数理解析研究所講究録
第 1593 巻 2008 年 213-218

On d-dual hyperovals in $PG(2d, 2)$

詫間電波高専　谷口浩朗 (Hiroaki Taniguchi)
Takuma National College of Technology

1 はじめに

射影空間 $PG(m, 2)$ 内の高次元双対超卵形 (dimensional dual hyperoval, DHO) は C. Huybrechts と A. Pasini [2] により以下のように定義されました.

定義 1 (DHO). A family S of d-dimensional subspaces of $PG(m, 2)$ is called a d-dimensional dual hyperoval in $PG(m, 2)$ 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 $PG(m, 2)$, and
4. there are exactly 2^{d+1} members of S.

この稿では、概体 (quasifield) から構成された高次元双対超卵形、その中でもとくに擬体 (nearfield) から構成される DHO について考察します.

定義 2 (概体). 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 $1 \in Q\backslash\{0\}$ 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 $x \circ a - x \circ b = c$.

擬体 (near field) とは，積 $\circ$ に関して結合法則が成り立つ概体のことです．また半体 (semifield) とは，左分配法則が成り立つ概体のことです．標数 2 の概体から以下のようにして射影空間 $PG(2d, 2)$ 内の d 次元双対超卵形が構成できます．

命題 1. *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 Tr the trace function from $GF(2^{d+1})$ to $GF(2)$. Let σ be a generator of the galois group $Gal(GF(2^{d+1})/GF(2))$.*

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

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

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

本稿の主な目的は次の定理の証明の概要を説明することです．また，半体から構成される DHO の同型判定についても考察します．

定理 1. *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 $(N_2; *, +)$.*

たとえばnがメルセンヌ素数$n = 2^p - 1$で $q = 2^l$ (ただし $l = p, 2p, 4p, 8p, \ldots$) ならば位数 q^n の擬体の同型類が非常にたくさん存在し [3]，それにともない，この定理より同型でない DHO が非常にたくさん存在することがわかります．

2 特別な自己同型

擬体から命題 1 のようにして構成された DHO には，以下のような特別な自己同型が存在します．

補題 1. *For $b \in N\backslash\{0\}$, 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 $X(0) := \{(x,0) | x \in N\}$. Hence we see that the multiplicative group $(N\backslash\{0\}, \circ)$ acts regularly on $S(N)\backslash\{X(0)\}$.

上記の自己同型は，次の補題によって特徴付けられます．

補題 2. *Let Ψ be an automorphism of $S(N)$ defined by*

$$\Psi((x,y)) = (f(x), y),$$

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

3 定理 1の証明の概要

Cooperstein-Thas [1] による $PG(2d,2)$ における d 次元 DHO の次の特徴付けがあるので非常に助かります．

命題 2. *The subset*

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

is a $(d-1)$-dimensional subspace in $PG(2d,2)$.

我々の考察している状況に当てはめれば，次のようになります．

系 1. *Let $S(Q) = \{X(t) \mid t \in Q\}$ with $X(t) = \{(x, (x \circ t)^\sigma + x \circ t) \mid x \in Q\backslash\{0\}\}$ be a dual hyperoval constructed from a quasifield Q. Then, in $PG(2d,2) = \{(x,y) \mid x, y \in Q, Tr(y) = 0\}\backslash\{(0,0)\}$, we have*

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

これらにより，同型写像の形が次の補題のようになることが分かります．

補題 3. *Let* $(N_1; \circ, +)$ *and* $(N_2; *, +)$ *be Nearfields. We regard that the ambient space* $PG(2d, 2) = \{(x, y) \mid x, y \in N_1, Tr(y) = 0\} = \{(x, y) \mid x, y \in N_2, Tr(y) = 0\}$. *If dual hyperovals* $S(N_1)$ *and* $S(N_2)$ *are isomorphic by the automorphism of the ambient space* $\Phi : PG(2d, 2) \to PG(2d, 2)$, *we may assume that* Φ *is represenred, using some* $GF(2)$*-linear mapping* $a(x)$ *and* $d(y)$, *as follows:*

