On some $d$-dimensional dual hyperovals in $\text{PG}(2d, 2)$

Hiroaki Taniguchi

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

Received 27 February 2008; revised 24 May 2008
Available online 3 July 2008
Communicated by Gary L. Mullen

Abstract

In [H. Taniguchi, On $d$-dimensional dual hyperovals in $\text{PG}(2d, 2)$, Innov. Incidence Geom., in press], we construct $d$-dimensional dual hyperovals in $\text{PG}(2d, 2)$ from quasifields of characteristic 2. In this note, we show that, if $d$-dimensional dual hyperovals in $\text{PG}(2d, 2)$ constructed from nearfields are isomorphic, then those nearfields are isomorphic. Some results on dual hyperovals constructed from quasifields are also proved. © 2008 Elsevier Inc. All rights reserved.

Keywords: Dual hyperoval; Quasifield; Nearfield

1. Introduction

Let $\text{GF}(q)$ be finite field with $q$ elements. Let $d$, $m$ be integers with $d \geq 2$ and $m > d$. Let $\text{PG}(m, 2)$ be an $m$-dimensional projective space over the binary field $\text{GF}(2)$. C. Huybrechts and A. Pasini define higher dimensional dual hyperovals in [5]. (R. Shaw [9] also defines conclaves in $\text{PG}(m, q)$, which coincide our Definition 1 except the condition (3).)

Definition 1. 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:

1. any two distinct members of $S$ intersect in a projective point,
2. any three mutually distinct members of $S$ intersect in the empty projective set,
(3) the members of $S$ generate $\text{PG}(m, 2)$, and
(4) there are exactly $2^{d+1}$ members of $S$.

We want to know the relations between quasifields and higher dimensional dual hyperovals constructed from quasifields.

**Definition 2.** (See [6].) An algebraic structure $(Q; +, \circ)$ is called a quasifield if it satisfies the following conditions:

1. $Q$ is an abelian group under $+$ with identity 0,
2. for all $a \in Q$, $a \circ 0 = 0 \circ a = 0$,
3. there exists an element $1 \in Q \setminus \{0\}$ such that $1 \circ a = a \circ 1 = a$ for all $a \in Q$,
4. for all $a, b, c \in Q$, $(a + b) \circ c = a \circ c + b \circ c$,
5. for $a, c \in Q$ with $a \neq 0$, there exists exactly one $x \in Q$ such that $a \circ x = c$, and
6. for $a, b, c \in Q$ with $a \neq b$, there exists exactly one $x \in Q$ such that $x \circ a - x \circ b = c$.

A nearfield is a quasifield $N$ in which the multiplication $\circ$ is associative; that is, in which $(N \setminus \{0\}, \circ)$ is a group. A semifield is a quasifield $S$ in which the left distributive law $a \circ (b + c) = a \circ b + a \circ c$ holds for all $a, b, c \in S$.

In [10], a construction of $d$-dimensional dual hyperovals in $\text{PG}(2d, 2)$ using spreads of vector spaces over $GF(2)$ is given. Using this construction, we have $d$-dimensional dual hyperovals from quasifields of characteristic 2, as follows.

**Proposition 3.** Let $d \geq 2$. Let $(Q; +, \circ)$ be a quasifield of characteristic 2 which is a $(d + 1)$-dimensional vector space over $GF(2)$. We fix an isomorphism $\phi : Q \cong GF(2^{d+1})$ as a vector space over $GF(2)$ which sends $1 \in Q$ to $1 \in GF(2^{d+1})$. We denote by $\text{Tr}$ the trace function from $GF(2^{d+1})$ to $GF(2)$. Let $\sigma$ be a generator of the Galois group $\text{Gal}(GF(2^{d+1})/GF(2))$.

In $Q \oplus Q \setminus \{(0, 0)\} = \text{PG}(2d + 1, 2)$, for $t \in Q$, let

$$X(t) = \{(x, (x \circ t)^{\sigma} + x \circ t) \mid x \in Q \setminus \{0\}\}.$$ 

Then $S(Q) := \{X(t) \mid t \in Q\}$ is a $d$-dimensional dual hyperoval in $\text{PG}(2d, 2)$ where $\text{PG}(2d, 2) = \{(x, y) \mid x, y \in Q, \text{Tr}(y) = 0\} \setminus \{(0, 0)\}$.

