A variation of the dual hyperoval $\mathcal{S}_c$ using a presemifield

Finite Geometries Fifth Irsee Conference,
September 10–16, 2017.

Hiroaki Taniguchi
National Institute of Technology, Kagawa College

Definitions: (Huybrechts and Pasini, 1999)

d-**dimensional dual hyperoval** $\mathcal{S}$ **in** $V(n,q)$ is a set of $(d+1)$-subspaces:

(1) $\mathcal{S}$ consists of $q^d + q^{d-1} + \cdots + q + 2$ $(d+1)$-subspaces, $(= 2^{d+1}$ if $q = 2.)$

(2) any two distinct $(d+1)$-subspaces of $\mathcal{S}$ meet a one dimensional subspace,

(3) any three distinct $(d+1)$-subspaces of $\mathcal{S}$ intersect trivially,

(4) $(d+1)$-subspaces of $\mathcal{S}$ span $V(n,q)$.

[Bilinear DHO $\mathcal{S}_B$ with the bilinear mappig $B(x,t)$]

V: $(d+1)$-dimensional vector space over $GF(2)$ with $d \geq 2$.

$B : V \oplus V \to W$: a $GF(2)$-bilinear mapping with

$\exists$ 1 non-zero solution for (i) $B(x,a) = 0$ and (ii) $B(a,x) = 0$ for any $a \neq 0$.

In $V \oplus W$, for $t \in V$, let

$$X(t) = \{\ (x,\ \ B(x,t))\ |\ x \in V\ \}.$$

Then $\mathcal{S} = \{X(t) \mid t \in V\}$ is a d-dimensional DHO in $V \oplus W$.

[Bilinear DHO $\mathcal{S}_B$ with the bilinear mappig $B(x,t)$]

V: $(d+1)$-dimensional vector space over $GF(2)$ with $d \geq 2$.

$B : V \oplus V \to W$: a $GF(2)$-bilinear mapping with

$\exists$ 1 non-zero solution for $B(x,a) = 0$ for any $a \neq 0$ if $B(x,y) = B(y,x)$.

In $V \oplus W$, for $t \in V$, let

$$X(t) = \{\ (x,\ \ B(x,t)) \mid x \in V\ \}.$$

Then $\mathcal{S} = \{X(t) \mid t \in V\}$ is a d-dimensional DHO in $V \oplus W$.

[DHO $\mathcal{S}_c(n, GF(2^r))$] [T,2014]

Let $K = GF(2^r) \ni c$ with $Tr(c) = 1$(i.e, $xy + cx^2 + cy^2 \neq 0$ for $x, y \in K^*$).
$V_1 := \langle e_1, \ldots, e_n \rangle$: n-dimensional K-vector space.
$W := S(V_1 \otimes_K V_1)$ (symmetric tensor space: $x \otimes y = y \otimes x$)

$V := V_1 \oplus \langle e_0 \rangle$ direct sum of $GF(2)$-vector spaces.

[Definition of $B(x, t)$ for $x, t \in V$] ($B : V \oplus V \to W$)
Define $B(x + \alpha e_0, t + \beta e_0) = x \otimes t + \alpha c y \otimes y + \beta c x \otimes x$,
where $\alpha, \beta \in GF(2)$.

[Definition of DHO $\mathcal{S}_c(n, GF(2^r))$]
In $U = V \oplus W$, for $t \in V$, let $X(t) = \{ \ (x, \ B(x, t)) \mid x \in V \ \}$
Then $\mathcal{S}_c(n, GF(2^r)) = \{X(t) \mid t \in V\}$
is a $d = rn$-dim. DHO in $U = V \oplus W$

[Definition of Bilinear Mapping B of $\mathcal{S}_c(n, GF(2^r))$]

Let $K = GF(2^r)$. Define V, W as direct sum of $GF(2)$-vector spaces as follows.

$$V := (\overbrace{K \oplus \cdots \oplus K}^{n}) \oplus GF(2) = (\overbrace{K \oplus \cdots \oplus K}^{n}) \oplus \langle e_0 \rangle$$

$$W := (\overbrace{K \oplus \cdots \oplus K}^{n}) \oplus (\overbrace{K \oplus \cdots \oplus K \oplus \cdots \oplus K}^{\binom{n}{2}}).$$

Define a $GF(2)$-bilinear mapping $B : V \oplus V \to W$ by

$$B : V \oplus V \ni ((\ldots, x_i, \ldots, x_j, \ldots, \alpha), (\ldots, y_i, \ldots, y_j, \ldots, \beta)) \mapsto$$
$$(\ldots, x_i y_i + \alpha c y_i^2 + \beta c x_i^2, \ldots, x_i y_j + y_i x_j, \ldots) \in W$$

for $(\ldots, x_i, \ldots, \alpha), (\ldots, y_i, \ldots, \beta) \in V = (K \oplus \cdots \oplus K) \oplus GF(2) = V_1 \oplus \langle e_0 \rangle$.

