Symmetric Doubly Dual Hyperovals Have an Odd Dimension

Ulrich Dempwolff
Department of Mathematics,
University of Kaiserslautern, Erwin-Schroedinger-Strasse,
67653 Kaiserslautern, Germany
email: dempwolff@mathematik.uni-kl.de

Abstract

We show that a symmetric, doubly dual hyperoval has an odd dimension. This is a weak support for the conjecture that doubly dual hyperovals over $\mathbb{F}_2$ only exist, if the dimension of the dual hyperoval is odd (see [2]).

1 Introduction

Motivated by an unsuccessful computer search for doubly dual, 4-dimensional dual hyperovals over $\mathbb{F}_2$ we conjectured (see [2]), that doubly dual hyperovals over $\mathbb{F}_2$ only exist for odd dimensions. H. Taniguchi proved in [5, Thm. 11] the following remarkable result:

Theorem 1.1. (H. Taniguchi) An alternating, dual hyperoval is doubly dual if and only if it has an odd dimension.

This provides additional evidence for the correctness of the conjecture stated above. In [4, Sec. 5] Y. Edel gives an alternative proof of Theorem 1.1. Edel’s proof of the ”only if part” of Taniguchi’s Theorem uses the so called Knuth operations. We show that the Knuth operations also lead to a verification of the ”if part” of the proof of this theorem. Moreover we will use this tool to support further the conjecture by giving an elementary proof of

Theorem 1.2. A symmetric, doubly dual hyperoval has an odd dimension.

2 Definitions, preliminaries and the proofs of Theorems 1.1 and 1.2

A set $S$ of $n$-spaces of the finite dimensional $\mathbb{F}_q$-space $U$ is a $n$-dimensional dual hyperoval if (DHO1) $|S| = 2^n$, (DHO2) $\dim S \cap S' = 1$ for two different
$S, S' \in S$. (DHO3) $S \cap S' \cap S'' = 0$ for three different $S, S', S'' \in S$, and (DHO4) $U = \langle S | S \in S \rangle$. The dual hyperoval is doubly dual, if $S$ is in addition a $n$-dimensional dual hyperoval with respect to the dual space of $U$, i.e. if $\dim(S + S') = 2n - 1$ and $U = S + S' + S''$ for three different $S, S', S'' \in S$ (note that $\dim U = 2n$ in this case). An important subclass of dual hyperovals are the bilinear dual hyperovals, which are only defined over $\mathbb{F}_2$. Let $X$ and $Y$ be finite dimensional $\mathbb{F}_2$-spaces, $\dim X = n$, and set $U = X \oplus Y$. We call a $n$-dimensional dual hyperoval $S$ bilinear, if there exists a monomorphism $\beta : X \to \text{Hom}(X, Y)$, such that $S = S_\beta$ is a dual hyperoval in $U$. Here $S_\beta = \{S_e | e \in X\}$, with $S_e = \{(x, x\beta(e)) | x \in X\}$. Note: the map $X \times X \ni (x, e) \mapsto x\beta(e) \in X$ is bilinear. On the other hand a monomorphism $\beta : X \to \text{Hom}(X, Y)$, will produce a bilinear dual hyperoval if:

1. $\text{rk}(\beta(e)) = n - 1$ for all $0 \neq e \in X$.
2. $\ker(\beta(e)) \neq \ker(\beta(e'))$ for all $0 \neq e, e' \in X$, $e \neq e'$.

The monomorphism $\beta^o : X \to \text{Hom}(X, Y)$ defined by $x\beta^o(e) = e\beta(x)$, defines an $n$-dimensional dual hyperoval $S_{\beta^o}$ too, the dual hyperoval opposite to $S_\beta$. The dual hyperoval $S_\beta$ is symmetric, if $\beta^o = \beta$ and the dual hyperoval is alternating, if $e\beta(e) = 0$ for all $e \in X$. Clearly, alternating dual hyperovals are symmetric.