**Proof.** $S(Q) := \{X(t) \mid t \in Q\}$ consists of $|Q| = 2^{d+1}$ members of $d$-subspaces. Let $X(s) \cap X(t) \ni (x, (x \circ s)^{\sigma} + x \circ s) = (x, (x \circ t)^{\sigma} + x \circ t)$ with $s \neq t$, then $(x \circ s)^{\sigma} + (x \circ s) = (x \circ t)^{\sigma} + (x \circ t)$, hence we have $(x \circ s + x \circ t)^{\sigma} = x \circ s + x \circ t$. Since $X(s) \cap X(t)$ consists of projective points, we must have $x \circ s + x \circ t = 1$. By the (6) of quasifield, there exists unique $x$ such that $x \circ s + x \circ t = 1$, hence two distinct members $X(s)$ and $X(t)$ intersect in a projective point. Let $X(s) \cap X(t) \cap X(u) \ni (x, (x \circ s)^{\sigma} + x \circ s) = (x, (x \circ t)^{\sigma} + x \circ t) = (x, (x \circ u)^{\sigma} + x \circ u)$ with $s \neq t, t \neq u$ and $u \neq s$. Then we have $x \circ s + x \circ t = 1$ and $x \circ s + x \circ u = 1$, as above. By substituting one equation from another, we have $x \circ t + x \circ u = 0$, which means $x = 0$ by the definition (6) of quasifield. However, $x = 0$ contradicts to $x \circ s + x \circ t = 1$ and $x \circ s + x \circ u = 1$. Therefore, we must have $X(s) \cap X(t) \cap X(u) = \emptyset$ in $\text{PG}(2d, 2)$. By the construction, the ambient space of $S(Q)$ must be $\text{PG}(2d, 2)$. □
In this note, we prove the following theorem.

**Theorem 10.** Let \((N_1; \circ, +)\) and \((N_2; *, +)\) be nearfields. If \(S(N_1)\) is isomorphic to \(S(N_2)\), then \((N_1; \circ, +)\) is isomorphic to \((N_2; *, +)\).

According to Lüneburg [8], for nearfields of size \(q^n\) with \(q = 2^l\) for some \(l\) such that \((q, n)\) satisfies the conditions of being a Dickson pair, there exist \(\phi(n)/f\) non-isomorphic nearfields of size \(q^n\) with \(q = 2^l\) for infinitely many \(l\). (Indeed, if \(n = 2^p - 1\) is a Mersenne prime, then \((q, n)\) is a Dickson pair for \(q = 2^l\) with \(l = p, 2p, 4p, 8p, \ldots\)). Therefore, as a consequence of this theorem, since \(d\) is defined by the size of the nearfield as \(2^{d+1} = q^n\), for infinitely many \(d\), there exist a lot of non-isomorphic \(d\)-dimensional dual hyperovals in PG(2d, 2).

2. Some automorphisms of \(S(N)\)

Let \((N; +, \circ)\) be a nearfield. Let \(S(N) = \{X(t) \mid t \in N\}\) be a dual hyperoval where \(X(t) = \{(x, (x \circ t)^\sigma + x \circ t) \mid x \in N \setminus \{0\}\}\). We regard PG(2d, 2) = \(\{(x, y) \mid x, y \in N, \ Tr(y) = 0\} \setminus \{(0, 0)\}\). In this section, we first show that the dual hyperoval \(S(N)\) have special automorphisms \(\{m_b\}\) for \(b \in N \setminus \{0\}\).

**Lemma 4.** For \(b \in N \setminus \{0\}\), let us define an automorphism \(m_b\) of PG(2d, 2) as follows:

\[
m_b((x, y)) := (x \circ b^{-1}, y).
\]

Then, \(m_b\) is a automorphism of the dual hyperoval \(S(N)\), which satisfies that \(m_b(X(t)) = X((b \circ t)\) and that \(m_b(X(0)) = X(0)\), where \(X(0) := \{(x, 0) \mid x \in N\}\). Hence we see that the multiplicative group \((N \setminus \{0\}, \circ)\) acts regularly on \(S(N) \setminus \{X(0)\}\).

**Proof.** Since the multiplication \(\circ\) is associative in the nearfield, for \(b \in N \setminus \{0\}\), we have \(m_b(X(t)) = m_b((x, (x \circ t)^\sigma + x \circ t) \mid x \in N \setminus \{0\}) = \{(x \circ b^{-1}, (x \circ t)^\sigma + x \circ t) \mid x \in N \setminus \{0\}\} = \{(x \circ b^{-1} \circ (b \circ t)) \circ (b \circ t) + (x \circ b^{-1}) \circ (b \circ t) \mid x \in N \setminus \{0\}\} = X(b \circ t)\). It is easy to see that \(m_{b_2}(m_{b_1}(X(t))) = m_{b_2 \circ b_1}(X(t))\). \(\square\)

Next, we prove the following characterization of the automorphisms \(\{m_b\}\) of the dual hyperoval \(S(N)\) for \(b \in N \setminus \{0\}\).

**Lemma 5.** Let \(\Psi\) be an automorphism of \(S(N)\) defined by

\[
\Psi((x, y)) = (f(x), y),
\]

where \(f\) is some GF(2)-linear mapping. Then there exists non-zero element \(b\) in \(N\) such that \(f(x) = x \circ b^{-1}\). Therefore, we have \(\Psi = m_b\) for some \(b \in N \setminus \{0\}\).