[Presemifield]

Let $GF(q)$ be a finite field of q elements.

$S = (GF(q), +, \circ)$: a presemifield $\Longleftrightarrow$ S: an additive group $(GF(q), +)$ and $\circ$ satisfies distributive laws and $x \circ y = 0$ iff $x = 0$ or $y = 0$.

S: a semifield if $S = (GF(q), +, \circ)$ has a multiplicative identity.

[Presemifield]

Let $GF(q)$ be a finite field of q elements.

$S = (GF(q), +, \circ)$: a presemifield $\iff S$: an additive group $(GF(q), +)$ and $\circ$ satisfies distributive laws and $x \circ y = 0$ iff $x = 0$ or $y = 0$.

S: a semifield if $S = (GF(q), +, \circ)$ has a multiplicative identity.

Let $S_1 = (GF(q), +, \circ_1)$ and $S_2 = (GF(q), +, \circ_2)$ be presemifields. S_1 and S_2 are isotopic if $\exists\ \lambda_1, \lambda_2, \rho : GF(q) \to GF(q)$ such that

$$x^{\lambda_1} \circ_2 y^{\lambda_2} = (x \circ_1 y)^{\rho}.$$

It is known that any presemifield is isotopic to a semifield.

[Albert Presemifield]

Let q_1 be a prime power and $m > 1$ an integer. Let $F := GF(q)$ with $q = q_1^m$. Let $\sigma, \tau \in Gal(F/GF(q_1))$, with $1 \neq \sigma \neq \tau \neq 1$ and $\langle \sigma, \tau \rangle = Gal(F/GF(q_1))$. Let $N = F^{\sigma-1}F^{\tau-1}$. Let $\alpha \in F \backslash N$. Define

$$x \star y := xy - \alpha x^{\sigma} y^{\tau}$$

for any $x, y \in F$. Then $S = (F, +, \star)$ is the Albert presemifield.

[Albert Presemifield]

Fact [Biliotti, Jha, Johnson, 1999]

For $i = 1, 2$, $S_i = (F, +, \star_i)$: the Albert presemifields by $x \star_i y := xy - \alpha_i x^{\sigma_i} y^{\tau_i}$.
Then S_1 and S_2 are isotopic if and only if
(1) $\sigma_1 = \sigma_2$, $\tau_1 = \tau_2$ and $\alpha_1^{\mu} = \alpha_2(\beta^{\sigma_2 - 1}\gamma^{\tau_2 - 1}) = \alpha_2(\beta^{\sigma_1 - 1}\gamma^{\tau_1 - 1})$ for some $\mu \in Aut(F)$ and $\beta, \gamma \in F \backslash \{0\}$, or
(2) $\sigma_1^{-1} = \sigma_2$, $\tau_1^{-1} = \tau_2$ and $\alpha_1^{\mu} = -\alpha_2^{-1}(\beta^{1-\sigma_2}\gamma^{1-\tau_2}) = -\alpha_2^{-1}(\beta^{1-\sigma_1^{-1}}\gamma^{1-\tau_1^{-1}})$ for some $\mu \in Aut(F)$ and $\beta, \gamma \in F \backslash \{0\}$.

Cor. Let $S = (F, +, \star)$: the Albert presemifield by $x \star y := xy - \alpha x^{\sigma} y^{\tau}$.
If $\sigma \neq \tau$ and $\sigma \neq \tau^{-1}$ then
$S = (F, +, \star)$ is non-isotopic to any commutative presemifields.

[Definition of Bilinear Mapping]

For $i = 1, \ldots, n$, let $K_i = K = GF(2^r)$. Let $S_{ij} = (GF(2^r), +, \star_{ij})$ be presemifields for $1 \leq i < j \leq n$.

$$V: \quad = (\overbrace{K_1 \oplus \cdots \oplus K_n}^{n}) \oplus GF(2) = (\overbrace{K \oplus \cdots \oplus K}^{n}) \oplus \langle e_0 \rangle,$$

$$W: \quad = (\overbrace{K_1 \oplus \cdots \oplus K_n}^{n}) \oplus (\overbrace{S_{12} \oplus \cdots \oplus S_{ij} \oplus \cdots \oplus S_{n-1n}}^{\binom{n}{2}})$$

direct sums as $GF(2)$-vector spaces.

xy for $x, y \in K = GF(2^r)$ is the ordinary field multiplication.
Assume $c \in K \backslash \{0\} = GF(2^r) \backslash \{0\}$ satisfies the following conditions
(c1) $Tr(c) = 1$ (which means $xy + cx^2 + cy^2 \neq 0$ for $x, y \in GF(2^r) \backslash \{0\}$), and
(c2) $(cx) \star_{ij} y = x \star_{ij} (cy)$ for any $x, y \in GF(2^r)$.

