数理解析研究所講究録 1476 巻 2006 年 214-223

Automorphism Groups of Dimensional Dual Hyperovals

Satoshi Yoshiara
Department of Mathematics
Tokyo Woman's Christian University
Suginami-ku, Tokyo 167-8585, JAPAN

1 Introduction

The notion of dimensional dual arcs were introduced by the author [15] as a higher dimensional analogue of classical notion of arcs in a projective plane. Dimensional dual arcs with maximum size are called dimensional dual hyperovals, which were defined and investigated by A. Del Fra [3], C. Huybrechts and A. Pasini [6], earlier than the notion of dimensional dual arcs appeared. Since then several works have been done with those objects, including constructions of several infinite families.

In this article, we focus on their automorphism groups. After fundamental definitions are reviewed in Section 2, a survey is given in Section 3 on the structure of automorphism groups of known dimensional dual (hyper)ovals. In Section 4, it is shown that the substrucure fixed by an involutive automorphism in a dimensional dual (hyper)oval gives rise to a smaller dimensional dual (hyper)oval. This implies that the centralizer of an involution in the automorphism group of a dimensional dual (hyper)oval can be, in principle, inductively determined. Motivated by this fact, I propose a possible direction of research, which would be comparable with the classification of simple groups with given centralizer of an involution.

2 Fundamental definitions

Definition 2.1 *Let q be a prime power, and let V be a vector space over $GF(q)$. A family $\mathcal{A}$ of $(d+1)$-(vector) dimensional spaces of V is called a d-***dimensional dual arc*** over $GF(q)$, if the following two conditions are satisfied, where* $\dim(X)$ *denotes the vector dimension of a subspace X of V.*

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

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

The subspace $\langle X \mid X \in \mathcal{A}\rangle$ of V spanned by the members of $\mathcal{A}$ is called the **ambient space** *of $\mathcal{A}$, and is denoted* $\mathbf{A}(\mathcal{A})$.

For a d-dimensional dual arc $\mathcal{A}$, the following upper bound on the number of members of $\mathcal{A}$ can be easily obtained.

$$|\mathcal{A}| \leq \theta_q(d) + 1,$$

where $\theta_q(d) := (q^{d+1} - 1)/(q - 1)$, the number of projective points of a d-(projective) dimensional space $PG(d, q)$ over $GF(q)$.

Definition 2.2 *A d-dimensional dual arc $\mathcal{A}$ is called* **dual hyperoval** *(resp.* **dual oval***) if $|\mathcal{A}| = \theta_q(d) + 1$ (resp. $\theta_q(d)$).*

We now define some maps between two dimensional dual arcs.

Definition 2.3 *Let $\mathcal{A}$ and $\mathcal{B}$ be d-dimensional dual arcs with $|\mathcal{A}| = |\mathcal{B}|$. A $GF(q)$-semilinear map ρ from $\mathbf{A}(\mathcal{A})$ to $\mathbf{A}(\mathcal{B})$ is called a* **covering map**, *if ρ sends each member of $\mathcal{A}$ to a member of $\mathcal{B}$. A covering map from $\mathcal{A}$ to $\mathcal{B}$ is called an* **isomorphism**, *if it is bijective. When $\mathcal{A} = \mathcal{B}$, each isomorphism is called an* **automorphism** *of $\mathcal{A}$.*

Definition 2.4 *The group of all automorphisms of a dimensional dual arc $\mathcal{A}$ (with respect to composition of maps) is denoted $\Gamma L(\mathcal{A})$, and its linear part, that is, the group of all $GF(q)$-linear bijections on $\mathbf{A}(\mathcal{A})$ preserving $\mathcal{A}$, is denoted $GL(\mathcal{A})$:*

$$\begin{aligned} \Gamma L(\mathcal{A}) &:= \{\rho \in \Gamma L(\mathbf{A}(\mathcal{A})) \mid X^\rho = X \ (\forall X \in \mathcal{A})\}, \\ GL(\mathcal{A}) &:= \{\rho \in GL(\mathbf{A}(\mathcal{A})) \mid X^\rho = X (\forall X \in \mathcal{A})\} \end{aligned}$$

Notice that the group Z of scalar trasformations on $\mathbf{A}(\mathcal{A})$ is always contained in $\Gamma L(\mathcal{A})$. In earlier papers e.g. [6], the automorphism group of $\mathcal{A}$ is defined to be the quotient group

$$Aut(\mathcal{A}) := \Gamma L(\mathcal{A})/Z.$$

Namely, $Aut(\mathcal{A})$ is the group of automorphisms of $PG(\mathbf{A}(\mathcal{A}))$ (the projective space associated with $\mathbf{A}(\mathcal{A})$) which preserve $\mathcal{A}$.