**Proof.** Since \(\Psi\) is an automorphism of \(S(N)\), \(\Psi\) permutes \(d\)-subspaces \(\{X(t) \mid t \in N\}\). We assume that \(\Psi(X(g(t))) = X(t)\), where \(g : N \to N\) is a one-to-one mapping. It is easy to see
from the definition of $\Psi$ that $\Psi(X(0)) = X(0)$. Hence we have $g(0) = 0$. Since $X(g(t)) = \{(x, (x \circ g(t))^\sigma + x \circ g(t)) \mid x \in N \setminus \{0\}\}$ and $X(t) = \{(x, (x \circ t)^\sigma + x \circ t) \mid x \in N \setminus \{0\}\}$, we have

$$\Psi((x, (x \circ g(t))^\sigma + x \circ g(t))) = (f(x), (x \circ g(t))^\sigma + x \circ g(t)) = (f(x), (f(x) \circ t)^\sigma + f(x) \circ t).$$

By $(x \circ g(t))^\sigma + x \circ g(t) = (f(x) \circ t)^\sigma + f(x) \circ t$, we have $(x \circ g(t) + f(x) \circ t)^\sigma = x \circ g(t) + f(x) \circ t$. Hence, we have $x \circ g(t) + f(x) \circ t = 0$ or $x \circ g(t) + f(x) \circ t = 1$. Therefore, we see that, for any $t \in N \setminus \{0\}$, the mapping $N \ni x \mapsto x \circ g(t) + f(x) \circ t \in GF(2)$ is a GF(2)-linear mapping. Now let us define $V_t$ for any $t \in N \setminus \{0\}$ as the Kernel of the mapping $N \ni x \mapsto x \circ g(t) + f(x) \circ t \in GF(2)$.

If $V_1 = N$, that is, if $x \circ g(1) + f(x) \circ 1 = 0$ for any $x \in N$, we have $f(x) = x \circ g(1)$ for any $x \in N$. Hence, we have $f(x) = x \circ b^{-1}$ if we put $b^{-1} := g(1)$. (Note that $g(1) \neq 0$ since $g$ is a one-to-one mapping with $g(0) = 0$.)

Note that, for $t \neq 0$, $V_t = N$, or a hyperplane of $N$. Now assume that $V_1 \neq N$. Then $V_1$ is a $d$-dimensional GF(2)-vector subspace (hyperplane) of $N$. Since $N$ is a $(d + 1)$-dimensional vector space over GF(2) with $d \geq 2$, for any $t \in N$ with $t \neq 0, 1$, $V_1 \cap V_t$ contains non-zero element. Let $t \neq 0, 1$, and $x \in V_1 \cap V_t$ with $x \neq 0$. Then, since $x \in V_1$, we have $x \circ g(1) + f(x) = 0$ and since $x \in V_t$, we have $x \circ g(t) + f(x) \circ t = 0$. From these equations, we have $x \circ g(t) = (x \circ g(1)) \circ t$. Therefore, if we multiply $x^{-1}$ from the left-hand side, since $N \setminus \{0\}$ is the multiplicative group, we have $g(t) = g(1) \circ t$ for $t \neq 0, 1$. Note also that $g(t) = g(1) \circ t$ holds for any $t \in N$. Let us define the complement $V_1^\perp$ and $V_t^\perp$ of $V_1$ and $V_t$ in $N$ as: $V_1^\perp := N \setminus V_1$ and $V_t^\perp := N \setminus V_t$. Now, if $V_1 \neq N$, then there exists $x \in V_1^\perp$, hence there exists $x \in V_1^\perp \cap V_t$ or there exists $x \in V_1^\perp \cap V_t$. If there exists $x \in V_1^\perp \cap V_t$, then we have $x \circ g(1) + f(x) = 1$ since $x \in V_1^\perp$ and $x \circ g(t) + f(x) \circ t = 0$ since $x \in V_t$. From these equations, and from $g(t) = g(1) \circ t$ above, we have $x \circ g(1) \circ t + x \circ g(1) \circ t + t = 0$, hence we have $t = 0$, which contradicts to the assumption that $t \neq 0$. If there exists $x \in V_1^\perp \cap V_t$, then we have $x \circ g(1) + f(x) = 1$ since $x \in V_1^\perp$ and $x \circ g(t) + f(x) \circ t = 1$ since $x \in V_t$. From these equations, and from $g(t) = g(1) \circ t$ above, we have $x \circ g(1) \circ t + x \circ g(1) \circ t + t = 1$, hence we have $t = 1$, which also contradicts to our assumption that $t \neq 1$. Thus, we conclude that $V_1$ must be $N$. Hence we have $f(x) = x \circ b^{-1}$ if we put $b^{-1} := g(1)$ as we explained before. Therefore we have $\Psi = m_b$ for some $b \in N \setminus \{0\}$ by Lemma 4.

\section{3. Proof of Theorem 10}

We need the following characterization of $d$-dimensional dual hyperovals in PG($2d, 2$).

