Innovations in Incidence Geometry
Volume 8 (2008), Pages 137–145
ISSN 1781-6475

On d-dimensional dual hyperovals in $\mathsf{PG}(2d, 2)$

Hiroaki Taniguchi

Abstract

We show that d-dimensional dual hyperovals in $\mathsf{PG}(2d, 2)$ constructed from a regular nearfield of characteristic 2 are not isomorphic to Yoshiara's d-dimensional dual hyperovals in $\mathsf{PG}(2d, 2)$ constructed in [5]. Thus we show that, in Cooperstein-Thas's family [1], there exist non-isomorphic dual hyperovals.

Keywords: dual hyperoval

MSC 2000: 05-xx

1 Introduction

Let $\mathsf{GF}(q)$ be a finite field with q elements. Let d, m be integers with $d \geq 2$ and $m > d$. Let $\mathsf{PG}(m, 2)$ be an m-dimensional projective space over the binary field $\mathsf{GF}(2)$.

Definition 1.1. A family S of d-dimensional subspaces of $\mathsf{PG}(m, 2)$ is called a d-dimensional dual hyperoval in $\mathsf{PG}(m, 2)$ if it satisfies the following conditions:

(1) any two distinct members of S intersect in a projective point,

(2) no three mutually distinct members of S have a common projective point,

(3) all members of S generate $\mathsf{PG}(m, 2)$, and

(4) there are exactly 2^{d+1} members of S.

In Example 2.5 and Theorem 6.1 of [1] (see also Proposition 3.1 of [2]), B. N. Cooperstein and J. A. Thas showed that each d-dimensional dual hyperoval in $\mathsf{PG}(2d, 2)$ is obtained as a dual of a partition of $\mathsf{PG}(2d, 2) \setminus \mathsf{PG}(d, 2)$.

Theorem 1.2 ([1, Example 2.5 and Theorem 6.1]). *Let* $\mathsf{PG}(d,2)$ *be a* d*-dimensional subspace of* $\mathsf{PG}(2d,2)$. *Consider a partition of* $\mathsf{PG}(2d,2) \setminus \mathsf{PG}(d,2)$ *into* 2^{d+1} $(d-1)$*-dimensional subspaces. Then the set* S *of the dual subspaces of these* $(d-1)$*-dimensional subspaces in* $\mathsf{PG}(2d,2)$ *is a* d*-dimensional dual hyperoval in* $\mathsf{PG}(2d,2)$. *The converse also holds.*

This family is called as Cooperstein-Thas's family in [2]. In [5] (see also [6]), Yoshiara constructed a family of d-dimensional dual hyperovals in $\mathsf{PG}(2d,2)$ in a different way, as follows.

Theorem 1.3 ([5, Proposition 3]). *Let* σ *be a generator of the automorphism group of* $\mathsf{GF}(2^{d+1})$ *over* $\mathsf{GF}(2)$. *Inside* $\mathsf{GF}(2^{d+1}) \oplus \mathsf{GF}(2^{d+1})$, *let us define* $X_Y(t)$ *for* $t \in \mathsf{GF}(2^{d+1})$ *as*

$$X_Y(t) := \left\{(x, x^{\sigma}t + xt^{\sigma^{-1}}) \mid x \in \mathsf{GF}(2^{d+1}) \setminus \{0\}\right\}.$$

Then $S_Y := \left\{X_Y(t) \mid t \in \mathsf{GF}(2^{d+1})\right\}$ *is a* d*-dimensional dual hyperoval in* $\mathsf{PG}(2d,2)$.

Then, it is quite natural to ask whether all the members of the Cooperstein-Thas's family are the Yoshiara's dual hyperovals or not. In the case $d = 2$, the answer is affirmative ([2, Theorem 1]). In this paper, we will give a negative answer to this question in general.