For d-dimensional dual arcs $\mathcal{A}$ and $\mathcal{B}$ with $|\mathcal{A}| = |\mathcal{B}|$, it is known [16, Proposition 13] that there is a covering map from $\mathcal{A}$ to $\mathcal{B}$ if and only if there exists a subspace K of $\mathbf{A}(\mathcal{A})$ with $\dim(K) = \dim(\mathbf{A}(\mathcal{A})) - \dim(\mathbf{A}(\mathcal{B}))$ such that

$K \cap \langle X, Y \rangle = \{0\}$ for every distinct members X, Y of $\mathcal{A}$.

Sometimes we consider dual arcs which can be embedded in polar spaces.

Definition 2.5 *A d-dimensional dual arc $\mathcal{A}$ is said to be of* **polar type** *(with respect to f), if there exists a non-degenerate alternating, hermitian or quadratic from f on $\mathbf{A}(\mathcal{A})$ for which each member of $\mathcal{A}$ is a maximal totally isotropic subspace of $\mathbf{A}(\mathcal{A})$.*

Notice that this definition gives very strong restictions between the dimension $d+1$ and the dimension $n+1$ of the ambient space:
If $n+1$ is odd, then f is either hermitian or quadratic, and we have $n = 2(d+1)$.
If $n+1$ is even, then one of the following holds:
$n+1 = 2(d+1)$ and f is either alternating, hermitian or quadratic form of positive type.
$n+1 = 2(d+2)$ and f is a quadratic form of negative type.

It is known [16, Theorem 1] that if a d-dimensional dual oval $\mathcal{A}$ over $GF(q)$ with $q > 2$ exists then

$$2d+1 \leq \dim(\mathbf{A}(\mathcal{A})) \leq \frac{d(d+3)}{2} + 1.$$

It is conjectured that the same inequality holds even if $q = 2$, although the upper bound obtained in [16, Theorem 1] is $\dim(\mathbf{A}(\mathcal{A})) \leq (d(d+3)/2) + 3$.

3 Automorpshism groups of known dual (hyper)ovals

3.1 Matheiu dual hyperoval $\mathcal{M}$

It is known that a 2-dimensional dual hyperoval $\mathcal{M}$ over $GF(4)$ with $\dim \mathbf{A}(\mathcal{M}) = 6$ exists. It is also of polar type with respect to a hermitian form f. Its automorphism groups are described as follows, where M_{22} denotes the sporadic simple group of Mathieu of degree 22:

$$\Gamma L(\mathcal{M}) \cong (3 \cdot M_{22}) : 2, \; GL(\mathcal{M}) \cong 3 \cdot M_{22}, \; Aut(\mathcal{M}) \cong M_{22} : 2.$$

Notice that $|\mathcal{M}| = \theta_4(2) + 1 = 22$ and the action of $\Gamma L(\mathcal{M})$ on $\mathcal{M}$ is equivalent to the natural action of M_{22} on 22 letters.

It can be verified that $GL(\mathcal{M})$ is a subgroup of the unitary group $GU_6(4)$, the subgroup of $GL(\mathbf{A}(\mathcal{M}))$ preserving the unitary form f, and that the central extension $GL(\mathcal{M})/Z(GL(\mathcal{M}))$ does not split.

3.2 Veronesean dual ovals $\mathcal{AV}_d(q)$ over $GF(q)$

This infinite family was first constructed by J. Thas and H. van Maldeghem [12, 11]. Here we adopt its presentation given in [16, Subsection 3.1].

