Discrete Mathematics 340 (2017) 3154–3166

Contents lists available at ScienceDirect

Discrete Mathematics

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

On some bilinear dual hyperovals

Hiroaki Taniguchi

National Institute of Technology, Kagawa College, 355, chokushicho, takamatsu city, kagawa, 761-8058, Japan

ARTICLE INFO

Article history:
Received 3 October 2015
Received in revised form 25 June 2016
Accepted 4 July 2016
Available online 3 August 2016

Keywords:
Dual hyperoval
Buratti–Del Fra dual hyperoval
Huybrechts dual hyperoval
APN dual hyperoval

ABSTRACT

It is shown in Yoshiara (2004) that, if d-dimensional dual hyperovals exist in $V(n,2)$ ($GF(2)$-vector space of rank n), then $2d+1 \leq n \leq (d+1)(d+2)/2+2$, and conjectured that $n \leq (d+1)(d+2)/2$. Known bilinear dual hyperovals in $V((d+1)(d+2)/2, 2)$ are the Huybrechts dual hyperoval and the Buratti–Del Fra dual hyperoval. In this paper, we investigate on the covering map $\pi : \mathcal{S}'_c(l', GF(2^{r'})) \to \mathcal{S}_c(l, GF(2^r))$, where the dual hyperovals $\mathcal{S}'_c(l', GF(2^{r'}))$ and $\mathcal{S}_c(l, GF(2^r))$ are constructed in Taniguchi (2014). Using the result, we show that the Buratti–Del Fra dual hyperoval has a bilinear quotient in $V(2d+1, 2)$ if d is odd. On the other hand, we show that the Huybrechts dual hyperoval has no bilinear quotient in $V(2d+1, 2)$. We also determine the automorphism group of $\mathcal{S}_c(l, GF(2^r))$, and show that $Aut(\mathcal{S}_c(l_2, GF(2^{rl_1}))) < Aut(\mathcal{S}_c(l, GF(2^r)))$.

1. Introduction

Higher dimensional dual hyperovals are defined by Huybrechts and Pasini in [7]. In this paper, we only consider dual hyperovals over the binary field $GF(2)$.

Let n and d be integers with $n > d+1 \geq 3$. Let $U = V(n,2)$ be a vector space of rank n over $GF(2)$. A family $\mathcal{S}$ of vector subspaces of rank $d+1$ in U is called a d-dimensional dual hyperoval if it satisfies the following conditions:

(1) any two distinct members of $\mathcal{S}$ intersect at a subspace of rank one,
(2) any three mutually distinct members of $\mathcal{S}$ intersect trivially,
(3) the union of the members of $\mathcal{S}$ generates U, and
(4) there are exactly 2^{d+1} members of $\mathcal{S}$.

We call the vector space U the ambient space of the dual hyperoval $\mathcal{S}$, and we say that $\mathcal{S}$ is a dual hyperoval in U.

Let $\mathcal{S}_1$ be a d-dimensional dual hyperoval in U_1 and $\mathcal{S}_2$ a d-dimensional dual hyperoval in U_2. If there is a surjective $GF(2)$-linear mapping $\pi : U_1 \to U_2$ such that $\pi(\mathcal{S}_1) = \mathcal{S}_2$, which we sometimes say a covering map $\pi : \mathcal{S}_1 \to \mathcal{S}_2$, we call $\mathcal{S}_1$ a cover of $\mathcal{S}_2$ and $\mathcal{S}_2$ a quotient of $\mathcal{S}_1$. If π induces an isomorphism of U_1 and U_2, we say that $\mathcal{S}_1$ is isomorphic to $\mathcal{S}_2$. We also say a dual hyperoval $\mathcal{S}$ is simply connected if any cover $\mathcal{S}'$ of $\mathcal{S}$ is isomorphic to $\mathcal{S}$.

It is proved in [12] that, if d-dimensional dual hyperovals exist in $V(n,2)$, then $2d+1 \leq n \leq (d+1)(d+2)/2+2$, and conjectured that $n \leq (d+1)(d+2)/2$.

We recall the definition of bilinear dual hyperovals. Let V be a $GF(2)$-vector space of rank $d+1$, and W a $GF(2)$-vector space of rank l. A dual hyperoval $\mathcal{S} = \{X(t) \mid t \in V\}$ in $V \oplus W$ is said to be a bilinear dual hyperoval if there is a $GF(2)$-bilinear mapping $B : V \oplus V \to W$ such that $X(t) = \{(x, B(x,t)) \mid x \in V\} \subset V \oplus W$ for any $t \in V$. A bilinear dual hyperoval has a translation group $T := \{t_a \mid a \in V\}$, which acts regularly on $\mathcal{S} = \{X(t) \mid t \in V\}$ as $X(t)^{t_a} = X(t+a)$ for any $t \in V$, defined by the linear transformation $t_a : V \oplus W \ni (x,y) \mapsto (x, y+B(x,a)) \in V \oplus W$. We recall that T stabilizes $W = \{(0,y) \mid y \in W\}$

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

http://dx.doi.org/10.1016/j.disc.2016.07.002

and the centralizer $C_{V\oplus W}(T)$ of T in $V\oplus W$ coincides with W. We call a bilinear dual hyperoval symmetric if the bilinear mapping is symmetric, i.e., $B(x,t)=B(t,x)$ for any $x,t\in V$. (See [5] or [8] for more details.)

