

page 1 / 15

go back

full screen

close

quit

# New quotients of the $d$ -dimensional Veronesean dual hyperoval in $\text{PG}(2d + 1, 2)$

Hiroaki Taniguchi

Satoshi Yoshiara

## Abstract

Let  $d \geq 3$ . For each  $e \geq 1$ , Thas and Van Maldeghem constructed a  $d$ -dimensional dual hyperoval in  $\text{PG}(d(d+3)/2, q)$  with  $q = 2^e$ , called the Veronesean dual hyperoval [5]. A quotient of the Veronesean dual hyperoval with ambient space  $\text{PG}(2d+1, q)$ , denoted  $S_\sigma$ , is constructed in [3] and [4], using a generator  $\sigma$  of the Galois group  $\text{Gal}(\text{GF}(q^{d+1})/\text{GF}(q))$ .

In this note, using the above generator  $\sigma$  for  $q = 2$  and a  $d$ -dimensional vector subspace  $H$  of  $\text{GF}(2^{d+1})$  over  $\text{GF}(2)$ , we construct a quotient  $S_{\sigma, H}$  of the Veronesean dual hyperoval in  $\text{PG}(2d+1, 2)$  in case  $d$  is even. Moreover, we prove the following: for generators  $\sigma$  and  $\tau$  of the Galois group  $\text{Gal}(\text{GF}(2^{d+1})/\text{GF}(2))$ ,

- (1)  $S_\sigma$  above (for  $q = 2$ ) is not isomorphic to  $S_{\tau, H}$ ,
- (2)  $S_{\sigma, H}$  is isomorphic to  $S_{\sigma, H'}$  for any  $d$ -dimensional vector subspaces  $H$  and  $H'$  of  $\text{GF}(2^{d+1})$ , and
- (3)  $S_{\sigma, H}$  is isomorphic to  $S_{\tau, H}$  if and only if  $\sigma = \tau$  or  $\sigma = \tau^{-1}$ .

Hence, we construct many new non-isomorphic quotients of the Veronesean dual hyperoval in  $\text{PG}(2d+1, 2)$ .

Keywords: dual hyperoval, Veronesean, quotient

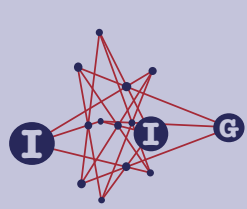
MSC 2000: 05Bxx, 05Exx, 51Exx

## 1. Introduction

Let  $m$  and  $d$  be integers with  $m > d \geq 2$ . For a prime power  $q$ , we denote by  $\text{PG}(m, q)$  an  $m$ -dimensional projective space over a finite field  $\text{GF}(q)$  with  $q$  elements. For a subset  $W$  of  $\text{GF}(q)$ , we denote the set of non-zero elements of  $W$  by  $W^\times$ .

ACADEMIA  
PRESS





page 2 / 15

go back

full screen

close

quit

Throughout this note, we use the letter  $K$  to denote  $\text{GF}(2^{d+1})$ . We regard  $K$  and  $K \times K = \{(x, y) \mid x, y \in K\}$  as vector spaces over  $\text{GF}(2)$  of dimension  $d + 1$  and  $2(d + 1)$  respectively. We sometimes identify  $(K \times K) \setminus \{(0, 0)\}$  with  $\text{PG}(2d + 1, 2)$ , regarding nonzero vectors of  $K \times K$  as projective points of  $\text{PG}(2d + 1, 2)$ .

The Galois group and the trace function for the extension  $K/\text{GF}(2)$  are denoted by  $\text{Gal}(K)$  and  $\text{Tr}$ , respectively, for short.

A family  $S$  of  $d$ -dimensional subspaces of  $\text{PG}(m, 2)$  is called a *d-dimensional dual hyperoval* in  $\text{PG}(m, 2)$  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 trivially,
- (D3) the union of the members of  $S$  generates  $\text{PG}(m, 2)$ , and
- (D4) there are exactly  $2^{d+1}$  members of  $S$ .

The definition of higher dimensional dual hyperovals was first given by C. Huybrechts and A. Pasini in [2]. The space  $\text{PG}(m, 2)$  in (D3) above is called the *ambient space* of the dual hyperoval  $S$ . For  $d$ -dimensional dual hyperovals  $S_1$  and  $S_2$  in  $\text{PG}(m, 2)$ , we say that  $S_1$  is isomorphic to  $S_2$  by a mapping  $\Phi$ , if  $\Phi$  is a linear automorphism of  $\text{PG}(m, 2)$  which sends the members of  $S_1$  onto the members of  $S_2$ .

In case  $d = 2$ ,  $d$ -dimensional dual hyperovals over  $\text{GF}(2)$  are completely classified by Del Fra [1]. Hence, in this note, we assume that  $d \geq 3$ . We shall prove the following three theorems:

**Theorem 1.1.** *Let  $\sigma$  be a generator of the Galois group  $\text{Gal}(K)$ , and let  $H := \{x \mid \text{Tr}(hx) = 0\}$  be a hyperplane of  $K$  for some  $h \in K^\times$ . For  $s, t \in K$ , define a vector  $b(s, t)$  of  $K \times K$  by*

$$b(s, t) := (\text{Tr}(ht)s^2 + st + \text{Tr}(hs)t^2, s^\sigma t + st^\sigma).$$

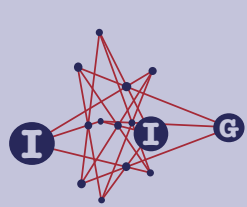
*Then, if  $d$  is even, the collection  $S_{\sigma, H}$  of subsets  $X(s) := \{b(s, t) \mid t \in K^\times\}$  of  $\text{PG}(2d + 1, 2) = (K \times K) \setminus \{(0, 0)\}$  for  $s \in K^\times$  together with the subset  $X(\infty) := \{b(s, s) \mid s \in K^\times\}$  of  $\text{PG}(2d + 1, 2)$  is a  $d$ -dimensional dual hyperoval in  $\text{PG}(2d + 1, 2)$ .*

**Theorem 1.2.** *The dual hyperoval  $S_{\sigma, H}$  in  $\text{PG}(2d + 1, 2)$  with  $d$  even is a quotient of the Veronesean dual hyperoval in  $\text{PG}(d(d + 3)/2, 2)$ .*

In [3], for every  $q = 2^e$  the first author constructed a quotient  $S_\sigma$  of the Veronesean dual hyperoval with ambient space  $\text{PG}(2d + 1, q)$  using a generator  $\sigma$  of the Galois group  $\text{Gal}(\text{GF}(q^{d+1})/\text{GF}(q))$  (see Example 2.3 of this note in case

ACADEMIA  
PRESS





page 3 / 15

go back

full screen

close

quit

$q = 2$ ). The following theorem shows that  $S_{\tau,H}$  is not isomorphic to  $S_\sigma$  for any generator  $\tau$  of  $\text{Gal}(K)$  and any hyperplane  $H$ , hence  $S_{\tau,H}$  is a new quotient of the Veronesean dual hyperoval with ambient space  $\text{PG}(2d + 1, 2)$ .

**Theorem 1.3.** Assume that  $d$  is even. Let  $\sigma$  and  $\tau$  be generators of  $\text{Gal}(K)$ , and let  $H$  and  $H'$  be hyperplanes of  $K$ . Then

- (1) The quotient  $S_\sigma$  is not isomorphic to  $S_{\tau,H}$ ,
- (2)  $S_{\sigma,H}$  is isomorphic to  $S_{\sigma,H'}$ , and
- (3)  $S_{\sigma,H}$  is isomorphic to  $S_{\tau,H}$  if and only if  $\sigma = \tau$  or  $\sigma = \tau^{-1}$ .

## 2. The construction of $S_{\sigma,H}$

We review a general construction of  $d$ -dimensional dual hyperovals in projective spaces over  $\text{GF}(2)$ .