Let q be any prime power. We take natural numbers d and $D := d(d+3)/2$. Consider vector spaces V and W of dimensions $d+1$ and $D+1$ over $GF(q)$ respectively. Let $I := \{0, \ldots, d\}$ and let J be the set of ordered pairs (i,j) of $i, j \in I$ with $i \leq j$. As $|I| = d+1$ and $|J| = D+1$, we may use I and J to index bases for V and W respectively. Let $\{\mathbf{e}_i \mid i \in I\}$ and $\{\mathbf{e}_{(i,j)} \mid (i,j) \in J\}$ be bases of V and W respectively. We define natural biliner forms b and B on V and W respectively as follows: $b(\sum_{i\in I} x_i\mathbf{e}_i, \sum_{i\in I} y_i\mathbf{e}_i) :=$

$\sum_{i\in I} x_i y_i$, $B(\sum_{(i,j)\in J} x_{(i,j)}\mathbf{e}_{(i,j)}, \sum_{(i,j)\in J} y_{(i,j)}\mathbf{e}_{(i,j)}) := \sum_{(i,j)\in J} x_{(i,j)} y_{(i,j)}$.
The **Veronesean map** ζ is a map from V to W given by

$$\sum_{i\in I} x_i \mathbf{e}_i \mapsto \sum_{(i,j)\in J} x_i x_j \mathbf{e}_{(i,j)}.$$

Let $\mathbf{P}(V)$ be the set of projective points of the projective space $PG(V)$ associated with V. For each $P \in \mathbf{P}(V)$, consider a subspace $A(P)$ of W defined by

$$A(P) := (\zeta(P^{\perp}))^{\perp},$$

where $P^{\perp} := \{\mathbf{v} \in V \mid b(\mathbf{v}, P) = 0\}$ is the dual space to P in V with respect to the form b, and $Y^{\perp} := \{\mathbf{w} \in W \mid B(\mathbf{w}, \mathbf{y}) = 0\ (\forall \mathbf{y} \in Y)\}$ is the subspace of W dual to a subset Y (or the subspace $\langle Y \rangle$) of W with respect to B. Finally we set

$$\mathcal{V}_d(q) := \{A(P) \mid P \in \mathbf{P}(V)\}.$$

In [16, Subsection 3.1], the following are shown. The family $\mathcal{V}_d(q)$ is a d-dimensional dual oval over $GF(q)$ with $\mathbf{A}(\mathcal{V}_d(q)) = W$. For q even, $\mathcal{V}_d(q)$ is uniquely extended to a d-dimemsional dual hyperoval $\tilde{\mathcal{V}}_d(q) = \mathcal{V}_d(q) \cup \{H\}$ over $GF(q)$.

We now calculate the automorphism group of this dual oval.

Proposition 3.1 *We have $Aut(\mathcal{V}_d(q)) \cong Aut(PG(V)) \cong P\Gamma L_{d+1}(q)$. In particular, $Aut(\mathcal{V}_d(q))$ is transitive on $\mathcal{V}_d(q)$.*

For q even, $Aut(\tilde{\mathcal{V}}_d(q)) = Aut(\mathcal{V}_d(q))$ has two orbits $\mathcal{V}_d(q)$ and $\{H\}$ on $\tilde{\mathcal{V}}_d(q)$.

Sketch of proof It can be shown that $Aut(PG(V))$ induces a subgroup of $Aut(PG(W))$ preserving the image of the Veronesean map. This shows that $Aut(\mathcal{V}_d(q))$ contains a subgroup inherited from $Aut(PG(V))$. The point of the proof is to show the converse.

From [16, Proposition 7(2)], we have the following.

For mutually distinct projective points P, Q, R in $PG(V)$,
they lie on a line of $PG(V)$ iff $\langle A(P), A(Q)\rangle \geq A(R)$.
Moreover, H is always contained in $\langle A(P), A(Q)\rangle$, if q is even.

Since the inclusion relation among subspaces of W is preserved by $Aut(\mathcal{V}_d(q))$, this implies that the collinearity relation for the points of $PG(V)$ is preserved by $Aut(\mathcal{V}_d(q))$. Thus $Aut(\mathcal{V}_d(q))$ induces a subgroup of $Aut(PG(V))$. It is easy to see that the kernel is trivial, whence $Aut(PG(V)) \cong Aut(\mathcal{V}_d(q))$.