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

2節の「特別な自己同型」の作用については，以下の命題が成り立ちます．

命題 3. *Let* $(N_1; \circ, +)$ *and* $(N_2; *, +)$ *be nearfields. Let the dual hyperovals* $S(N_1)$ *and* $S(N_2)$ *are isomorphic by the mapping* Φ, *then there is a group isomorphism* $\theta : (N_1 \backslash \{0\}, \circ) \mapsto (N_2 \backslash \{0\}, *)$ *such that, for any* $b \in N_1 \backslash \{0\}$ *and for any* $X_1(t) \in S(N_1)$, *we have*

$$\Phi(m_b(X_1(t))) = m_{\theta(b)}(\Phi(X_1(t))).$$

これらを用いますと，定理の証明が次のように出来ます．

定理 1. *Let* $(N_1; \circ, +)$ *and* $(N_2; *, +)$ *be nearfields. If dual hyperovals* $S(N_1)$ *and* $S(N_2)$ *are isomorphic, then* $(N_1, \circ, +)$ *and* $(N_2, *, +)$ *are isomorphic.*

Proof. We assume that dual hyperovals $S(N_1)$ and $S(N_2)$ are isomorphic by Φ. Hence, we may assume that $\Phi(X_1(0)) = X_2(0)$. Therefore, Φ is represenred as $\Phi((x, y)) = (a(x), d(y))$ for some $GF(2)$-linear mapping $a(x)$ and $d(y)$. Moreover, we may assume that $\Phi(X_1(1)) = X_2(1)$. We define ρ by $\Phi(X_1(t)) = X_2(\rho(t))$. Then we have $\rho(0) = 0$ and $\rho(1) = 1$. We have

$$\Phi(m_b(X_1(t))) = m_{\theta(b)}(\Phi(X_1(t))) \tag{1}$$

using the group isomorphism $N_1 \backslash \{0\} \ni b \mapsto \theta(b) \in N_2 \backslash \{0\}$. 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 the equation (1), we have

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

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

$$a(x \circ b^{-1}) = a(x) * \theta(b^{-1}). \tag{2}$$

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

$$(a(x), d((x \circ t)^\sigma + x \circ t)) = (a(x), (a(x) * \rho(t))^\sigma + a(x) * \rho(t)),$$

hence we have $d((x \circ t)^\sigma + x \circ t) = (a(x) * \rho(t))^\sigma + a(x) * \rho(t)$ 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 $X_2(0)$;

$$\Phi : X_1(0) \ni (x, 0) \mapsto (a(x), 0) \in X_2(0), \tag{3}$$

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 the equation (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 the equation (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 $X_2(0) = \{(x, 0) \mid x \in N_2\}$, 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 $(N_1; \circ, +) \cong (N_2; *, +)$. □

4 半体から構成されるDHOについて

定義 3. Let $(Q; +, \circ)$ be a quasifield.

(1) The set

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

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 $N_m(Q) \backslash \{0\}$ is a subgroup of Q.

一般の概体から構成されるDHOにおいても，次の「特別な自己同型」が存在します．

補題 4. *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 $S(Q)\setminus\{X(0)\}$.

また，この自己同型は次のように特徴付けられます.

補題 5. *We assume that $K(Q)\supsetneq GF(2)$. Inside $PG(2d,2)=\{(x,y)\mid x,y\in Q, Tr(y)=0\}\setminus\{(0,0)\}$, let Ψ 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 $b\in N_m(Q)\setminus\{0\}$.

この特徴付けの応用として, とくに半体から構成されるDHOが同型でないことの判定に次の系が使えます.

系 2. *Let S_1 and S_2 be semifields. We assume that $K(S_1)$, $K(S_2)\supsetneq GF(2)$. 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.*

小さい位数$|S_1|=|S_2|=16$でしかも$|N_m(S_1)|\neq|N_m(S_2)|$となる半体S_1 S_2があるので，半体から構成されるDHOで同型でないものが非常に多くあることが期待されます.

References

[1] B. N. Cooperstein and J. A. Thas, On Generalized k-Arcs in $PG(2n,q)$, Annals of Combinatorics. 5 (2001), 141–152.

[2] C. Huybrechts and A. Pasini, Frag-transitive extensions of dual affine spaces, Contrib. Algebra Geom. 40. (1999), 503–532.

[3] H. Lüneburg, Translation Planes, Springer-Verlag (1980).

[4] H. Taniguchi, On d-dimensional dual hyperovals in $PG(2d,2)$, to appear in Innovations in Incidence Geometry.