[Definition of Bilinear Mapping]

Let $S_{ij} = (GF(2^r), +, \star_{ij})$ be presemifields for $1 \leq i < j \leq n$.

$$V := (\overbrace{K \oplus \cdots \oplus K}^{n}) \oplus GF(2) = (\overbrace{K \oplus \cdots \oplus K}^{n}) \oplus \langle e_0 \rangle$$

$$W := (\overbrace{K \oplus \cdots \oplus K}^{n}) \oplus (\overbrace{S_{12} \oplus \cdots \oplus S_{ij} \oplus \cdots \oplus S_{n-1n}}^{\binom{n}{2}}).$$

Define a $GF(2)$-bilinear mapping $B : V \oplus V \to W$ by

$$B : V \oplus V \ni ((\ldots, x_i, \ldots, x_j, \ldots, \alpha), (\ldots, y_i, \ldots, y_j, \ldots, \beta)) \mapsto$$
$$(\ldots, x_i y_i + \alpha c y_i^2 + \beta c x_i^2, \ldots, x_i \star_{ij} y_j + y_i \star_{ij} x_j, \ldots) \in W$$

for $(\ldots, x_i, \ldots, \alpha), (\ldots, y_i, \ldots, \beta) \in V = (K \oplus \cdots \oplus K) \oplus GF(2) = V_1 \oplus \langle e_0 \rangle$.

[Definition of Bilinear Mapping]

Define a $GF(2)$-bilinear mapping $B : V \oplus V \to W = (\oplus_i K_i) \oplus (\oplus_{i<j} S_{ij})$ by

$$B((\ldots, x_i, \ldots, \alpha), (\ldots, y_i, \ldots, \beta)) := \\ (\ldots, x_i y_i + \alpha c y_i^2 + \beta c x_i^2, \ldots, x_i \star_{ij} y_j + y_i \star_{ij} x_j, \ldots)$$

for $(\ldots, x_i, \ldots, \alpha), (\ldots, y_i, \ldots, \beta) \in V = (K_1 \oplus \cdots \oplus K_n) \oplus GF(2) = V_1 \oplus \langle e_0 \rangle$.

[Definition of Bilinear Mapping]

Define a $GF(2)$-bilinear mapping $B : V \oplus V \to W = (\oplus_i K_i) \oplus (\oplus_{i<j} S_{ij})$ by

$$B((\ldots, x_i, \ldots, \alpha), (\ldots, y_i, \ldots, \beta)) := (\ldots, x_i y_i + \alpha c y_i^2 + \beta c x_i^2, \ldots, x_i \star_{ij} y_j + y_i \star_{ij} x_j, \ldots)$$

for $(\ldots, x_i, \ldots, \alpha), (\ldots, y_i, \ldots, \beta) \in V = (K_1 \oplus \cdots \oplus K_n) \oplus GF(2) = V_1 \oplus \langle e_0 \rangle$.

If $B(x, (y_1, \ldots, y_i, \ldots, y_n, 0)) = 0$ then $x = (cy_1, \ldots, cy_i, \ldots, cy_n, 1)$.

If $B(x, (0, \ldots, 0, \ldots, 0, 1)) = 0$ then $x = (0, \ldots, 0, \ldots, 0, 1) = e_0$.

If $B(x, (y_1, \ldots, y_i, \ldots, y_n, 1)) = 0$ then $x = (c^{-1}y_1, \ldots, c^{-1}y_i, \ldots, c^{-1}y_n, 0)$.

$$B(x,(y_1,\ldots,y_i,\ldots,y_n,0))=0 \implies x=(cy_1,\ldots,cy_i,\ldots,cy_n,1).$$
$$B(x,(0,\ldots,0,\ldots,0,1))=0 \implies x=(0,\ldots,0,\ldots,0,1)=e_0.$$
$$B(x,(y_1,\ldots,y_i,\ldots,y_n,1))=0 \implies x=(c^{-1}y_1,\ldots,c^{-1}y_i,\ldots,c^{-1}y_n,0).$$

Thus the condition "$\exists$ 1 non-zero solution for $B(x,a)=0$ for any $a\neq 0$" is satisfied.

Let $\mathcal{S}=\{X(t)\mid t\in V\}$ be a set of vector subspaces defined by

$$X(t)=\{(x,B(x,t))\mid x\in V\}\subset V\oplus W.$$

[Theorem 1] $\mathcal{S}$ is a DHO in $V\oplus W$.

[Def. $\mathcal{S}_1$ and $\mathcal{S}_2$ are isomorphic]

$\mathcal{S}_1$ and $\mathcal{S}_2$ are isomorphic $\Longleftrightarrow$
$\exists$ linear isomorphism $\phi : \langle \mathcal{S}_1 \rangle \mapsto \langle \mathcal{S}_2 \rangle$ which induces one-to-one mapping $\mathcal{S}_1 \to \mathcal{S}_2$.