Furthermore, the latter property above shows that H is always stabilized by $Aut(\tilde{\mathcal{V}}_d(q))$ if q is even. Thus we have the claims when q is even. **q.e.d.**

3.3 Characteristic dual hyperovals $\mathcal{S}(X_i)$ $(i = 0, 1)$ over $GF(2)$

Let W be a $(d+2)$-dimensional vector space over $GF(2)$. Choose a chain $V \subset H$ of subspaces of W with $\dim(V) = d$ and $\dim(H) = d+1$, and a vector e_0 of H not contained in V. Take subsets $X_0 := \emptyset$ and $X_1 := V \setminus \{0\}$ of V.

Associated with X_i $(i = 0, 1)$ and e_0, Buratti and Del Fra [1] constructed a d-dimensional dual hyperoval $\mathcal{S}(X_i)$ over $GF(2)$ with ambient space $\mathbf{A}(\mathcal{S}(X_i)) = W \wedge W$. (The isomorphism class of $\mathcal{S}(X_i)$ depends only on X_i, not on the choice of e_0, whence we do not indicate e_0.)

It is a bit complicated to give the explicit shapes of members of $\mathcal{S}(X_i)$. Thus we do not attempt to do so here (see the paragraphs before [4, Proposition 4] for the details). The main future of this dual hyperoval is that we can define a structure of a Steiner quadruple system on the members of $\mathcal{S}(X_i)$ $(i = 0, 1)$. It turns out that $\mathcal{S}(X_0)$ coincides with the so called Huybrechts dual hyperoval, which was first constructed by Huybrechts [7].

The automorphism group of $\mathcal{S}(X_i)$ is determined by Del Fra and the author [4, Theorem 2].

Proposition 3.2 *Assume that $d \geq 3$. Then $Aut(\mathcal{S}(X_0)) \cong 2^{d+1} : GL_{d+1}(2)$, which is doubly transitive on $\mathcal{S}(X_0)$. While, $Aut(\mathcal{S}(X_1)) \cong 2^{d+1} : 2^d GL_d(2)$, which is transitive but not primitive on $\mathcal{S}(X_1)$.*

In the statement above, the normal subgroup of $Aut(\mathcal{S}(X_i))$ denoted by 2^{d+1} corresponds to the group of "translations" by vectors in H. The complements $GL_{d+1}(2)$ and $2^d GL_d(2)$ respectively correspond to the general linear group on H and its parabolic subgroup stabilizing the specified vector e_0.

3.4 Dual hyperovals $\mathcal{S}^d_{\sigma,\phi}$ over $GF(2)$

Take a natural number d with $d \geq 2$ and let $F := GF(2^{d+1})$. Choose a generator σ of a Galois group $Gal(F/GF(2))$. Let ϕ be the bijection on F induced by an o-polynomial $\phi(X)$ in $F[X]$ (see e.g. [5, Subsection 8.4] or [22]).

Inside the direct sum $V = F \oplus F$, regarded as a $2(d+1)$-dimensional vector space over $GF(2)$, consider the following subspaces $X(t)$ for each $t \in F$ and the family $\mathcal{S}^{d+1}_{\sigma,\phi}$:

$$\begin{aligned} X(t) &:= \{(x, x^\sigma t + x t^\phi) \mid x \in F\}, \\ \mathcal{S}^{d+1}_{\sigma,\phi} &:= \{X(t) \mid t \in F\}. \end{aligned}$$

Then $\mathcal{S}^{d+1}_{\sigma,\phi}$ is a d-dimensional dual hyperoval over $GF(2)$ with ambient space $\mathbf{A}(\mathcal{S}^{d+1}_{\sigma,\phi}) = V$ or a hyperplane of V according to $\sigma\phi \neq id_F$ or $\sigma\phi = id_F$ [14, Lemma 1,2], [13, Proposition 2.1].

In the case $\sigma = \phi$, this construction does not give an essentially new dual hyperoval, because $\mathcal{S}^{d+1}_{\sigma,\sigma}$ is covered by the Huybrechts dual hyperoval $\mathcal{S}(X_0)$ [8, Proposition 6.8].

However, except this case, $\mathcal{S}^{d+1}_{\sigma,\phi}$ with σ lying in $Gal(F/GF(2))$ is not properly covered by other dimensional dual hyperovals in general [9, Conjecture].

