Oyama, T.
Osaka J. Math.
22 (1985), 35-54

ON QUASIFIELDS

Dedicated to Professor Kentaro Murata on his 60th birthday

Tuyosi OYAMA

(Received August 22, 1983)

1. Introduction

A finite translation plane Π is represented in a vector space $V(2n, q)$ of dimension $2n$ over a finite field $GF(q)$, and determined by a spread $\pi=\{V(0), V(\infty)\} \cup \{V(\sigma) | \sigma \in \Sigma\}$ of $V(2n, q)$, where Σ is a subset of the general linear transformation group $GL(V(n, q))$. Furthermore Π is coordinatized by a quasifield of order q^n.

In this paper we take a $GF(q)$-vector space in $V(2n, q^n)$ and a subset Σ^* of $GL(n, q^n)$, and construct a quasifield. This quasifield consists of all elements of $GF(q^n)$, and has two binary operations such that the addition is the usual field addition but the multiplication is defined by the elements of Σ^*.

2. Preliminaries

Let q be a prime power. For $x \in GF(q^n)$ put $x=x^{(0)}$, $\bar{x}=x^{(1)}=x^q$ and $x^{(i)}=x^{q^i}$, $i=2, 3, \cdots, n-1$. Then the mapping $x \rightarrow x^{(i)}$ is the automorphism of $GF(q^n)$ fixing the subfield $GF(q)$ elementwise.

For a matrix $\alpha=(a_{ij}) \in GL(n, q^n)$ put $\bar{\alpha}=(\overline{a_{ij}})$. Let

$$\omega=\begin{pmatrix} 0 & \cdots & \cdots & 0 & 1 \\ 1 & 0 & \cdots & \cdots & 0 \\ 0 & \ddots & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 1 & 0 \end{pmatrix}$$

be an $n \times n$ permutation matrix. Set $\mathfrak{A}=\{\alpha \in GL(n, q^n) | \bar{\alpha}=\alpha\omega\}$.

Lemma 2.1. *$\mathfrak{A}=GL(n, q)\alpha_0$ for any $\alpha_0 \in \mathfrak{A}$. Furthermore let α be an $n \times n$ matrix over $GF(q^n)$. Then $\alpha \in \mathfrak{A}$ if and only if*

$$\alpha=\begin{pmatrix} a_0 & a_0^{(1)} & \cdots & a_0^{(n-1)} \\ a_1 & a_1^{(1)} & \cdots & a_1^{(n-1)} \\ \vdots & \vdots & & \vdots \\ a_{n-1} & a_{n-1}^{(1)} & \cdots & a_{n-1}^{(n-1)} \end{pmatrix}$$

and $a_0, a_1, \cdots, a_{n-1}$ are linearly independent over the field $GF(q)$.

Proof. For any element δ of $GL(n, q)$, $\overline{\delta\alpha_0}=\delta\bar{\alpha}_0=\delta\alpha_0\omega$. Hence $\delta\alpha_0\in\mathfrak{A}$. Conversely for any element α of $\mathfrak{A}$, $\overline{\alpha\alpha_0^{-1}}=\alpha\omega\omega^{-1}\alpha_0^{-1}=\alpha\alpha_0^{-1}\in GL(n, q)$ and so $\alpha\in GL(n, q)\alpha_0$. Thus $\mathfrak{A}=GL(n, q)\alpha_0$.

Let $\alpha=(a_{ij})$ be any element of $\mathfrak{A}$. Since $\bar{\alpha}=\alpha\omega$, $\overline{a_{i1}}=a_{i2}$, $\overline{a_{i2}}=a_{i3}, \cdots, \overline{a_{i\,n-1}}=a_{in}$, $i=1, 2, \cdots, n$. Hence $a_{ij}=a_{i1}^{(j-1)}$, $i=1, 2, \cdots, n, j=2, 3, \cdots, n$. Furthermore since α is a non-singular matrix, $a_{11}, a_{21}, \cdots, a_{n1}$ are linearly independent over $GF(q)$.

The converse is clear.

Lemma 2.2. *If $\alpha\in\mathfrak{A}$, then*

$$\alpha^{-1}=\begin{pmatrix} a_0 & a_1 & \cdots a_{n-1} \\ a_0^{(1)} & a_1^{(1)} & \cdots a_{n-1}^{(1)} \\ \vdots & \vdots & \vdots \\ a_0^{(n-1)} & a_1^{(n-1)} & \cdots a_{n-1}^{(n-1)} \end{pmatrix}\in GL(n, q^n).$$

Proof. Since $\alpha\in\mathfrak{A}$, $\bar{\alpha}=\alpha\omega$. Hence $\overline{\alpha^{-1}}=\omega^{-1}\alpha^{-1}$. Then the proof is similar to the proof of Lemma 2.1.

Lemma 2.3. *Let $\alpha\in\mathfrak{A}$. Then $GL(n, q)^{\alpha}=\{\gamma\in GL(n, q^n)\,|\,\bar{\gamma}=\gamma^{\omega}\}$.*

Proof. For any $\delta\in GL(n, q)$ $\overline{\delta^{\alpha}}=\delta^{\bar{\alpha}}=(\delta^{\alpha})^{\omega}$. Conversely let $\gamma\in GL(n, q^n)$ with $\bar{\gamma}=\gamma^{\omega}$. Then $\overline{\gamma^{\alpha^{-1}}}=\bar{\gamma}^{\overline{\alpha^{-1}}}=\gamma^{\omega\omega^{-1}\alpha^{-1}}=\gamma^{\alpha^{-1}}$. Thus $\gamma^{\alpha^{-1}}\in GL(n, q)$ and so $GL(n, q)^{\alpha}=\{\gamma\in GL(n, q^n)\,|\,\bar{\gamma}=\gamma^{\omega}\}$.