[Dempwolff and Edel, 2014]

Let $V^{(i)}$ and $W^{(i)}$ be $GF(2)$-vector spaces for $i = 1, 2$. Let $B_i : V^{(i)} \oplus V^{(i)} \to W^{(i)}$ be $GF(2)$-bilinear mappings for $i = 1, 2$. Let $\mathcal{S}_1$, $\mathcal{S}_2$ be bilinear dual hyperovals with the bilinear mappings B_1, B_2. Then $\mathcal{S}_1$ and $\mathcal{S}_2$ are isomorphic $\Longleftrightarrow \exists\ \lambda, \mu : V^{(1)} \to V^{(2)}$, $\rho : W^{(1)} \to W^{(2)}$ s.t.

$$B_2(x^{\lambda}, y^{\mu}) = B_1(x, y)^{\rho}.$$

[On isomorphism problem]

[Definition of Bilinear Mappings B_i for $i = 1, 2$]

Let $K^{(i)} = K = GF(2^r)$.
Let $S_{jk}^{(i)} = (GF(2^r), +, \star_{ijk})$ be presemifields for $1 \leq j < k \leq n$.

$$\begin{aligned} V^{(i)} : &= (\overbrace{K^{(i)} \oplus \cdots, \oplus K^{(i)}}^{n}) \oplus GF(2) = (\overbrace{K^{(i)} \oplus \cdots, \oplus K^{(i)}}^{n}) \oplus \langle e_0 \rangle \\ W^{(i)} : &= (\overbrace{K^{(i)} \oplus \cdots \oplus K^{(i)}}^{n}) \oplus (\overbrace{S_{12}^{(i)} \oplus \cdots \oplus S_{jk}^{(i)} \oplus \cdots \oplus S_{n-1n}^{(i)}}^{\binom{n}{2}}) \end{aligned}$$

direct sums as $GF(2)$-vector spaces.

Let $B_i : V^{(i)} \oplus V^{(i)} \to W^{(i)}$ be biliner mappings for $i = 1, 2$.

[Theorem 2]

For $i = 1, 2$, let $\mathcal{S}_i$ be dual hyperovals with the bilinear mappings

$$B_i((x,\alpha),(y,\beta)) = (\ldots, x_j y_j + \alpha c_i y_j^2 + \beta c_i x_j^2, \ldots, x_j \star_{ijk} y_k + y_j \star_{ijk} x_k, \ldots).$$

Assume $\mathcal{S}_{jk}^{(2)}$ are non-isotopic to commutative presemifields for $1 \leq j < k \leq n$, and $c_2 \neq 1$. Let $\mathcal{S}_1$ and $\mathcal{S}_2$ be isomorphic. Then

- $\exists \mu \in Gal(GF(2^r)/GF(2))$ such that ${c_1}^{\mu} = c_2$.
- $\exists$ a permutation $\sigma \in S_n$ such that $S_{ij}^{(1)}$ is isotopic to $S_{\sigma(i)\sigma(j)}^{(2)}$ if $\sigma(i) < \sigma(j)$, or $S_{ij}^{(1)}$ is anti-isotopic to $S_{\sigma(j)\sigma(i)}^{(2)}$ if $\sigma(i) > \sigma(j)$.
  (anti-isotopic means $\exists \lambda, \mu, \rho$ such that $(x \star_1 y)^{\rho} = y^{\lambda} \star_2 x^{\mu}$.)

[Dempwolff and Edel]

$B_i : V^{(i)} \oplus V^{(i)} \to W^{(i)}$ be $GF(2)$-bilinear mappings for $i = 1, 2$.
Let $\mathcal{S}_1$, $\mathcal{S}_2$ be bilinear dual hyperovals with the bilinear mappings B_1, B_2.
Then $\mathcal{S}_1$ and $\mathcal{S}_2$ are isomorphic $\iff \exists\ \lambda, \mu : V^{(1)} \to V^{(2)}$, $\rho : W^{(1)} \to W^{(2)}$ s.t.

$$B_2(x^\lambda, y^\mu) = B_1(x, y)^\rho.$$

Recall $V^{(i)} = (\overbrace{K^{(i)} \oplus \cdots , \oplus K^{(i)}}^{n}) \oplus GF(2) = (\oplus_{j=1}^n K_j^{(i)}) \oplus \langle e_0 \rangle$. Then:

- ${e_0}^\lambda = {e_0}^\mu = e_0$,
- if $c_2 \neq 1$ then $\lambda = \mu$
- if $c_2 \neq 1$ then $(\oplus_{i=1}^n K_i^{(1)})^\lambda = \oplus_{i=1}^n K_i^{(2)}$ and $(c_1 x)^\lambda = c_2 x^\lambda$ for $x \in \oplus_{i=1}^n K_i^{(1)}$.

