数理解析研究所講究録
第 1564 巻 2007 年 27-31

On some d-dual hyperovals in $PG(d(d+3)/2,2)$

詫間電波高専　谷口 浩朗 (Hiroaki Taniguchi)
Takuma National College of Technology

1 Introduction

Let d, m be integers with $d \geq 2$ and $m > d$. Let $PG(m,2)$ be an n-dimensional projective space over the binary field $GF(2)$.

Definition 1. A family S of d-dimensional subspaces of $PG(m,2)$ is called a d-dimensional dual hyperoval in $PG(m,2)$ if it satisfies the following conditions;

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

(2) any three mutually distinct members of S intersect in the empty projective set,

(3) all members of S generate $PG(m,2)$, and

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

Known dual hyperovals in $PG(d(d+3)/2,2)$ are Huybrechts' dual hyperovals ([3]), Veronesean dual hyperovals ([4]), and Characteristic dual hyperovals ([2]). Huybrechts' dual hyperovals and Characteristic dual hyperovals satisfy the Property (T): for any distinct members X, Y and Z of S, the intersection $\langle X,Y\rangle \cap Z$ is a line, where $\langle X,Y\rangle$ is the projective subspace spanned by X and Y. On the other hand, Veronesean dual hyperovals do not satisfy Property (T). In this note, we show the other construction of d-dimensional dual hyperovals in $PG(d(d+3)/2,2)$ based on Veronesean dual hyperovals in section 2, which will appear in [1]. These dual hyperovals are not isomorphic to any Veronesean dual hyperoval, and that they do not satisfy the property (T). Hence, we have a new family of dual hyperovals in $PG(d(d+3)/2,2)$. In section 3, we study the automorphism group of S.

2 A construction

Let $n \geq d+1$ and σ a generator of $Gal(GF(2^n)/GF(2))$. Let H be a $d+1$-dimensional $GF(2)$-vector subspace of $GF(2^n)$. We may assume that H has a basis $\{e_0, e_1, \ldots, e_d\}$ such that $\{e_i e_j | 0 \leq i \leq j \leq d\}$ are linearly independent over $GF(2)$. Let us denote by $\overline{H}$ the vector space generated by $\{(e_i e_j, e_i^\sigma e_j + e_i e_j^\sigma) | 0 \leq i \leq j \leq d\} \subset GF(2^d) \times GF(2^d)$. For a non-zero vector u of H, its support, denoted as $Supp(u)$, is the subset M of $\{e_0, e_1, e_2, \ldots, e_d\}$ for which $u = \sum_{e_i \in M} e_i$. Let $V \subset H$ be a vector subspace generated by $\{e_1, e_2, \ldots, e_d\}$ over $GF(2)$, and let $H \ni s = \sum_{i=0}^d \alpha_i e_i \mapsto \bar{s} = \sum_{i=1}^d \alpha_i e_i \in V$ be a natural projection, where $\alpha_i \in GF(2)$ for $0 \leq i \leq d$.

Definition 2. Let $x_{s,t} \in GF(2)$ for $s, t \in H$ which satisfy the following conditions:

(1) $x_{s,t} = x_{s,t+e_0} = x_{s+e_0,t} = x_{s+e_0,t+e_0}$,

(2) $x_{s,w} = 0$ for $w \in \{0, e_0, e_1, \ldots, e_d\}$,

(3) $x_{s,t} = x_{w,t}$ for $w \in Supp(\bar{s}) \backslash Supp(\bar{t})$,

(4) $x_{s,t} + x_{t,s} = x_{w,s} + x_{w,t}$ for $w \in Supp(\bar{s}) \cap Supp(\bar{t})$,

(5) $x_{s,s} = x_{w,s}$ for $w \in Supp(\bar{s})$, *and*

(6) $x_{s,t} + x_{s,s} = x_{s,s+t}$.

Using this $\{x_{s,t}\}$, we define $b(s,t)$ for $s, t \in H \backslash \{0\}$ as follows:

Definition 3. In $GF(2^n) \times GF(2^n)$, let us define $b(s,t)$ for $s, t \in H \backslash \{0\}$ as

$$\begin{aligned} b(s,t) &= (st, s^\sigma t + st^\sigma) \\ &+ x_{s,t} \sum_{w \in Supp(s)} (we_0 + w^2, w^\sigma e_0 + we_0^\sigma) \\ &+ \sum_{w \in Supp(t)} x_{w,s}(we_0 + w^2, w^\sigma e_0 + we_0^\sigma). \end{aligned}$$

We are able to show that $b(s,t) \neq 0$ for $s, t \in H \backslash \{0\}$. So we may regard that $b(s,t) \in PG(2n-1, 2) = GF(2^n) \times GF(2^n) \backslash \{(0,0)\}$ for $s, t \in H \backslash \{0\}$. We prove the following $(b1)$–$(b6)$ for $b(s,t)$ with $s, t \in H \backslash \{0\}$ in [1].