Since α is any element of $\mathfrak{A}$, we denote $GL(n, q)^{\alpha}$ by $GL(n, q)^*$.

Lemma 2.4. *Let γ be an $n\times n$ matrix over $GF(q^n)$. Then $\bar{\gamma}=\gamma^{\omega}$ if and only if*

$$\gamma=\begin{pmatrix} a_0 & a_{n-1}^{(1)} & \cdots & a_1^{(n-1)} \\ a_1 & a_0^{(1)} & \cdots & a_2^{(n-1)} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n-1} & a_{n-2}^{(1)} & \cdots & a_0^{(n-1)} \end{pmatrix}.$$

Proof. Let $\gamma=(a_{ij})$ with $\bar{\gamma}=\gamma^{\omega}$. Then

$$\begin{pmatrix} \overline{a_{11}}\,\overline{a_{12}}\cdots\overline{a_{1n}} \\ \overline{a_{21}}\,\overline{a_{22}}\cdots\overline{a_{2n}} \\ \cdots\cdots\cdots\cdots \\ \cdots\cdots\cdots\cdots \\ \overline{a_{n1}}\,\overline{a_{n2}}\cdots\overline{a_{nn}} \end{pmatrix}=\begin{pmatrix} a_{22}\,a_{23}\cdots a_{21} \\ a_{23}\,a_{33}\cdots a_{31} \\ \cdots\cdots\cdots\cdots \\ \cdots\cdots\cdots\cdots \\ a_{12}\,a_{13}\cdots a_{11} \end{pmatrix}.$$

Thus $a_{ij}=\overline{a_{i-1\,j-1}}$, $i, j=1, 2, \cdots, n$ modulo n. Hence $a_{i1}^{(j)}=a_{i+j\,1+j}$, $i, j=1, 2, \cdots, n$ modulo n, and so γ has the required form.

The converse is clear.

From Lemma 2.3 and Lemma 2.4 we have

Lemma 2.5.

$$GL(n, q)^{\alpha}=\left\{\begin{pmatrix} a_0 & a_{n-1}^{(1)} & \cdots & a_1^{(n-1)} \\ a_1 & a_0^{(1)} & \cdots & a_2^{(n-1)} \\ \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots \\ a_{n-1} & a_{n-2}^{(1)} & \cdots & a_0^{(n-1)} \end{pmatrix} \in GL(n, q^n)\right\}.$$

Let $V(2n, q)$ be a vector space of dimension $2n$ over $GF(q)$, and π be a nontrivial partition of $V(2n, q)$. If $V(2n, q)=V\oplus W$ for all V, $W\in\pi$ with $V\neq W$, then π is called a spread of $V(2n, q)$. Then the component of π is a n-dimensional $GF(q)$-subspace of $V(2n, q)$ [1].

Let π be a spread of $V(2n, q)$, then we can construct a translation plane $\pi(V(2n, q))$ of order q^n as follows [1]:

a) The points of $\pi(V(2n, q))$ are the vectors in $V(2n, q)$.

b) The lines are all cosets of all the components of π.

c) Incidence is inclusion.

Conversely any translation plane is isomorphic to some $\pi(V(2n, q))$.

We may assume that $V(2n, q)=V(n, q)\oplus V(n, q)$ is the outer sum of two copies of $V(n, q)$. Set $V(\infty)=\{(0, v)\,|\,v\in V(n, q)\}$, $V(0)=\{(v, 0)\,|\,v\in V(n, q)\}$ and $V(\sigma)=\{(v, v^{\sigma})\,|\,v\in V(n, q)\}$ for $\sigma\in GL(V(n, q))$. Then the followings hold ([6], Theorem 2.2, Theorem 2.3):

(I) Let π be a spread of $V(2n, q)$ containing $V(0)$, $V(\infty)$. Then we have:

a) If $V\in\pi$ and if $V\neq V(0)$, $V(\infty)$, then there is exactly one $\sigma\in GL(V(n, q))$ such that $V=V(\sigma)$. Set $\Sigma=\{\sigma\,|\,\sigma\in GL(V(n, q)),\ V(\sigma)\in\pi\}\cup\{0\}$.

b) If u, $v\in V(n, q)$, then there is exactly one σ in Σ such that $u^{\sigma}=v$.

c) If σ, $\rho\in\Sigma$ and if $\sigma\neq\rho$, then $\sigma-\rho\in GL(V(n, q))$.

(II) Conversely if a union Σ of a subset of $GL(V(n, q))$ and $\{0\}$ satisfies b) and c) of (I), then $\pi=\{V(\infty)\}\cup\{V(\sigma)\,|\,\sigma\in\Sigma\}$ is a spread of $V(2n, q)$.

3. Construction of quasifields

Let Q be a set with two binary operations $+$ and $\circ$. We call $Q(+, \circ)$ a quasifield, if the following conditions are satisfied:

1) $Q(+)$ is an abelian group.