Let  $n \geq d + 1$ . We regard  $\text{GF}(2^n)$  and  $\text{GF}(2^n) \times \text{GF}(2^n) = \{(x, y) \mid x, y \in \text{GF}(2^n)\}$  as  $n$  and  $2n$ -dimensional vector spaces over  $\text{GF}(2)$  respectively. Take a subspace  $W$  of  $\text{GF}(2^n)$  of dimension  $d + 1$ . Assume that a collection of vectors  $b(s, t) \in \text{GF}(2^n) \times \text{GF}(2^n)$  for  $s, t \in W^\times$  satisfies the following conditions:

- (B1)  $b(s, s) = (s^2, 0)$  for each  $s \in W^\times$ ,
- (B2)  $b(s, t) = b(t, s)$  for any  $s, t \in W^\times$ ,
- (B3)  $b(s, t) \neq (0, 0)$  for any  $s, t \in W^\times$ ,
- (B4) for  $s, t, s', t' \in W^\times$ , we have  $b(s, t) = b(s', t')$  if and only if  $\{s, t\} = \{s', t'\}$ ,
- (B5) for each  $s \in W^\times$ , the subset  $\{b(s, t) \mid t \in W^\times\} \cup \{(0, 0)\}$  is a subspace of  $\text{GF}(2^n) \times \text{GF}(2^n)$ .

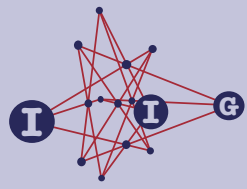
Then we can construct a dual hyperoval  $S$  in the following manner, although the dimension of its ambient space is not determined in general.

**Proposition 2.1.** Assume that  $b(s, t)$  ( $s, t \in W^\times$ ) satisfy the above conditions (B1)–(B5). Inside  $\text{PG}(2n - 1, 2) = (\text{GF}(2^n) \times \text{GF}(2^n)) \setminus \{(0, 0)\}$ , let us define subsets  $X(s) := \{b(s, t) \mid t \in W^\times\}$  for  $s \in W^\times$ , and  $X(\infty) := \{b(s, s) \mid s \in W^\times\}$ . Then,  $X(s)$  and  $X(\infty)$  are  $d$ -dimensional subspaces of  $\text{PG}(2n - 1, 2)$ , and  $S := \{X(s) \mid s \in W^\times\} \cup \{X(\infty)\}$  is a  $d$ -dimensional dual hyperoval.

*Proof.* By (B3), (B4) and (B5), the subset  $X(s)$  is a  $d$ -dimensional subspace of  $\text{PG}(2n - 1, 2)$  for each  $s \in W^\times$ . By (B1), the subset  $X(\infty)$  is a  $d$ -dimensional subspace of  $\text{PG}(2n - 1, 2)$ . For distinct  $s, t \in W^\times$ , we have  $X(s) \cap X(t) = b(s, t)$  by (B2), (B3) and (B4). For  $s \in W^\times$ ,  $X(s) \cap X(\infty) = b(s, s)$  by (B1), (B3) and (B4). From these facts, no three mutually distinct members of  $S$  have a common

ACADEMIA  
PRESS





page 4 / 15

go back

full screen

close

quit

point. The cardinality  $|S|$  is equal to  $|\{X(s) \mid s \in W^\times\}| + |\{X(\infty)\}| = 2^{d+1}$ . Hence  $S$  is a  $d$ -dimensional dual hyperoval.  $\square$

**Example 2.2.** Let  $e_i$  ( $i = 0, \dots, d$ ) be linearly independent vectors of  $\text{GF}(2^n)$ . Choosing  $n$  to be sufficiently large, we may assume that the products  $e_i e_j$  ( $0 \leq i \leq j \leq d$ ) are linearly independent vectors of  $\text{GF}(2^n)$ . Fix a generator  $\sigma$  of the Galois group  $\text{Gal}(\text{GF}(2^n)/\text{GF}(2))$ . Then the vector subspace  $W$  of  $\text{GF}(2^n)$  (resp.  $R$  of  $\text{GF}(2^n) \times \text{GF}(2^n)$ ) generated by  $e_i$  ( $i = 0, \dots, d$ ) (resp.  $(e_i e_j, e_i^\sigma e_j^\sigma + e_i e_j^\sigma)$  ( $0 \leq i \leq j \leq d$ )) is of dimension  $(d+1)$  (resp.  $(d+1)(d+2)/2$ ). We define  $b(s, t)$  for  $s, t \in W$  by

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

Then  $b(s, t)$  for  $s, t \in K^\times$  satisfy the conditions (B1)–(B5), and hence we have a  $d$ -dimensional dual hyperoval  $S$  in  $\text{PG}(d(d+3)/2, 2) = \text{PG}(R)$ . See [3] and [7]. Yoshiara [7] proved that this  $S$  is isomorphic to the Veronesean dual hyperoval constructed by Thas and Van Maldeghem in [5]. We note that the  $b(s, t)$ 's satisfy the addition formula  $b(s, t_1) + b(s, t_2) = b(s, t_1 + t_2)$  for any  $s, t_1, t_2 \in W$ .

**Example 2.3.** Let  $\sigma$  be a generator of the Galois group  $\text{Gal}(K)$ . In  $K \times K$ , let us define  $b(s, t)$  for  $s, t \in K$  to be

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

Then,  $b(s, t)$  for  $s, t \in K^\times$  satisfy the above conditions (B1)–(B5), and hence we have a  $d$ -dimensional dual hyperoval, denoted by  $S_\sigma$ , in  $\text{PG}(2d+1, 2)$ . See [3] and [7]. Yoshiara [7] proved that this  $S_\sigma$  is a quotient of the Veronesean dual hyperoval in  $\text{PG}(d(d+3)/2, 2)$ . The vectors  $b(s, t)$  also satisfy the addition formula  $b(s, t_1) + b(s, t_2) = b(s, t_1 + t_2)$  for  $s, t_1, t_2 \in K$ .

### The proof of Theorem 1.1

In the rest of this section, we will establish Theorem 1.1, exploiting Proposition 2.1. Namely, we shall verify that the following vectors  $b(s, t)$  of  $K \times K$  for  $s, t \in K$  satisfy the conditions (B1)–(B5):

$$b(s, t) := (\text{Tr}(ht)s^2 + st + \text{Tr}(hs)t^2, s^\sigma t + st^\sigma), \quad (1)$$

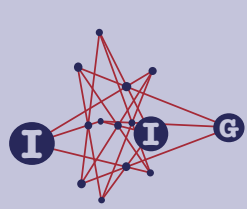
where  $h$  is a fixed nonzero element of  $K$  and  $\sigma$  is a generator of the Galois group  $\text{Gal}(K)$ . From definition (1), it is easy to see that  $b(s, t) = (0, 0)$  if  $s = 0$  or  $t = 0$ , and that the following addition formula holds: for any  $s, t_1, t_2 \in K$ , we have

$$b(s, t_1) + b(s, t_2) = b(s, t_1 + t_2). \quad (2)$$

It is easy to verify the conditions (B1)–(B5), other than (B4). As for (B1), we have  $b(s, s) = (\text{Tr}(hs)s^2 + s^2 + \text{Tr}(hs)s^2, 0) = (s^2, 0)$ . The condition (B2) (even

ACADEMIA  
PRESS





page 5 / 15

go back

full screen

close

quit

when  $s = 0$  or  $t = 0$ ) is obviously satisfied in view of definition (1). As for (B3), if  $s = t \in K^\times$  then  $b(s, s) = (s^2, 0) \neq (0, 0)$  by (B1). On the other hand, if  $s \neq t$ , we have  $s^\sigma t + st^\sigma \neq 0$ , because 1 is the unique nonzero element of  $K$  fixed by a generator  $\sigma$  of the Galois group for  $K/\text{GF}(2)$ . As  $s^\sigma t + st^\sigma$  appears as the second component of  $b(s, t)$ , we conclude that  $b(s, t) \neq (0, 0)$  in this case as well. The condition (B5) follows from the addition formula (2).