\textbf{Proposition 6. (See Cooperstein and Thas [1], also see Del Fra [3].) The subset}

$$\text{PG}(2d, 2) \setminus \bigcup \{\text{the points on the members of the dual hyperoval}\}$$

\text{is a $(d - 1)$-dimensional subspace in PG($2d, 2$).}

By Proposition 6, we easily have the following corollary.
Corollary 7. Let $S(Q) = \{X(t) \mid t \in Q\}$ with $X(t) = \{(x, (x \circ t)^o + x \circ t) \mid x \in Q \setminus \{0\}\}$ be a dual hyperoval constructed from a quasifield $Q$. Then, in $\text{PG}(2d, 2) = \{(x, y) \mid x, y \in Q, \text{Tr}(y) = 0\} \setminus \{(0, 0)\}$, we have

$$\{(0, y) \mid y \in Q, y \neq 0, \text{Tr}(y) = 0\} = \text{PG}(2d, 2) \setminus \bigcup_{t \in Q} X(t).$$

Now we consider the dual hyperovals $S(N)$ constructed from nearfields $N$. For nearfields $N_1$ and $N_2$, we denote by $X_1(t)$ for $t \in N_1$ the member of $S(N_1)$ and by $X_2(t)$ for $t \in N_2$ the member of $S(N_2)$.

We recall that, for the dual hyperovals $S_1$ and $S_2$ in $\text{PG}(n, 2)$, the isomorphism $\Phi$ from $S_1$ to $S_2$ is defined as an automorphism of the ambient space $\text{PG}(n, 2)$ which sends the members of $S_1$ to the members of $S_2$.

Lemma 8. Let $(N_1; \circ, +)$ and $(N_2; *, +)$ be nearfields. We regard that the ambient space $\text{PG}(2d, 2) = \{(x, y) \mid x, y \in N_1, \text{Tr}(y) = 0\} = \{(x, y) \mid x, y \in N_2, \text{Tr}(y) = 0\}$. If dual hyperovals $S(N_1)$ and $S(N_2)$ are isomorphic by the automorphism of the ambient space $\Phi : \text{PG}(2d, 2) \rightarrow \text{PG}(2d, 2)$, we may assume that $\Phi$ is represented, using some $\text{GF}(2)$-linear mappings $a(x)$ and $d(y)$, as follows:

$$\Phi((x, y)) = (a(x), d(y)).$$

Proof. We note that any automorphism $\Phi : \text{PG}(2d, 2) \rightarrow \text{PG}(2d, 2)$ is represented as:

$$\Phi((x, y)) = (a(x) + b(y), c(x) + d(y)),$$

where $a(x)$, $b(y)$, $c(x)$ and $d(y)$ are some $\text{GF}(2)$-linear mappings. By Corollary 7, since

$$\Phi(\{(0, y) \mid y \in N_1, \text{Tr}(y) = 0\}) = \{(0, y) \mid y \in N_2, \text{Tr}(y) = 0\},$$

we have $b(y) = 0$. Next, we may assume that $\Phi(X_1(0)) = X_2(0)$. Indeed if $\Phi(X_1(0)) = X_2(a)$, $\Phi(X_1(b)) = X_2(c)$, $\Phi(X_1(d)) = X_2(0)$, for some non-zero $a$, $b$, $c$ and $d$, we easily have

$$\Phi(m_{\circ b}^{-1}(\Phi^{-1}(m_{*a}^{-1}(\Phi(X_1(0)))))) = X_2(0).$$

Hence if we replace $\Phi((x, y))$ by $\Phi(m_{\circ b}^{-1}(\Phi^{-1}(m_{*a}^{-1}(\Phi((x, y))))))$, we may assume that $\Phi(X_1(0)) = X_2(0)$. Hence, we may assume that $\Phi(\{(x, 0) \mid y \in N_1\}) = \{(x, 0) \mid y \in N_2\}$. Therefore, we have $c(x) = 0$. Thus, we may assume that $\Phi$ is represented as $\Phi((x, y)) = (a(x), d(y)).$ \qed

The following proposition plays an important role in the proof of Theorem 10.

Proposition 9. Let $(N_1; \circ, +)$ and $(N_2; *, +)$ be nearfields. Let the dual hyperovals $S(N_1)$ and $S(N_2)$ be isomorphic by the mapping $\Phi$ as in Lemma 8, then there is a group isomorphism $\theta : (N_1 \setminus \{0\}, \circ) \rightarrow (N_2 \setminus \{0\}, *)$ such that, for any $b \in N_1 \setminus \{0\}$ and for any $X_1(t) \in S(N_1)$, we have

$$\Phi(m_b(X_1(t))) = m_{\theta(b)}(\Phi(X_1(t))).$$
Proof. By Lemma 8, we may assume that \( \Phi \) is represented as \( \Phi((x, y)) = (a(x), d(y)) \). Hence, the automorphism \((x, y) \mapsto (f(x), y)\) of \( S(N_1) \) maps to the automorphism \((x, y) \mapsto (a(f(a^{-1}(x))), y)\) of \( S(N_2) \). Therefore, for any \( b \in N_1 \setminus \{0\} \), since the automorphism \( m_b : (x, y) \mapsto (x \circ b^{-1}, y) \) of \( S(N_1) \) has the form \((x, y) \mapsto (f(x), y)\) where \( f(x) = x \circ b^{-1} \), it maps to the automorphism of \( S(N_2) \) which has the form \((x, y) \mapsto (a(f(a^{-1}(x))), y)\). By Lemma 5, for any automorphism of \( S(N_2) \) which has the form \((x, y) \mapsto (a(f(a^{-1}(x))), y)\), there exists \( c \in N_2 \setminus \{0\} \) such that \( a(f(a^{-1}(x))) = x \circ c^{-1} \), hence this automorphism is \( m_c \). Therefore, the automorphism \( m_b \) of \( S(N_1) \) maps to \( m_c \) of \( S(N_2) \) by \( \Phi \). Conversely, for any automorphism \( m_c \) of \( S(N_2) \) for \( c \in N_2 \setminus \{0\} \), it is easy to see that there exists \( b \in N_1 \setminus \{0\} \) such that \( m_c \) maps to the automorphism \( m_b \) of \( S(N_1) \) by \( \Phi^{-1} \). Let us define the mapping \( \theta : N_1 \setminus \{0\} \mapsto N_2 \setminus \{0\} \) by \( \theta(b) = c \). Then we see that \( \theta \) is a one-to-one mapping. Moreover, it is easy to see that \( \theta \) is a group isomorphism. By the definition of \( \theta \), we have \( \Phi(m_b(X_1(t))) = m_{\theta(b)}(\Phi(X_1(t))) \). \( \square \)