Let us express $\lambda : V_1^{(1)} = \oplus_{i=1}^n K_i^{(1)} \to V_1^{(2)} = \oplus_{i=1}^n K_i^{(2)}$ by

$$\lambda : (\ldots, x_i, \ldots) \mapsto (\ldots, \sum_{j=1}^{n} x_j^{\lambda_{ij}}, \ldots)$$

using $GF(2)$-linear maps $\lambda_{ij} : K_j^{(1)} = K \to K_i^{(2)} = K$.

By "Dempwolff-Edel" $B_1(x,y)^\rho = B_2(x^\lambda, y^\lambda)$ for $x, y \in V_1^{(1)} = \oplus_{i=1}^n K_i^{(1)}$,

$$(\ldots, x_i y_i, \ldots, x_j y_j, \ldots, \ldots, x_i \star y_j + y_i \star x_j, \ldots)^\rho =$$

$$(\ldots, (\sum_{i=1}^{n} x_i{}^{\lambda_{ki}})(\sum_{i=1}^{n} y_i{}^{\lambda_{ki}}), \ldots, (\sum_{i=1}^{n} x_i{}^{\lambda_{li}})(\sum_{i=1}^{n} y_i{}^{\lambda_{li}}), \ldots,$$

$$\ldots, (\sum_{i=1}^{n} x_i{}^{\lambda_{ji}}) \star_{jk} (\sum_{i=1}^{n} y_i{}^{\lambda_{ki}}) + (\sum_{i=1}^{n} y_i{}^{\lambda_{ji}}) \star_{jk} (\sum_{i=1}^{n} x_i{}^{\lambda_{ki}}), \qquad \ldots).$$

if we put $y_i := x_i$ and $x_j = y_j = 0$ for $j \neq i$, we have

$$(0, \dots, 0, x_i^2, 0, \dots, 0)^\rho =$$
$$({(x_i}^{\lambda_{1i}})^2, \dots, ({x_i}^{\lambda_{ji}})^2, \dots, ({x_i}^{\lambda_{ni}})^2, 0, \dots, 0).$$

Hence there exist $GF(2)$-linear maps $f_{ij} : K_i^{(1)} \ni x_i^2 \mapsto ({x_i}^{\lambda_{ji}})^2 \in K_j^{(2)}$ such that

$$(0, \dots, 0, t_i, 0, \dots, 0, 0)^\rho = (f_{i1}(t_i), \dots, f_{ij}(t_i), \dots, f_{in}(t_i), 0, \dots, 0).$$

if we put $y_i := x_i$ and $x_j = y_j = 0$ for $j \neq i$, we have

$$(0, \ldots, 0, x_i^2, 0, \ldots, 0)^\rho =$$
$$(({x_i}^{\lambda_{1i}})^2, \ldots, ({x_i}^{\lambda_{ji}})^2, \ldots, ({x_i}^{\lambda_{ni}})^2, 0, \ldots, 0).$$

Hence there exist $GF(2)$-linear maps $f_{ij} : K_i^{(1)} \ni x_i^2 \mapsto ({x_i}^{\lambda_{ji}})^2 \in K_j^{(2)}$ such that

$$(0, \ldots, 0, t_i, 0, \ldots, 0, 0)^\rho = (f_{i1}(t_i), \ldots, f_{ij}(t_i), \ldots, f_{in}(t_i), 0, \ldots, 0).$$

Thus, substitute t_i by $x_i y_i$, we have

$$\begin{aligned} & (0, \ldots, 0, x_i y_i, 0, \ldots, 0)^\rho \\ = \quad & (f_{i1}(x_i y_i), \ldots, f_{ij}(x_i y_i), \ldots, f_{in}(x_i y_i), 0, \ldots, 0). \end{aligned}$$

Thus, for $(0,\ldots,0,x_i,0,\ldots,0),(0,\ldots,0,y_i,0,\ldots,0) \in V_1^{(1)} = \oplus_{i=1}^n K_i^{(1)}$,

$$
\begin{aligned}
B_1(x,y)^\rho &= (0,\ldots,0,x_iy_i,0,\ldots,0,\ldots,0)^\rho \\
&= (\ldots,f_{ij}(x_iy_i),\ldots,\overbrace{0,\ldots,0}^{\binom{n}{2}}) \\
B_2(x^\lambda,y^\lambda) &= (\ldots,{x_i}^{\lambda_{ji}}{y_i}^{\lambda_{ji}},\ldots,\overbrace{\ldots,{x_i}^{\lambda_{ji}} \star_{jk} {y_i}^{\lambda_{ki}} + {y_i}^{\lambda_{ji}} \star_{jk} {x_i}^{\lambda_{ki}},\ldots}^{\binom{n}{2}}).
\end{aligned}
$$