In the rest of this section, we will verify (B4). For this purpose, take  $s, t, s', t' \in K^\times$  satisfying  $b(s, t) = b(s', t')$ . Our end is to show that  $\{s, t\} = \{s', t'\}$  under this assumption. We divide the cases according to the trace values  $\text{Tr}(hx)$  for  $x = s, t, s', t'$ .

We first consider the case where both  $(\text{Tr}(hs), \text{Tr}(ht))$  and  $(\text{Tr}(hs'), \text{Tr}(ht'))$  are not equal to  $(1, 1)$ . Exchanging  $s$  for  $t$  (and  $s'$  for  $t'$ ) if necessary, we may assume that  $\text{Tr}(hs) = \text{Tr}(hs') = 0$ . Then the first component of  $b(s, t)$  is  $\text{Tr}(ht)s^2 + st$  (see definition (1)), which is written as  $s_1 t_1$ , if we set  $s_1 := s$  and  $t_1 := \text{Tr}(ht)s + t$ . The second component of  $b(s, t)$  is  $s^\sigma t + st^\sigma$ , which is written as  $s_1^\sigma t_1 + s_1 t_1^\sigma$ . Similarly we have  $b(s', t') = (s_2 t_2, s_2^\sigma t_2 + s_2 t_2^\sigma)$ , where  $s_2 := s'$  and  $t_2 := \text{Tr}(ht')s' + t'$ . Notice that none of  $s_i, t_i$  ( $i = 1, 2$ ) is zero, because  $b(s_i, t_i) = b(s, t) \neq (0, 0)$  ( $i = 1, 2$ ) for  $s, t \in K^\times$  by (B3). Thus we may apply the following fact (see e.g. [3]), which is straightforward to verify, using the fact that 1 is the unique nonzero element of  $K^\times$  fixed by  $\sigma$ .

**Fact 2.4.** *Let  $s_1, t_1, s_2, t_2 \in K^\times$ . Then  $(s_1 t_1, s_1^\sigma t_1 + s_1 t_1^\sigma) = (s_2 t_2, s_2^\sigma t_2 + s_2 t_2^\sigma)$  if and only if  $\{s_1, t_1\} = \{s_2, t_2\}$ .*

Then we have either  $(s_2, t_2) = (s_1, t_1)$  or  $(s_2, t_2) = (t_1, s_1)$ . In the former case, we have  $s' = s$  and  $\text{Tr}(ht)s + t' = \text{Tr}(ht')s + t$ . From the latter equation, we have  $\text{Tr}(h(t+t'))s = t+t'$ . Taking the trace of the product of  $h$  with the last equation, we have  $0 = \text{Tr}(h(t+t')) \text{Tr}(hs) = \text{Tr}(\text{Tr}(h(t+t'))hs) = \text{Tr}(h(t+t'))$  as  $\text{Tr}(hs) = 0$ . Thus  $\text{Tr}(ht) = \text{Tr}(ht')$  and  $t' = t$ . In the latter case, we have  $s' = \text{Tr}(ht)s + t$  and  $s = \text{Tr}(ht')s' + t'$ . As  $\text{Tr}(hs) = \text{Tr}(hs') = 0$ , we have  $0 = \text{Tr}(ht) \text{Tr}(hs) + \text{Tr}(ht) = \text{Tr}(ht)$  by taking the trace of the product of  $h$  with the former equation. Similarly,  $0 = \text{Tr}(ht')$  from the latter equation. Thus we have  $s' = t$  and  $s = t'$ . We established  $\{s, t\} = \{s', t'\}$  in this case.

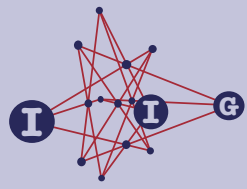
Hence we may assume that  $(\text{Tr}(hs), \text{Tr}(ht)) = (1, 1)$ , exchanging  $(s, t)$  for  $(s', t')$  if necessary. Then the following three cases for  $(\text{Tr}(hs'), \text{Tr}(ht'))$  are remained to verify, exchanging  $s'$  for  $t'$  if necessary.

$$(\text{Tr}(hs'), \text{Tr}(ht')) = (1, 1), (0, 0) \text{ or } (1, 0).$$

We will show that the first case is reduced to the case we already treated above. To see this, assume that  $\text{Tr}(hx) = 1$  for all  $x = s, t, s', t'$ . Adding  $b(s, s')$  to the equation  $b(s, t) = b(s', t')$ , we have  $b(s, t + s') = b(s', t' + s)$  from the addition

ACADEMIA  
PRESS





page 6 / 15

go back

full screen

close

quit

formula (2). If  $t + s' = 0$  or  $t' + s = 0$ , then we have  $(s', t') = (t, s)$  from this equation. Thus we may assume that none of  $s, t + s', s'$  and  $t' + s$  is zero. Now we have  $\text{Tr}(h(s)) = 1, \text{Tr}(h(s+t')) = 0, \text{Tr}(hs') = 1$  and  $\text{Tr}(h(s+t')) = 0$ . Thus it follows from the conclusion of the above paragraph that we have  $\{s, t + s'\} = \{s', t' + s\}$ . As  $t'$  is nonzero, we have  $(s', t') = (s, t)$ .

Similarly, we can reduce the second case above to the last case, by adding  $b(t, t')$  to  $b(s, t) = b(s', t')$ . In this case we have  $b(s + t', t) = b(s' + t, t')$  from the addition formula (2) with  $\text{Tr}(h(s + t')) = 1, \text{Tr}(ht) = 1, \text{Tr}(h(s' + t)) = 1$  and  $\text{Tr}(ht') = 0$ .

Thus the last case above is the unique remaining case, where we have  $b(s, t) = b(s', t')$  for  $s, t, s', t' \in K^\times$  with  $\text{Tr}(hs) = \text{Tr}(ht) = \text{Tr}(hs') = 1$  and  $\text{Tr}(ht') = 0$ . Notice that up to here we did not use the assumption that  $d$  is even.

This case requires some technical calculations. To avoid somewhat cumbersome notation such as  $s', t'$ , we replace the letters  $s, t, s', t'$  by  $u, ux, v$  and  $vy$  respectively. With this notation, it suffices to show the following claim to verify (B4), and hence to complete the proof of Theorem 1.1. (Notice that the ambient space of  $S_{\sigma, H}$  coincides with  $K \times K$ , as it contains  $X(\infty) = \{(s^2, 0) \mid s \in K\}$  and  $K$  is spanned by  $s^\sigma t + st^\sigma$  for  $s, t \in K$ ; see the arguments in Lemma 3.3.)

Assume that  $d$  is even. For  $u, x, v, y \in K^\times$  with  $\text{Tr}(hu) = \text{Tr}(hxy) = \text{Tr}(hv) = 1$  and  $\text{Tr}(hyv) = 0$ , we have  $b(u, xu) \neq b(v, yv)$ .

This is obtained as a direct corollary of the following lemma, where we do not put any restrictions on  $xu$  and  $yv$ .

**Lemma 2.5.** *Assume that  $d$  is even. If  $b(u, xu) = b(v, yv)$  for nonzero elements  $u, v, x$  and  $y$  of  $K$  with  $\text{Tr}(hu) = \text{Tr}(hv) = 1$ , then we have*

$$\text{Tr}(hxy) = \text{Tr}(hyv).$$

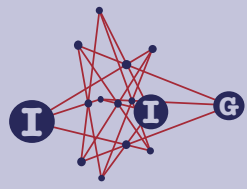
*Proof.* Assume  $b(u, xu) = b(v, yv)$  for  $u, v, x, y \in K^\times$  with  $\text{Tr}(hu) = \text{Tr}(hv) = 1$ . If  $u = v$ , then  $0 = b(u, xu) + b(u, yu) = b(u, (x + y)u)$  by equation (2), whence (B3) implies that  $(x + y)u = 0$  and  $x = y$ . Thus the lemma holds in this case. In the following, we assume that  $u \neq v$ .

