by all members of $\mathcal{S}^{d+1}_{m,h}$ (this is also referred to as the *ambient space* of $\mathcal{S}^{d+1}_{m,h}$). We have either $A = U$ or A is a hyperplane of U, according as $m + h \neq d + 1$ or $m + h = d + 1$ [7, Proposition 3].

Then the family $\mathcal{S}^{d+1}_{m,h} := \{S(t) \mid t \in GF(2^{d+1})\}$ is a d-dimensional dual hyperoval in $PG(A)$. For convenience, $\mathcal{S}^{d+1}_{m,h}$ is sometimes denoted $\mathcal{S}^{d+1}_{\alpha,\beta}$ or $\mathcal{S}^{d+1}_{m',h}$ with an integer m' congruent to m modulo $d+1$.

We now examine when $\mathcal{S}^{d+1}_{m,h}$ is of polar type, that is, there exists a symplectic, orthogonal or unitary form f on A with respect to which each member of $\mathcal{S}^{d+1}_{m,h}$ is a maximal totally isotropic (or singular if f is orthogonal) subspace. As the scalar field is $GF(2)$, the form f is not unitary. Notice that $A = U$, for otherwise A is of rank $2d + 1$ and any member of $\mathcal{S}^{d+1}_{m,h}$, which is a totally isotropic subspace of A, would have rank at most d. Thus $A = U$ and then $m + h \neq d + 1$. Furthermore, as we work in characteristic 2, the associated bilinear form with an orthogonal form is symplectic. Thus we may assume that f is symplectic (and then examine whether it is associated with an orthogonal form).

Proposition 6. *The following conditions are equivalent for the d-dimensional dual hyperoval $\mathcal{S}^{d+1}_{m,h}$ with $m + h \neq d + 1$, $1 \leq m, h \leq d$ and $(m, d+1) = (h, d+1) = 1$.*

(i) $\mathcal{S}^{d+1}_{m,h}$ is of polar type with respect to a symplectic form f on U.

(ii) The dimension d is even, $m \equiv -2h \pmod{d+1}$ and each member of $\mathcal{S}^{d+1}_{-2h,h}$ is totally isotropic with respect to the symplectic form f on U given by

$$f((x, y), (u, v)) \quad = \quad Tr(xv^{2^h} + uy^{2^h}) \tag{2}$$

for any (x, y), $(u, v) \in U$, where Tr denotes the trace function of the extension $GF(2^{d+1})/GF(2)$.

Proof. We first check that Condition (ii) implies Condition (i). Note that $m \equiv -2h \pmod{d+1}$ is coprime with $d+1$, as d is even and $(h, d+1) = 1$. Then $\mathcal{S}^{d+1}_{-2h,h} = \mathcal{S}^{d+1}_{\beta^{-2},\beta}$ is well-defined. It is immediate to see that the form defined by Equation (2) is $GF(2)$-bilinear. As $f((x, y), (x, y)) = Tr(xy^{2^h} + y^{2^h}x) = Tr(0) = 0$ for every $(x, y) \in U$, the form f is alternating. If $f((x, y), (u, v)) = 0$ for all $(u, v) \in U$, then $Tr(bx) = 0 = Tr(cy^{2^h})$ for all $b, c \in GF(2^{d+1})$. From the separability of extension $GF(2^{d+1})/GF(2)$ this implies that $x = y^{2^h} = 0$ (see for example, [3, Theorem 2.24]), whence $(x, y) = (0, 0)$. Thus the form f is nondegenerate.

It remains to check that every member of $\mathcal{S}^{d+1}_{\beta^{-2},\beta}$ is isotropic. Each member $S(t)$ $(t \in GF(2^{d+1}))$ of $\mathcal{S}^{d+1}_{-2h,h} = \mathcal{S}^{d+1}_{\beta^{-2},\beta}$ consists of vectors $(x, x^{\beta^{-2}}t + xt^{\beta})$ for $x \in$

$GF(2^{d+1})$. Then for every $x, y \in GF(2^{d+1})$ we have

$$\begin{aligned} & f((x, x^{\beta^{-2}}t + xt^{\beta}), (y, y^{\beta^{-2}}t + yt^{\beta})) \\ = \ & Tr(x \cdot (y^{\beta^{-2}}t + yt^{\beta})^{\beta}) + y \cdot (x^{\beta^{-2}}t + xt^{\beta})^{\beta}) \\ = \ & Tr(xy^{\beta^{-1}}t^{\beta} + xy^{\beta}t^{\beta^2} + x^{\beta^{-1}}yt^{\beta} + x^{\beta}yt^{\beta^2}) \\ = \ & Tr((xy^{\beta^{-1}}t^{\beta} + x^{\beta^{-1}}yt^{\beta}) + (xy^{\beta^{-1}}t^{\beta} + x^{\beta^{-1}}yt^{\beta})^{\beta}) \\ = \ & 0. \end{aligned}$$

This shows that each member of $\mathcal{S}^{d+1}_{\beta^{-2},\beta}$ is in fact isotropic.