The automorphism group of $\mathcal{S}^{d+1}_{\sigma,\phi}$ is determined in [14] in the case when ϕ lies in $Gal(F/GF(2))$, which is generalized in [13] (with some correction to the arguments in the proof of [14, Lemma 6]) to the case when $\phi(X)$ is a monomial polynomial.

Proposition 3.3 *Assume that $\sigma\phi \neq id_F$.*

(1) [14, Proposition 7] If $\phi \in Gal(F/GF(2))$, then $Aut(\mathcal{S}^{d+1}_{\sigma,\phi}) \cong 2^{d+1}.Z_{2^{d+1}-1}.Z_{d+1}$ for $d \geq 2$, except when $d = 2$ and $\sigma = \phi$. In the exceptional case, we have $Aut(\mathcal{S}^{d+1}_{\sigma,\phi}) \cong 2^{d+1}.GL_3(2)$. For $d \geq 2$, $Aut(\mathcal{S}^{d+1}_{\sigma,\phi})$ is doubly transitive on $\mathcal{S}^{d+1}_{\sigma,\phi}$.

(2) [13, Theorem 1.1] Assume that $\phi(X)$ is monomial but $\phi \notin Gal(F/GF(2))$. Then $Aut(\mathcal{S}^{d+1}_{\sigma,\phi}) \cong Z_{2^{d+1}-1}.Z_{d+1}$ for $d \geq 3$, and $Aut(\mathcal{S}^{d+1}_{\sigma,\phi}) \cong GL_3(2)$ if $d = 2$.

For $d \geq 2$, $Aut(\mathcal{S}^{d+1}_{\sigma,\phi})$ stabilizes $X(0)$ and is transitive on $\mathcal{S}^{d+1}_{\sigma,\phi} \setminus \{X(0)\}$.

In the above statement (1), 2^{d+1} corresponds to the group of translations by F. In both statements, $Z_{2^{d+1}-1}$ and Z_{d+1} correspond respectively to the group of multiplications by $F^\times$ and the group of field automorphisms of F.

3.5 Taniguchi's dual ovals $\mathcal{T}_\sigma(F)$ over $GF(q)$

The construction below is first given by Taniguchi [10] in the case when q is even, and is generalized later [21] to the general case.

Let q be any prime power, and let d and n be positive integers with $2 \leq d \leq n$. Inside $GF(q^{n+1})$, regarded as an $(n+1)$-dimensional vector space over $GF(q)$, take a subspace F of dimension $d+1$ over $GF(q)$. Choose a generator σ of the Galois group $Gal(GF(q^{n+1})/GF(q))$. Regard $V := GF(q^{n+1}) \oplus GF(q^{n+1})$ as a vector space over $GF(q)$. As in Subsection 3.2, $\mathbf{P}(F)$ denotes the set of projective points of the projective space $PG(F) \cong PG(d,q)$ associated with $F\mathbf{P}(F)$. For a projective point $P = \{\alpha t \mid \alpha \in GF(q)\}$, $t \in F$, of $\mathbf{P}(F)$, define a subspace $T(P)$ of V and a family $\mathcal{T}_\sigma(F)$ as follows:

$$
\begin{aligned}
T(P) &:= \{(xt, x^\sigma t + xt^\sigma) \mid x \in F\}, \\
\mathcal{T}_\sigma(F) &:= \{T(P) \mid P \in \mathbf{P}(F)\}
\end{aligned}
$$

Then $\mathcal{T}_\sigma(K)$ is a d-dimensional dual oval over $GF(q)$ [21, Subsection 2.2]. For q even, $\tilde{\mathcal{T}}_\sigma(K) := \mathcal{T}_\sigma(K) \cup \{T(\infty)\}$ forms a d-dimensional dual hyperoval, where $T(\infty)$ denotes the subspace $\{(x^2, 0) \mid x \in F\}$ [10].