We now turn to bilinear, doubly dual hyperovals, i.e. we assume in addition $X = Y$, $\text{Hom}(X, Y) = \text{End}(X)$, and $\dim U = 2n$. Let $(\cdot, \cdot)$ be a non-degenerate, symmetric bilinear form on $X$. For $\phi \in \text{End}(X)$ we denote by $\phi^t$ the operator, which is adjoint to $\phi$ with respect to the bilinear form, i.e. $(x\phi, x') = (x, x'\phi^t)$ for all $x, x' \in X$. We define $\beta^t : X \to \text{End}(X)$ by $\beta^t(e) = \beta(e)^t$. Usually, $\beta^t$ does not define a dual hyperoval. But the following criterion is obvious (see also [2, Lemma 3.2]):

**Lemma 2.1.** Let $\beta : X \to \text{End}(X)$ define a bilinear dual hyperoval $S_\beta$. Equivalent are:

(a) $S_\beta$ is doubly dual.
(b) $\beta^t$ defines a dual hyperoval.

We call the mappings $\beta \mapsto \beta^o$ and $\beta \mapsto \beta^t$ the Knuth operations in analogy to the corresponding notion in the theory of semifields. The Knuth operations produce at most six bilinear dual hyperovals associated to $\beta, \beta^o, \beta^t, \beta^{o^t}, \beta^{o^t}$, and $\beta^{o^t}$ (see [4]). For all $x, e, y \in X$ we have the equations

\[
(x\beta(e) + e\beta(x), y) = (x, \beta^t(e) + (e, y\beta^t(x)) = (x, e\beta^o(y)) + (x\beta^o(y), e) \tag{1}
\]

and

\[
(x\beta(x), y) = (x, y\beta^t(x)) = (x, x\beta^o(y)) \tag{2}
\]

If these equations are identical zero, one obtains the following special case of [4].

---

1In our note the dimension of a dual hyperoval refers to the vector space dimension. More common is the reference to the projective dimension of vectorspaces (see [6, Def. 2.1, 2.3]).
Proposition 2.2. (Y. Edel) Let $\beta : X \to \text{End}(X)$ define a bilinear, doubly dual hyperoval $S_\beta$.

(a) Equivalent are:

1) $\beta$ is symmetric.

2) $\beta^\text{to}$ is self-adjoint (i.e. $\beta^\text{to} = (\beta^\text{to})^t$).

(b) Equivalent are:

1) $\beta$ is alternating.

2) $\beta^\text{to}$ is skew symmetric (i.e. $(x, x\beta^\text{to}(e)) = 0$ for all $x, e \in X$).

We now give a verification of Theorem 1.1 based on the Knuth operations. For this purpose we use Lemma 2.3.

Let $\beta : X \to \text{End}(X)$, $\dim X = n$, define a bilinear dual hyperoval.

Assume $\text{rk } \beta^\text{to}(e) \leq n - 1$ for $0 \neq e \in X$. Then $\beta$ defines a doubly dual hyperoval.

Proof. We express $\text{rk } \beta^\text{to}(e) = n - 1$ by the equation

$$\dim \{y \in X | (x, \beta^\text{to}(e), y) = 0, \text{ all } x \in X\} = 1.$$  

Using the Knuth operations we obtain

$$\dim \{y \in X | (x, \beta^\text{tot}(y), e) = 0, \text{ all } x \in X\} = 1.$$  

So for $e \in X^\star$, there exists precisely one vector $y = \tau(e) \in X^\star$ such that

$$\text{Im } \beta^\text{tot}(y) \subseteq \langle e \rangle^\perp.$$  

Define the relation $\sim$ on $X^\star$ by $y \sim e$ iff $\text{Im } \beta^\text{tot}(y) \subseteq \langle e \rangle^\perp$. Then $k_e = |\{y \in X^\star | y \sim e\}| = 1$ as we have seen. On the other hand $\text{rk } \beta^\text{tot}(y) \leq n - 1$ implies also $\text{rk } \beta^\text{tot}(y) \leq n - 1$. We get $r_y = |\{e \in X^* | y \sim e\}| \geq 1$. As $2^n - 1 = \sum_e k_e = \sum_y r_y \geq 2^n - 1$ we see that $r_y = 1$ for all $y$. Hence $\tau$ is a bijection on $X^\star$. This implies $\text{Im } \beta^\text{tot}(e) = \langle \tau^{-1}(e) \rangle^\perp$ for all $e \in X^\star$. Thus $\beta^\text{tot}$ defines a dual hyperoval in the dual space. Hence $\beta^\text{to}$ and then $\beta$ define dual hyperovals. Using Lemma 2.1 we conclude that $\beta$ is doubly dual.

Proof. (Theorem 1.1) Let $\beta : X \to \text{End}(X)$, $\dim X = n$, define an alternating dual hyperoval.