Thus, for $(0,\ldots,0,x_i,0,\ldots,0),(0,\ldots,0,y_i,0,\ldots,0) \in V_1^{(1)} = \oplus_{i=1}^n K_i^{(1)}$,

$$
\begin{aligned}
B_1(x,y)^\rho &= (0,\ldots,0,x_i y_i,0,\ldots,0,\ldots,0)^\rho \\
&= (\ldots,f_{ij}(x_i y_i),\ldots,\overbrace{0,\ldots,0}^{\binom{n}{2}}) \\
B_2(x^\lambda,y^\lambda) &= (\ldots,{x_i}^{\lambda_{ji}}{y_i}^{\lambda_{ji}},\ldots,\overbrace{\ldots,{x_i}^{\lambda_{ji}} \star_{jk} {y_i}^{\lambda_{ki}} + {y_i}^{\lambda_{ji}} \star_{jk} {x_i}^{\lambda_{ki}},\ldots}^{\binom{n}{2}}).
\end{aligned}
$$

Since $B_1(x,y)^\rho = B_2(x^\lambda,y^\lambda)$, for $i=1,\ldots,n$, and for $1 \le j < k \le n$,

1. $f_{ij}(x_i y_i) = {x_i}^{\lambda_{ji}}{y_i}^{\lambda_{ji}}$ in $K_j^{(2)} = K$, and
2. ${x_i}^{\lambda_{ji}} \star_{jk} {y_i}^{\lambda_{ki}} = {y_i}^{\lambda_{ji}} \star_{jk} {x_i}^{\lambda_{ki}}$ in $S_{jk}^{(2)}$.

For $i = 1, \ldots, n$, and for $1 \le j < k \le n$, we have

1. $f_{ij}(x_i y_i) = {x_i}^{\lambda_{ji}} {y_i}^{\lambda_{ji}}$ in $K_j^{(2)} = K$, and

2. ${x_i}^{\lambda_{ji}} \star_{jk} {y_i}^{\lambda_{ki}} = {y_i}^{\lambda_{ji}} \star_{jk} {x_i}^{\lambda_{ki}}$ in $S_{jk}^{(2)}$.

Using these equations, and since ρ is an isomorphism, we have

- λ_{ki} is not an isomorphism $\Longrightarrow$ λ_{ki} is a 0-mapping.
- $\exists k$ such that λ_{ki} is an isomorphism for $i = 1, \ldots, n$.
- if $\exists j \neq k$ such that $\lambda_{ji}, \lambda_{ki}$ are isomorphisms for some i, then $S_{jk}^{(2)}$ is isotopic to a commutative presemifield, contradicts to our assumption.

For $i = 1, \ldots, n$, and for $1 \leq j < k \leq n$, we have

1. $f_{ij}(x_i y_i) = {x_i}^{\lambda_{ji}} {y_i}^{\lambda_{ji}}$ in $K_j^{(2)} = K$, and

2. ${x_i}^{\lambda_{ji}} \star_{jk} {y_i}^{\lambda_{ki}} = {y_i}^{\lambda_{ji}} \star_{jk} {x_i}^{\lambda_{ki}}$ in $S_{jk}^{(2)}$.

Using these equations, and since ρ is an isomorphism, we have

- λ_{ki} is not an isomorphism $\Longrightarrow$ λ_{ki} is a 0-mapping.
- $\exists k$ such that λ_{ki} is an isomorphism for $i = 1, \ldots, n$.
- $\exists$ a permutation σ s.t. $\lambda_{\sigma(i)i}$ is an isomorphism, and $\{\lambda_{ki} \mid k \neq \sigma(i)\}$ are 0-mappings.

From $f_{ij}(x^2) = (x^{\lambda_{ji}})^2$ and $f_{ij}(xy) = x^{\lambda_{ji}}y^{\lambda_{ji}}$, we have

$x^{\lambda_{ji}} = \gamma x^{\mu}$ for some $\gamma \in GF(2^r)$ and $\mu \in Gal(GF(2^r)/GF(2))$.

From $f_{ij}(x^2) = (x^{\lambda_{ji}})^2$ and $f_{ij}(xy) = x^{\lambda_{ji}} y^{\lambda_{ji}}$, we have

$$x^{\lambda_{ji}} = \gamma x^{\mu} \text{ for some } \gamma \in GF(2^r) \text{ and } \mu \in Gal(GF(2^r)/GF(2)).$$

Since $\lambda_{\sigma(i)i}$ is an isomorphism, and $\lambda_{ki} = 0$-mapping for $k \neq \sigma(i)$, we have $(\ldots, x_i, \ldots, 0)^{\lambda} = (\ldots, x_i^{\lambda_{\sigma(i)i}}, \ldots, 0)$.

Since $(c_1 x)^{\lambda} = c_2 x^{\lambda}$ for $x \in V_1^{(1)} = \oplus_{i=1}^{n} K_i^{(1)}$, we have $(\ldots, c_1 x_i, \ldots, 0)^{\lambda} = (\ldots, (c_1 x_i)^{\lambda_{\sigma(i)i}}, \ldots, 0) = (\ldots, c_2 x_i^{\lambda_{\sigma(i)i}}, \ldots, 0)$.