Now, we prove the Main Theorem.

**Theorem 10.** Let \((N_1; \circ, +)\) and \((N_2; \ast, +)\) be nearfields. If dual hyperovals \( S(N_1) \) and \( S(N_2) \) are isomorphic, then \((N_1, \circ, +)\) and \((N_2, \ast, +)\) are isomorphic.

**Proof.** We assume that dual hyperovals \( S(N_1) \) and \( S(N_2) \) are isomorphic by \( \Phi \). Hence, as in the proof of Lemma 8, we may assume that \( \Phi(X_1(0)) = X_2(0) \). Therefore, \( \Phi \) is represented as \( \Phi((x, y)) = (a(x), d(y)) \) for some GF(2)-linear mapping \( a(x) \) and \( d(y) \). Moreover, we may assume that \( \Phi(X_1(1)) = X_2(1) \), because, if \( \Phi(X_1(a)) = X_2(1) \) for some \( a \neq 0 \), then \( \Phi(m_a(X_1(1))) = \Phi(X_1(a)) = X_2(1) \), hence we may replace \( \Phi(x, y) \) by \( \Phi(m_a(x, y)) \). We define \( \rho \) by \( \Phi(X_1(t)) = X_2(\rho(t)) \). Then we have \( \rho(0) = 0 \) and \( \rho(1) = 1 \). By Proposition 9, we have

\[
\Phi(m_b(X_1(t))) = m_{\theta(b)}(\Phi(X_1(t)))
\]

(1)

using the group isomorphism \( N_1 \setminus \{0\} \ni b \mapsto \theta(b) \in N_2 \setminus \{0\} \). Since

\[
\Phi : X_1(t) \ni (x, (x \circ t)^\sigma + x \circ t) \mapsto (a(x), d((x \circ t)^\sigma + x \circ t)) \in \Phi(X_1(t)),
\]

and by Eq. (1) (if we recall the definitions of the mappings \( m_b \) and \( m_{\theta(b)} \)), we have

\[
\Phi((x \circ b^{-1}, (x \circ t)^\sigma + x \circ t)) = (a(x) \ast \theta(b^{-1}), d((x \circ t)^\sigma + x \circ t)),
\]

hence, by \( \Phi((x, y)) = (a(x), d(y)) \), we have

\[
a(x \circ b^{-1}) = a(x) \ast \theta(b^{-1}).
\]

(2)

On the other hand, since \( \Phi(X_1(t)) = X_2(\rho(t)) \) and since \( X_2(\rho(t)) = \{(x, (x \ast \rho(t))^{\sigma} + x \ast \rho(t)) \mid x \in N_2 \setminus \{0\} \} \), we have

\[
\Phi(X_1(t)) \ni (a(x), d((x \circ t)^\sigma + x \circ t)) = (a(x), (a(x) \ast \rho(t))^{\sigma} + a(x) \ast \rho(t)) \in X_2(\rho(t)),
\]

hence we have \( d((x \circ t)^\sigma + x \circ t) = (a(x) \ast \rho(t))^{\sigma} + a(x) \ast \rho(t) \) for any \( x \) and \( t \) in \( N_1 \). Since \( \rho(1) = 1 \), we have \( d(x^{\sigma} + x) = a(x)^{\sigma} + a(x) \) if we put \( t = 1 \). Since \( d \) is a linear mapping, if we
put $x = 1$, we have $a(1)^{\sigma} + a(1) = 0$. Since the mapping $a$ induces the following GF(2)-linear isomorphism of $d$-subspaces $X_1(0)$ and $X_2(0)$;

$$
\Phi : X_1(0) \ni (x, 0) \mapsto (a(x), 0) \in X_2(0),
$$

(3)

we have $a(1) \neq 0$, hence we have $a(1) = 1$. Now, since $a(1) = 1$, we have $a(b^{-1}) = \theta(b^{-1})$ by Eq. (2) if we put $x = 1$. Hence we have $a(x) = \theta(x)$ for $x \in N_1$ if we define $\theta(0) = 0$. Therefore, by Eq. (2), we conclude that $a(x \circ y) = a(x) * a(y)$ for any $x, y \in N_1$. By (3), and since $X_1(0) = \{(x, 0) \mid x \in N_1\}$ and $X_2(0) = \{(x, 0) \mid x \in N_1\}$, we see that the mapping $a$ induces an isomorphism $a : N_1 \cong N_2$ of vector spaces over GF(2). Since $a(x \circ y) = a(x) * a(y)$ for any $x, y \in N_1$, and $a$ induces an isomorphism from $N_1$ to $N_2$ as vector spaces over GF(2), we see that the mapping $a$ induces $(N_1; \circ, +) \cong (N_2; *, +)$. \hfill \Box

4. Some results on dual hyperovals constructed from quasifield $Q$

Firstly, we give some definitions.