(b1) $b(s,s)=(s^2,0)$,

(b2) $b(s,t)=b(t,s)$ for any s, t,

(b3) $b(s,t)\neq 0$,

(b4) $b(s,t)=b(s',t')$ if and only if $\{s,t\}=\{s',t'\}$,

(b5) $\{b(s,t)|t\in H\backslash\{0\}\}\cup\{0\}$ is a vector space over $GF(2)$,

(b6) $b(w,w')=(ww',w^\sigma w'+ww'^\sigma)$ for $w,w'\in\{e_0,e_1,\ldots,e_d\}$.

Using $(b1)$–$(b6)$, we are able to prove the following theorem.

Theorem 1. *Inside $PG(2n-1,2)=GF(2^n)\times GF(2^n)\backslash\{(0,0)\}$, let $X(s):=\{b(s,t)|t\in H\backslash\{0\}\}$ for $s\in H\backslash\{0\}$ and $X(\infty):=\{b(s,s)|s\in H\backslash\{0\}\}$. Then $X(s)$ for $s\in H\backslash\{0\}$ and $X(\infty)$ are d-dimensional subspaces of $PG(2n-1,2)$. Moreover, we have that $S:=\{X(s)|s\in H\backslash\{0\}\}\cup\{X(\infty)\}$ is a d-dimensional dual hyperoval in $PG(d(d+3)/2,2)$.*

Let χ be the characteristic function of $V\backslash\{0\}$, that is, χ is a map from V to $GF(2)$ defined by $\chi(v)=0$ or 1 according to whether $v=0$ or not. We use the symbol $J(u)$ for $u\in H$ to denote $\{0\}$ if $\bar{u}=0$, or $Supp(\bar{u})$ if $\bar{u}\neq 0$. With the above convention, we consider the following function from $H\times H$ to $GF(2)$: $x_{s,t}:=\chi(\bar{s}+\bar{t})+\sum_{w\in J(t)}\chi(\bar{s}+w)$. Then we have the following Theorem.

Theorem 2. *$\{x_{s,t}\}$ defined above satisfies (1)–(6). Moreover, if S is a dual hyperoval in Theorem 1 defined by $\{x_{s,t}\}$ above, we have that*

(1) S is not isomorphic to the Veronesean dual hyperoval, and

(2) S does not satisfy Property (T).

As a consequence of Theorem 2, we have a new family of dual hyperoval S in $PG(d(d+3)/2)$.

We define $\alpha\{s,t_1,t_2\}\in GF(2)$ as: $\alpha\{s,t_1,t_2\}:=x_{s,t_1}+x_{s,t_2}+x_{s,s}+x_{s,s+t_1+t_2}$. Then we see the following proposition.

Proposition 1. *Let s, t_1, $t_2\in H\backslash\{0\}$. Assume that $t_1\neq t_2$. Then, we have $b(s,t_1)+b(s,t_2)=b(s,t_1+t_2+\alpha\{s,t_1,t_2\}(s+e_0))$,where $\alpha\{s,t_1,t_2\}=\chi(\bar{s}+\bar{t_1})+\chi(\bar{s}+\bar{t_2})+\chi(\bar{t_1}+\bar{t_2})$ if $\bar{t_1}\neq 0$, $\bar{t_2}\neq 0$ and $\bar{s}\neq\bar{t_1}+\bar{t_2}$. Otherwise, we have $\alpha\{s,t_1,t_2\}=0$.*

3 The automorphism group

Theorem 3. *The automorphism group of S is $2^d : GL(d, 2)$.*

We recall that a automorphism of S is an element Φ of $PGL(d(d+3)/2, 2)$ which permute the members of S in $PG(d(d+3)/2, 2)$, which means, for any automorhism Φ, there exists a one-to-one mapping ρ from $H\backslash\{0\} \cup \{\infty\}$ onto itself such that Φ sends any member $X(s)$ to $X(\rho(s))$. We note that, by the definition of dual hyperoval, for any automorphism Φ, there exists only one ρ which satisfies that Φ sends any member $X(s)$ to $X(\rho(s))$. So, to prove Theorem 3, it is sufficient to prove that ρ is a linear mapping of H which fixes e_0, and that any such mapping ρ defines an automorphism Φ, because the group consists of linear mappings of H which fixes e_0 is $2^d : GL(d, 2)$.

In this note, we only prove that, for any linear mapping ρ from H onto itself which fixes e_0, there exists an automorphism Φ which maps $X(t)$ to $X(\rho(t))$ for $t \in H\backslash\{0\}$ and fixes $X(\infty)$.