2) If a, b, $c\in Q$, then $(a+b)\circ c=a\circ c+b\circ c$.

3) $a\circ 0=0$ for all $a\in Q$.

4) For a, $b\in Q$ with $a\neq 0$, there exists exactly one $x\in Q$ such that $a\circ x=b$.

5) For $a, b, c \in Q$ with $a \neq b$ there exists exactly one $x \in Q$ such that $x \circ a - x \circ b = c$.

6) There exists an element $1 \in Q \setminus \{0\}$ such that $1 \circ a = a \circ 1 = a$ for all $a \in Q$ (see [6] p. 22).

It is well known that an affine plane is a translation plane if and only if it is coordinatized by a quasifield (see [4], Theorem 6.1). Using this result, we give a new description of a quasifield.

After fixing a suitable basis in $V(n, q)$, we denote a vector v of $V(n, q)$ by the form $(x_0, x_1, \cdots, x_{n-1})$, $x_i \in GF(q)$. Let α be a fixed element of $\mathfrak{A}$ in the section 2. Then

$$\alpha = \begin{pmatrix} a_0 & a_0^{(1)} & \cdots & a_0^{(n-1)} \\ a_1 & a_1^{(1)} & \cdots & a_1^{(n-1)} \\ \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots \\ a_{n-1} & a_{n-1}^{(1)} & \cdots & a_{n-1}^{(n-1)} \end{pmatrix}.$$

Hence $v\alpha = (x, x^{(1)}, \cdots, x^{(n-1)}) \in V(n, q^n)$, $x = \sum_{i=0}^{n-1} x_i a_i$.

Conversely, let v^* be a vector of $V(n, q^n)$ of the form $(x, x^{(1)}, \cdots, x^{(n-1)})$, $x \in GF(q^n)$. Since $a_0, a_1, \cdots, a_{n-1}$ are linearly independent over $GF(q)$, x is uniquely represented by $a_0, a_1, \cdots, a_{n-1}$ such that $x = \sum_{i=0}^{n-1} x_i a_i$, $x_i \in GF(q)$. Hence $v^{*\alpha^{-1}} = (x_0, x_1, \cdots, x_{n-1}) \in V(n, q)$. Thus $V(n, q)^\alpha = \{(x, x^{(1)}, \cdots, x^{(n-1)}) \mid x \in GF(q^n)\}$, and $V(n, q)^\alpha$ is a $GF(q)$-vector space isomorphic to $V(n, q)$.

Set $V(2n, q)^\alpha = \{(u\alpha, v\alpha) \mid u, v \in V(n, q)\}$. Then similarly $V(2n, q)^\alpha$ is a $GF(q)$-vector space isomorphic to $V(2n, q)$.

Denote a vector $(x, x^{(1)}, \cdots, x^{(n-1)})$ of $V(n, q)^\alpha$ by $((x))$. Then any vector of $V(2n, q)^\alpha$ is denoted by $(((x)), ((y)))$. The additive group of $GF(q^n)$ is isomorphic to $V(n, q)^\alpha$ under a mapping $x \to ((x))$. In this mapping the inverse image of $v^* \in V(n, q)^\alpha$ is denoted by $\widehat{v^*}$.

Let M be any element of $GL(n, q)$. Since by Lemma 2.5

$$M^\alpha = \begin{pmatrix} x_0 & x_{n-1}^{(1)} & \cdots & x_1^{(n-1)} \\ x_1 & x_0^{(1)} & \cdots & x_2^{(n-1)} \\ \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots \\ x_{n-1} & x_{n-2}^{(1)} & \cdots & x_0^{(n-1)} \end{pmatrix},$$

M^α is uniquely determined by the first column $\begin{bmatrix} x_0 \\ x_1 \\ \vdots \\ x_{n-1} \end{bmatrix}$. Hence we denote M^α by $\begin{bmatrix} x_0 \\ x_1 \\ \vdots \\ x_{n-1} \end{bmatrix}$.

Let $\pi=\{V(\infty)\}\cup\{V(M)\mid M\in\Sigma\}$ be a spread of $V(2n, q)$, where Σ is a union of a subset of $GL(n, q)$ and $\{0\}$. Set $\pi^{\alpha}=\{V^*(\infty)\}\cup\{V^*(M^{\alpha})\mid M\in\Sigma\}$, where $V^*(\infty)=\{(((0)), ((x)))\mid((x))\in V(n, q)^{\alpha}\}$ and $V^*(M^{\alpha})=\{(((x)), ((x))M^{\alpha})\mid ((x))\in V(n, q)^{\alpha}\}$.

Then since $(v\alpha)M^{\alpha}=(vM)\alpha$, π^{α} is a spread of $V(2n, q)^{\alpha}$. Hence π^{α} determines a translation plane, which is denoted by Π^*. From now on we may assume that a spread π^{α} contains $V^*(1)=\{(((x)), ((x)))\mid((x))\in V(n, q)^{\alpha}\}$ ([6], Lemma 2.1).

For any two vectors $((x))\neq((0))$, $((y))$ of $V(n, q)^{\alpha}$, there is a unique matrix $M^{\alpha}\in\Sigma^{\alpha}$ such that $((x))M^{\alpha}=((y))$. Set $((x))=((1))=(1, 1, \cdots, 1)$. Then any element y of $GF(q^n)$ uniquely determines $M^{\alpha}=\begin{bmatrix} y_1 \\ y_0 \\ \vdots \\ y_{n-1}\end{bmatrix}\in\Sigma^{\alpha}$ such that $((1))M^{\alpha}=((y))$.