From the definition of  $b(s, t)$ , the first and second components of  $b(u, xu) = b(v, yv)$  are respectively given by

$$a := \text{Tr}(hxy)u^2 + xu^2 + x^2u^2 = \text{Tr}(hyv)v^2 + yv^2 + y^2v^2 \quad \text{and} \\ c := x^\sigma u^\sigma u + xuu^\sigma = y^\sigma v^\sigma v + yvv^\sigma.$$

ACADEMIA  
PRESS





page 7 / 15

go back

full screen

close

quit

Thus  $a/u^2 = \text{Tr}(hxu) + x + x^2$ ,  $a/v^2 = \text{Tr}(hyv) + y + y^2$ ,  $c/u^{\sigma+1} = x^\sigma + x$ , and  $c/v^{\sigma+1} = y^\sigma + y$ . We easily have

$$c/u^{\sigma+1} + (c/u^{\sigma+1})^2 = a/u^2 + (a/u^2)^\sigma, \quad (3)$$

$$c/v^{\sigma+1} + (c/v^{\sigma+1})^2 = a/v^2 + (a/v^2)^\sigma, \quad (4)$$

since both sides of the equation coincide with  $x + x^2 + x^\sigma + x^{2\sigma}$  in (3), and  $y + y^2 + y^\sigma + y^{2\sigma}$  in (4). Let  $\alpha := u^{\sigma-1} + v^{\sigma-1}$  and  $\beta := u^{\sigma+1} + v^{\sigma+1}$ . Since  $d+1$  is odd and  $\sigma$  is a generator of the Galois group  $\text{Gal}(K)$ , we can verify that  $\alpha \neq 0$  and  $\beta \neq 0$  in  $\text{GF}(2^{d+1})$  in the following manner: Assume to the contrary that  $\alpha = 0$ , then from  $u^\sigma/u = v^\sigma/v$ , we have  $(u/v)^\sigma = (u/v)$ , which implies that  $u = v$ , contradicting our assumption that  $u \neq v$ . If  $\beta = 0$ , then from  $u^\sigma u = v^\sigma v$ , we have  $(u/v)^{-\sigma} = (u/v)$ , hence  $(u/v)^{\sigma^2} = (u/v)$ . Since  $d+1$  is odd,  $\sigma^2$  is a generator of the Galois group  $\text{Gal}(K)$ , hence we have  $u/v = 1$ , that is,  $u = v$ , which also contradicts our assumption that  $u \neq v$ .

Adding (3) times  $u^{2(\sigma+1)}$  and (4) times  $v^{2(\sigma+1)}$ , we have

$$c = [(u+v)^{2\sigma}/\beta]a + [(u+v)^2/\beta]a^\sigma. \quad (5)$$

Adding (3) times  $u^{2(\sigma+1)}v^{\sigma+1}$  and (4) times  $u^{\sigma+1}v^{2(\sigma+1)}$ , we have

$$c^2 = [(u^{\sigma+1}v^{\sigma+1}\alpha)/\beta]a + [(u^2v^2\alpha)/\beta]a^\sigma. \quad (6)$$

Eliminating  $c$  from (5) and (6), we have

$$(u+v)^4 a^{2\sigma} + (u+v)^{4\sigma} a^2 + \alpha\beta(u^{\sigma+1}v^{\sigma+1}a + u^2v^2a^\sigma) = 0. \quad (7)$$

Let us set  $g := u^{\sigma+1}v^{\sigma+1}a + u^2v^2a^\sigma$ . Then, from the defining equation of  $g$ , we have  $a^{2\sigma} = (u^{2(\sigma+1)}v^{2(\sigma+1)}/u^4v^4)a^2 + (1/u^4v^4)g^2$ . Using these  $g$  and  $a^{2\sigma}$ , we obtain from (7) that

$$(1/u + 1/v)^4 u^{2(\sigma+1)}v^{2(\sigma+1)}a^2 + (u+v)^{4\sigma}a^2 + (1/u + 1/v)^4 g^2 + \alpha\beta g = 0. \quad (8)$$

We easily check that  $(1/u + 1/v)^4 u^{2(\sigma+1)}v^{2(\sigma+1)}a^2 + (u+v)^{4\sigma}a^2 = (\alpha\beta)^2 a^2$ . Using this equation, we finally have from (8) that

$$(1/u + 1/v)^4 g^2 + \alpha\beta g = \alpha^2 \beta^2 a^2.$$

Now, multiplying both sides of the equation by  $(1/u + 1/v)^4 / (\alpha^2 \beta^2)$ , we have

$$[(1/u + 1/v)^8 / \alpha^2 \beta^2] g^2 + [(1/u + 1/v)^4 / \alpha\beta] g = (1/u + 1/v)^4 a^2.$$

Hence we have  $\text{Tr}((1/u + 1/v)^4 a^2) = 0$ , that is,  $\text{Tr}((1/u + 1/v)^2 a) = 0$ , or equivalently  $\text{Tr}(a/u^2) = \text{Tr}(a/v^2)$ . Here we have

$$\text{Tr}(a/u^2) = \text{Tr}(\text{Tr}(hxu) + x + x^2) = \text{Tr}(hxu) \text{Tr}(1) = \text{Tr}(hxu),$$

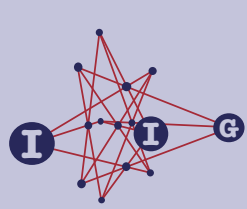
as  $\text{Tr}(1) = d+1$  is odd. Similarly we have

$$\text{Tr}(a/v^2) = \text{Tr}(\text{Tr}(hyv) + y + y^2) = \text{Tr}(hyv).$$

Thus Lemma 2.5 is established. □

ACADEMIA  
PRESS





### 3. Isomorphisms of some dual hyperovals

In this section, we study isomorphisms of the dimensional dual hyperovals constructed in Proposition 2.1, which satisfy the “addition formula” (equation (9)). We identify a nonzero vector of  $K \times K$  with the projective point of  $\text{PG}(K \times K) \cong \text{PG}(2d + 1, 2)$  spanned by it.

**Proposition 3.1.** *For  $i \in \{1, 2\}$ , let  $S_i = \{X_i(t) \mid t \in K^\times \cup \{\infty\}\}$  be the  $d$ -dimensional dual hyperoval inside  $\text{PG}(2d + 1, 2) \cong \text{PG}(K \times K)$  constructed in Proposition 2.1 from a collection  $\{b_i(s, t) \mid s, t \in K^\times\}$  of vectors of  $K \times K$  satisfying the conditions (B1)–(B5). Assume that  $\{b_i(s, t) \mid s, t \in K^\times\}$  satisfies the following equations for all  $s, t_1, t_2 \in K$ :*

$$b_i(s, t_1) + b_i(s, t_2) = b_i(s, t_1 + t_2). \quad (9)$$

(In particular,  $b_i(s, t) = 0$  if  $s = 0$  or  $t = 0$ .)

Assume now that  $S_1$  is isomorphic to  $S_2$  by a map  $\Phi$  on  $K \times K$ . Then there exists  $\text{GF}(2)$ -linear bijections  $F$  and  $L$  on  $K$  and a  $\text{GF}(2)$ -linear map  $G$  on  $K$  which satisfy the following:

- (a)  $\Phi(x, y) = (F(x) + G(y), L(y))$  for all  $x, y \in K$ ;
- (b)  $\Phi(X_1(\infty)) = X_2(\infty)$  and  $\Phi(X_1(s)) = X_2(\rho(s))$  for all  $s \in K^\times$ , where  $\rho$  is a bijection on  $K^\times$  given by  $\rho(s) = F(s^2)^{1/2}$ ;
- (c)  $\Phi(b_1(s, t)) = b_2(\rho(s), \rho(t))$  for all  $s, t \in K^\times$ .