Definition 1.4 ([3]). Let Π be a vector space over $\mathsf{GF}(q)$. A spread T of Π is a collection of at least two subspaces of Π which satisfies the following conditions:

(1) two distinct elements of T are isomorphic subspaces,

(2) every point except $\{0\}$ of Π is on exactly one subspace in T, and

(3) for any U_1, $U_2 \in T$ with $U_1 \neq U_2$, Π is a direct (vector space) sum of U_1 and U_2.

It is known that the vector space Π has even dimension $2m$ with $m > 0$. Moreover, the cardinality of the spread $|T| = q^m + 1$. (See [3] or [4].)

From spreads of the vector space $V \oplus V$, where V is a $(d+1)$-dimensional vector space over $\mathsf{GF}(2)$, we are able to construct d-dimensional dual hyperovals as follows:

Theorem 1.5. *Let* $V := \mathsf{GF}(2)^{d+1}$ *be a* $(d+1)$*-dimensional vector space over* $\mathsf{GF}(2)$, *and* $T := \{K_0, K_1, \ldots, K_{2^{d+1}}\}$ *a spread of* $V \oplus V$. *Let* v *be a non-zero element of* $V \oplus V$. *We may assume that* v *is contained in* K_0. *Let*

$$\pi\colon V \oplus V \ni x \mapsto \bar{x} \in \overline{V \oplus V} := (V \oplus V)/\langle v \rangle$$

be a $\mathsf{GF}(2)$*-linear mapping with kernel* $\{0,v\}$ *(which we denote by* $\langle v\rangle$*), and image* $(V\oplus V)/\langle v\rangle$*. We regard* $\mathsf{PG}\big((V\oplus V)/\langle v\rangle\big)=\mathsf{PG}(2d,2)$*. Then,*

$$S:=\big\{\pi(K_1)\setminus\{0\},\pi(K_2)\setminus\{0\},\dots,\pi(K_{2^{d+1}})\setminus\{0\}\big\}$$

is a d*-dimensional dual hyperoval in* $\mathsf{PG}(2d,2)$*.*

We will give the proof of this theorem in the following section. We refer the relations among spreads, quasifields and translation affine planes to Kallaher [3] or Lüneburg [4].

Example 1. *We regard* $V:=\mathsf{GF}(2^{d+1})$ *as a* $(d+1)$*-dimensional vector space over* $\mathsf{GF}(2)$*. Let* σ *be a generator of the Galois group* $\mathrm{Gal}(\mathsf{GF}(2^{d+1})/\mathsf{GF}(2))$*. Let*

$$\pi'\colon \mathsf{GF}(2^{d+1})\oplus\mathsf{GF}(2^{d+1})\ni(x,y)\mapsto(x,y^\sigma+y)\in\mathsf{GF}(2^{d+1})\oplus\mathsf{GF}(2^{d+1})\,.$$

Then it is easy to see that the kernel of π' *is* $\{(0,0),(0,1)\}$*, and the image of* π' *is* $W:=\{(x,y)\mid\mathrm{Tr}(y)=0\}$*, which is a* $(2d+1)$*-dimensional vector space over* $\mathsf{GF}(2)$*, where* Tr *is a trace function from* $\mathsf{GF}(2^{d+1})$ *to* $\mathsf{GF}(2)$*.*

In $V\oplus V$*, let*

$$K_\infty:=\big\{(0,x)\mid x\in\mathsf{GF}(2^{d+1})\big\}\text{ and}$$
$$K_a:=\big\{(x,xa)\mid x\in\mathsf{GF}(2^{d+1})\big\}\text{ for }a\in\mathsf{GF}\big(2^{d+1}\big)\,.$$

Then, $T:=\{K_\infty\}\cup\{K_a\mid a\in\mathsf{GF}(2^{d+1})\}$ *is a spread of* $V\oplus V$*. (It is well known that the translation affine plane constructed from this spread is a Desarguesian affine plane.) Let* $S':=\big\{\pi'(K_a)\setminus\{0\}\mid a\in\mathsf{GF}(2^{d+1})\big\}$*. Then, by Theorem 1.5,* S' *is a* d*-dimensional dual hyperoval in* $\mathsf{PG}(2d,2)=\mathsf{PG}(W)$*.*