**Definition 11.** (See Kallaher [6].) Let $(Q; +, \circ)$ be a quasifield.

(1) The set

$$
K(Q) := \{a \in Q \mid a \circ (x \circ y) = (a \circ x) \circ y \text{ and } a \circ (x + y) = a \circ x + a \circ y \text{ for all } x, y \in Q\}
$$

is called the kernel of $Q$. We note that $K(Q)$ is a subfield of $Q$.

(2) The middle nucleus $N_m(Q)$ of $Q$ is defined as:

$$
N_m(Q) := \{n \in Q \mid x \circ (n \circ y) = (x \circ n) \circ y \text{ for all } x, y \in Q\}.
$$

We note that $N_m(Q) \setminus \{0\}$ is a subgroup of $Q$.

In the following lemma, as in Lemma 4, we define some special automorphisms $\{m_b\}$ for $b \in N_m(Q) \setminus \{0\}$ of the dual hyperoval $S(Q) = \{X(t) \mid t \in Q\}$ constructed from quasifield $Q$.

**Lemma 12.** Let $(Q; +, \circ)$ be a quasifield, and $S(Q)$ a dual hyperoval constructed from $Q$. Let $b$ be any non-zero element of the middle nucleus $N_m(Q) \setminus \{0\}$. Inside $PG(2d, 2) = \{(x, y) \mid x, y \in Q, Tr(y) = 0\} \setminus \{(0, 0)\}$, let us define the mapping $m_b$ as follows:

$$
m_b((x, y)) := (x \circ b^{-1}, y).
$$

Then $m_b$ is an automorphism of $S(Q)$. Moreover, we have $m_b(X(t)) = X(b \circ t)$, and $m_b(X(0)) = X(0)$. Thus, the group $N_m(Q) \setminus \{0\}$ acts semi-regularly on $S(Q) \setminus \{X(0)\}$.

**Proof.** Since $b \in N_m(Q) \setminus \{0\}$, we have $(x \circ b^{-1}) \circ (b \circ t) = x \circ t$ by the definition of $N_m(Q)$, hence we have

$$
m_b(X(t)) = \{(x \circ b^{-1}, ((x \circ b^{-1}) \circ (b \circ t))^\sigma + (x \circ b^{-1}) \circ (b \circ t))\} = X(b \circ t).
$$

Therefore, we have $m_{b_2}(m_{b_1}(X(t))) = m_{b_2 \circ b_1}(X(t))$ since $N_m(Q) \setminus \{0\}$ is a subgroup. \hfill \Box
Next, we give a characterization of the automorphisms \( m_b \) for \( b \in N_m(Q) \setminus \{0\} \). We note that \( K(Q) \supseteq GF(2) \) since \( Q \) is a vector space over \( GF(2) \).

**Lemma 13.** We assume that \( K(Q) \supseteq GF(2) \). Inside \( PG(2d, 2) = \{(x, y) \mid x, y \in Q, \ Tr(y) = 0\} \setminus \{(0, 0)\} \), let \( \Psi \) be an automorphism of \( S(Q) \) defined by

\[
\Psi((x, y)) = (f(x), y),
\]

where \( f \) is a \( GF(2) \)-linear mapping. Then we have \( f(x) = x \circ b^{-1} \) for \( b \in N_m(Q) \setminus \{0\} \). Hence \( \Psi = m_b \) for some \( b \in N_m(Q) \setminus \{0\} \).

**Proof.** We may assume that \( \Psi(X(g(t))) = X(t) \), where \( g : Q \to Q \) is a one-to-one mapping with \( g(0) = 0 \). (Note that \( \Psi(X(0)) = X(0) \) by the definition of \( \Psi \).) Then, we have \( \Psi((x, (x \circ g(t))^\sigma + x \circ g(t))) = (f(x), (x \circ g(t))^\sigma + x \circ g(t)) \) by the definition of \( \Psi \). By \( \Psi(X(g(t))) = X(t) \) and since \( X(t) = \{(x, (x \circ t)^\sigma + x \circ t) \mid x \in Q \setminus \{0\}\} \), we have \( (f(x), (x \circ g(t))^\sigma + x \circ g(t)) = (f(x), f(x \circ t)^\sigma + f(x) \circ t) \). Hence we have \( x \circ g(t) + f(x) \circ t = 0 \) or \( x \circ g(t) + f(x) \circ t = 1 \).