*Proof.* By the construction given in Proposition 2.1,

$$\begin{aligned} X_i(s) &= \{b_i(s, t) \mid t \in K^\times\} \text{ for } s \in K^\times \text{ and} \\ X_i(\infty) &= \{b_i(t, t) \mid t \in K^\times\}. \end{aligned}$$

(Notice that we take  $d + 1$  and  $K \cong \text{GF}(2^{d+1})$  respectively as  $n$  and  $W$  in Proposition 2.1.) From the definition of an isomorphism of dimensional dual hyperovals, the map  $\Phi$  is a  $\text{GF}(2)$ -linear bijection on  $K \times K$  which induces a bijection from the members  $X_1(s)$  ( $s \in K^\times \cup \{\infty\}$ ) of  $S_1$  onto the members  $X_2(s)$  ( $s \in K^\times \cup \{\infty\}$ ) of  $S_2$ . Thus there exist  $\text{GF}(2)$ -linear maps  $F, G, M$  and  $L$  on  $K$  such that

$$\Phi(x, y) = (F(x) + G(y), M(x) + L(y)) \quad (10)$$

for all  $x, y \in K$ . Furthermore, there exists a bijection  $\rho$  on  $K^\times \cup \{\infty\}$  which satisfies the following equation for all  $t \in K^\times \cup \{\infty\}$ :

$$\Phi(X_1(t)) = X_2(\rho(t)). \quad (11)$$



page 8 / 15

go back

full screen

close

quit

ACADEMIA  
PRESS







page 9 / 15

go back

full screen

close

quit

Take any distinct elements  $s$  and  $t$  of  $K^\times \cup \{\infty\}$ . As  $S_1$  is a  $d$ -dimensional dual hyperoval,  $X_1(s) \cap X_1(t)$  is a projective point. This point is mapped by  $\Phi$  to a point contained in both  $\Phi(X_1(s)) = X_2(\rho(s))$  and  $\Phi(X_1(t)) = X_2(\rho(t))$ . As  $S_2$  is a  $d$ -dimensional dual hyperoval as well,  $X_2(\rho(s)) \cap X_2(\rho(t))$  is a projective point. Hence for any  $s, t \in K^\times \cup \{\infty\}$  with  $s \neq t$ , we have

$$\Phi(X_1(s) \cap X_1(t)) = X_2(\rho(s)) \cap X_2(\rho(t)). \quad (12)$$

For every distinct elements  $s, t$  in  $K^\times \setminus \{\rho^{-1}(\infty)\}$ , we have  $X_1(s) \cap X_1(t) = b_1(s, t)$  and  $X_2(\rho(s)) \cap X_2(\rho(t)) = b_2(\rho(s), \rho(t))$ . Thus equation (12) implies

$$\Phi(b_1(s, t)) = b_2(\rho(s), \rho(t)) \quad (13)$$

for every  $s, t \in K^\times \setminus \{\rho^{-1}(\infty)\}$  with  $s \neq t$ . If  $k := \rho^{-1}(\infty)$  lies in  $K^\times$ , then  $X_1(k) \cap X_1(t) = b_1(k, t)$  and  $X_2(\rho(k)) \cap X_2(\rho(t)) = X_2(\infty) \cap X_2(\rho(t)) = b_2(\rho(t), \rho(t))$  for any  $t \in K^\times \setminus \{k\}$ . Thus it follows from equation (12) that

$$\Phi(b_1(k, t)) = b_2(\rho(t), \rho(t)) \quad (14)$$

for any  $t \in K^\times \setminus \{\rho^{-1}(\infty)\}$ , if  $\rho^{-1}(\infty) \in K^\times$ .

Next we shall show that  $\rho(\infty) = \infty$ . We will derive a contradiction, assuming that  $\rho^{-1}(\infty) =: k$  lies in  $K^\times$ . Notice that  $|K^\times \setminus \{k\}| = 2^{d+1} - 2 \geq 6$ , as  $d + 1 \geq 3$ . Fix an element  $s$  of  $K^\times \setminus \{k\}$ , and take an arbitrary element  $t$  in  $K^\times \setminus \{k, s, s+k\}$ . By the assumption (9) with  $i = 1$ , we have  $b_1(t, k) + b_1(t, s) = b_1(t, k+s)$ . Applying the linear map  $\Phi$  to both sides of this equation, we obtain  $\Phi(b_1(t, k)) + \Phi(b_1(t, s)) = \Phi(b_1(t, k+s))$ . As  $t, s$  and  $k+s$  are mutually distinct elements of  $K^\times \setminus \{k\}$ , we have  $\Phi(b_1(t, s)) = b_2(\rho(t), \rho(s))$  and  $\Phi(b_1(t, k+s)) = b_2(\rho(t), \rho(k+s))$  by equation (13). On the other hand,  $\Phi(b_1(t, k)) = b_2(\rho(t), \rho(t))$  by equation (14). Hence we obtain

$$b_2(\rho(t), \rho(t)) + b_2(\rho(t), \rho(s)) = b_2(\rho(t), \rho(k+s)).$$

Then the assumption (9) with  $i = 2$  yields  $b_2(\rho(t), \rho(s) + \rho(t) + \rho(k+s)) = 0$ . As  $\rho(t) \neq 0$ , this implies

$$\rho(s) + \rho(t) + \rho(k+s) = 0.$$

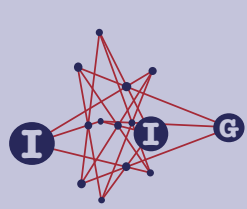
Notice that this equation holds for any  $t$  in  $K^\times \setminus \{k, s, k+s\}$ . Thus we have  $\rho(t_1) = \rho(t_2) = \rho(s) + \rho(s+k)$  for any elements  $t_1, t_2$  of  $K^\times \setminus \{k, s, k+s\}$ . As  $K^\times \setminus \{k, s, k+s\}$  contains  $2^{d+1} - 4 \geq 2$  elements, this contradicts the bijectivity of  $\rho$ . Hence we established that  $\rho(\infty) = \infty$ .

It is now easy to verify the proposition. The claim (c) follows from equation (13), as  $K^\times = K^\times \setminus \{\rho^{-1}(\infty)\}$ . We also have  $\Phi(X_1(\infty)) = X_2(\rho(\infty)) = X_2(\infty)$ . Thus equation (12) implies that

$$\Phi((s^2, 0)) = \Phi(X_1(\infty) \cap X_1(s)) = X_2(\infty) \cap X_2(\rho(s)) = (\rho(s)^2, 0)$$

ACADEMIA  
PRESS





page 10 / 15

go back

full screen

close

quit

for all  $s \in K^\times$ . Then it follows from equation (10) applied to  $x = s^2$  and  $y = 0$  that for any  $s \in K^\times$  we have

$$F(s^2) = \rho(s)^2 \text{ and } M(s^2) = 0.$$

The claim (b) follows from the former equation above and the definition of  $\rho$  and the fact that  $\rho(\infty) = \infty$ . The latter equation above implies that  $M$  is the zero map. It follows from equation (10) that  $\Phi(x, y) = (F(x) + G(y), L(y))$  for all  $x, y \in K$ . As  $\Phi$  is a bijection, this implies that  $F$  and  $L$  are bijections on  $K$ . Thus the claim (a) is established.  $\square$

Notice that both  $S_1 = S_\sigma$  in Example 2.3 and  $S_2 = S_{\sigma, H}$  in Theorem 1.1 are  $d$ -dimensional dual hyperovals in  $\text{PG}(K \times K) = \text{PG}(2d + 1, 2)$  satisfying equation (9). To examine isomorphisms among these dimensional dual hyperovals, the following proposition turns out to be useful. It is worthwhile mentioning that this proposition about  $\text{GF}(2)$ -linear maps can be established using dimensional dual hyperovals.

**Proposition 3.2.** *Let  $L$  and  $\rho$  be  $\text{GF}(2)$ -linear bijections on  $K$ . Assume that there exist generators  $\sigma$  and  $\tau$  of the Galois group  $\text{Gal}(K)$  which satisfy*

$$L(s^\sigma t + st^\sigma) = \rho(s)^\tau \rho(t) + \rho(s)\rho(t)^\tau \quad (15)$$

for all  $s, t \in K^\times$ . Then we have  $\tau = \sigma$  or  $\tau = \sigma^{-1}$ . Moreover, there exists  $\mu \in \text{Gal}(K)$  and  $b \in K^\times$  such that  $\rho(x) = bx^\mu$  for all  $x \in K$ .