Now we will show that Condition (i) implies Condition (ii). We consider the following subspace of $GF(2^{d+1})$ for each $t \in GF(2^{d+1})^{\times}$.

$$Y(t) \ := \ \{x^{\alpha}t + xt^{\beta} \ | \ x \in GF(2^{d+1})\}$$

Then $Y(t)$ is the image of a $GF(2)$-linear map $GF(2^{d+1})$ to itself given by $x \mapsto x^{\alpha}t + t^{\beta}x$. As $\beta - 1$ and $1/(\alpha - 1)$ are well-defined, it is easy to see that the kernel of this map coincides with $\{0, t^{(\beta-1)/(\alpha-1)}\}$. Thus $Y(t)$ is a hyperplane of $GF(2^{d+1})$. On the other hand, for $t \in GF(2^{d+1})^{\times}$ and $x \in GF(2^{d+1})$ we have

$$\begin{aligned} & Tr((t^{-(\alpha\beta-1)/(\alpha-1)})(x^{\alpha}t + xt^{\beta})) \\ = \ & Tr(x^{\alpha}t^{1-(\alpha\beta-1)/(\alpha-1)} + xt^{\beta-(\alpha\beta-1)/(\alpha-1)}) \\ = \ & Tr((xt^{-(\beta-1)/(\alpha-1)})^{\alpha} + (xt^{-(\beta-1)/(\alpha-1)})) \\ = \ & 0, \end{aligned}$$

where Tr denotes the trace function of extension $GF(2^{d+1})/GF(2)$. Hence $Y(t)$ is contained in the kernel of the function $T_{t^{-(\alpha\beta-1)/(\alpha-1)}}$, where T_b for $b \in GF(q)$ is defined by

$$T_b(x) \ := \ Tr(bx)$$

As T_b ($b \in GF(2^{d+1})^{\times}$) is a $GF(2)$-linear form onto $GF(2)$, the kernel of T_b is a hyperplane of $GF(2^{d+1})$. Hence we conclude that the following holds for every $t \in GF(2^{d+1})^{\times}$.

$$Y(t) \ = \ Ker(T_{t^{-(\alpha\beta-1)/(\alpha-1)}}) \tag{3}$$

We assume that there is a symplectic form f on $U = GF(2^{d+1}) \times GF(2^{d+1})$ with respect to which every member of $\mathcal{S}^{d+1}_{\alpha,\beta}$ is totally isotropic. As $S(0) = \{(x, 0) \ | \ x \in GF(2^{d+1})\}$ is totally isotropic, we have

$$f((x, 0), (y, 0)) \ = \ 0 \tag{4}$$

for all $x, y \in GF(2^{d+1})$. For every $t \in GF(2^{d+1})^{\times}$, the member $S(t)$ is a totally isotropic space containing $S(t) \cap S(0) = \{(0, 0), (t^{(\beta-1)/(\alpha-1)}, 0)\}$. Thus for every $x \in GF(2^{d+1})$ we have

$$\begin{aligned} 0 \ = \ & f((t^{(\beta-1)/(\alpha-1)}, 0), (x, x^{\alpha}t + xt^{\beta})) \\ = \ & f((t^{(\beta-1)/(\alpha-1)}, 0), (x, 0)) + f((t^{(\beta-1)/(\alpha-1)}, 0), (0, x^{\alpha}t + xt^{\beta})) \\ = \ & f((t^{(\beta-1)/(\alpha-1)}, 0), (0, x^{\alpha}t + xt^{\beta})), \end{aligned} \tag{5}$$

using Equation (4).

The above calculation motivates the definition of the following form g on U:

$$g(x,y) \;:=\; f((x,0),(0,y)) = f((0,y),(x,0)) \tag{6}$$

for $x, y \in GF(2^{d+1})$. As f is $GF(2)$-bilinear, it is easy to see that g is $GF(2)$-bilinear as well. For fixed $a \in GF(2^{d+1})^{\times}$, we define a $GF(2)$-linear form on $GF(2^{d+1})$ by

$$g_a(y) \;:=\; g(a,y). \tag{7}$$

With this notation, the above result (5) shows

$$g_{t^{(\beta-1)/(\alpha-1)}}(x^{\alpha}t + xt^{\beta}) \;=\; 0$$

for all $t \in GF(2^{d+1})^{\times}$ and $x \in GF(2^{d+1})$. Hence $Y(t)$ is contained in the kernel of a $GF(2)$-linear form $g_{t^{(\beta-1)/(\alpha-1)}}$. Notice that $Ker(g_b)$ is a hyperplane for every $b \in GF(2^{d+1})^{\times}$, for otherwise $0 = g_b(y) = g(b,y) = f((b,0),(0,y))$ for every $y \in GF(2^{d+1})$ and then $f((b,0),(x,y)) = 0$ for all $(x,y) \in U$ by Equation (4), which contradicts the nondegeneracy of f. Thus for all $t \in GF(2^{d+1})^{\times}$ we have