As a special case of (4), we have \( f(x) = x \circ g(1) \) or \( f(x) = x \circ g(1) + 1 \) for any \( x \in Q \) if we put \( t = 1 \). By the assumption \( K(Q) \supseteq GF(2) \), there exists \( \alpha \in K(Q) \) with \( \alpha \neq 0, 1 \). We also assume that \( |Q| > 8 \). (Recall that \( d \geq 2 \). If \( |Q| = 2^{d+1} = 8 \), then \((Q; +, \circ)\) is a finite field and \( N_m(Q) \setminus \{0\} = Q \setminus \{0\} \), hence, in this case, we are able to prove this lemma as in the proof of Lemma 5.) Hence we may assume that there exists \( t \in Q \) with \( t \neq 0, 1 \) such that

\[
\{1, t, 1 + t\} \cap \{\alpha, \alpha \circ t, \alpha \circ t + \alpha\} = \emptyset,
\]

if we choose \( t \) which satisfies that \( t \notin \{0, 1, \alpha, \alpha + 1, \alpha^{-1}, (\alpha + 1)^{-1}, \alpha^{-1} + 1, (\alpha + 1)^{-1} \circ \alpha\} \).

(Here, for \( b \in Q \setminus \{0\} \), we denote by \( b^{-1} \) the right inverse of \( b \) in \( Q \).

Let us take \( t \) which satisfies (5). Since \( f(x) = x \circ g(1) \) or \( f(x) = x \circ g(1) + 1 \), and since \( x \circ g(t) = f(x) \circ t \) or \( x \circ g(t) = f(x) \circ t + 1 \) by (4), we only have the following four cases for any \( x \in Q \):

(a-1) \( x \circ g(t) = (x \circ g(1)) \circ t \), or
(a-2) \( x \circ g(t) = (x \circ g(1)) \circ t + t \), or
(a-3) \( x \circ g(t) = (x \circ g(1)) \circ t + 1 \), or
(a-4) \( x \circ g(t) = (x \circ g(1)) \circ t + t + 1 \).

We recall the definition of \( K(Q) \). Then, if we multiply \( \alpha \in K(Q) \) from the left-hand side of the above equations (a-1)–(a-4), we have

\[
(\alpha \circ x) \circ g(t) = ((\alpha \circ x) \circ g(1)) \circ t, \text{ or }
(\alpha \circ x) \circ g(t) = ((\alpha \circ x) \circ g(1)) \circ t + \alpha \circ t, \text{ or }
(\alpha \circ x) \circ g(t) = ((\alpha \circ x) \circ g(1)) \circ t + \alpha, \text{ or }
(\alpha \circ x) \circ g(t) = ((\alpha \circ x) \circ g(1)) \circ t + \alpha \circ t + \alpha.
\]
Since $Q \ni x \mapsto \alpha \circ x \in Q$ is surjective mapping, if we replace $\alpha \circ x$ by $x$, we only have the following four cases for any $x \in Q$:

(b-1) $x \circ g(t) = (x \circ g(1)) \circ t$, or
(b-2) $x \circ g(t) = (x \circ g(1)) \circ t + \alpha \circ t$, or
(b-3) $x \circ g(t) = (x \circ g(1)) \circ t - \alpha$, or
(b-4) $x \circ g(t) = (x \circ g(1)) \circ t + \alpha \circ t + \alpha$.

By the assumption on $t$ of (5), (a-2), (a-3), (a-4) and (b-2), (b-3), (b-4) do not occur, hence we only have (a-1) = (b-1): $x \circ g(t) = (x \circ g(1)) \circ t$ for any $x \in Q$ and for any $t \in Q$ which satisfies the condition (5). Moreover, we also have $f(x) = x \circ g(1)$ and $x \circ g(t) = f(x) \circ t$. (That is, the cases $f(x) = x \circ g(1) + 1$ and $x \circ g(t) = f(x) \circ t + 1$ do not occur.) Hence, we have $f(x) = x \circ b^{-1}$ if we put $b^{-1} := g(1)$.

Now, let us take a general $t \in Q$, that is, we do not assume the condition (5) on $t$. Since $f(x) = x \circ b^{-1}$, we have from Eq. (4) that only the cases

(d-1) $x \circ g(t) = (x \circ b^{-1}) \circ t$ or
(d-2) $x \circ g(t) = (x \circ b^{-1}) \circ t + 1$

occur for any $x, t \in Q$. Hence if we multiply $\alpha$ from the left-hand side, we see that only the cases $(\alpha \circ x) \circ g(t) = ((\alpha \circ x) \circ b^{-1}) \circ t$ or $(\alpha \circ x) \circ g(t) = ((\alpha \circ x) \circ b^{-1}) \circ t + \alpha$ occur. Since $Q \ni x \mapsto \alpha \circ x \in Q$ is surjective mapping, if we replace $\alpha \circ x$ by $x$, only the cases

(e-1) $x \circ g(t) = (x \circ b^{-1}) \circ t$ or
(e-2) $x \circ g(t) = (x \circ b^{-1}) \circ t + \alpha$

occur for any $x$ and $t$ in $Q$. Since $\alpha \neq 0, 1$, we see that the cases (d-2) and (e-2) do not occur, and we only have (d-1) = (e-1) $x \circ g(t) = (x \circ b^{-1}) \circ t$, and $g(t) = b^{-1} \circ t$ if we put $x = 1$. Therefore we have $(x \circ b^{-1}) \circ t = x \circ (b^{-1} \circ t)$ for any $x$ and $t$ in $Q$, and we have $b \in N_m(Q) \setminus \{0\}$. □

Now, we have the following proposition.