Proposition 1.6. *The dual hyperoval* S' *above is isomorphic to Yoshiara's dual hyperoval* S_Y*.*

Proof. We have $\pi'(K_a)\setminus\{0\}=\big\{(x,(ax)^\sigma+ax)\mid x\in\mathsf{GF}(2^{d+1})\setminus\{0\}\big\}$. If we put $a^\sigma:=t$, then $a=t^{\sigma^{-1}}$, hence we have

$$\big\{(x,(ax)^\sigma+ax)\mid x\in\mathsf{GF}(2^{d+1})\setminus\{0\}\big\}$$
$$=\big\{(x,x^\sigma t+xt^{\sigma^{-1}})\mid x\in\mathsf{GF}(2^{d+1})\setminus\{0\}\big\}\,.$$

Therefore, we have $\pi'(K_a)\setminus\{0\}=X_Y(t)$, where $X_Y(t)$ is as in Theorem 1.3. Hence, we have $\big\{\pi'(K_a)\setminus\{0\}\mid a\in\mathsf{GF}(2^{d+1})\big\}=\big\{X_Y(t)\mid t\in\mathsf{GF}(2^{d+1})\big\}$ and consequently, we have $S'=S_Y$. □

Now, we will use quasifields Q to construct spreads of $Q\oplus Q$.

Definition 1.7 ([3, 4]). An algebraic structure $(Q;+,\circ)$ is called a quasifield if it satisfies the following conditions:

(i) Q is an abelian group under $+$ with identity 0 ;

(ii) for $a, c \in Q$ with $a \neq 0$, there exists exactly one $x \in Q$ such that $a \circ x = c$;

(iii) for $a, b, c \in Q$ with $a \neq b$, there exists exactly one $x \in Q$ such that $x \circ a - x \circ b = c$;

(iv) for all $a \in Q$, $a \circ 0 = 0 \circ a = 0$;

(v) there exists an element $1 \in Q \setminus \{0\}$ such that $1 \circ a = a \circ 1 = a$ for all $a \in Q$;

(vi) for all $a, b, c \in Q$, $(a+b) \circ c = a \circ c + b \circ c$.

A nearfield is a quasifield N in which the multiplication $\circ$ is associative; that is, in which $(N \setminus \{0\}, \circ)$ is a group. A semifield is a quasifield S in which the left distributive law

$$a \circ (b+c) = a \circ b + a \circ c$$

holds for all $a, b, c \in S$.

In $Q \oplus Q$, we define $K_\infty := \{(0, y) \mid y \in Q\}$ and $K_a := \{(x, x \circ a) \mid x \in Q\}$ for $a \in Q$. Then it is known that $\{K_\infty\} \cup \{K_a \mid a \in Q\}$ is a spread of $Q \oplus Q$.

Example 2 ([3, 2.1 and 2.3]). *Consider the field* $\mathsf{GF}(q^n)$ *where* $n \geq 1$ *and* $q = p^s$ *with* p *a prime and* $s \geq 1$. *Let* $\lambda : \mathsf{GF}(q^n) \to I_n = \{0, 1, \ldots, n-1\}$ *be a mapping satisfying:* (i) $\lambda(0) = \lambda(1) = 0$, *and* (ii) *given* $a, b \in \mathsf{GF}(q^n) \setminus \{0\}$ *there exists* $x \neq 0$ *with*

$$x^{q^{\lambda(a)}} a = x^{q^{\lambda(b)}} b$$

if and only if $a = b$. *We define* $x \circ y := x^{q^{\lambda(y)}} y$. *Then* $\big(\mathsf{GF}(q^n), +, \circ\big)$ *is a quasifield called a generalized André system.*