Known bilinear dual hyperovals in $V((d+1)(d+2)/2,2)$ are the Huybrechts dual hyperoval [6] and the Buratti–Del Fra dual hyperoval (see [1,11]). In this paper, we investigate on the covering map $\pi:\mathcal{S}'_c(l',GF(2^{r'}))\to\mathcal{S}_c(l,GF(2^r))$ in Sections 3 and 7, where the dual hyperovals $\mathcal{S}'_c(l',GF(2^{r'}))$ and $\mathcal{S}_c(l,GF(2^r))$ are constructed in [9]. Using this result, we show that the Buratti–Del Fra dual hyperoval has a bilinear quotient in $V(2d+1,2)$ if d is odd. On the other hand, we show that the Huybrechts dual hyperoval has no bilinear quotient in $V(2d+1,2)$ in Section 4. We also determine the automorphism group of $\mathcal{S}_c(l,GF(2^r))$ in Sections 5 and 6, and show that $Aut(\mathcal{S}_c(l_2,GF(2^{rl_1})))<Aut(\mathcal{S}_c(l,GF(2^r)))$ in Section 7.

2. A dual hyperoval $\mathcal{S}_c(l,GF(2^r))$ for $c\in GF(2^r)$ with $Tr(c)=1$

In this section, we recall the dual hyperovals constructed in [9]. Let $l\geq 1$ and $r\geq 1$ be integers with $d=lr\geq 4$ and $GF(2^r)$ a finite field of 2^r elements. We denote by $I(d)$ the set of triples $(l,r;c)$ of positive integers l,r with $lr=d$ and an element c of $GF(2^r)$ with $1=Tr(c)=\sum_{i=0}^{r-1}c^{2^i}$. In [9], for every $d\geq 4$ and every triple $(l,r;c)$ in $I(d)$, we construct a symmetric bilinear dual hyperoval, denoted by $\mathcal{S}_c(l,GF(2^r))$, with the ambient space of rank $((1/r)d^2+3d+2)/2$ as follows.

Let V_1 be a $GF(2^r)$-vector space of rank l with a basis $\{e_i\mid 1\leq i\leq l\}$ and V_2 a $GF(2^r)$-vector space of rank $l+1$ with a basis $\{e_i\mid 0\leq i\leq l\}$. Let $V\subset V_2$ be a $GF(2)$-vector space of rank $rl+1$ generated by V_1 and e_0, i.e., $V=V_1\oplus\langle e_0\rangle$ as a $GF(2)$-vector space. Let $c\in GF(2^r)$ be a non-zero element such that the absolute trace $Tr(c)=1$. Let $I=\{0,1,\ldots,l\}$ and $I_0=I\setminus\{0\}$. In $V_2\otimes_{GF(2^r)}V_2$, let W_c be the $GF(2^r)$-vector subspace generated by

$$e_i\otimes_{GF(2^r)}e_j-e_j\otimes_{GF(2^r)}e_i\quad\text{for all } i,j\in I \text{ with } i<j,$$
$$e_0\otimes_{GF(2^r)}e_0\quad\text{and}\quad c(e_i\otimes_{GF(2^r)}e_i)-e_0\otimes_{GF(2^r)}e_i\quad\text{for all } i\in I_0.$$

We denote by $\overline{x\otimes_{GF(2^r)}y}$, or sometimes simply by $x\otimes_c y$, the image $x\otimes_{GF(2^r)}y+W_c$ of a vector $x\otimes_{GF(2^r)}y\in V_2\otimes_{GF(2^r)}V_2$ under the canonical projection of $V_2\otimes_{GF(2^r)}V_2$ onto $(V_2\otimes_{GF(2^r)}V_2)/W_c$. (If we consider the image of the tensor products of x and y above over several different fields, such as extension fields of $GF(2^r)$ or subfields of $GF(2^r)$, we have to use the former symbol to distinguish them.) Notice that $x\otimes_c e_0=e_0\otimes_c x=(cx)\otimes_c x=x\otimes_c(cx)$ for any $x\in V_1$ and $e_0\otimes_c e_0=0$ in $(V_2\otimes_{GF(2^r)}V_2)/W_c$.

Let us define $W_s\subset V_1\otimes_{GF(2^r)}V_1$ as a $GF(2^r)$-vector subspace generated by $e_i\otimes_{GF(2^r)}e_j-e_j\otimes_{GF(2^r)}e_i$ for $1\leq i<j\leq l$. By the universal property of the tensor product there exists a $GF(2^r)$-linear mapping $i:V_1\otimes V_1\to V_2\otimes V_2$ with $i(x\otimes y)=x\otimes y$. Moreover if $\nu:V_2\otimes V_2\to(V_2\otimes V_2)/W_c$ is the natural surjection, then νi has the kernel W_s, thus we have Fact 1.