The ambient space $\mathbf{A}(\mathcal{T}_\sigma(F))$ (and $\mathbf{A}(\tilde{\mathcal{T}}_\sigma(F))$ for q even) is described as follows. Let $\{e_i \mid i \in I\}$ be a basis of F, where $I = \{0, \ldots, d\}$. Then $\mathbf{A}(\mathcal{T}_\sigma(K))$ (and $\mathbf{A}(\tilde{\mathcal{T}}_\sigma(F))$ for q even) is spanned by

$$e_{(i,j)} := (e_i e_j, e_i^\sigma e_j + e_i e_j^\sigma),$$

where (i, j) ranges over the set J defined in the same way as in Subsection 3.2. Notice that the vectors $e_{(i,j)}$ $((i,j) \in J)$ may be linearly dependent over $GF(q)$. We can verify that the map ρ from $\mathbf{A}(\mathcal{V}_d(q))$ to $\mathbf{A}(\mathcal{T}_\sigma(F))$ sending each $\mathbf{e}_{(i,j)}$ to $e_{(i,j)}$ is a covering map of $\mathcal{T}_\sigma(F)$ by $\mathcal{V}_d(q)$ [21, Proposition 1]. If q is even, the same map is a covering of $\tilde{\mathcal{T}}_\sigma(F)$ by $\tilde{\mathcal{V}}_d(q)$.

Let $K := Ker(\rho)$. Then we can verify that every element of $\Gamma L(\mathcal{V}_d(q))$ $(\cong \Gamma L_{d+1}(q))$ stabilizing K induces an element of $\Gamma L(\mathcal{T}_\sigma(F))$. Since $\mathcal{V}_d(q)$ is, in a sense, the universal cover of $\mathcal{T}_\sigma(F)$, it is expected that every element of $\Gamma L(\mathcal{T}_\sigma(F))$ is induced by an element of $\Gamma L(\mathcal{V}_d(q))$ stabilizing K. However, the author have not yet verified this.

4 Substructure fixed by an involution

Assume that $\mathcal{A}$ is a d-dimensional dual arc $\mathcal{A}$ over $GF(q)$ with ambient space V. For $\alpha \in \Gamma L(\mathcal{A})$, set

$$\mathcal{A}(\alpha) := \{X \in \mathcal{A} \mid X^\alpha = X\}.$$

For each $X \in \mathcal{A}(\alpha)$, consider the subset $C_X(\alpha) := \{x \in X \mid x^\alpha = x\}$ of X fixed by α. If $\alpha \in GL(\mathcal{A})$, $C_X(\alpha)$ is a subspace of X over $GF(q)$, but not in general. It is just a subspace over $GF(p)$, where $GF(p)$ is the prime subfield contained in $GF(q)$. We now set

$$\mathcal{A}[\alpha] := \{C_X(\alpha) \mid X \in \mathcal{A}(\alpha)\}.$$

A general version of the next theorem was first announced in [19], but its prototype has already appeared in [14, Lemma 4]. There are several vesions of this statement: one for automorphisms of prime order, and one for dual arcs with large members (specifically ovals). However, we restrict the situation given in the statement for simplicity.

Theorem 4.1 *Let q be a power of 2. Assume that $\mathcal{S}$ is a d-dimensional dual hyperoval over $GF(q)$ with ambient space V. Then one of the following holds:*

(1) The order of a Sylow 2-subgroup of $GL(\mathcal{S})$ divides $|\mathcal{S}| = \theta_q(d) + 1$.

(2) There exists a subset Ω of $\mathcal{S}$ with $|\Omega| = 1$ or 2 which is invariant under the action of any 2-elements of $GL(\mathcal{S})$.

(3) $GL(\mathcal{S})$ has strongly embedded subgroup H, that is, H is a subgroup of even order such that $|H \cap H^g|$ is odd for every $g \in GL(\mathcal{S}) \setminus H$.

(4) There exists an involution α of $GL(\mathcal{S})$ such that $\mathcal{S}[\alpha]$ is an e-dimensional dual hyperoval for some $0 \le e \le d-1$, where a 0-dimensional dual hyperoval is understood to be just a set of two members.

The crucial point of the claim in case (4) is that $\dim(C_X(\alpha))$ does not depend on the particular choice of X in $\mathcal{S}(\alpha)$.

Now we examine the substructure $\mathcal{S}[\alpha]$ fixed by an involution α for the examples $\mathcal{S}$ of dual (hyper)ovals given in Section 3.