*Proof.* First note that equation (15) holds even in cases  $s = 0$  or  $t = 0$ , since  $L$  and  $\rho$  are linear. For  $\alpha = \sigma$  or  $\tau$ , we define  $\mathcal{S}_\alpha$  to be a collection  $\{X_\alpha(t) \mid t \in K\}$  of subsets  $X_\alpha(t) := \{(x, x^\alpha t + xt^\alpha) \mid x \in K\}$  of  $K \times K$  for  $t \in K$ . By [6],  $\mathcal{S}_\sigma$  and  $\mathcal{S}_\tau$  are  $d$ -dimensional dual hyperovals. Define a  $\text{GF}(2)$ -linear bijection  $\Phi$  on  $K \times K$  by

$$\Phi(x, y) = (\rho(x), L(y)).$$

From the assumption (equation (15)), we have

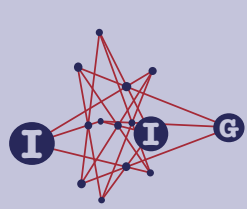
$$(x, x^\sigma t + xt^\sigma)^\Phi = (\rho(x), \rho(x)^\tau \rho(t) + \rho(x)\rho(t)^\tau) \in X_2(\rho(t)).$$

Thus  $\Phi$  sends each  $X_\sigma(t)$  to  $X_\tau(\rho(t))$  ( $t \in K$ ), whence it gives an isomorphism from  $\mathcal{S}_\sigma$  to  $\mathcal{S}_\tau$ . Then, by [6, Proposition 11], we must have  $\sigma = \tau$  or  $\sigma = \tau^{-1}$ .

Now, if  $\tau = \sigma$ , then  $\mathcal{S}_\sigma = \mathcal{S}_\tau$  and  $\Phi$  is an automorphism of  $\mathcal{S}_\sigma$  stabilizing a  $d$ -subspace  $X_\sigma(0) = X_\tau(0) = \{(x, 0) \mid x \in K^\times\}$ . Recall that the stabilizer of  $X_\sigma(0)$  in  $\text{Aut}(\mathcal{S}_\sigma)$  is generated by the field automorphisms  $\tilde{\mu}: (x, y) \mapsto (x^\mu, y^\mu)$  for  $\mu \in \text{Gal}(K)$  and the multiplications  $m(b): (x, y) \mapsto (bx, b^{\sigma+1}y)$  for

ACADEMIA  
PRESS





page 11 / 15

go back

full screen

close

quit

$b \in K^\times$ . (See [6, Proposition 7]. The explicit shapes of  $\tilde{\mu}$  and  $m(b)$  are given in [6, Section 4]). Hence we have  $\rho(x) = bx^\mu$  for some  $\mu \in \text{Gal}(K)$  and  $b \in K^\times$ .

If  $\tau = \sigma^{-1}$ , then  $\mathcal{S}_\tau$  is isomorphic to  $\mathcal{S}_\sigma$  by  $\Psi_\sigma: (x, y) \mapsto (x, y^\sigma)$ , since

$$\Psi_\sigma(X_\tau(t)) := \{(x, (x^{\sigma^{-1}}t + xt^{\sigma^{-1}})^\sigma)\} = \{(x, x^\sigma t + xt^\sigma)\} = X_\sigma(t).$$

Hence  $\Psi_\sigma \circ \Phi: (x, y) \mapsto (\rho(x), L(y)^\sigma)$  is an automorphism of  $\mathcal{S}_\sigma$  which stabilizes the  $d$ -subspace  $X_\sigma(0)$ . Then, by the conclusion in the above paragraph, we have  $\rho(x) = bx^\mu$  for some  $\mu \in \text{Gal}(K)$  and  $b \in K^\times$  in this case as well.  $\square$

The next lemma will be used in the proof of Theorem 1.3(1).

**Lemma 3.3.** *For a hyperplane  $H_1$  of  $K \cong \text{GF}(2^{d+1})$  with  $d \geq 4$  and a generator  $\sigma$  of the Galois group  $\text{Gal}(K)$ , the subset  $\{s^\sigma t + st^\sigma \mid s, t \in H_1\}$  spans  $K$  as a vector space over  $\text{GF}(2)$ .*

*Proof.* Take  $\alpha \in K^\times$  with  $H_1 = \{x \in K \mid \text{Tr}(\alpha x) = 0\}$ . Assume on the contrary that  $X := \{s^\sigma t + st^\sigma \mid s, t \in H_1\}$  spans a proper subspace of  $K$ . Then  $X$  is contained in a hyperplane of  $K$ , and hence there is some  $\beta \in K^\times$  such that  $X \subset \{x \in K \mid \text{Tr}(\beta x) = 0\}$ . We have

$$0 = \text{Tr}(\beta(s^\sigma t + st^\sigma)) = \text{Tr}((\beta s^\sigma + \beta^{\sigma^{-1}} s^{\sigma^{-1}})t)$$

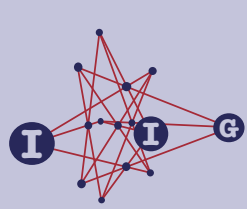
for all  $t \in H_1$ . Thus  $\beta s^\sigma + \beta^{\sigma^{-1}} s^{\sigma^{-1}} = \varepsilon(s)\alpha$  for an element  $\varepsilon(s)$  in  $\text{GF}(2)$  depending on  $s \in H_1$ . Then there exists a hyperplane  $K_1$  of  $H_1$  such that  $\beta s^\sigma + \beta^{\sigma^{-1}} s^{\sigma^{-1}} = 0$  for all  $s \in K_1$ . The last equation for  $s \in K_1^\times$  is equivalent to the condition that  $s^{\sigma^2-1} = \beta^{1-\sigma}$ , which is equivalent to  $s^{\sigma+1} = \beta^{-1}$ , because  $\sigma - 1$  is bijective on  $K^\times$  for a generator  $\sigma$  of  $\text{Gal}(K)$ . As this holds for every  $s \in K_1^\times$ , fixing an element  $t \in K_1^\times$ , we have  $(s/t)^{\sigma+1} = \beta^{-1}/\beta^{-1} = 1$  for every  $s \in K_1^\times$ . Then  $\sigma^2$  fixes  $s/t$  for every  $s \in K_1$ . Since  $\sigma$  is a generator of  $\text{Gal}(K)$ , the subfield  $L := \{x \in K \mid x^{\sigma^2} = x\}$  is a subfield of  $\text{GF}(2^2)$ . Thus we conclude that  $2^{d-1} = |\{s/t \mid s \in K_1\}| \leq |L| \leq 4$ , which contradicts the fact that  $d \geq 4$ .  $\square$

## 4. $\mathcal{S}_{\sigma, H}$ is a new quotient

In this section, we prove Theorem 1.2 and Theorem 1.3.

*Proof of Theorem 1.2.* The Veronesean dual hyperoval is isomorphic to the dual hyperoval  $S$  in Example 2.2 by [7]. Thus we take the latter as a model of the Veronesean dual hyperoval, and denote it by  $S_V$ . As in Example 2.2,  $W$  denotes





page 12 / 15

go back

full screen

close

quit

a  $(d + 1)$ -dimensional vector subspace of  $\text{GF}(2^n)$  for sufficiently large  $n$  with a basis  $\{e_0, e_1, \dots, e_d\}$  such that  $\{e_i e_j \mid 0 \leq i \leq j \leq d\}$  are linearly independent. Moreover,  $R$  denotes the vector subspace of  $\text{GF}(2^n) \times \text{GF}(2^n)$  spanned by  $(e_i e_j, e_i^\sigma e_j + e_i e_j^\sigma)$  for  $1 \leq i \leq j \leq n$ . Then  $\text{PG}(R) = \text{PG}(d(d + 3)/2, 2)$  is the ambient space of  $S_V$ .