$$Y(t) \;=\; Ker(g_{t^{(\beta-1)/(\alpha-1)}}). \tag{8}$$

For each $t \in GF(2^{d+1})^{\times}$ we have two linear forms $g_{t^{(\beta-1)/(\alpha-1)}}$ and $T_{t^{-(\alpha\beta-1)/(\alpha-1)}}$ on $GF(2^{d+1})$ which have the same kernels, in view of (3) and (8). As these forms are maps into the two element field, we conclude that $g_{t^{(\beta-1)/(\alpha-1)}} = T_{t^{-(\alpha\beta-1)/(\alpha-1)}}$ for every $t \in GF(2^{d+1})^{\times}$, or equivalently,

$$g_t \;=\; T_{t^{\gamma}} \tag{9}$$

where $t^{\gamma} := t^{-(\alpha\beta-1)/(\beta-1)}$ for every $t \in GF(2^{d+1})^{\times}$. Notice that γ is multiplicative on $GF(2^{d+1})^{\times}$, that is,

$$(ts)^{\gamma} \;=\; t^{\gamma}s^{\gamma} \tag{10}$$

for all $s, t \in GF(2^{d+1})^{\times}$

Then it follows from $GF(2)$-linearity of g in the first variable and Equation (9) that for every $s, t \in GF(2^{d+1})^{\times}$ with $s \neq t$ and $y \in GF(2^{d+1})$ we have

$$\begin{aligned} Tr((s+t)^{\gamma}y) &= T_{(s+t)^{\gamma}}(y) \\ = g(s+t,y) &= g(s,y) + g(t,y) \\ = Tr(s^{\gamma}y) + Tr(t^{\gamma}y) &= Tr((s^{\gamma}+t^{\gamma})y). \end{aligned}$$

In particular, we have

$$(s+t)^{\gamma} \;=\; s^{\gamma} + t^{\gamma} \tag{11}$$

for all $s, t \in GF(2^{d+1})^{\times}$ with $s \neq t$. We extend γ to $GF(2^{d+1})$ by setting $0^{\gamma} = 0$. Then γ is a $GF(2)$-linear map on $GF(2^{d+1})$, which is not identically 0. Furthermore, γ is multiplicative on $GF(2^{d+1})$ by Equation (10). Hence γ is an automorphism of extension $GF(2^{d+1})/GF(2)$, and there exists an integer ℓ with $\gamma = \beta^{\ell}$ and $0 \leq \ell \leq d$, as the automorphism β is a generator of $Gal(GF(2^{d+1})/GF(2))$. We also set $\alpha = \beta^n$ for some integer n with $1 \leq n \leq d$.

From the definition of γ (just after claim (9)) that $y^\gamma y^{(\alpha\beta-1)/(\beta-1)} = 1$ for every $y \in GF(2^{d+1})^\times$. Take any $x \in GF(2^{d+1})^\times$ and apply this definition to $y = x^{\beta-1}$. As $\gamma = \beta^\ell$ and $\alpha = \beta^n$, we have $(x^\beta/x)^{\beta^\ell}(x^{\alpha\beta-1}) = (x^{\beta^{\ell+1}}/x^{\beta^\ell})(x^{\beta^{n+1}}/x) = 1$. Hence

$$x^{\beta^{\ell+1}+\beta^{n+1}} = x^{\beta^\ell+1}$$

for every $x \in GF(2^{d+1})^\times$. As $y^\beta = y^{2^h}$ $(y \in GF(2^{d+1}))$, this implies that

$$2^{h(\ell+1)} + 2^{h(n+1)} \equiv 2^{h\ell} + 1 \pmod{2^{d+1} - 1}. \tag{12}$$

Applying [2, p.273, 4.4(c)], we conclude that $\{h(\ell+1), h(n+1)\} \equiv \{0, h\ell\} \pmod{d+1}$, and therefore

$$\{\ell + 1, n + 1\} \equiv \{0, l\} \pmod{d + 1},$$

as $(h, d + 1) = 1$. If $n + 1 = d + 1$, then $\alpha\beta = \beta^{d+1} = 1$ and then $t^\gamma = 1$ for all $t \in GF(2^{d+1})^\times$ from definition of γ, which is impossible. Thus $n+1 \neq 0 \pmod{d+1}$, and therefore $\ell + 1 = d + 1$ and $n + 1 = l = d$. Then we have $\alpha = \beta^{d-1} = \beta^{-2}$, which is equivalent to $m \equiv -2h \pmod{d + 1}$. Then d is even, as m and h are coprime with $d + 1$. Furthermore, $x^\gamma = x^{-(\alpha\beta-1)/(\beta-1)} = x^{-(\beta^{-1}-1)/(\beta-1)} = x^{\beta^{-1}}$ for all $x \in GF(2^{d+1})^\times$. Summarizing, we have

$\alpha = \beta^{-2}$, $m \equiv -2h \pmod{d+1}$, d is even, $\gamma = \beta^{-1}$, so that
$g_t = T_{t^{\beta^{-1}}}$ and $Y(t^{(\alpha-1)/(\beta-1)}) = Ker(g_t) = Ker(T_{t^{\beta^{-1}}})$