Consider also the field $\mathsf{GF}(q^n)$ *and* $q = p^s$ *with* p *a prime and* $s \geq 1$, *and assume every prime divisor of* n *divides* $q-1$. *Also assume* $n \not\equiv 0 \pmod 4$ *if* $q \equiv 3 \pmod 4$. *Choosing a primitive element* ω *of* $\mathsf{GF}(q^n)$, *define* λ: $\mathsf{GF}(q^n) \setminus \{0\} \to I_n = \{0, 1, \ldots, n-1\}$ *by*

$$(q^{\lambda(a)} - 1)(q-1)^{-1} \equiv i \pmod n, \text{ where } a = w^i \in \mathsf{GF}(q^n)\,.$$

With $\lambda(0) = 0$, *the mapping* λ *satisfies the conditions* (i) *and* (ii) *for a generalized André system. This system, denoted by* $N(q, n)$, *is a nearfield and is called a regular nearfield (or a Dickson nearfield).*

Proposition 1.8 ([4, Theorem 7.3 and Theorem 7.4]). *The group consisting of non-zero elements of the regular nearfield* $(N(q, n) \setminus \{0\}, \circ)$ *in Example 2 is a non-abelian metacyclic group. Moreover, there exist* $\phi(n)/m$ *non-isomorphic* $N(q, n)$*'s, where* ϕ *is the Euler function and* m *is the order of* p *mod* n.

Moreover, it is known that, in GF(2^{d+1}), using a natural addition of the field GF(2^{d+1}), we are able to define more multiplications $\circ$ so that we have some semifields, such as Knuth semifields, Kantor semifields or Albert semifields, and so on. (See [3].)

Definition 1.9 (Dual hyperoval S_K). Let $\bigl(\mathrm{GF}(2^{d+1}), +, \circ\bigr)$ be a quasifield, and regard $V := \mathrm{GF}(2^{d+1})$ as a vector space over GF(2). In $V \oplus V$, we define

$$K_\infty := \bigl\{(0, x) \mid x \in \mathrm{GF}(2^{d+1})\bigr\} \text{ and}$$
$$K_a := \bigl\{(x, x \circ a) \mid x \in \mathrm{GF}(2^{d+1})\bigr\} \text{ for } a \in \mathrm{GF}(2^{d+1}).$$

Then, $T := \{K_\infty\} \cup \bigl\{K_a \mid a \in \mathrm{GF}(2^{d+1})\bigr\}$ is a spread of $V \oplus V$. Let σ be a generator of the Galois group $\mathrm{Gal}(\mathrm{GF}(2^{d+1})/\mathrm{GF}(2))$. Let π' be a GF(2)-linear mapping defined by

$$\pi' \colon \mathrm{GF}(2^{d+1}) \oplus \mathrm{GF}(2^{d+1}) \ni (x, y) \mapsto (x, y^\sigma + y) \in \mathrm{GF}(2^{d+1}) \oplus \mathrm{GF}(2^{d+1}).$$

Then, as in Example 1, the image of π' is $W := \{(x, y) \mid \mathrm{Tr}(y) = 0\}$, which is a $(2d + 1)$-dimensional vector space over GF(2). We note that the kernel of π', $\{(0, 0), (0, 1)\}$, is contained in K_∞. We define $X_K(a) := \pi'(K_a) \setminus \{0\}$. Then, by Theorem 1.5, $S_K := \bigl\{X_K(a) \mid a \in \mathrm{GF}(2^{d+1})\bigr\}$ is a d-dimensional dual hyperoval in PG$(2d, 2)$ = PG(W), where

$$X_K(a) = \bigl\{(x, (x \circ a)^\sigma + x \circ a) \mid x \in \mathrm{GF}(2^{d+1}) \setminus \{0\}\bigr\}.$$

Then we have the following proposition.