From $f_{ij}(x^2) = (x^{\lambda_{ji}})^2$ and $f_{ij}(xy) = x^{\lambda_{ji}} y^{\lambda_{ji}}$, we have

$$x^{\lambda_{ji}} = \gamma x^{\mu} \text{ for some } \gamma \in GF(2^r) \text{ and } \mu \in Gal(GF(2^r)/GF(2)).$$

Since $\lambda_{\sigma(i)i}$ is an isomorphism, and $\lambda_{ki} = 0$-mapping for $k \neq \sigma(i)$, we have $(\ldots, x_i, \ldots, 0)^{\lambda} = (\ldots, x_i^{\lambda_{\sigma(i)i}}, \ldots, 0)$.

Since $(c_1 x)^{\lambda} = c_2 x^{\lambda}$ for $x \in V_1^{(1)} = \oplus_{i=1}^{n} K_i^{(1)}$, we have $(\ldots, c_1 x_i, \ldots, 0)^{\lambda} = (\ldots, (c_1 x_i)^{\lambda_{\sigma(i)i}}, \ldots, 0) = (\ldots, c_2 x_i^{\lambda_{\sigma(i)i}}, \ldots, 0)$.

Since $x^{\lambda_{\sigma(i)i}} = \gamma x^{\mu}$ for some $\gamma \in GF(2^r)$ and $\mu \in Gal(GF(2^r)/GF(2))$, we have $c_1^{\mu} = c_2$ for some $\mu \in Gal(GF(2^r)/GF(2))$.

Recall by “Dempwolff and Edel”

$$(\ldots, x_s y_s, \ldots, x_i \star_{ij} y_j + y_i \star_{ij} x_j, \ldots)^\rho =$$

$$\Big(\ldots, (\sum_{s=1}^{n} x_s^{\lambda_{is}})(\sum_{t=1}^{n} y_t^{\lambda_{it}}) \quad , \quad \ldots,$$

$$(\sum_{i=1}^{n} {x_i}^{\lambda_{si}}) \star_{st} (\sum_{j=1}^{n} {y_j}^{\lambda_{tj}}) \quad + \quad (\sum_{j=1}^{n} {y_j}^{\lambda_{sj}}) \star_{st} (\sum_{i=1}^{n} {x_i}^{\lambda_{ti}})\Big).$$

If we put $x_s = 0$ for $s \neq i$ and $y_t = 0$ for $t \neq j$ with $i < j$, we have

$$(0, \ldots, 0, x_i \star_{ij} y_j, 0, \ldots, 0)^\rho =$$

$$(\ldots, {x_i}^{\lambda_{ki}} {y_j}^{\lambda_{kj}}, \ldots, {x_i}^{\lambda_{si}} \star_{st} {y_j}^{\lambda_{tj}} + {y_j}^{\lambda_{sj}} \star_{st} {x_i}^{\lambda_{ti}}, \ldots).$$

Recall by "Dempwolff and Edel"

$$(\dots, x_s y_s, \dots, x_i \star_{ij} y_j + y_i \star_{ij} x_j, \dots)^\rho =$$

$$\Big(\dots, (\sum_{s=1}^{n} x_s^{\lambda_{is}})(\sum_{t=1}^{n} y_t^{\lambda_{it}}) \quad , \quad \dots,$$

$$(\sum_{i=1}^{n} {x_i}^{\lambda_{si}}) \star_{st} (\sum_{j=1}^{n} {y_j}^{\lambda_{tj}}) \quad + \quad (\sum_{j=1}^{n} {y_j}^{\lambda_{sj}}) \star_{st} (\sum_{i=1}^{n} {x_i}^{\lambda_{ti}})\Big).$$

Since $\lambda_{\sigma(i)i}$ isomorphism, λ_{ki} 0-mapping for $k \neq \sigma(i)$,

$$(0, \dots, 0, x_i \star_{ij} y_j, 0, \dots, 0)^\rho =$$

$$(\dots, {x_i}^{\lambda_{ki}} {y_j}^{\lambda_{kj}}, \dots, {x_i}^{\lambda_{si}} \star_{st} {y_j}^{\lambda_{tj}} + {y_j}^{\lambda_{sj}} \star_{st} {x_i}^{\lambda_{ti}}, \dots).$$

Recall by "Dempwolff and Edel"

$$(\ldots, x_s y_s, \ldots, x_i \star_{ij} y_j + y_i \star_{ij} x_j, \ldots)^\rho =$$

$$(\ldots, (\sum_{s=1}^{n} x_s^{\lambda_{is}})(\sum_{t=1}^{n} y_t^{\lambda_{it}}) \quad , \quad \ldots,$$

$$(\sum_{i=1}^{n} {x_i}^{\lambda_{si}}) \star_{st} (\sum_{j=1}^{n} {y_j}^{\lambda_{tj}}) \quad + \quad (\sum_{j=1}^{n} {y_j}^{\lambda_{sj}}) \star_{st} (\sum_{i=1}^{n} {x_i}^{\lambda_{ti}})).$$