Proof. Recall that the vectors $b(w, w') = (ww', w^\sigma w' + ww'^\sigma)$ form a basis of the underlying vectorspace of the ambient space $\overline{H}$ for $w, w' \in \{e_0, e_1, \ldots, e_d\}$. We define a map Φ from $\overline{H}$ to itself on this basis as follows; $\Phi(b(w, w')) = b(\rho(w), \rho(w'))$ for $w, w' \in \{e_0, e_1, \ldots, e_d\}$. This map is uniquely extended to a linear map on $\overline{H}$, which we also denote by Φ. We have to show that, for every $u, v \in H$,

$$\Phi(b(u, v)) = b(\rho(u), \rho(v)). \tag{1}$$

If $u = v$, it is easy to see that $\Phi(b(u, u)) = b(\rho(u), \rho(u))$. From now on, we consider the case that $u \neq v$. We note that a subspace $X(u) = \{b(u, v) | v \in H\backslash\{0\}\}$ is generated by the vectors $b(u, w)$ for $w \in \{u, e_0, \ldots, e_d\}$, since $b(u, v) = \sum_{w \in Supp(v)} b(u, w) + x_{u,v}(b(u, u) + b(u, e_0))$. Let $m(u, v)$ be the minimal number m such that $b(u, v) = \sum_{i=1}^{m} b(u, w_i)$ for some distinct elements w_i $(i = 1, \ldots, m)$ in $\{u, e_0, e_1, \ldots, e_d\}$. Any such expression with $m = m(u, v)$ is called a minimal expression of $b(u, v)$. We prove claim (1) by induction on $m(u, v)$.

Step 1: Assume first that $u \in \{e_0, e_1, \ldots, e_d\}$. If $m(u, v) = 1$, then $b(u, v)$ is one of the basis vectors $b(w, w')$ $(w, w' \in \{e_0, \ldots . e_d\})$ of $\overline{H}$, and hence claim (1) follows from the definition of Φ. Assume $m(u, v) > 1$ and that the claim holds for every $v' \in H$ with $m(u, v') < m(u, v)$. Let $b(u, v) = \sum_{i=1}^{m} b(u, w_i)$ with $m := m(u, v)$ be minimal expression of $b(u, v)$. Since $X(u) \cup \{0\} = \{b(u, h) | h \in H\}$ is a subspace with a bijection $H \ni h \mapsto b(u, h) \in X(u)$, there exists a unique $v_1 \in H$ such that $b(u, v_1) = \sum_{i=1}^{m-1} b(u, w_i)$. We have $b(u, v) = b(u, v_1) + b(u, w_m)$. In particular, we have $v = v_1 + w_m + \alpha\{u, v_1, w_m\}(u + e_0)$, and hence we have $\rho(v) = \rho(v_1) + \rho(w_m) + \alpha\{\rho(u), \rho(v_1), \rho(w_m)\}(\rho(u) + e_0)$. Now, since $u \in \{e_0, \dots, e_d\}$, we have $\Phi(b(u, w_i)) = b(\rho(u), \rho(w_i))$ by definition. As $m(u, v_1) \leq m - 1$, we have $\Phi(b(u, v_1)) = b(\rho(u), \rho(v_1))$ by the induction hypothesis. Combining these remarks, it follows the linearity of Φ that $\Phi(b(u, v)) = \Phi(b(u, v_1)) + \Phi(b(u, w_m))$. Note that $b(\rho(u), \rho(v_1)) + b(\rho(u), \rho(w_m)) = b(\rho(u), \rho(v_1) + \rho(w_m) + \alpha\{\rho(u), \rho(v_1), \rho(w_m)\}(\rho(u) + e_0))$. Hence we have $\Phi(b(u, v)) = b(\rho(u), \rho(v))$. Thus, the claim is verified.

Step 2: Next, we prove (1) for $u \in H$ with $wt(u) \geq 2$ by induction on $m(u, v)$. The starting point in this case is a minimum number $m(u, v)$ for $u \in H$. Remark that with fixed $u \in H$, the minimality of $m(u, v)$ implies that $v \in \{u, e_0, \dots, e_d\}$. Then, claim (1) has already been established in Steep 1. Then, the verbatim repetition of the proof above goes through, execept at one point where we claim $\Phi(b(u, w_m)) = (b(\rho(u), \rho(w_m))$. In these case when $wt(u) \geq 2$, this claim holds from the conclusion of Step 1, replacing (u, v) by (w_m, u). Hence we have claim (1) for every $u, v \in H$.

Since ρ is a bijection on H, the vectors $b(\rho(u), \rho(v))$ for $u, v \in H$ generate $\overline{H}$. Thus claim (1) implies that the linear map Φ is surjective, and hence bijective on $\overline{H}$. Furthermore, claim (1) shows that Φ maps each member $X(u)$ isomorphically onto a member $X(\rho(u))$. Thus we conclude that Φ is an automorphism with associated bijection ρ. $\square$

References

[1] H. Taniguchi, A new family of dual hyperovals in $PG(d(d+3)/2, 2)$ with $d \geq 3$, to appear in Discrete Math.

[2] M. Buratti and A. Del Fra, Semi-Boolean quadruple systems and dimensional dual hyperovals, Adv. Geom. 3 (2003), 245–253.

[3] C. Huybrechts, Dimensional dual hyperovals in projective spaces and $c.AC^*$ geometries, Discrete Math. 255 (2002), 503–532.

[4] J. A. Thas and H. Van Maldeghem, Characterizations of the finite quadric Veroneseans $\mathcal{V}_n^{2^n}$, Quart. J. Math. Oxford. 55 (2004), 99–113.

[5] S. Yoshiara, Notes on Taniguchi's dimensional dual hyperovals, Europ. J. Combin. 28 (2007), 674–684.