Proposition 1.10. *If the algebraic system $\bigl(\mathrm{GF}(2^{d+1}), +, \circ\bigr)$ is a regular nearfield, then the automorphism group G_K of the dual hyperoval S_K contains the subgroup $N := \bigl\{n_b \mid b \in \mathrm{GF}(2^{d+1}) \setminus \{0\}\bigr\}$ with $n_b(X_K(t)) = X_K(b \circ t)$ defined by*

$$n_b((x, y)) := (x \circ b', y),$$

where b' is an element which satisfies that $b' \circ b = 1$. Moreover, N is isomorphic to the group $(\mathrm{GF}(2^{d+1}) \setminus \{0\}, \circ)$, and so, by Proposition 1.8, N is a non-abelian metacyclic group with the cardinality $|N| = 2^{d+1} - 1$. If the algebraic system $(\mathrm{GF}(2^{d+1}), +, \circ)$ is a semifield, then the automorphism group G_K of the dual hyperoval S_K contains the subgroup $T := \bigl\{t_a \mid a \in \mathrm{GF}(2^{d+1})\bigr\}$ with $t_a(X_K(t)) = X_K(t + a)$, defined by

$$t_a((x, y)) := \bigl(x, y + (x \circ a)^\sigma + x \circ a\bigr),$$

and T is isomorphic to GF(2^{d+1}) as an additive group.

Proof. Since the multiplication $\circ$ is associative in the regular nearfield, we have

$$n_b(X_K(t)) = \big\{(x \circ b', ((x \circ b') \circ (b \circ t))^\sigma + (x \circ b') \circ (b \circ t))\big\} = X_K(b \circ t)$$

for $b \in \mathsf{GF}(2^{d+1}) \setminus \{0\}$. Hence

$$n_{b_2}\big(n_{b_1}(X_K(t))\big) = n_{b_2}(X_K(b_1 \circ t)) = X_K((b_2 \circ b_1) \circ t) = n_{b_2 \circ b_1}(X_K(t))$$

for $b_1, b_2 \in \mathsf{GF}(2^{d+1}) \setminus \{0\}$. Therefore $N := \big\{n_b \mid b \in \mathsf{GF}(2^{d+1}) \setminus \{0\}\big\}$ is isomorphic to the group $\big(\mathsf{GF}(2^{d+1}) \setminus \{0\}, \circ\big)$. Since the multiplication $\circ$ has left distributive law in the semifield, we also have

$$t_a(X_K(t)) = \big\{(x, (x \circ t)^\sigma + x \circ t + (x \circ a)^\sigma + x \circ a)\big\} = X_K(t + a)\,,$$

hence we have $T \cong \mathsf{GF}(2^{d+1})$ as an additive group. $\square$

By Theorem 1.2 (see also [2, 1.2. Examples (a)]), the complement of the points on the members of the dual hyperoval in $\mathsf{PG}(2d, 2)$, that is,

$$\mathsf{PG}(2d, 2) \setminus \bigcup\big\{\text{the points on the members of the dual hyperoval}\big\}$$

is a $(d-1)$-dimensional subspace. Hence we have the following lemma.

Lemma 1.11. *Let* $U := \big\{(0, y) \mid y \in \mathsf{GF}(2^{d+1}), \mathrm{Tr}(y) = 0\big\}$. *Note that* $U \subset W := \big\{(x, y) \mid x, y \in \mathsf{GF}(2^{d+1}), \mathrm{Tr}(y) = 0\big\}$. *Then, in* $\mathsf{PG}(2d, 2) = \mathsf{PG}(W)$*, the* $(d-1)$*-dimensional subspace* $\mathsf{PG}(U)$ *is the complement of the set* $\bigcup X_K(a)$ *of the points which are on some members of the dual hyperoval* S_K *in Definition 1.9, that is,*

$$\mathsf{PG}(U) = \mathsf{PG}(W) \setminus \textstyle\bigcup_{a \in \mathsf{GF}(2^{d+1})} X_K(a)\,.$$

In section 3, we will prove the following theorem, hence we give a negative answer to the previous question.