This implies $y=\sum_{i=0}^{n-1} y_i$. Conversely $M^{\alpha}=\begin{bmatrix} y_0 \\ y_1 \\ \vdots \\ y_{n-1}\end{bmatrix}\in\Sigma^{\alpha}$ uniquely determines $y\in FG(q^n)$ such that $((1))M^{\alpha}=((y))$ with $y=\sum_{i=0}^{n-1} y_i$. Hence we denote $M^{\alpha}=\begin{bmatrix} y_0 \\ y_1 \\ \vdots \\ y_{n-1}\end{bmatrix}\in\Sigma^{\alpha}$ by $[y]$, where $y=\sum_{i=0}^{n-1} y_i$. Then a mapping $GF(q^n)\to\Sigma^{\alpha}$ is a bijection under $y\to[y]$. Hence $\Sigma^{\alpha}=\{[x]\mid x\in GF(q^n)\}$. In this mapping the inverse image of $M^*\in\Sigma^{\alpha}$ is denoted by $\hat{M}^*$.

Let Π^* be a translation plane with a spread π^{α} defined in $V(2n, q)^{\alpha}$. If a point of Π^* is represented by $(((x)), ((y)))$ as a vector of $V(2n, q)^{\alpha}$, then we give a coordinate (x, y), $x, y\in GF(q^n)$, for this point. Then the set Q consisting of all elements of $GF(q^n)$ coordinates the plane Π, and Q is a quasifield with the following two binary operations $+$ and $\circ$:

(1) The addition $+$ is the usual field addition.

(2) The multiplication $\circ$ is given by $x\circ y=\widehat{((x))[y]}$, and if $[y]=\begin{bmatrix} y_0 \\ y_1 \\ \vdots \\ y_{n-1}\end{bmatrix}$, then $x\circ y=\sum_{i=0}^{n-1} x^{(i)}y_i$.

Using this coordinate, we can write the lines of Π^* as follows:

$$\begin{aligned} V^*(m)+k &= \{(x, x\circ m+k)\mid x\in GF(q^n)\}\cup\{(m)\}\,, \\ V^*(\infty)+k &= \{(k, y)\mid y\in GF(q^n)\}\cup\{(\infty)\}\,, \\ l_\infty &= \{(m)\mid m\in GF(q^n)\}\cup\{(\infty)\}\,. \end{aligned}$$

Assume that Σ^* consists of q^n-1 matrices of $GL(n, q)^{\alpha}$ and 0. We call Σ^* a spread set of degree n over $GF(q^n)$ if Σ^* has the following properties:

a) For $m=\begin{bmatrix} y_0 \\ y_1 \\ \vdots \\ y_{n-1} \end{bmatrix} \in \Sigma^*$, put $\beta(m)=\sum_{i=0}^{n-1} x_i$. Then $\{\beta(m) \mid m\in\Sigma^*\}=GF(q^n)$.

Hence we may set $m=[\beta(m)]$.

b) If $m_1, m_2\in\Sigma^*$ and if $m_2 \neq m_2$, then $m_1-m_2\in GL(n, q)^{\alpha}$.

Clearly for any vector $((x)) \neq ((0)) \in V(n, q)^{\alpha}$, $\{((x))m \mid m\in\Sigma^*\}=V(n, q)^{\alpha}$. Set

$$V^*(\infty) = \{(((0)), ((x))) \mid ((x))\in V(n, q)^{\alpha}\} ,$$
$$V^*(m) = \{(((x)), ((x))m) \mid ((x))\in V(n, q)^{\alpha} .$$

Then $\{V^*(\infty)\} \cup \{V^*(m) \mid m\in\Sigma^*\}$ is a spread of $V(2n, q)^{\alpha}$, and so defines a translation plane Π^*.

Conversely let Q be any finite quasifield with binary two operations $+$ and $\circ$. The kernel of Q is the set $K(Q)$ consisting of all elements $k\in Q$ such that $(k\circ a)\circ b=k\circ(a\circ b)$ and $k\circ(a+b)=k\circ a+k\circ b$ for all a, $b\in Q$. Then $K(Q)$ is a finite field, and Q is a $K(Q)$-vector space. Let $K(Q)$ be of order q and let Q be of dimension n over $K(Q)$. Then *M.* Hall has proved the following ([3]):

Let $V(2n, q)=Q\oplus Q$, the outer direct sum of two copies of the $K(Q)$-vector space Q. If $V(m)=\{(x, x\circ m) \mid x\in Q\}$ and $V(\infty)=\{(0, x) \mid x\in Q\}$, then $\pi=\{V(m) \mid m\in Q \cup \{\infty\}\}$ is a spread of $V(2n, q)$. Furthermore the spread set is $\Sigma=\{(x\rightarrow x\circ m) \mid m\in Q\}$.