Fact 1 (*Lemma 5 of [9]*)**.** $(V_1\otimes_{GF(2^r)}V_1)/W_s=(V_2\otimes_{GF(2^r)}V_2)/W_c$.

We call $(V_1\otimes_{GF(2^r)}V_1)/W_s$ *the symmetric tensor space* of V_1 over $GF(2^r)$, and denote it by $Sym(V_1\otimes_{GF(2^r)}V_1)$. In this note, we sometimes use the following proposition.

Proposition 2. *Let $L\in GL(V_1,2)$ such that $\overline{(xL)\otimes_{GF(2^r)}y}=\overline{x\otimes_{GF(2^r)}(yL)}$ for any $x,y\in V_1$, then $xL=ax$ for some $a\in GF(2^r)\setminus\{0\}$ and for any $x\in V_1$.*

Proof. Let $B:=\{e_i\mid i\in I_0\}$ be a basis of V_1 over $GF(2^r)$. Then $\{\overline{e_i\otimes_{GF(2^r)}e_j}\mid 1\leq i\leq j\leq l\}$ is a basis of $Sym(V_1\otimes_{GF(2^r)}V_1)$ as a $GF(2^r)$-vector space. By assumption, we have $\overline{e_i\otimes_{GF(2^r)}e_i}=\overline{(e_iL^{-1})\otimes_{GF(2^r)}(e_iL)}$ for $1\leq i\leq l$. Let $e_iL^{-1}=\sum x_se_s$ and $e_iL=\sum y_te_t$ with $x_s,y_t\in GF(2^r)$ for $1\leq s,t\leq l$. Then $\overline{e_i\otimes_{GF(2^r)}e_i}=(x_iy_i)\overline{e_i\otimes_{GF(2^r)}e_i}+\sum_{s\neq i}(x_sy_s)\overline{e_s\otimes_{GF(2^r)}e_s}+\sum_{s<t}(x_sy_t+x_ty_s)\overline{e_s\otimes_{GF(2^r)}e_t}$. Hence $x_iy_i=1$, $x_sy_s=0$ for any $s\neq i$ and $x_sy_t+x_ty_s=0$ for any $s\neq t$. If $x_s=0$ and $y_s\neq 0$ for some $s\neq i$, then we have $x_t=0$ for any $t\neq s$ as $x_sy_t+x_ty_s=0$ for any $s\neq t$, which contradicts to $x_i\neq 0$. Thus we have $x_s=0$ and $y_s=0$ for any $s\neq i$. Therefore, there exist $a_i\in GF(2^r)\setminus\{0\}$ such that $e_iL^{-1}=a_i^{-1}e_i$ and $e_iL=a_ie_i$ for any $e_i\in B$. Next, since $\overline{e_i\otimes_{GF(2^r)}e_j}=\overline{(e_iL^{-1})\otimes_{GF(2^r)}(e_jL)}=\overline{(a_i^{-1}e_i)\otimes_{GF(2^r)}(a_je_j)}=(a_i^{-1}a_j)\overline{e_i\otimes_{GF(2^r)}e_j}$ for $1\leq i<j\leq l$, we must have $a_i=a_j$ for $1\leq i<j\leq l$. Let us put $a:=a_i$. Then we have $e_iL=ae_i$ for any $e_i\in B$. Since $\overline{(\alpha e_i)L\otimes_{GF(2^r)}e_j}=\overline{(\alpha e_i)\otimes_{GF(2^r)}(e_jL)}=\overline{(a\alpha e_i)\otimes_{GF(2^r)}e_j}$ for $\alpha\in GF(2^r)$ and for $1\leq i,j\leq l$, we have $(\alpha e_i)L=a\alpha e_i$ for $e_i\in B$. As $V_1=GF(2^r)e_1+\cdots+GF(2^r)e_l$ as a $GF(2)$-space, the assertions follow. □

We also use the following fact in this note for several times.

Fact 3 (*Proposition 11 of [9]*)**.** *For non-zero $x,y\in V$, we have $x\otimes_c y=0$ if and only if $x=cy+e_0\notin V_1$ in case $y\in V_1$, $x=c^{-1}(y+e_0)\in V_1$ in case $y\notin V_1$ with $y\neq e_0$, and $x=e_0$ in case $y=e_0$.*

We set $d:=rl$. We regard $Sym(V_1\otimes_{GF(2^r)}V_1)$ as a $GF(2)$-vector space of rank $((1/r)d^2+d)/2$. Inside $V(((1/r)d^2+3d+2)/2,2):=V\oplus(V_2\otimes V_2)/W_c=V\oplus Sym(V_1\otimes_{GF(2^r)}V_1)$, for each $t\in V$, define a subspace $X(t)$ of rank $d+1$ by

$$X(t):=\{(x,x\otimes_c t)\mid x\in V\}.$$

Let us define $\mathcal{S}_c(l,GF(2^r)):=\{X(t)\mid t\in V\}$.