It remains to find the explicit shape of f. First we will show that the subspace $\{(0, y) \mid y \in GF(2^{d+1})\}$ of $U = GF(2^{d+1}) \times GF(2^{d+1})$ is isotropic. Since $Y(t^{(\alpha-1)/(\beta-1)}) = Ker(T_{t^{\beta^{-1}}})$, we have $Y(t^{(\alpha-1)/(\beta-1)}) = Y(s^{(\alpha-1)/(\beta-1)})$ if and only if the map $T_{t^{\beta^{-1}}}$ coincides with the map $T_{s^{\beta^{-1}}}$, as these maps take values in $GF(2)$. Furthermore, we have $T_{t^{\beta^{-1}}} = T_{s^{\beta^{-1}}}$ if and only if $t^{\beta^{-1}} = s^{\beta^{-1}}$ (see [3, Theorem 2.24]), which is equivalent to to the condition $t = s$. Thus $\{Y(t) \mid t \in GF(2^{d+1})^\times\}$ exhausts $2^{d+1}-1$ hyperplanes of $GF(2^{d+1})$. Now choose any two vectors $(0, a)$ and $(0, b)$ of U. From the above remark, there is a hyperplane $Y(t)$ for some $t \in GF(2^{d+1})^\times$ which contains a subspace of $GF(2^{d+1})$ spanned by a and b. (Note that $d \geq 2$.)

We will show that $f((0, u), (0, v)) = 0$ for every $u, v \in Y(t)$. This implies that $f((0, a), (0, b)) = 0$ and shows that the subspace $\{(0, y) \mid y \in GF(2^{d+1})\}$ is isotropic, as we claimed. Recall that $S(t) = \{(x, x^{\beta^{-2}}t + xt^\beta) \mid x \in GF(2^{d+1})\}$ is isotropic. Then for every $x, y \in GF(2^{d+1})^\times$ we have

$$\begin{aligned}
0 &= f((x, x^{\beta^{-2}}t + xt^\beta), (y, y^{\beta^{-2}}t + yt^\beta)) \\
&= g(x, y^{\beta^{-2}}t + yt^\beta) + g(y, x^{\beta^{-2}}t + xt^\beta) + f((0, x^{\beta^{-2}}t + xt^\beta), (0, y^{\beta^{-2}}t + yt^\beta)) \\
&= Tr(x^{\beta^{-1}}y^{\beta^{-2}}t + x^{\beta^{-1}}yt^\beta + y^{\beta^{-1}}x^{\beta^{-2}}t + y^{\beta^{-1}}xt^\beta) \\
&\quad + f((0, x^{\beta^{-2}}t + xt^\beta), (0, y^{\beta^{-2}}t + yt^\beta)) \\
&= Tr((x^{\beta^{-1}}y^{\beta^{-2}} + y^{\beta^{-1}}x^{\beta^{-2}})t + \{(x^{\beta^{-1}}y^{\beta^{-2}} + y^{\beta^{-1}}x^{\beta^{-2}})t\}^\beta) \\
&\quad + f((0, x^{\beta^{-2}}t + xt^\beta), (0, y^{\beta^{-2}}t + yt^\beta)) \\
&= f((0, x^{\beta^{-2}}t + xt^\beta), (0, y^{\beta^{-2}}t + yt^\beta)),
\end{aligned}$$

using Equation (4) and Equation (9) with $\gamma = \beta^{-1}$. Thus we have $f((0,u),(0,v)) = 0$ for all $u, v \in Y(t)$, and therefore the subspace $\{(0,y) \mid y \in GF(2^{d+1})\}$ is totally isotropic.

Finally, we derive the explicit shape of f. For any $(x,y),(u,v) \in GF(2^{d+1})$, we have

$$\begin{aligned} f((x,y),(u,v)) &= f((x,0),(u,0)) + f((x,0),(0,v)) \\ &\quad + f((0,y),(u,0)) + f((0,y),(0,v)) \\ &= g(x,v) + g(u,y), \end{aligned}$$

as $S(0) = \{(x,0) \mid x \in GF(2^{d+1})\}$ and $\{(0,y) \mid y \in GF(2^{d+1})\}$ are totally isotropic and $f((0,y),(u,0)) = f((u,0),(0,y)) = g(u,y)$. As $g(x,v) = g_x(v) = Tr(x^{\beta^{-1}}v)$, it follows from the above equation that

$$\begin{aligned} f((x,y),(u,v)) &= Tr(x^{\beta^{-1}}v + u^{\beta^{-1}}y) \\ &= Tr(xv^{\beta} + uy^{\beta}) \end{aligned}$$

for all $(x,y),(u,v) \in U = GF(2^{d+1}) \times GF(2^{d+1})$. This completes the proof that condition (i) implies condition (ii). ■

In fact, the dual hyperovals $\mathcal{S}^{d+1}_{-2h,h}$ with d even and h coprime with $d+1$ are not only of symplectic type, but also of plus orthogonal type.