$\mathcal{M}$: There is a single class of involutions in $GL(\mathcal{M}) \cong 3M_{22}$. For an involution α of $GL(\mathcal{M})$, we have $|\mathcal{M}(\alpha)| = 6 = |\theta_4(1)| + 1$. The substructure $\mathcal{M}[\alpha]$ is a 1-dimensional dual hyperoval over $GF(4)$ with ambient space of dimension 3 (that is, the classical dual hyperoval on the projective plane over $GF(4)$). The centralizer $C_{GL(\mathcal{M})}(\alpha)$ of α in $GL(\mathcal{M})$ induces a transitive permutation group S_6 on $\mathcal{M}[\alpha]$.

On the other hand, there are two classes of involutions in $\Gamma L(\mathcal{M})\backslash GL(\mathcal{M})$. Involutions in one class do not fix any members of $\mathcal{M}$, while $|\mathcal{M}(\beta)| = 8 = 2^{2+1}$ for each involution β in the other class. In fact $\mathcal{M}[\beta]$ forms a 2-dimensional dual hyperoval over $GF(2)$, the prime subfield in $GF(4)$. Notice that involutions in $\Gamma L(\mathcal{M}) \setminus GL(\mathcal{M})$ induce odd permutations on $\mathcal{M}$.

$\mathcal{V}_d(q)$: We use the same notation as in Subsection 3.2. Let q be even. Assume that α is an involution of $GL(\mathcal{V}_d(q)) \cong GL(V) \cong GL_{d+1}(q)$. Then $\mathcal{V}_d(q)(\alpha)$ corresponds to the set of projective points of $PG(C_V(\alpha))$, where $C_V(\alpha)$ is the subspace of V fixed by α. If $\dim(C_V(\alpha)) = e+1$, then $\mathcal{V}_d(q)[\alpha]$ is isomorphic to the e-dimensional dual oval $\mathcal{V}_e(q)$. Similar statement holds for $\tilde{\mathcal{V}}_d(q)$.

$\mathcal{S}(X_i)$ $(i = 0,1)$: Let α be an involution of $GL(\mathcal{S}(X_i))$ which fixes at least three members. Then there exists a subspace W of V containing e_0 fixed by α such that $\mathcal{S}(X_i)[\sigma] = \mathcal{S}(X_i')$, where $X_0' = \emptyset$, regarded as a subset of W, and $X_1' = W - \{0\}$.

$\mathcal{S}^{d+1}_{\sigma,\phi}$: If α is an involution of $GL(\mathcal{S}^{d+1}_{\sigma,\phi})$ fixing a member, then α corresponds to a field automorphism. Thus such an involution exists only when $d+1$ is even. In this case, we have $\mathcal{S}^{d+1}_{\sigma,\phi}(\alpha) = \{S(t) \mid t \in GF(2^{(d+1)/2})$ and $\mathcal{S}^{d+1}_{\sigma,\phi}[\alpha] = \mathcal{S}^{(d+1)/2}_{\sigma',\phi'}$, where σ' and ϕ' are restrictions of σ and ϕ to the subfield $GF(2^{(d+1)/2})$ fixed by α.

Motivated by the above theorem, the author would like to propose the following type of problem.

Problem 4.2 *Let q be a power of 2. Given e-dimensional dual hyperoval $\mathcal{T}$ over $GF(q)$, determine d-dimensional dual hyperovals $\mathcal{S}$ over $GF(q)$ such that $GL(\mathcal{S})$ contains an involusion α with $\mathcal{S}[\alpha]$ isomorphic to $\mathcal{T}$.*

There are several versions of this problem: replace $\mathcal{S}$ by dual hyperovals over some field containing $GF(q)$ and replace $GL(\mathcal{S})$ by $\Gamma L(\mathcal{S})$; or replace dual hyperovals by ovals.

In the above strict version, there are finitely many possibilities for $\mathcal{S}$, because we have the following inequality:

$$d+1 \leq 2(e+1).$$

This can be easily verified as follows. Choose a member X of $\mathcal{S}(\alpha)$. Since X (with respect to the addition defining a vector space structure on X) is an elementary abelian 2-group on which an involution α acts, we have $C_X(\alpha) \leq [X, \alpha] := \{x + x^\alpha \mid x \in X\}$ and the map $X \ni x \mapsto x + x^\alpha \in [X, \alpha]$ is a $GF(2)$-linear surjection with kernel $C_X(\alpha)$. Thus $|X/C_X(\alpha)| = |[X, \alpha]| \leq |C_X(\alpha)|$. Hence

$$q^{d+1} = |X| \leq |C_X(\alpha)|^2 = q^{2(e+1)},$$

because $C_X(\alpha)$ is a member of an e-dimensional dual hyperoval $\mathcal{S}[\alpha] \cong \mathcal{T}$ over $GF(q)$.