Theorem 1.12. *Let the algebraic system* $\big(\mathsf{GF}(2^{d+1}), +, \circ\big)$ *in Example 2 be a regular nearfield. Then, a* d*-dimensional dual hyperoval* S_K *in* $\mathsf{PG}(2d, 2)$ *in Definition 1.9 is not isomorphic to the Yoshiara's dual hyperoval* S_Y.

2 Proof of Theorem 1.5

Since $K_i \not\ni v$ for $1 \le i \le 2^{d+1}$, $\pi(K_i) \setminus \{0\}$ is a d-dimensional subspace in $\mathsf{PG}(2d, 2) = \mathsf{PG}((V \oplus V)/\langle v\rangle)$ for $1 \le i \le 2^{d+1}$. Let $\pi(K_i) \setminus \{0\}$ and $\pi(K_j) \setminus \{0\}$ have a common point $\pi(x_i) = \pi(x_j)$ for $x_i \in K_i \setminus \{0\}$ and $x_j \in K_j \setminus \{0\}$ with $1 \le i < j \le 2^{d+1}$. Then, since $\pi(x_i + x_j) = 0$, we have $x_i + x_j = v$. However, since $V \oplus V$ is a direct sum of K_i and K_j by (3) of Definition 1.4, there exist unique $x_i \in K_i \setminus \{0\}$ and unique $x_j \in K_j \setminus \{0\}$ which satisfies that $x_i + x_j = v$. Thus, we have proved that $\pi(K_i) \setminus \{0\}$ and $\pi(K_j) \setminus \{0\}$ have only one common point. Assume that $\pi(K_s) \setminus \{0\}$, $\pi(K_t) \setminus \{0\}$ and $\pi(K_u) \setminus \{0\}$ have a common point $\pi(x_s) = \pi(x_t) = \pi(x_u)$ for $x_s \in K_s \setminus \{0\}$, $x_t \in K_t \setminus \{0\}$ and $x_t \in K_t \setminus \{0\}$ with $1 \leq s < t < u \leq 2^{d+1}$. Then, since $\pi(x_s + x_t) = 0$, we have $x_s + x_t = v$. We also have $x_s + x_u = v$. However, we have $x_t = x_u$ from these equations, which contradicts (2) of Definition 1.4. Hence $\pi(K_s) \setminus \{0\}$, $\pi(K_t) \setminus \{0\}$ and $\pi(K_u) \setminus \{0\}$ with $1 \leq s < t < u \leq 2^{d+1}$ have no common point. Since the cardinality

$$\left|S\right| = \left|\{\pi(K_1) \setminus \{0\}, \pi(K_2) \setminus \{0\}, \dots, \pi(K_{2^{d+1}}) \setminus \{0\}\}\right| = 2^{d+1},$$

and since it is trivial that all members of S generate PG$(2d,2)$, we conclude that S is a d-dimensional dual hyperoval in PG$(2d,2) =$ PG$\big((V \oplus V)/\langle v \rangle\big)$. □

3 Proof of Theorem 1.12

We consider the dual hyperovals inside the projective space

$$\mathsf{PG}(2d,2) = \left\{(x,y) \mid (x,y) \in \mathsf{GF}(2^{d+1}) \oplus \mathsf{GF}(2^{d+1}) \setminus \{(0,0)\}, \mathrm{Tr}(y) = 0\right\}.$$

We recall that an automorphism of the dual hyperoval S in PG$(2d,2)$ is a linear transformation which permute the members of S. We also define an isomorphism of the dual hyperovals S to S' as a linear transformation of PG$(2d,2)$ which sends each member of S to that of S'.