Proposition 7. *Let d be an even integer with $d \geq 2$ and let h be an integer with $1 \leq h \leq d$ coprime with $d+1$. Then there exists a unique orthogonal form f of plus type on the ambient space of $PG(2d+1,2)$ with respect to which $\mathcal{S}^{d+1}_{-2h,h}$ is of polar type.*

Proof. Define a form Q on U by

$$Q((x,y)) := Tr(xy^{2^h}).$$

It is straightfroward to verify that the associated form with Q coincides with a symplectic form f given in Proposition 6. As

$$\begin{aligned} Q((x, x^{2^{-2h}}t + xt^{2^h})) &= Tr(x^{1+2^{-h}}t^{2^h}) + Tr(x^{1+2^h}t^{2^{2h}}) \\ &= Tr(x^{1+2^{-h}}t^{2^h}) + Tr(x^{1+2^{-h}}t^{2^h}) = 0, \end{aligned}$$

we conclude that each member $S(t)$ of $\mathcal{S}^{d+1}_{-2h,h}$ is totally singular with respect to Q. In particular, Q is a nonsingular orthogonal form of plus type. If both Q and Q' are associated with the form f, the form $Q - Q'$ satisfies that $Q(x+y) - Q(x) - Q(y) = f(x,y) = Q'(x+y) - Q'(x) - Q'(y)$ for every $x, y \in U$, whence $Q' - Q$ is a $GF(2)$-linear form on U, which vanishes on all members $S(t)$ of $\mathcal{S}$. As $\mathcal{S}$ generates U, we conclude $Q' = Q$. ■

4 Taniguchi's dimensional dual hyperovals

Let $q = 2^e$ and let n be any positive integer. Regard $GF(q^n)$ and $U := GF(q^n) \times GF(q^n)$ as vector spaces over $GF(q)$ of rank n and $2n$ respectively, and choose a subspace V of $GF(q^n)$ of rank $d+1$ over $GF(q)$. For $X = V$, $GF(q^n)$ or U, we denote by $PG(X)$ the projective space associated with the vector space X over $GF(q)$. Then $PG(V) \cong PG(d,q)$, $PG(GF(q^n)) \cong PG(n-1,q)$ and $PG(U) \cong PG(2n-1,q)$. Take a generator σ of Galois group $Gal(GF(q^n)/GF(q))$.

With these settings, a d-dimensional dual hyperoval $\mathcal{T}(n,q;V,\sigma)$ with ambient space inside $PG(U)$ is constructed by Taniguchi as follows: for a projective point $[\alpha]$ of $PG(V)$, define

$$T[\alpha] := \{(\alpha x, x^\sigma \alpha + x\alpha^\sigma) \mid x \in V\}.$$

Observe that $T[\alpha]$ is a subspace of U of rank $d+1$, which does not depend on the choice of a representative $\alpha \in V - \{0\}$ for a projective point $[\alpha]$. Then the family $\mathcal{T}(n,q;V,\sigma)$ consisting of these d-dimensional subspaces $T[\alpha]$ of $PG(U)$ for $[\alpha] \in PG(V)$ together with the special subspace $T[\infty]$ of $PG(U)$ defined below is a d-dimensional dual hyperoval [5]:

$$T[\infty] := \{(x^2, 0) \mid x \in V\}.$$

We examine when $\mathcal{T}(n,q;V,\sigma)$ is of polar type; that is, there exists a symplectic, orthogonal or unitary form f on the ambient space A (with $q = r^2$ if f is hermitian) such that each member of $\mathcal{T}(n,q;V,\sigma)$ is a maximal totally isotropic (singular if f is orthogonal) subspace of A with respect to the form f. As the associated bilinear form of an orthogonal form is symplectic, we may assume that f is symplectic or unitary. The maximality of members of $\mathcal{T}(n,q;V,\sigma)$ as totally isotropic subspaces of A implies that the rank of A is $2(d+1)$. If $n = d+1$ and $V = GF(q^{d+1})$, we have $U = A$ and the above requirement is satisfied. In the sequel, we restrict ourselves to examine $\mathcal{T}(d+1,q;GF(q^{d+1}),\sigma)$. Note that in this case $T[\infty] = \{(x,0) \mid x \in GF(q^{d+1})\}$.

Proposition 8. *For every $q = 2^e$, positive integer d with $d \geq 2$ and a generator σ of $Gal(GF(q^{d+1})/GF(q))$, the d-dimensional hyperoval $\mathcal{T}(d+1,q;GF(q^{d+1}),\sigma)$ is not of polar type.*

Proof. We rewrite the original description of $T[\alpha]$ ($[\alpha] \in PG(V) = PG(q^{d+1})$) as follows:

$$T[\alpha] = \{(y, \alpha^{1-\sigma}y^\sigma + \alpha^{\sigma-1}y) \mid y \in GF(q^{d+1})\},$$

where $\alpha^{1-\sigma} := \alpha/\alpha^\sigma$ for $\alpha \in GF(q^{d+1})^\times$. We consider the following subspace of $GF(q^{d+1})$ for each $[\alpha] \in PG(V)$:

$$Y[\alpha] := \{\alpha^{1-\sigma}x^\sigma + \alpha^{\sigma-1}x \mid x \in GF(q^{d+1})\}.$$