Hence the translation plane defined by π is coordinatized by Q. Thus we have

Theorem 1. *Let $\Sigma^*=\{[x] \mid x\in GF(q^n)\}$ be a spread set of degree n over $GF(q^n)$. Then we have a quasifield Q with two binary operations $+$ and $\circ$ satisfying the followings*:

(1) *$Q=GF(q^n)$ as a set.*

(2) *The addition $+$ is the usual field addition of $GF(q^n)$.*

(3) *The multiplication $\circ$ is given by $x\circ y=\widehat{((x))}[y]$, where $((x))=(x, x^{(1)}, \cdots, x^{(n-1)})\in V(n, q^n)$ and $[y]\in\Sigma^*$.*

Furthermore any finite quasifield is isomorphic to some quasifield constructed by the above method.

A quasifield Q with a spread set Σ^* of degree n over $GF(q^n)$ is denoted by $Q(n, q^n, \Sigma^*)$. Since $((k))=(k, k, \cdots, k)$ for $k\in GF(q)$ in $Q(n, q^n, \Sigma^*)$, $k\circ x=\widehat{((k))}[x]=kx$ for any $x\in Q$. Hence $(k\circ a)\circ b=\widehat{((ka))}[b]=k\widehat{((a))}[b]=k\circ(a\circ b)$ and $k\circ(a+b)=k(a+b)=ka+kb=k\circ a+k\circ b$. Thus $GF(q)$ is contained in the kernel $K(Q)$ of $Q(n, q^n, \Sigma^*)$.

4. Examples

A quasifield is determined by the spread set. In this section we show some spread sets of the known quasifields. To construct spread sets we need a condition for two spread sets to define isomorphic quasifields or translation planes.

First using the spread set, we prove the following Maduram's Theorem. From now on $GL(n, q)^{\alpha}$ is denoted by G^*.

Theorem A (D.M. Maduram [7]). *Let $Q_1=Q(n, q^n, \Sigma_1^*)$ and $Q_2=Q(n, q^n, \Sigma_\sigma^*)$. Then Q_1 and Q_2 are isomorphic if and only if there is N in G^* and θ in $Aut\,GF(q^n)$ such that $\Sigma_2^*=N^{-1}\Sigma_1^{*\theta}N$ and $(\!(1)\!)N=(\!(1)\!)$.*

Furthermore let f be the isomorphism from Q_1 to Q_2, then $f(x)=\widehat{(\!(x^\theta)\!)}N$ and $[f(x)]=N^{-1}[x]^\theta N$ for $x\in Q_1$.

Proof. Let f be an isomorphism from Q_1 to Q_2. Then f fixes $GF(q)$ as a set and so f induces an automorphism of $GF(q)$. Hence there is θ in $\mathrm{Aut}\,GF(q^n)$ such that $f(k)=k^\theta$ for any element k of $GF(q)$. Then for $a\in Q_1$

$$f(ka)=f(k\circ a)=f(k)\circ f(a)=k^\theta f(a)\,.$$

Let $\bar{f}$ be a mapping of $V(n, q)^{\alpha}$ onto itself defined by $\bar{f}((\!(x)\!))=(\!(f(x))\!)$ for $(\!(x)\!)\in V(n, q)^{\alpha}$. Then

$$\begin{aligned}\bar{f}((\!(x)\!)+(\!(y)\!)) &= \bar{f}((\!(x+y)\!)) = (\!(f(x+y))\!) = (\!(f(x)+f(y))\!)\\ &= (\!(f(x))\!)+(\!(f(y))\!) = \bar{f}((\!(x)\!))+\bar{f}((\!(y)\!))\end{aligned}$$

and for $k\in GF(q)$

$$\bar{f}((\!(kx)\!)) = (\!(f(kx))\!) = (\!(k^\theta f(x))\!) = k^\theta(\!(f(x))\!) = k^\theta\bar{f}((\!(x)\!))\,.$$

Thus $\bar{f}$ is a non-singular semi-linear transformation of $V(n, q)^{\alpha}$.

Next let ϕ be a mapping of $V(n, q)$ onto itself defined by $\phi(v)=\bar{f}(v\alpha)\alpha^{-1}$. Then clearly $\phi(v_1+v_2)=\phi(v_1)+\phi(v_2)$ and $\phi(kv)=k^\theta\phi(v)$. Thus ϕ is also a non-singular semi-linear transformation of $V(n, q)$. Hence there is N_1 in $GL(n, q)$ such that

$$\phi((x_1, \cdots, x_n)) = (x_1, \cdots, x_n)^\theta N_1$$

for $(x_1, \cdots, x_n)\in V(n, q)$. On the other hand set $(x_1, \cdots, x_n)\alpha=(\!(x)\!)$. Then

$$\phi((x, \cdots, x_n)) = \bar{f}((\!(x)\!))\alpha^{-1}\,.$$

Hence

$$\bar{f}((\!(x)\!)) = (x_1, \cdots, x_n)^\theta N_1\alpha\,.$$

By Lemma 2.1 $\alpha^\theta=N_2\alpha$, $N_2\in GL(n, q)$. Hence

$$((x^\theta)) = (x_2, \cdots, x_n)^\theta \alpha^\theta \alpha = (x_2, \cdots, x_n)^\theta N_2 \alpha$$

and so

$$(x_1, \cdots, x_n)^\theta = ((x^\theta))\alpha^{-1} N_2^{-1} .$$

Thus

$$\bar{f}(((x))) = ((x^\theta))\alpha^{-1} N_2^{-1} N_1 \alpha .$$

Set $N = \alpha^{-1} N_2^{-1} N_1 \alpha \in G^*$. Then

$$\bar{f}(((x))) = ((x^\theta))N .$$

Since $\bar{f}(((x))) = ((f(x)))$,

$$((1)) = ((f(1))) = \bar{f}(((1))) = ((1))N \quad \text{and} \quad f(x) = \widehat{((x^\theta))N} .$$

Then since $f(x \circ y) = f(x) \circ f(y) = \widehat{((f(x)))}[f(y)] = \widehat{((x^\theta))N}[f(y)]$ and $f(x \circ y) = \widehat{((x \circ y))^\theta N}$ $= \widehat{((x^\theta))[y]}^\theta N$, $((x^\theta))N[f(y)] = ((x^\theta))[y]^\theta N$ for any $((x)) \in V(n, q)^\omega$.