Let $d+1 = sn$ with $s \geq 1$, and assume every prime divisor of n divides $2^s - 1$. (For example, $(s,n) = (4,3)$, etc.) Then, by Example 2, we are able to define a multiplication $\circ$ of GF(2^{d+1}) such that $\big(\mathsf{GF}(2^{d+1}), +, \circ\big)$ is a regular near field. Hence, by Definition 1.9, we have a dual hyperoval

$$S_K = \left\{X_K(t) \mid t \in \mathsf{GF}(2^{d+1})\right\},$$

where

$$X_K(t) := \left\{(x, (x \circ t)^\sigma + x \circ t) \mid x \in \mathsf{GF}(2^{d+1}) \setminus \{0\}\right\}.$$

By Proposition 1.10, the automorphism group G_K of the dual hyperoval S_K contains a subgroup $N := \left\{n_b \mid b \in \mathsf{GF}(2^{d+1}) \setminus \{0\}\right\}$ with $n_b(X_K(t)) = X_K(b \circ t)$ defined by

$$n_b((x,y)) := (x \circ b', y),$$

where $b' \circ b = 1$. Let $G_K(0)$ be a subgroup of G_K which fixes $X_K(0) := \{(x,0) \mid x \in \mathsf{GF}(2^{d+1})\}$. Then it is easy to see that $N \subset G_K(0)$. By Proposition 1.8, N is a non-abelian metacyclic group with the cardinality $|N| = 2^{d+1} - 1$.

We recall that the automorphism group G_Y of Yoshiara's dual hyperoval S_Y is generated by the groups T, M and F, where $T = \{t_a \mid a \in \mathsf{GF}(2^{d+1})\}$ with $t_a(X_Y(t)) = X_Y(t+a)$ defined by

$$t_a\colon (x,y) \mapsto (x, x^\sigma a + x a^{\sigma^{-1}} + y)\,,$$

$M = \{m_b \mid b \in \mathsf{GF}(2^{d+1}) \setminus \{0\}\}$ with $m_b(X_Y(t)) = X_Y(bt)$ defined by

$$m_b\colon (x,y) \mapsto (xb^{-1}, y)\,,$$

and $F = \{f_\tau \mid \tau \in \mathrm{Gal}(\mathsf{GF}(2^{d+1})/\mathsf{GF}(2))\}$ with $f_\tau(X_Y(t)) = X_Y(t^\tau)$ defined by

$$f_\tau\colon (x,y) \mapsto (x^\tau, y^\tau)\,.$$

We also have $G_Y = T : (M : F)$. Hence G_Y is doubly transitive on the members of S_Y. (See [5, Proposition 7].) We note that M is a cyclic group with cardinality $|M| = 2^{d+1} - 1$.

Let $G_Y(0)$ be a subgroup of G_Y which fixes $X_Y(0) := \{(x,0) \mid x \in \mathsf{GF}(2^{d+1})\}$. Then, we have $G_Y(0) = M : F$ from the expressions of T, M and F and the fact that $G_Y = T : (M : F)$.

Lemma 3.1. *Let g be an element of $G_Y(0) = M : F$ with the action $g\colon (x,y) \mapsto (g_1(x,y), g_2(x,y))$, where g_1 and g_2 are $\mathsf{GF}(2)$-linear mapping. If $g_2(x,y) = y$ for any $(x,y) \in \mathsf{GF}(2^{d+1}) \oplus \mathsf{GF}(2^{d+1})$ with $\mathrm{Tr}(y) = 0$, then we have $g \in M$.*

Proof. Let $g = m_b f_\tau \in G_Y(0) = M : F$, then $g(x,y) = \big(x^\tau (b^{-1})^\tau, y^\tau\big)$ by definition. Assume that $g_2(x,y) = y^\tau = y$ for any $y \in \mathsf{GF}(2^{d+1})$ with $\mathrm{Tr}(y) = 0$. Then, since the subset $\{y \in \mathsf{GF}(2^{d+1}) \mid \mathrm{Tr}(y) = 0\}$ is not contained in any proper subfield of $\mathsf{GF}(2^{d+1})$, we have $\tau = \mathrm{id} \in \mathrm{Gal}\big(\mathsf{GF}(2^{d+1})/\mathsf{GF}(2)\big)$. Hence we have $g \in M$. $\square$