This does not depend on the choice of a representative for a point $[\alpha]$, as $(k\alpha)^{1-\sigma} = \alpha^{1-\sigma}$ for $k \in GF(q)^\times$. For $x \in GF(q^{d+1})^\times$, we have $\alpha^{1-\sigma}x^\sigma + \alpha^{\sigma-1}x = 0$ if and only if $x^{\sigma-1} = (\alpha^2)^{\sigma-1}$, which is equivalent to the condition that x/α^2 is fixed by

$\langle\sigma\rangle = Gal(GF(q^{d+1})/GF(q))$, whence $x \in GF(q)\alpha^2 = [\alpha^2]$. Thus the kernel of the linear map $GF(q^{d+1}) \ni x \mapsto \alpha^{1-\sigma}x^\sigma + \alpha^{\sigma-1}x \in GF(q^{d+1})$ is of rank 1, and the image $Y[\alpha]$ of this map is a hyperplane of $GF(q^{d+1})$ over $GF(q)$.

Notice that $Tr(\alpha^{-(1+\sigma)}(\alpha^{1-\sigma}x^\sigma + \alpha^{\sigma-1}x)) = Tr((\alpha^{-2}x)^\sigma) + Tr(\alpha^{-2}x) = 0$ for every $x \in GF(q^{d+1})$, where Tr denotes the trace function for the Galois extension $GF(q^{d+1})/GF(q)$. Thus the hyperplane $Y[\alpha]$ is contained in $Ker(T_{\alpha^{-(1+\sigma)}})$, where T_b for $b \in GF(q^{d+1})$ denotes as in [3, Section 2] the linear form from $GF(q^{d+1})$ to $GF(q)$ defined by

$$T_b(x) := Tr(bx).$$

As $\alpha \neq 0$, the form $T_{\alpha^{-(1+\sigma)}}$ is surjective on $GF(q)$, and hence we have

$$Y[\alpha] \quad = \quad Ker(T_{\alpha^{-(1+\sigma)}}) \tag{13}$$

by comparing the ranks of these subspaces of $GF(q^{d+1})$ over $GF(q)$.

Assume now that f is a symplectic or unitary form on U for which every member of $\mathcal{T}(d+1, q; GF(q^{d+1}), \sigma)$ is totally isotropic. If f is unitary, we assume that $q = r^2$ is a square. Define a map g from $GF(q^{d+1}) \times GF(q^{d+1})$ to $GF(q)$ by

$$g(x, y) := f((x, 0), (0, y)),$$

If f is symplectic, it is immediate to see that g is $GF(q)$-bilinear. If f is unitary, then f is $GF(q)$-linear in the first variable but $GF(q)$-semilinear in the second variable (that is, $f(x, cy + dz) = c^r f(x, y) + d^r f(x, z)$ for $x, y, z \in GF(q^{d+1})$, $c, d \in GF(q)$)

For each $b \in GF(q^{d+1})^\times$, we denote by g_b the map from $GF(q^{d+1})$ to $GF(q)$ defined by

$$g_b(y) := g(b, y).$$

If f is symplectic, g_b is $GF(q)$-linear, while if f is hermitian, g_b is $GF(q)$-semilinear. However, note that, in either case, the kernel $Ker(g_b)$ is a subspace of $GF(q^{d+1})$ over $GF(q)$ of rank at least d.

As $T[\infty] = \{(x, 0) |\ x \in GF(q^{d+1})\}$ is totally isotropic, we have $f((x, 0), (y, 0)) = 0$ for all $x, y \in GF(q^{d+1})$. As $T[\alpha]$ is totally isotropic and $(\alpha^2, 0) \in T[\alpha] \cap T[\infty]$, we have

$$f((\alpha^2, 0), (x, \alpha^{1-\sigma}x^\sigma + \alpha^{\sigma-1}x)) = 0$$

for all $x \in GF(q^{d+1})$. The left hand side of this equation is

$$f((\alpha^2, 0), (x, 0)) + f((\alpha^2, 0), (0, \alpha^{1-\sigma}x^\sigma + \alpha^{\sigma-1}x)) \quad = \quad g(\alpha^2, \alpha^{1-\sigma}x^\sigma + \alpha^{\sigma-1}x),$$

using the additivity of f for the second variable, the definition of g and the above remark that $f((\alpha^2, 0), (x, 0)) = 0$. Hence we showed that $g(\alpha^2, y) = 0$ for all $y \in Y[\alpha]$, namely the kernel of g_{α^2} contains a hyperplane $Y[\alpha]$ of $GF(q^{d+1})$. Notice that $Ker(g_{\alpha^2})$ is a hyperplane of $GF(q^{d+1})$, for otherwise $0 = g(\alpha^2, y) = f((\alpha^2, 0), (0, y))$ for all $y \in GF(q^{d+1})$ and then $f((\alpha^2, 0), (x, y)) = f((\alpha^2, 0), (x, 0)) + f((\alpha^2, 0), (0, y)) = 0$ for all $x, y \in GF(q^{d+1})$, which contradicts the nondegeneracy of f. Hence we proved

$$Y[\alpha] \quad = \quad Ker(g_{\alpha^2}) \tag{14}$$

for all $\alpha \in GF(q^{d+1})^\times$.