Since $\lambda_{\sigma(i)i}$ isomorphism, λ_{ki} 0-mapping for $k \neq \sigma(i)$, if $\sigma(i) < \sigma(j)$ we have

$$(0, \ldots, 0, x_i \star_{ij} y_j, 0, \ldots, 0)^\rho =$$

$$(0, \ldots, 0, {x_i}^{\lambda_{\sigma(i)i}} \star_{\sigma(i)\sigma(j)} {y_j}^{\lambda_{\sigma(j)j}}, 0, \ldots, 0)$$

Recall by “Dempwolff and Edel”

$$(\ldots, x_s y_s, \ldots, x_i \star_{ij} y_j + y_i \star_{ij} x_j, \ldots)^\rho =$$

$$\Big(\ldots, (\sum_{s=1}^{n} x_s^{\lambda_{is}})(\sum_{t=1}^{n} y_t^{\lambda_{it}}) \quad , \quad \ldots,$$

$$(\sum_{i=1}^{n} {x_i}^{\lambda_{si}}) \star_{st} (\sum_{j=1}^{n} {y_j}^{\lambda_{tj}}) \quad + \quad (\sum_{j=1}^{n} {y_j}^{\lambda_{sj}}) \star_{st} (\sum_{i=1}^{n} {x_i}^{\lambda_{ti}})\Big).$$

Since $\lambda_{\sigma(i)i}$ isomorphism, λ_{ki} 0-mapping for $k \neq \sigma(i)$, if $\sigma(i) > \sigma(j)$ we have

$$(0, \ldots, 0, x_i \star_{ij} y_j, 0, \ldots, 0)^\rho =$$

$$(0, \ldots, 0, {y_j}^{\lambda_{\sigma(j)j}} \star_{\sigma(j)\sigma(i)} {x_i}^{\lambda_{\sigma(i)i}}, 0, \ldots, 0).$$

If $\lambda_{\sigma(i)i}$ isomorphism, λ_{ki} 0-mapping for $k \neq \sigma(i)$ for $\sigma \in S_n$, we have

$$(0,\ldots,0,x_i \star_{ij} y_j, 0,\ldots,0)^{\rho} =$$
$$(0,\ldots,0,{x_i}^{\lambda_{\sigma(i)i}} \star_{\sigma(i)\sigma(j)} {y_j}^{\lambda_{\sigma(j)j}}, 0,\ldots,0)$$

if $\sigma(i) < \sigma(j)$, and for $\sigma(i) > \sigma(j)$

$$(0,\ldots,0,x_i \star_{ij} y_j, 0,\ldots,0)^{\rho} =$$
$$(0,\ldots,0,{y_j}^{\lambda_{\sigma(j)j}} \star_{\sigma(j)\sigma(i)} {x_i}^{\lambda_{\sigma(i)i}}, 0,\ldots,0).$$

Proposition . *Assume $S_{ij}^{(2)}$ for $i < j$ are non-isotopic to commutative semifields,*
$\Longrightarrow \exists$ *a permutation $\sigma \in S_n$ such that*
(1) $S_{ij}^{(1)}$ and $S_{\sigma(i)\sigma(j)}^{(2)}$ are isotopic if $\sigma(i) < \sigma(j)$,
(2) $S_{ij}^{(1)}$ and $S_{\sigma(j)\sigma(i)}^{(2)}$ are anti-isotopic if $\sigma(i) > \sigma(j)$.

[Theorem 2]

For $i = 1, 2$, let $\mathcal{S}_i$ be dual hyperovals with the bilinear mappings

$$B_i((x, \alpha), (y, \beta)) = (\ldots, x_j y_j + \alpha c_i y_j^2 + \beta c_i x_j^2, \ldots, x_j \star_{ijk} y_k + y_j \star_{ijk} x_k, \ldots).$$

Assume $\mathcal{S}_{jk}^{(2)}$ are non-isotopic to commutative presemifields for $1 \leq j < k \leq n$, and $c_2 \neq 1$. Let $\mathcal{S}_1$ and $\mathcal{S}_2$ be isomorphic. Then

- $\exists \mu \in Gal(GF(2^r)/GF(2))$ such that ${c_1}^{\mu} = c_2$.
- $\exists$ a permutation $\sigma \in S_n$ such that $S_{ij}^{(1)}$ is isotopic to $S_{\sigma(i)\sigma(j)}^{(2)}$ if $\sigma(i) < \sigma(j)$, or $S_{ij}^{(1)}$ is anti-isotopic to $S_{\sigma(j)\sigma(i)}^{(2)}$ if $\sigma(i) > \sigma(j)$.
  (anti-isotopic means $\exists \lambda, \mu, \rho$ such that $(x \star_1 y)^{\rho} = y^{\lambda} \star_2 x^{\mu}$.)

Thank you for your attention.