**Proposition 14.** Let $Q_1$ and $Q_2$ be quasifields. We assume that $K(Q_1), K(Q_2) \supseteq \text{GF}(2)$. If dual hyperovals $S(Q_1)$ and $S(Q_2)$ are isomorphic by $\Psi$ and $\Psi(X_1(0)) = X_2(0)$, then the group $N_m(Q_1) \setminus \{0\}$ of $Q_1$ is isomorphic to the group $N_m(Q_2) \setminus \{0\}$ of $Q_2$.

**Proof.** By the assumption $\Psi(X_1(0)) = X_2(0)$ and by Corollary 7, we may assume that $\Psi((x, y)) = (a(x), d(y))$ for some GF(2)-linear mapping $a(x)$ and $d(y)$ as in the proof of Lemma 8. Hence, the automorphism $(x, y) \mapsto (f(x), y)$ of $S(Q_1)$ maps to the automorphism $(x, y) \mapsto (a(f(a^{-1}(x))), y)$ of $S(Q_2)$. Therefore, for any $b \in N_m(Q_1) \setminus \{0\}$, since the automorphism $m_b : (x, y) \mapsto (x \circ b^{-1}, y)$ of $S(Q_1)$ has the form $(x, y) \mapsto (f(x), y)$, it maps to the automorphism of $S(Q_2)$ which has the form $(x, y) \mapsto (a(f(a^{-1}(x))), y)$. By Lemma 13, for any automorphism of $S(Q_2)$ which has the form $(x, y) \mapsto (a(f(a^{-1}(x))), y)$, there exists $c \in N_m(Q_2) \setminus \{0\}$ such that $a(f(a^{-1}(x))) = x \circ c^{-1}$, hence this automorphism is $m_c$ by definition. Conversely, for automorphism $m_c$ of $S(Q_2)$ with $c \in N_m(Q_2) \setminus \{0\}$, it is easy to see that there exists $b \in N_m(Q_1) \setminus \{0\}$ such that $m_c$ maps to the automorphism $m_b$ of $S(Q_1)$ by $\Psi^{-1}$. Let
us define the mapping \( \theta : N_m(Q_1) \setminus \{0\} \mapsto N_m(Q_2) \setminus \{0\} \) by \( \theta(b) = c \). Then \( \theta \) is a one-to-one mapping. Moreover, it is easy to see that \( \theta \) is a group isomorphism. □

Corollary 15. Let \( S_1 \) and \( S_2 \) be semifields. We assume that \( K(S_1), K(S_2) \supseteq GF(2) \). If dual hyperovals \( S(S_1) \) and \( S(S_2) \) are isomorphic, then the groups \( N_m(S_1) \setminus \{0\} \) and \( N_m(S_2) \setminus \{0\} \) are isomorphic.

Proof. Since the multiplication \( \circ \) has left distributive law in the semifields \( S_1 \) and \( S_2 \), for any \( a \in S_1 \), there exists an automorphism \( t_a \) of \( S(S_1) \) such that \( t_a(X_1(t)) = X_1(t + a) \) for any \( X_1(t) \in S(S_1) \) by the mapping \( t_a(x, y) = (x, y + (x \circ a)\sigma + x \circ a) \), since

\[
t_a(X_1(t)) = \{ (x, (x \circ t)\sigma + x \circ t + (x \circ a)\sigma + x \circ a) \mid x \in S_1 \setminus \{0\} \} = X_1(t + a).
\]

If dual hyperovals \( S(S_1) \) and \( S(S_2) \) are isomorphic by \( \Psi \) and \( \Psi(X_1(a)) = X_2(0) \) for some \( a \in N_1 \setminus \{0\} \), then \( S(S_1) \) and \( S(S_2) \) are isomorphic by the mapping \( \Psi(t_a(x, y)) = X_2(0) \), hence the assumptions of Proposition 14 are satisfied by the isomorphism \( \Psi(t_a(x, y)) \). Therefore, the groups \( N_m(S_1) \setminus \{0\} \) and \( N_m(S_2) \setminus \{0\} \) are isomorphic by Proposition 14. □

By now, not so many middle nucleus of known semifields are determined. However, there exist semifields \( S_1 \) and \( S_2 \) with \( |S_1| = |S_2| = 16 \) such that \( |N_m(S_1)| \neq |N_m(S_2)| \). (See [2] or [7, 2.2 and 2.6].) So, it is likely that there are a lot of non-isomorphic \( d \)-dimensional dual hyperovals constructed from semifields of size \( 2^{d+1} \) for \( d \geq 3 \).

Acknowledgments

This work was supported by grant in aid for scientific research of Japan, No. 20540034.

References