I conclude this article by the following result, which can be thought of as a partial solution for this type of problem.

Theorem 4.3 *Let $\mathcal{T}$ be a 1-dimensional dual hyperoval in $PG(2, q)$. Assume that $\mathcal{S}$ is a d-dimensional dual hyperoval over $GF(q)$ such that there is an involution α of $GL(\mathcal{S})$ with $\mathcal{S}[\alpha]$ isomorphic to $\mathcal{T}$. Assume, furthermore, that $\mathcal{S}$ is of polar type. Then one of the following holds:*

(1) $(q, d) = (4, 2)$ and $\mathcal{S}$ is isomorphic to the Mathieu dual hyperoval $\mathcal{M}$.

(2) $(q, d) = (2, 2)$ and $\mathcal{S}$ is isomorphic to the Huybrechts dual hyperoval $\mathcal{S}(X_0)$ $(= \mathcal{S}^3_{\sigma,\sigma})$.

References

[1] M. Buratti and A. Del Fra, Semi-Boolean Steiner quadruple systems and dimensional dual hyperovals, Advances in Geometry 3 (2003), Special Volume, S245–S253.

[2] B. Cooperstein and J. Thas, On generalized k-arcs in $PG(2n, q)$, Ann. Combin. 5 (2001), 141–152.

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

[4] A. Del Fra and S. Yoshiara, Dimensional dual hyperovals assosiated with Steiner systems, Europ. J. Combin. 26 (2005), 173–194.

[5] J. W. P. Hirschfeld, *Projective Geometries over Finite Fields,* Second Edition, Oxford Math. Monographs, Clarendon Press, Oxford, 1998.

[6] C. Huybrechts and A. Pasini, Flag-transitive extensions of dual affine spaces, Contrib. Algebra Geom. 40 (1999), 503–532.

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

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

[9] A. Pasini and S. Yoshiara, New distance regular graphs arising from dimensional dual hyperovals, European J. Combin. 22 (2001), 547–560.

[10] H. Taniguchi, A family of dual hyperovals over $GF(q)$ with q even, Europ. J. Combin. 26 (2005), 195–199.

[11] J. Thas and H. van Maldeghem, Characterizations of the finite quadric and Hermitian Veroneseans over finite fields, J. Geom. 76 (2003), 282–293.

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

[13] H. Taniguchi and S. Yoshiara, On the dimensional dual hyperovals $\mathcal{S}_{\sigma,\phi}^{d+1}$, Innovations in Incidence Geometry, 1 (2005), 197–219.

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

[15] S. Yoshiara, On a family of planes of a polar space, Europ. J. Combin., 22 (2001), 107–118.

[16] S. Yoshiara, Ambient spaces of dimensional dual arcs, J. Alg. Combin. 19 (2004), 5–23.

[17] S. Yoshiara, Some remarks on dimensional dual hyperovals of polar type, to appear in Simon Steven. (The proceeding of La Roche Conference on Incidence Geometry, May, 2004.)

[18] S. Yoshiara, Automorphism groups of some dimensional dual hyperovals, Preprint, April, 2004.

[19] S. Yoshiara, 極空間中の双対弧 (Dimensional dual arcs of polar type), 第２１回代数的組合せ論シンポジウム報告集 (June 28–30, 2004, Shinhu Univ., Matsumoto), p.57–68, October, 2004.

[20] S. Yoshiara, Dimensional dual arcs–a survey, to appear in the proceeding of the Pingree Park conference on Groups, Geometries and Computations, September, 2004.

[21] S. Yoshiara, Notes on Taniguchi's dimensional dual hyperovals, submitted for publication, 2005.

[22] S.Yoshiara, 高次元の双対弧 — 平面上の二次曲線の高次元化 (Dimensional dual arcs– higher dimensional analogue of quadratic curves in a plane), 第２２回代数的組合せ論シンポジウム報告集 (June 27–29, 2005, Ehime Univ., Matsuyama), to appear.

2005年10月25日提出