Thus $N[f(y)] = [y]^\theta N$ and so $[f(y)] = N^{-1}[y]^\theta N$ for any $y \in Q_1$. Hence we have $\Sigma_2^* = N^{-1} \Sigma_1^{*\theta} N$.

Conversely let f be a mapping from Q_1 to Q_2 defined by $f(x) = \widehat{((x^\theta))N}$. Then

$$f(x+y) = \widehat{(((x+y)^\theta))N} = \widehat{((x^\theta))N} + \widehat{((y^\theta))N} = f(x) + f(y)$$

and

$$f(x \circ y) = \widehat{((x \circ y))^\theta N} = \widehat{((x^\theta))[y]}^\theta N = \widehat{((x^\theta))N N^{-1}}[y]^\theta N .$$

Since $\Sigma_2^* = N^{-1} \Sigma_1^{*\theta} N$,

$$f(x \circ y) = f(x) \circ N^{-1} \widehat{[y]}^\theta N .$$

Furthermore

$$((1))N^{-1}[y]^\theta N = ((1))[y]^\theta N = ((y^\theta))N .$$

On the other hand

$$((1))[\widehat{((y^\theta))N}] = ((y^\theta))N .$$

Hence

$$N^{-1}[y]^\theta N = [\widehat{((y^\theta))N}]$$

and so

$$f(x \circ y) = f(x) \circ \widehat{((y^\theta))N} = f(x) \circ f(y) .$$

Thus f is an isomorphism from Q_1 to Q_2.

Let π_1 and π_2 be two spreads in $V(2n, q)$ both containing $V(\infty)$. Let Π_1 and Π_2 be translation planes defined by π_1 and π_2. Then Π_1 and Π_2 are isomorphic if and only if there is a non-singular semi-linear transformation in $V(2n, q)$ taking π_1 onto π_2 ([5], p. 82).

Let $M(n, q)$ be the set of all $n\times n$ matrices over $GF(q)$. Then all elements of $M(n, q)^{\alpha}$ have the forms as in Lemma 2.4. Using elements of $M(n, q)^{\alpha}$ and Aut $GF(q^n)$, we describe Sherk's Theorem with the following extended form.

Theorem B (F.A. Sherk [8]). *Let Π_1 and Π_2 be translation planes coordinatized by quasifields $Q_1=Q(n, q^n, \Sigma_1^*)$ and $Q_2=Q(n, q^n, \Sigma_2^*)$. Then Π_1 and Π_2 are isomorphic if and only if there exist A, B, C and D in $M(n, q)^{\alpha}$ and θ in Aut $GF(q^n)$ with the following properties:*

a) $\det\begin{pmatrix} A & B \\ C & D\end{pmatrix}\neq 0$.

b) *Either*

i) $B=0$, $A\in G^*$ *and* $\Sigma_2^*=\{A^{-1}(C+[m]^{\theta}D)\mid [m]\in\Sigma_1^*\}$.

ii) $B\in G^*$, $B^{-1}D\in\Sigma_2^*$. *Also, there is* $[m_0]\in\Sigma_1^*$ *such that* $A+[m_0]^{\theta}B=0$. *For any* $[m]\in\Sigma_1^*\backslash\{[m_0]\}$, $A+[m]^{\theta}B\in G^*$ *and* $(A+[m]^{\theta}B)^{-1}(C+[m]^{\theta}D)\in\Sigma_2^*$.

From now on we denote the operations of $GF(q^n)$ by $+$ and $\cdot$, and the operations of a quasifield by $+$ and $\circ$.

(I) Finite fields

A quasifield $Q(n, q^n, \Sigma^*)$ with $\Sigma^*=\left\{[a]=\begin{bmatrix} a \\ 0 \\ \vdots \\ 0\end{bmatrix}\,\middle|\, a\in GF(q^n)\right\}$ is isomorphic to $GF(q^n)$.

(II) Finite generalized Andre quasifields

Let $Q=Q(n, q^n, \Sigma^*)$ be a quasifield. If the mapping $x\to(x\circ a)a^{-1}$ is an automorphism of $GF(q^n)$, then Q is called a generalized Andre quasifield.