First we repeat Edel’s argument for the ”only if part” of Taniguchi’s Theorem and assume therefore, that $\beta$ is doubly dual. Then by (b,2) of Proposition 2.2 $\beta^\text{to}(e)$ is skew symmetric and thus has an even rank. So $\text{rk } \beta^\text{to}(e) = n - 1$ must be even for $0 \neq e \in X$. Hence $n$ is odd.

Next we assume that $n$ is odd. Set $X^\star = X - \{0\}$. As $\beta$ is alternating Equation 2 shows that the operator $\beta^\text{to}(y)$ is skew symmetric for all $y \in X$, i.e. $\beta^\text{tot}(y)$ has an even rank. Thus $\text{rk } \beta^\text{to}(y) \leq n - 1$. Now $\beta$ is doubly dual by Lemma 2.3.
Remark 2.4. Taniguchi’s proof of the “if part” of his theorem uses a Fourier transformation (of a quadratic APN function associated to the alternating dual hyperoval), whereas Edel’s proof relies on a result of Delsarte and Goethals [1] on codes generated by alternating forms.

We now prove Theorem 1.2.

Proof. (Theorem 1.2) Let \( \beta : X \to \text{End}(X) \) define a symmetric, doubly dual hyperoval \( S_\beta \). We define the mapping \( \kappa : X \to X \) by

\[
\kappa(e) = \begin{cases} 
0, & e = 0, \\
y, & e \neq 0, \quad \ker \beta(e) = \langle y \rangle .
\end{cases}
\]

By (DHO1-3) \( \kappa \) is a permutation of \( X \), which fixes 0. As \( \beta \) is symmetric, we have \( \kappa^2 = 1 \). So \( \kappa \) permutes \( X \setminus \{0\} \) and as this set has an odd size, there exist \( 0 \neq e \in X \) with \( \kappa(e) = e \).

Define the diagonal map \( \delta : X \to X \) by \( \delta(x) = x\beta(x) \). The diagonal map is \( \mathbb{F}_2 \)-linear, since \( \beta \) is symmetric. Clearly, \( e \in \ker \delta \). So the image of \( \delta \) is a proper subspace of \( X \). Hence there exists an \( 0 \neq f \in X \), such that \( f \) is perpendicular to the image of \( \delta \) with respect to the symmetric bilinear form. This implies for all \( x \in X \), that

\[
0 = \langle \delta(x), f \rangle = \langle x\beta(x), f \rangle = \langle x, f\beta'(x) \rangle = \langle x, x\beta^{\alpha}(f) \rangle .
\]

We conclude that the operator \( \beta^{\alpha}(f) \) is skew symmetric. In particular the rank of \( \beta^{\alpha}(f) \) is even. But as \( \beta^{\alpha} \) defines a dual hyperoval the rank of \( \beta^{\alpha}(f) \) is \( n-1 \), i.e. \( n \) is odd.

Remark 2.5. There is no complete analog to Taniguchi’s Theorem for symmetric dual hyperovals, since there exist symmetric dual hyperovals of odd dimension, which are not doubly dual. Already in dimension 5 it is easy to find such dual hyperovals. See for instance the example below. If one is willing to drop axiom (DHO4) (which is done sometimes) examples like [3, Ex. 6.3] are relevant too.

Example 2.6. The matrices

\[
\begin{align*}
\epsilon_1 &= \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 \\
\end{pmatrix}, & \epsilon_2 &= \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 \\
\end{pmatrix} \\
\epsilon_3 &= \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 \\
\end{pmatrix}, & \epsilon_4 &= \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 \\
\end{pmatrix}, & \epsilon_5 &= \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 \\
\end{pmatrix}
\end{align*}
\]

in \( \mathbb{F}_2^{5\times5} \) all have rank 4 and if \( \{e_1, \ldots, e_5\} \) is the standard basis of \( \mathbb{F}_2^5 \) we observe that \( e_i e_j = e_j e_i \) for all \( i, j \). It is easily checked, that \( \beta : \mathbb{F}_2^5 \to \mathbb{F}_2^{5\times5} \), \( \beta(x_1, \ldots, x_5) = \sum x_i e_i \), defines a dual hyperoval, hence a symmetric dual hyperoval. On the other hand \( \epsilon_1 \) and \( \epsilon_2 \) have the same image, i.e. \( S_\beta \) is not doubly dual.
References


