Discrete Mathematics 312 (2012) 498–508

Contents lists available at SciVerse ScienceDirect

Discrete Mathematics

journal homepage: www.elsevier.com/locate/disc

Quotients of the deformation of Veronesean dual hyperoval in $PG(3d, 2)$

Hiroaki Taniguchi

Kagawa National College of Technology, 551 Takuma, Kagawa, 769-1192, Japan

ARTICLE INFO

Article history:
Available online 27 March 2011

Keywords:
Dual hyperoval
Veronesean
Quotient

ABSTRACT

Let $d \geq 3$. In $PG(d(d+3)/2, 2)$, there are four known non-isomorphic d-dimensional dual hyperovals by now. These are Huybrechts' dual hyperoval by Huybrechts (2002) [4], Buratti-Del Fra's dual hyperoval by Buratti and Del Fra (2003) [1], Del Fra and Yoshiara (2005) [3], Veronesean dual hyperoval by Thas and van Maldeghem (2004) [9], Yoshiara (2004) [12] and the dual hyperoval, which is a deformation of Veronesean dual hyperoval by Taniguchi (2009) [6].

In this paper, using a generator σ of the Galois group $Gal(GF(2^{dm})/GF(2))$ for some $m \geq 3$, we construct a d-dimensional dual hyperoval T_σ in $PG(3d, 2)$, which is a quotient of the dual hyperoval of [6]. Moreover, for generators $\sigma, \tau \in Gal(GF(2^{dm})/GF(2))$, if T_σ and T_τ are isomorphic, then we show that $\sigma = \tau$ or $\sigma = \tau^{-1}$ on $GF(2^d)$. Hence, we see that there are many non-isomorphic quotients in $PG(3d, 2)$ for the dual hyperoval of [6] if d is large.

1. Introduction

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

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

(d1) any two distinct members of S intersect in a projective point,
(d2) any three mutually distinct members of S intersect in the empty projective set,
(d3) the members of S generate $PG(n, 2)$, and
(d4) there are exactly 2^{d+1} members of S.

The definition of higher dimensional dual hyperovals was first given by Huybrechts and Pasini in [5]. We call $PG(n, 2)$ of (d3) above the ambient space of the dual hyperoval S. For d-dimensional dual hyperovals S_1 and S_2 in $PG(n, 2)$, we say that S_1 is isomorphic to S_2 by the mapping Φ, if Φ is a linear automorphism of $PG(n, 2)$ which sends the members of S_1 onto the members of S_2.

In case $d = 2$, d-dimensional dual hyperovals over $GF(2)$ are completely classified by Del Fra [2]. Hence, from now on, we assume that $d \geq 3$. In [6], a new d-dimensional dual hyperoval S in $PG(d(d+3)/2, 2)$ for $d \geq 3$ was constructed using the Veronesean dual hyperoval. In this paper, we construct quotients of the dual hyperoval S of [6] in $PG(3d, 2)$. Moreover, we show that there exist many non-isomorphic quotients in $PG(3d, 2)$ if d is large.

2. Preliminaries

In this section, we recall the construction of the dual hyperoval S in [6] and present the theorems which we prove in this paper.

E-mail address: taniguchi@dg.kagawa-nct.ac.jp.

0012-365X/$ – see front matter © 2011 Elsevier B.V. All rights reserved.
doi:10.1016/j.disc.2011.02.033

Let $n \geq d+1$ and σ a generator of the Galois group $Gal(GF(2^n)/GF(2))$, where $GF(2^n)$ is a finite field consists of 2^n elements. Let H be a $(d+1)$-dimensional $GF(2)$-vector subspace of $GF(2^n)$ with a basis $\{e_0, e_1, \dots, e_d\}$. We denote by $H^\times$ the set consists of non-zero elements of H.

Let $b(s,t) \in GF(2^n) \oplus GF(2^n)$ for $s, t \in H^\times$, which satisfies the following conditions:

(b1) $b(s,s) = (s^2, 0)$,
(b2) $b(s,t) = b(t,s)$ for any s, t,
(b3) $b(s,t) \neq (0,0)$, and
(b4) $b(s,t) = b(s',t')$ if and only if $\{s,t\} = \{s',t'\}$,
(b5) $\{b(s,t) \mid t \in H^\times\} \cup \{(0,0)\}$ is a vector space over $GF(2)$.

From these $\{b(s,t) \mid s, t \in H^\times\}$, we have a dual hyperoval S, as follows.