Since $k\circ a=ka$ for $k\in GF(q)$, the automorphism $x\to(x\circ a)a^{-1}$ fixes $GF(q)$ elementwise. Hence $(x\circ a)a^{-1}=x^{q^{\rho(a)}}$, $\rho(a)\in\{0, 1, \cdots, n-1\}$. This yields $x\circ a=x^{q^{\rho(a)}}a=x^{(\rho(a))}a$. Let $[a]=\begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1}\end{bmatrix}$. Then

$$x\circ a = ((x))[a] = \sum_{i=1}^{n-1} x^{(i)}a_i = x^{(\rho(a))}a\,.$$

Hence

$$a_0x+a_1x^{(1)}+\cdots+(a_{\rho(a)}-a)x^{(\rho(a))}+\cdots+a_{n-1}x^{(n-1)} = 0$$

for all $x\in GF(q^n)$. Therefore $a_i=0$ if $i\neq\rho(a)$ and $a_{\rho(a)}=a$. A matrix $\begin{bmatrix} a_1 \\ \vdots \\ a_n\end{bmatrix}$ with exactly one nonzero entry $a_i=a$ is denoted by $[a(i)]$. Then the spread set is $\Sigma^*=\{[a]=[a(\rho(a)+1)] \mid a\in GF(q^n)\setminus\{0\}\}\cup\{0\}$.

For instance, spread sets of generalized Andre quasifields $Q(2, q^2, \Sigma^*)$ and $Q(3, q^3, \Sigma^*)$ are as follows. For $x\in GF(q^2)$ or $GF(q^3)$ set $N(x)=x^{1+q}$ or $N(x)=x^{1+q+q^2}$ respectively.

(1) $Q(2, q^2, \Sigma^*)$

$\Sigma^*=\Sigma_1^*\cup\Sigma_2^*\cup\{0\}$, where $\Sigma_1^*=\{[a]=\begin{bmatrix} a \\ 0 \end{bmatrix},\ a\neq 0\}$ and $\Sigma_2^*=\{[a]=\begin{bmatrix} 0 \\ a \end{bmatrix},\ a\neq 0\}$. Moreover $N(a_1)\neq N(a_2)$ for $[a_1]\in\Sigma_1^*$ and $[a_2]\in\Sigma_2^*$ since $\det([a_1]-[a_2])=N(a_1)-N(a_2)\neq 0$.

(2) $Q(3, q^3, \Sigma^*)$

$\Sigma^*=\Sigma_1^*\cup\Sigma_2^*\cup\Sigma_3^*\cup\{0\}$, where $\Sigma_1^*=\{[a]=\begin{bmatrix} a \\ 0 \\ 0 \end{bmatrix},\ a\neq 0\}$, $\Sigma_2^*=\{[a]=\begin{bmatrix} 0 \\ a \\ 0 \end{bmatrix},\ a\neq 0\}$ and $\Sigma_3^*=\{[a]=\begin{bmatrix} 0 \\ 0 \\ a \end{bmatrix},\ a\neq 0\}$. Moreover if $[a]\in\Sigma_i^*$, $[b]\in\Sigma_j^*$ and $i\neq j$, then $N(a)\neq N(b)$ since $\det([a]-[b])=N(a)-N(b)\neq 0$.

(III) Finite Dickson nearfields

We call a quasifield Q a nearfield, if the multiplication of Q is associative, i.e. $Q\setminus\{0\}$ is the multiplicative group. Let Q be a nearfield with a spread set Σ^*. Then for any $x\in Q$, $x\circ(a\circ b)=(x\circ a)\circ b$. Then $(\!(x)\!)[a\circ b]=(\!(x)\!)[a][b]$. Thus we have $[a\circ b]=[a][b]$ and so $[a][b]\in\Sigma^*$.

If a generalized Andre quasifield Q is a nearfield, then Q is called a Dickson nearfield. In a Dickson nearfield $Q(n, q^n, \Sigma^*)$, let ρ be the mapping defined in (II), i.e. $x\circ a=x^{q^{\rho(a)}}a$.

Lemma 4.1. *Let $Q=Q(n, q^n, \Sigma^*)$ be a Dickson nearfield. Then $K=\{a\in Q \mid a\circ x=ax$ for all $x\in Q\}$ is the subfield $GF(q^m)$ of $GF(q^n)$ with $n=mr$.*

Furthermore we have a Dickson nearfield $Q'=Q(r, (q^m)^r, \Sigma^{*\prime})$ as follows;

If $[a]=[a][a(\rho(a)+1)]$ in Σ^*, then $[a]=\left[a\left(\frac{\rho(a)}{m}+1\right)\right]$ in $\Sigma^{*\prime}$. Hence Q' is identified with Q.

Proof. Let $a, b\in K$. Then for any $x\in Q$, $(a+b)\circ x=a\circ x+b\circ x=ax+bx=(a+b)x$ and $(a\circ b)\circ x=a\circ(b\circ x)=a(bx)=(ab)x=(a\circ b)x$. Thus $a+b\in K$ and $a\circ b=ab\in K$ and so K is a subfield of $GF(q^n)$, say $K=GF(q^m)$. Then $n=mr$. Let $x\in K$ and $a\in Q\setminus\{0\}$. Then $xa=x\circ a=x^{q^{\rho(a)}}a$. Hence $x=x^{q^{\rho(a)}}$ and so $\rho(a)\equiv 0 \pmod m$. Thus $x\circ a=x^{q^{\rho(a)}}a=x^{(q^m)^{\frac{\rho(a)}{m}}}a$. Hence if we take a $r\times r$ matrix $[a]'=a\left[\left(\frac{\rho(a)}{m}+1\right)\right]$, and set $\Sigma^{*\prime}=\{[a]' \mid a\in GF(q^n)\setminus\{0\}\}\cup\{0\}$, then we can identify $Q(r, (q^m)^r, \Sigma^*)$ with $Q(n, q^n, \Sigma^*)$.