To distinguish  $S_V$  from  $S_{\sigma, H}$ , we denote  $b(s, t)$  in Example 2.2 by  $b_V(s, t)$ ; namely  $b_V(s, t) = (st, s^\sigma t + st^\sigma)$  for  $s, t \in W$ . Thus  $S_V$  is constructed from  $\{b_V(s, t) \mid s, t \in W^\times\}$  by the method in Proposition 2.1; namely,  $S_V$  is a collection of subspaces  $X_V(t)$  for  $t \in W^\times \cup \{\infty\}$ , where  $X_V(t) := \{b_V(s, t) \mid s \in W^\times\}$  ( $t \in W^\times$ ) and  $X_V(\infty) := \{b_V(s, s) \mid s \in W^\times\}$ . We recall that  $\{b_V(s, t)\}$  satisfies the addition formula (equation (9)):  $b_V(s, t_1) + b_V(s, t_2) = b_V(s, t_1 + t_2)$  for  $s, t_1, t_2 \in W$ .

Choose a basis  $\{\bar{e}_0, \dots, \bar{e}_d\}$  for  $K$  over  $\text{GF}(2)$ . To distinguish  $S_{\sigma, H}$  from  $S_V$ , we denote  $b(s, t)$  in Theorem 1.1 by  $b_H(s, t)$ ; namely

$$b_H(s, t) = (\text{Tr}(hs)t^2 + st + \text{Tr}(ht)s^2, s^\sigma t + st^\sigma).$$

We denote by  $X_H(t)$  for  $t \in K^\times$  (resp.  $X_H(\infty)$ ) the subspace  $\{b_H(s, t) \mid s \in K^\times\}$  (resp.  $\{b_H(s, s) \mid s \in K^\times\}$ ). Then  $S_{\sigma, H} = \{X_H(t) \mid t \in K^\times \cup \{\infty\}\}$ . We recall that  $\{b_H(s, t)\}$  satisfies the addition formula (equation (9)):  $b_H(s, t_1) + b_H(s, t_2) = b_H(s, t_1 + t_2)$  for  $s, t_1, t_2 \in K$ .

Note that  $b_V(e_i, e_j) = (e_i e_j, e_i^\sigma e_j + e_i e_j^\sigma)$  for  $0 \leq i \leq j \leq d$  are linearly independent over  $\text{GF}(2)$ , since  $\{e_i e_j \mid 0 \leq i \leq j \leq d\}$  are linearly independent by assumption. Thus  $b_V(e_i, e_j)$  ( $0 \leq i \leq j \leq d$ ) is a basis for the ambient space  $R$  of  $S_V$ . Hence there exists a  $\text{GF}(2)$ -linear map  $\pi$  from  $R$  to  $K \times K$  which sends  $b_V(e_i, e_j)$  to  $b_H(\bar{e}_i, \bar{e}_j)$  for  $0 \leq i \leq j \leq d$ . There also exists a  $\text{GF}(2)$ -linear bijection  $\kappa$  from  $W$  to  $K$  sending  $e_i$  to  $\bar{e}_i$  ( $0 \leq i \leq d$ ). For any  $s = \sum_{i=0}^d \alpha_i e_i$  ( $\alpha_i \in \text{GF}(2)$ ) and  $t = \sum_{i=0}^d \beta_j e_j$  ( $\beta_j \in \text{GF}(2)$ ) in  $W$ , we have  $b_V(s, t) = \sum_{i,j=0}^d \alpha_i \beta_j b_V(e_i, e_j)$  by the addition formula for  $S_V$ . From the addition formula for  $S_{\sigma, H}$ , we have

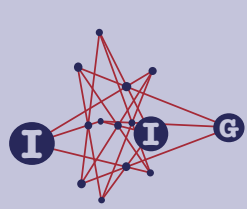
$$b_H(\kappa(s)) = b_H\left(\sum_{i=0}^d \alpha_i \kappa(e_i), \sum_{j=0}^d \beta_j \kappa(e_j)\right) = \sum_{i,j=0}^d \alpha_i \beta_j b_H(\bar{e}_i, \bar{e}_j).$$

As  $\pi$  is a  $\text{GF}(2)$ -linear map sending  $b_V(e_i, e_j)$  to  $b_H(\bar{e}_i, \bar{e}_j)$  ( $0 \leq i \leq j \leq d$ ), we conclude that  $\pi(b_V(s, t)) = b_H(s, t)$  for any  $s, t \in W$ . In particular,  $\pi$  bijectively maps  $X_V(t)$  (resp.  $X_V(\infty)$ ) onto  $X_H(\bar{t})$  (resp.  $X_H(\infty)$ ) for any  $t \in W^\times$ . Thus  $\pi$  gives a covering map of  $S_{\sigma, H}$  by the Veronesean dual hyperoval  $S_V$ .  $\square$

*Proof of Theorem 1.3.* Observe that  $d \geq 4$ , as  $d$  is even and  $d \geq 3$ . By Theorem 1.1, we may define a  $d$ -dual hyperoval  $S_{\tau, H}$  for a generator  $\tau$  of the Galois group  $\text{Gal}(K)$  and a hyperplane  $H$  of  $K$ .

ACADEMIA  
PRESS





page 13 / 15

go back

full screen

close

quit

- (1) Suppose that  $S_\sigma$  is isomorphic to  $S_{\tau,H}$  by a mapping  $\Phi$  for some generators  $\sigma$  and  $\tau$  of  $\text{Gal}(K)$  and a hyperplane  $H$  of  $K$ . Choose  $h \in K^\times$  so that  $H = \{x \in K \mid \text{Tr}(hx) = 0\}$ . Define  $b_1(s, t) := (st, s^\sigma t + st^\sigma)$  and  $b_2(s, t) := (\text{Tr}(ht)s^2 + st + \text{Tr}(hs)t^2, s^\tau t + st^\tau)$  for  $s, t \in K$ . Then the addition formula (equation (9)) holds for both  $\{b_1(s, t) \mid s, t \in K^\times\}$  and  $\{b_2(s, t) \mid s, t \in K^\times\}$ . As  $S_\sigma$  and  $S_{\tau,H}$  are constructed by the method in Proposition 2.1 from  $\{b_1(s, t) \mid s, t \in K^\times\}$  and  $\{b_2(s, t) \mid s, t \in K^\times\}$ , the assumptions of Proposition 3.1 are satisfied. We use the letters  $F$ ,  $G$  and  $L$  to denote the  $\text{GF}(2)$ -linear maps on  $K$  in Proposition 3.1(a); namely,  $\Phi(x, y) = (F(x) + G(y), L(y))$  for all  $x, y \in K$ . From Proposition 3.1(a and c), the second component  $s^\sigma t + st^\sigma$  of  $b_1(s, t)$  is mapped by  $L$  to the second component  $\rho(s)^\tau \rho(t) + \rho(s)\rho(t)^\tau$  of  $b_2(\rho(s), \rho(t)) = \Phi(b_1(s, t))$  for every  $s, t \in K^\times$ , where  $\rho$  is a bijection given by  $\rho(x) = F(x^2)^{1/2}$  ( $x \in K$ ) by Proposition 3.1(b). Then it follows from Proposition 3.2 that  $\rho(x) = bx^\mu$  ( $x \in K$ ) for some  $b \in K^\times$  and  $\mu \in \text{Gal}(K)$ . In particular,

$$F(st) = \rho((st)^{1/2})^2 = b^2(st)^\mu = \rho(s)\rho(t) \quad (16)$$

for  $s, t \in K^\times$ . Comparing the first components of  $b_1(s, t)$  and  $\Phi(b_1(s, t)) = b_2(\rho(s), \rho(t))$ , we have

$$F(st) + G(s^\sigma t + st^\sigma) = \text{Tr}(h\rho(t))\rho(s)^2 + \rho(s)\rho(t) + \text{Tr}(h\rho(s))\rho(t)^2.$$

By equation (16), we then have

$$G(s^\sigma t + st^\sigma) = \text{Tr}(h\rho(t))\rho(s)^2 + \text{Tr}(h\rho(s))\rho(t)^2 \quad (17)$$

for every  $s, t \in K^\times$ . As  $G$  is linear, equation (17) holds for all  $s, t \in K$ .