We assume to the contrary that there exists an isomorphism i from S_K to S_Y. Since G_Y is doubly transitive on the members of S_Y, we may assume that $i(X_K(0)) = X_Y(0)$, that is, i maps $\{(x,0) \mid x \in \mathsf{GF}(2^{d+1})\}$ onto itself. Hence, we may assume that i maps $G_K(0)$ to $G_Y(0)$. On the other hand, since i is an isomorphism from $S_K = \{X_K(t) \mid t \in \mathsf{GF}(2^{d+1})\}$ to $S_Y = \{X_Y(t) \mid t \in \mathsf{GF}(2^{d+1})\}$, we have

$$i\Big(\textstyle\bigcup_{t \in \mathsf{GF}(2^{d+1})} X_K(t)\Big) = \textstyle\bigcup_{t \in \mathsf{GF}(2^{d+1})} X_Y(t)\,.$$

Hence, by Lemma 1.11, we have

$$\begin{aligned} i(U) = i\Big(&\mathsf{PG}(2d,2) \setminus \textstyle\bigcup_{t \in \mathsf{GF}(2^{d+1})} X_K(t)\Big) \\ &= \mathsf{PG}(2d,2) \setminus \textstyle\bigcup_{t \in \mathsf{GF}(2^{d+1})} X_Y(t) = U\,, \end{aligned}$$

which means that i maps $\{(0, y) \mid y \in \mathsf{GF}(2^{d+1}), \mathrm{Tr}(y) = 0\}$ onto itself. Therefore, there exist $\mathsf{GF}(2)$-linear mapping f and g such that the isomorphism i is expressed as follows:

$$i((x, y)) = (f(x), g(y))\,. \tag{1}$$

Now, we have $i(N) = \{i(n_b) \mid b \in \mathsf{GF}(2^{d+1}) \setminus \{0\}\} \cong N$ as a subgroup of $G_Y(0) = M : F$ with the action $i(n_b)\big(X_Y(t)\big) = i\Big(n_b\big(i^{-1}(X_Y(t))\big)\Big)$ for $X_Y(t) \in S_Y$. Then, by (1), the action of $i(n_b)$ is

$$i(n_b) \colon (x, y) \mapsto \Big(f\big(f^{-1}(x) \circ b'\big), y\Big).$$

Hence, by Lemma 3.1, $i(N)$ is a subgroup of $M \subset G_Y(0)$. However, the cardinality $|i(N)| = |M| = 2^{d+1} - 1$. Moreover, N is a non-abelian metacyclic group and M is a cyclic group. This is impossible. Hence, we have a contradiction. Therefore, we finally have that the dual hyperoval S_K is not isomorphic to the Yoshiara's dual hyperoval S_Y. □

Acknowledgment. This work was supported by grant in aid for scientific research of Japan, No. 17540054.

References

[1] **B. N. Cooperstein** and **J. A. Thas**, On Generalized k-Arcs in $\mathsf{PG}(2n, q)$, *Ann. Comb.* **5** (2001), 141–152.

[2] **A. Del Fra**, On d-dimensional dual hyperovals, *Geom. Dedicata* **26** (2000), 157–178.

[3] **M. Kallaher**, Translation Planes, **in** *Handbook of Incidence Geometry*, Elsevier Science B. V., 1995, 137–192.

[4] **H. Lüneburg**, *Translation Planes*, Springer-Verlag, 1980.

[5] **S. Yoshiara**, A family of d-dimensional dual hyperovals in $\mathsf{PG}(2d + 1, 2)$, *European J. Combin.* **20** (1999), no. 6, 589–603.

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

Hiroaki Taniguchi

Takuma National College of Technology, 551 takuma, kagawa, 769-1192, Japan

e-mail: taniguchi@dg.takuma-ct.ac.jp