We now divide into cases. Assume first that f is symplectic. Then g_{α^2} is a $GF(q)$-linear map from $GF(q^{d+1})$ onto $GF(q)$. Recall that every nonzero linear form from $GF(q^{d+1})$ to $GF(q)$ is uniquely expressed as T_b for $b \in GF(q^{d+1})^\times$ [3, Theorem 2.24]. It is easily seen that we have $Ker(T_b) = Ker(T_c)$ for $b, c \in GF(q^{d+1})^\times$ if and only if $c = bk$ for some $k \in GF(q)^\times$. With these remarks and Equations (13) and (14), we conclude the following.

> Assume that f is a symplectic form. For each $\alpha \in GF(q^{d+1})^\times$ there exists a unique scalar $\kappa(\alpha)$ of $GF(q)^\times$ such that
>
> $$g_{\alpha^2} = \kappa(\alpha)T_{\alpha^{-(1+\sigma)}}. \tag{15}$$

From $GF(q)$-linearity of g for the first variable, we have

$$\begin{aligned}
\kappa(c\alpha + d\beta)Tr((c\alpha + d\beta)^{-(1+\sigma)}y) &= g((c\alpha + d\beta)^2, y) = g(c^2\alpha^2 + d^2\beta^2, y) \\
&= c^2 g(\alpha^2, y) + d^2 g(\beta^2, y) \\
&= c^2\kappa(\alpha)Tr(\alpha^{-(1+\sigma)}y) + d^2\kappa(\beta)Tr(\beta^{-(1+\sigma)}y) \\
&= Tr((c^2\kappa(\alpha)\alpha^{-(1+\sigma)} + d^2\kappa(\beta)\beta^{-(1+\sigma)})y)
\end{aligned}$$

for every $c, d \in GF(q)$, $\alpha, \beta \in GF(q^{d+1})^\times$ and $y \in GF(q^{d+1})$. Thus for $c, d \in GF(q)$ and $\alpha, \beta \in GF(q^{d+1})^\times$ we have

$$\kappa(c\alpha + d\beta)(c\alpha + d\beta)^{-(1+\sigma)} = c^2\kappa(\alpha)\alpha^{-(1+\sigma)} + d^2\kappa(\beta)\beta^{-(1+\sigma)} \tag{16}$$

Next we show that the map ρ on $GF(q^{d+1})^\times$ defined by

$$\rho(\alpha) := \alpha^{-(1+\sigma)} \tag{17}$$

induces an automorphism of the projective space $PG(GF(q^{d+1}))$ over $GF(q)$. To this end, it suffices to show that every projective line of $PG(GF(q^{d+1}))$ is mapped by ρ to a projective line of $PG(GF(q^{d+1}))$. Take independent vectors α, β in $GF(q^{d+1})$ over $GF(q)$, and let $c\alpha + d\beta$ ($c, d \in GF(q)$) be any nonzero vector in the line spanned by α and β. Then it follows from Equation (16) that

$$\rho(c\alpha + d\beta) = \frac{c^2\kappa(\alpha)}{\kappa(c\alpha + d\beta)}\rho(\alpha) + \frac{d^2\kappa(\beta)}{\kappa(c\alpha + d\beta)}\rho(\beta),$$

whence $\rho(c\alpha + d\beta)$ lies in the projective line spanned by $\rho(\alpha)$ and $\rho(\beta)$. This shows that ρ maps a line to a line, and hence it induces an automorphism of $PG(GF(q^{d+1}))$.

Then it follows from the fundamental theorem of projective geometry that ρ is a composite of a field automorphism θ and a $GF(q)$-linear bijection μ on $GF(q^{d+1})$. Notice that ρ is multiplicative on $GF(q^{d+1})^\times$ by definition (17). As θ is also multiplicative, $\theta^{-1}\rho = \mu$ is multiplicative as well. Hence μ lies in $Gal(GF(q^{d+1})/GF(q))$. Thus $\rho = \theta\mu$ lies in the group $Gal(GF(q^{d+1})/GF(2))$ of field automorphisms. As $q = 2^e$, we have

$$\rho(\alpha) = \alpha^{2^\ell}$$

for all $\alpha \in GF(q^{d+1})$, where ℓ is an integer with $1 \le \ell \le e(d+1) - 1$. From definition of ρ in (17), we have $\alpha^{1+\sigma}\rho(\alpha) = 1$ for all $\alpha \in GF(q^{d+1})^\times$. Thus

$$1 + q^m + 2^\ell \equiv 0 \pmod{q^{d+1} - 1},$$

where $\alpha^\sigma = \alpha^{q^m}$ for all $\alpha \in GF(q^{d+1})$ and m is an integer with $1 \leq m \leq d$ coprime with $d+1$. In particular, we have $q^{d+1} - 1 \leq 1 + 2^\ell + q^m \leq 1 + (q^{d+1}/2) + q^d$, and then $(q/2 - 1)q^d \leq 2$. This happens only when $q = 2$. In this case, at least one of m and l is less than or equal to $d-1$, for otherwise $2^{d+1} - 1$ would divide $1 + 2^\ell + q^m = 1 + 2^d + 2^d = 1 + 2^{d+1}$. Then $2^{d+1} - 1 \leq 1 + 2^\ell + q^m \leq 1 + 2^{d-1} + 2^d$, whence $2^{d-1} \leq 2$. This is possible only when $d = 2$.

