Finite Fields and Their Applications 42 (2016) 93–101

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Bilinear dual hyperovals from binary commutative presemifields

Hiroaki Taniguchi

National Institute of Technology, Kagawa College, 355, Chokushicho,
Takamatsu city, Kagawa, 761-8058, Japan

ARTICLE INFO

Article history:
Received 20 December 2015
Received in revised form 26 June 2016
Accepted 6 July 2016
Available online 28 July 2016
Communicated by Olga Polverino

Dedicated to Professor Y. Hiramine, who passed away on January, 2016

MSC:
05B25
51A45
51E20
51E21

Keywords:
Dual hyperoval
Binary commutative semifield

ABSTRACT

For a binary commutative presemifield S with an element $c \in S$, we can construct a bilinear dual hyperoval $\mathcal{S}_c(S)$ if c satisfies some conditions. Let $c_1 \in S_1$ and $c_2 \in S_2$ for commutative presemifields S_1 and S_2, and assume $c_1 \neq 1$ or $c_2 \neq 1$. Then the dual hyperovals $\mathcal{S}_{c_1}(S_1)$ and $\mathcal{S}_{c_2}(S_2)$ are isomorphic if and only if S_1 and S_2 are isotopic with some relation between c_1 and c_2 induced by the isotopy. For the Kantor commutative presemifield $S = (F, +, \circ)$ with $c \in F_n \subset F$, the dual hyperoval $\mathcal{S}_c(S)$ exists if and only if $Tr(c) = 1$, where Tr is the absolute trace of F_n. The dual hyperovals $\mathcal{S}_{c_1}(S_1)$ and $\mathcal{S}_{c_2}(S_2)$ for the Kantor commutative presemifields S_1 and S_2 are (under some conditions) isomorphic if and only if S_1 and S_2 are isotopic with $c_1^\sigma = c_2$, where σ is the field automorphism of F defined by the isotopy.

© 2016 Elsevier Inc. All rights reserved.

1. Introduction

Higher dimensional dual hyperoval is defined by Huybrechts and Pasini in [2]. In this note, we only concern with dual hyperovals over the binary field $GF(2)$. Let n and d be

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

http://dx.doi.org/10.1016/j.ffa.2016.07.003
1071-5797/© 2016 Elsevier Inc. All rights reserved.

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. We say $\mathcal{S}_1$ is isomorphic to $\mathcal{S}_2$ if there is a $GF(2)$-linear isomorphism $\pi : U_1 \to U_2$ such that $\pi(\mathcal{S}_1) = \mathcal{S}_2$.

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. If there is a dual hyperoval in $V \oplus W$, then $d \leq l \leq d(d + 1)/2 + 2$, and conjectured that $l \leq d(d + 1)/2$ by [7]. 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 $t \in V$. The conditions that B defines a bilinear dual hyperoval are the following: (i) $V \ni x \mapsto B(x, a) \in W$ are rank d linear mappings for $a \in V \backslash \{0\}$, and (ii) $V \ni t \mapsto B(b, t) \in W$ are rank d linear mappings for $b \in V \backslash \{0\}$. These two conditions are independent. (As for the condition (1) for a dual hyperoval, $X(t_1) \cap X(t_2)$ is a subspace of rank one for $t_1 \neq t_2$ because of (i). As for the condition (2) for a dual hyperoval, any three mutually distinct members of $\mathcal{S}$ intersect trivially because of (ii). We easily see that $\{X(t) \mid t \in V\}$ generates $V \oplus W$. The cardinality $|\mathcal{S}| = |V| = 2^{d+1}$, hence the condition (4) for a dual hyperoval is satisfied. See Section 1 of [6] for more details, where we use the notation $x * t$ instead of $B(x, t)$.) 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 $t \in V$, induced by the linear transformation $t_a : V \oplus W \ni (x, y) \mapsto (x, y + B(x, a)) \in V \oplus W$. We call a bilinear dual hyperoval symmetric if the bilinear mapping is symmetric, i.e., $B(x, t) = B(t, x)$ for any $x, t \in V$.

In [8], Yoshiara constructed bilinear dual hyperovals with symmetric bilinear mappings using quadratic APN functions. He also proved that these bilinear dual hyperovals are isomorphic if and only if quadratic APN functions are CCZ equivalent (see also [9]). Dempwolff and Edel studied on quadratic APN functions and bilinear dual hyperovals in [1].

In this note, we construct bilinear dual hyperovals with symmetric bilinear mappings using binary commutative presemifields. In this note, we will prove the following theorem and propositions. In Proposition 2, we construct a bilinear dual hyperoval $\mathcal{S}_c(S)$ from a binary commutative presemifield S and an element $c \in S$ which satisfies some conditions. Let $c_1 \in S_1$ and $c_2 \in S_2$ for commutative presemifields S_1 and S_2, and assume that $c_1 \neq 1$ or $c_2 \neq 1$. In Theorem 4, we show that the dual hyperovals $\mathcal{S}_{c_1}(S_1)$ and $\mathcal{S}_{c_2}(S_2)$ are isomorphic if and only if S_1 and S_2 are isotopic with some relation between c_1 and

Download English Version:

https://daneshyari.com/en/article/4582638

Download Persian Version:

https://daneshyari.com/article/4582638

Daneshyari.com