Notice that  $\rho$  is a  $\text{GF}(2)$ -linear bijection on  $K$  by the claims (a) and (b) of Proposition 3.1, whence  $H_1 := \rho^{-1}(H)$  is a hyperplane of  $K$ . It follows from equation (17) that we have

$$G(s^\sigma t + st^\sigma) = 0 \text{ for every } s, t \in H_1, \quad (18)$$

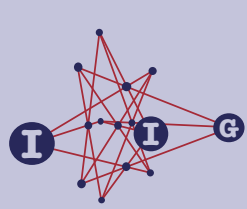
because  $\rho(s)$  and  $\rho(t)$  lie in  $H$  and hence

$$\text{Tr}(h\rho(t))\rho(s)^2 + \text{Tr}(h\rho(s))\rho(t)^2 = 0.$$

Now we apply Lemma 3.3 to conclude that  $\{s^\sigma t + st^\sigma \mid s, t \in H_1\}$  spans  $K$  as a vector space over  $\text{GF}(2)$ . (Note that  $d \geq 4$ .) This implies that  $G = 0$  from equation (18). However, it then follows from equation (17) that  $0 = \rho(s)^2 + \rho(t)^2$  and hence  $\rho(s) = \rho(t)$  for every  $s, t \in K \setminus H_1$ . As  $K \setminus H_1$  contains  $2^d \geq 2$  elements, this contradicts the bijectivity of  $\rho$ .

ACADEMIA  
PRESS





page 14 / 15

go back

full screen

close

quit

- (2) Choose  $\alpha$  and  $b$  of  $K^\times$  satisfying  $H = \{x \in K \mid \text{Tr}((\alpha b)x) = 0\}$  and  $H' = \{x \mid \text{Tr}(\alpha x) = 0\}$ . Define a GF(2)-linear bijection  $\Phi$  on  $K \times K$  by  $\Phi(x, y) := (b^2x, b^{\sigma+1}y)$ . Then for any  $s, t \in K$  we have

$$\begin{aligned} & \Phi(\text{Tr}((\alpha b)t)s^2 + st + \text{Tr}((\alpha b)s)t^2, s^\sigma t + st^\sigma) \\ &= (\text{Tr}((\alpha b)t)(bs)^2 + (bs)(bt) + \text{Tr}((\alpha b)s)(bt)^2, (bs)^\sigma(bt) + (bs)(bt)^\sigma). \end{aligned}$$

Thus  $\Phi$  induces an isomorphism from  $S_{\sigma, H}$  with  $S_{\sigma, H'}$ .

- (3) Let  $h$  be an element of  $K^\times$  with  $H = \{x \in K \mid \text{Tr}(hx) = 0\}$ . We first notice that the GF(2)-linear bijection on  $K \times K$  given by  $\Phi(x, y) := (x, y^{\sigma^{-1}})$  ( $x, y \in K$ ) induces an isomorphism between  $S_{\sigma, H}$  and  $S_{\sigma^{-1}, H}$ , because for  $s, t \in K$  we have

$$\begin{aligned} & \Phi(\text{Tr}(ht)s^2 + st + \text{Tr}(hs)t^2, s^\sigma t + st^\sigma) \\ &= (\text{Tr}(ht)s^2 + st + \text{Tr}(hs)t^2, s^{\sigma^{-1}}t + st^{\sigma^{-1}}). \end{aligned}$$

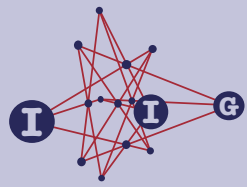
Conversely, assume that  $S_{\sigma, H} := \{X_\sigma(s) \mid s \in K^\times \cup \{\infty\}\}$  is isomorphic to  $S_{\tau, H} := \{X_\tau(s) \mid s \in K^\times \cup \{\infty\}\}$  by a GF(2)-linear bijection on  $K \times K$ . Then there exists a bijection  $\rho$  on  $K^\times \cup \{\infty\}$  such that  $\Phi(X_\sigma(s)) = X_\tau(\rho(s))$  for all  $s \in K^\times \cup \{\infty\}$ . As we saw in the proof of Theorem 1.1,  $S_{\mu, H}$  ( $\mu \in \{\sigma, \tau\}$ ) is constructed from the collection  $\{b_\mu(s, t) \mid s, t \in K^\times\}$  of vectors  $b_\mu(s, t) := (\text{Tr}(ht)s^2 + st + \text{Tr}(hs)t^2, s^\mu t + st^\mu)$  satisfying the addition formula (equation (9)). Thus the assumptions of Proposition 3.1 are satisfied by  $S_1 = S_\sigma$  and  $S_2 = S_\tau$ . Then it follows from Proposition 3.1(a and b) that  $\rho(\infty) = \infty$  and there exist GF(2)-linear bijections  $F, L$  on  $K$  and a GF(2)-linear map  $G$  on  $K$  such that  $\Phi(x, y) = (F(x) + G(y), L(y))$  for all  $x, y \in K$ . In particular, the second component  $y'$  of  $\Phi(b_\sigma(s, t)) =: (x', y') \in K \times K$  is equal to the image by  $L$  of the second component  $s^\sigma t + st^\sigma$  of  $b_\sigma(s, t)$ . As  $\Phi(b_\sigma(s, t)) = b_\tau(\rho(s), \rho(t))$  by Proposition 3.1(c), we conclude that  $L(s^\sigma t + st^\sigma) = \rho(s)^\tau \rho(t) + \rho(s)\rho(t)^\tau$  for all  $s, t \in K^\times$ . Then it follows from Proposition 3.2 that  $\tau = \sigma$  or  $\tau = \sigma^{-1}$ .  $\square$

## References

- [1] **A. Del Fra**, On  $d$ -dimensional dual hyperovals, *Geom. Dedicata* **79** (2000), 157–178.
- [2] **C. Huybrechts** and **A. Pasini**, Flag-transitive extensions of dual affine spaces, *Beiträge Algebra Geom.* **40** (1999), 503–532.

ACADEMIA  
PRESS





page 15 / 15

go back

full screen

close

quit

- [3] **H. Taniguchi**, On a family of dual hyperovals over  $\text{GF}(q)$  with  $q$  even, *European J. Combin.* **26** (2005), 195–199.
- [4] \_\_\_\_\_, On isomorphism problem of some dual hyperovals in  $\text{PG}(2d + 1, q)$  with  $q$  even, *Graphs Combin.* **23** (2007), 455–465.
- [5] **J. Thas** and **H. Van Maldeghem**, Characterizations of the finite quadric Veroneseans  $\mathcal{V}_n^{2^n}$ , *Q. J. Math.* **55** (2004), 99–113.
- [6] **S. Yoshiara**, A family of  $d$ -dimensional dual hyperovals in  $\text{PG}(2d + 1, 2)$ , *European J. Combin.* **20** (1999), 589–603.
- [7] \_\_\_\_\_, Notes on Taniguchi's dimensional dual hyperovals, *European J. Combin.* **28** (2007), 674–684.

Hiroaki Taniguchi

DEPARTMENT OF GENERAL EDUCATION, KAGAWA NATIONAL COLLEGE OF TECHNOLOGY,, 551 TAKUMA, KAGAWA, 769-1192 JAPAN

*e-mail*: [taniguchi@dg.kagawa-nct.ac.jp](mailto:taniguchi@dg.kagawa-nct.ac.jp)

Satoshi Yoshiara

DEPARTMENT OF MATHEMATICS, TOKYO WOMAN'S CHRISTIAN UNIVERSITY,, 2-6-1 ZEMPUKUJI, SUGINAMI-KU, TOKYO, 167-8585 JAPAN

*e-mail*: [yoshiara@lab.twcu.ac.jp](mailto:yoshiara@lab.twcu.ac.jp)

ACADEMIA  
PRESS