Proposition 2. *Inside $PG(2n-1,2) = (GF(2^n) \oplus GF(2^n)) \setminus \{(0,0)\}$, let us define $X(s) := \{b(s,t) \mid t \in H^\times\}$ for $s \in H^\times$, and $X(\infty) := \{b(s,s) \mid s \in H^\times\}$. Then, $X(s)$ and $X(\infty)$ are d-dimensional subspaces of $PG(2n-1,2)$, and $S := \{X(s) \mid s \in H^\times\} \cup \{X(\infty)\}$ is a d-dimensional dual hyperoval.*

Proof. Since the cardinality $|X(s) \cup \{(0,0)\}| = 2^{d+1}$ by (b3) and (b4), we see, by (b5), that $X(s)$ is a d-dimensional subspace of $PG(2n-1,2)$ for $s \in H^\times$. By (b1), $X(\infty)$ is a d-dimensional subspace of $PG(2n-1,2)$. For distinct $s, t \in H^\times$, we have $X(s) \cap X(t) = b(s,t)$ by (b2)–(b4). For $s \in H^\times$, we have $X(s) \cap X(\infty) = b(s,s)$ by (b1), (b3) and (b4). Since $X(s) \cap X(t) = b(s,t)$ and $X(s) \cap X(\infty) = b(s,s)$ for $s, t \in H^\times$ with $s \neq t$, no three distinct d-subspaces of S have a common point by (b4). We have the cardinality $|S| = |\{X(s) \mid s \in H^\times\}| + |\{X(\infty)\}| = 2^{d+1}$. Hence, S is a d-dimensional dual hyperoval. □

Example 3 (*Veronesean Dual Hyperoval*)**.** Let n be a sufficient large integer, and let us choose a $(d+1)$-dimensional $GF(2)$-vector subspace H of $GF(2^n)$ with a basis $\{e_0, e_1, \dots, e_d\}$ such that $\{e_ie_j \mid 0 \leq i \leq j \leq d\}$ are linearly independent over $GF(2)$. Let σ be a generator of the Galois group $Gal(GF(2^n)/GF(2))$. We define $b(s,t)$ for $s, t \in H^\times$ as

$$b(s,t) := (st, s^\sigma t + st^\sigma).$$

Then, we easily see that $b(s,t)$ satisfies the conditions (b1)–(b5); hence, we have a d-dimensional dual hyperoval S, which generates $PG(d(d+3)/2, 2) = PG(R)$, where R is the vector space generated by $\{(e_ie_j, e_i^\sigma e_j + e_ie_j^\sigma) \mid 0 \leq i \leq j \leq d\}$ in $GF(2^n) \oplus GF(2^n)$ (see [6,10] for detail). Yoshiara [10] proved that S is isomorphic to the Veronesean dual hyperoval constructed by Thas and Van Maldeghem in [9]. We note that $\{b(s,t)\}$ satisfies the following addition formula for $s, t_1, t_2 \in H^\times$ with $t_1 \neq t_2$: $b(s,t_1) + b(s,t_2) = b(s, t_1+t_2)$.

For a non-zero vector u of H, its support, denoted as $Supp(u)$, is the subset M of $\{e_0, e_1, \dots, e_d\}$ for which $u = \sum_{e_i \in M} e_i$. Let $H' \subset H$ be the vector subspace generated by $\{e_1, e_2, \dots, e_d\}$ over $GF(2)$, and let

$$H \ni s = \sum_{i=0}^{d} \alpha_i e_i \mapsto \bar{s} = \sum_{i=1}^{d} \alpha_i e_i \in H' \tag{1}$$

be the natural projection, where $\alpha_i \in GF(2)$ for $0 \leq i \leq d$.

Definition 4 (*[6]*)**.** Let χ be the characteristic function of $H' \setminus \{0\}$, that is, χ is a map from H' 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 this convention, we define the following function from $H \times H$ to $GF(2)$ determined by the basis $\{e_0, e_1, \dots, e_d\}$ of H:

$$x_{s,t} := \chi(\bar{s} + \bar{t}) + \sum_{w \in J(t)} \chi(\bar{s} + w).$$

Then $x_{s,t} \in GF(2)$ for $s, t \in H$ and satisfies the following conditions:

(x1) $x_{s,t} = x_{s,t+e_0} = x_{s+e_0,t} = x_{s+e_0,t+e_0}$,
(x2) $x_{s,w} = 0$ for $w \in \{0, e_0, e_1, \dots, e_d\}$,
(x3) $x_{s,t} + x_{s,s} = x_{s,s+t}$,
(x4) $x_{s,s} = x_{w,s}$ for $w \in Supp(\bar{s})$ (we regard that $Supp(\bar{0}) = \{0\}$),
(x5) $x_{s,t} + x_{t,s} = x_{w,s} + x_{w,t}$ for $w \in Supp(\bar{s}) \cap Supp(\bar{t})$, and
(x6) $x_{s,t} = x_{w,t}$ for $w \in Supp(\bar{s}) \setminus Supp(\bar{t})$.

Proof. (x1) is immediate by the definition of $x_{s,t}$. Since $J(w) = \{w\}$ for $w \in \{0, e_1, \dots, e_d\}$, we have $x_{s,w} = \chi(\bar{s} + \bar{w}) + \sum_{w \in J(t)} \chi(\bar{s} + w) = \chi(\bar{s} + \bar{w}) + \chi(\bar{s} + w) = 0$ for $w \in \{0, e_1, \dots, e_d\}$, and we have $x_{s,e_0} = x_{s,0} = 0$ by (x1); hence, we obtain (x2). (x3) is proved in Lemma 23 of Taniguchi [6], and (x4)–(x6) are proved in Lemma 24 of Taniguchi [6]. □

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