Thus $(q, d) = (2, 2)$ is the only remaining case. In this case, the ambient space of $\mathcal{T}(3, 2; GF(2^3), \sigma)$ is $PG(4, 2)$ or $PG(5, 2)$. In the first case, every 2-dimensional subspace is not totally isotropic. Thus the latter case should happen. There are exactly two isomorphism classes of 2-dimensional dual hyperovals in $PG(5, 2)$ [1, Theorem 2,3]. Every dimensional dual hyperoval in one class satisfies Condition (T); namely, $\dim(X \cap \langle Y, Z\rangle) = 1$ for all mutually distinct triple of members X, Y, Z, while the other class does not. By Lemma 1, any d-dimensional dual hyperoval in $PG(2d + 1, q)$ of polar type satisfies $\dim(X \cap \langle Y, Z\rangle) = d - 1$ for all triples X, Y, Z of mutually distinct members. Now Yoshiara's dual hyperoval $\mathcal{S}^3_{1,1}$ is a 2-dimensional dual hyperoval in $PG(5, 2)$ of symplectic polar type, by Proposition 6. As $\mathcal{T}(3, 2; GF(2^3), \sigma)$ is of polar type by assumption, we conclude that both $\mathcal{S}^3_{1,1}$ and $\mathcal{T}(3, 2; GF(2^3), \sigma)$ satisfy Property (T), and hence they are isomorphic. However, the automorphism group of $\mathcal{S}^3_{1,1}$ is (doubly) transitive on the members [7, Proposition 7], while the special member $T[\infty]$ is fixed by all automorphisms of $\mathcal{T}(3, 2; GF(2^3), \sigma)$ [6]. This contradiction shows that $\mathcal{T}(3, 2; GF(2^3), \sigma)$ is not of polar type.

Hence there is no Taniguchi's dual hyperoval $\mathcal{T}(d + 1, q; GF(q^{d+1}), \sigma)$ of symplectic polar type.

Assume that f is unitary and $q = r^2$. Then g_{α^2} is a $GF(q)$-semilinear map from $GF(q^{d+1})$ onto $GF(q)$. It is easy to verify that every nonzero $GF(q)$-semilinear from from $GF(q^{d+1})$ to $GF(q)$ is uniquely expressed as $\tilde{T}_b$ for $b \in GF(q^{d+1})^\times$, where

$$\tilde{T}_b(y) := Tr(by^r), \quad y \in GF(q^{d+1})$$

with $Tr = Tr_{GF(q^{d+1})/GF(q)}$. One can also easily verify that $Ker(\tilde{T}_b) = Ker(\tilde{T}_c)$ for $b, c \in GF(q^{d+1})^\times$ if and only if $c = kb$ for some $k \in GF(q)^\times$. Notice also that instead Equation (13) we have

$$Y[\alpha] \;=\; Ker(\tilde{T}_{\alpha^{-r(1+\sigma)}}).$$

With these remarks and Equation (14), we have the following.

> Assume that f is a unitary form. For each $\alpha \in GF(q^{d+1})^\times$, there exists a unique scalar $\kappa(\alpha)$ of $GF(q)^\times$ such that
>
> $$g_{\alpha^2} \;=\; \kappa(\alpha)\tilde{T}_{\alpha^{-r(1+\sigma)}}.$$

The remaining arguments are parallel to the symplectic case with α replaced by α^r, but one can obtain a final contradiction much earlier from the condition

$$1 + r^{2m} + r^{2^l} \equiv 0 \pmod{r^{2(d+1)} - 1}.$$

■

References

[1] A. Del Fra, On d-dimensional dual hyperovals, *Geom. Dedicata*, **79** (2000), 157–178.

[2] B. Huppert and N. Blackburn, *Finite Groups II*, Springer, 1982.

[3] R. Lidl and H. Niederreiter, *Finite Fields*, Second Ed., Cambridge Univ. Press, 1997.

[4] N. Nakagawa and S. Yoshiara, 2-dimensional dual hyperovals of polar type, in preparation.

[5] H. Taniguchi, A family of dual hyperovals over $GF(q)$ with q even, to appear in *Europ. J. Combin.*

[6] H. Taniguchi, A note on the automorphism of $\mathcal{T}_\sigma(V)$, preprint, 2003.

[7] S. Yoshiara, A family of d-dimensional dual hyperovals in $PG(2d+1,2)$, *Europ. J. Combin.* **20** (1999), 589–603.

Department of Mathematics
Tokyo Woman's Christian University
2-6-1 Zenpukuji, Suginami-ku,
Tokyo, 167-8585, JAPAN
email : yoshiara@ikoma.cc.osaka-kyoiku.ac.jp