Now we describe a theorem of E. Ellers and H. Karzl [2] using a spread set.

Theorem C (E. Eller and H. Karzel). *Let $Q(n, q^n, \Sigma^*)$ be a finite Dickson nearfield such that $GF(q)=\{k\in Q \mid k\circ x=kx$ for all $x\in Q\}$. Then the following hold:*

1) *Every prime divisor of n divides $q-1$.*

2) *If $n\equiv 0$ (moo 4), then $q\not\equiv 3$ (moo 4).*

Furthermore the spread set Σ^* is as follows:

Let ω be a generator of the multiplicative group $(GF(q^n), \cdot)$ and set $U=\langle\omega^n\rangle$. Then there is a positive integer t with $(n, t)=1$,

$$(GF(q^n), \cdot) = \bigcup_{i=0}^{n-1} \omega^t(q^i-1)(q-1)^{-1}U\,.$$

If $a\in\omega^{t(q^i-1)(q-1)^{-1}}U$, then $[a]=[a(i+1)]$.

Conversely by a theorem of H. Lüneburg ([6], Theorem 6.4) we can construct a Dickson nearfield as follows;

Assume that n and q satisfy the conditions 1) and 2) of Theorem C. Let ω be a generator of the multiplicative group $GF(q^n)$ and $(n, t)=1$. Then $\Sigma^*=\bigcup_{i=0}^{n-1}\{[a(i+1)] \mid a\in\omega^{t(q^i-1)(q-1)^{-1}}U\}\cup\{0\}$, where $U=\langle\omega^n\rangle$.

(IV) Quasifields of order 9

M. Hall has proved that there exist up to isomorphism exactly five quasifields of order 9 ([3]). We prove this theorem using a spread set.

Theorem 2. *There exist up to isomorphism exactly five quasifields with the following spread sets.*

$$\Sigma_1^* = \{[a]=\begin{bmatrix}a\\0\end{bmatrix} \mid a\in GF(9)\}\,,$$

$$\Sigma_2^* = \{\begin{bmatrix}0\\0\end{bmatrix}, \begin{bmatrix}\pm1\\0\end{bmatrix}, \begin{bmatrix}\pm\omega+1\\0\end{bmatrix}, \begin{bmatrix}1\\\pm\omega\pm1\end{bmatrix}\},$$

$$\Sigma_3^* = \{\begin{bmatrix}0\\0\end{bmatrix}, \begin{bmatrix}\pm1\\0\end{bmatrix}, \begin{bmatrix}\pm\omega\\0\end{bmatrix}, \begin{bmatrix}0\\\pm\omega\pm1\end{bmatrix}\},$$

$$\Sigma_4^* = \{\begin{bmatrix}0\\0\end{bmatrix}, \begin{bmatrix}\pm1\\0\end{bmatrix}, \begin{bmatrix}\pm\omega-1\\0\end{bmatrix}, \begin{bmatrix}-1\\\pm\omega\pm1\end{bmatrix}\},$$

$$\Sigma_5^* = \{\begin{bmatrix}0\\0\end{bmatrix}, \begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}-\omega\\0\end{bmatrix}, \begin{bmatrix}\pm(\omega-1)\\0\end{bmatrix}, \begin{bmatrix}\omega-1\\\pm1\end{bmatrix}, \begin{bmatrix}\omega-1\\\pm\ \omega\end{bmatrix}\},$$

where ω is the root of $f(x)=x^2+1$ in $GF(9)$.

Proof. $Q(1, 9, \Sigma^*)$ is isomorphic to $GF(9)$.

Next we construct $Q(2, 9, \Sigma^*)$. Take an irreducible polynomial $f(x)=x^2+1$ over $GF(3)$, and let ω and $-\omega$ be the roots of $f(x)$ in $GF(9)$. Set $N(x)=x^{1+3}=x^4$ for $x\in GF(9)$. Then $N(\pm1)=N(\pm\omega)=1$, $N(\pm\omega\pm1)=-1$ and $\det\begin{bmatrix}a\\b\end{bmatrix}=N(a)-N(b)$.

Lemma 4.2. Σ^* *has the following properties*:

1) *Let* $\begin{bmatrix} a \\ b \end{bmatrix} \in \Sigma^*$, *$a, b \neq 0$ and* $\begin{bmatrix} c \\ 0 \end{bmatrix} \in \Sigma^*$. *Then $a=c$ or $N(a-c)=N(a)$. If* $\begin{bmatrix} 0 \\ d \end{bmatrix} \in \Sigma^*$, *then $b=d$ or $N(b-d)=N(b)$.*

2) *If* $\begin{bmatrix} a \\ b \end{bmatrix} \in \Sigma^*$ *and $a, b \neq 0$, then $a=\pm 1$ or $\pm\omega-1$.*

3) *If* $\begin{bmatrix} 0 \\ b \end{bmatrix} \in \Sigma^* \setminus \{0\}$, *then $b=\pm\omega\pm 1$.*

Proof. 1) Since $\det(\begin{bmatrix} a \\ b \end{bmatrix} - \begin{bmatrix} c \\ 0 \end{bmatrix}) \neq 0$, $N(a-c) \neq N(b)$. Hence $a=c$ or $N(a-c)=N(a)$. Similarly if $\begin{bmatrix} 0 \\ d \end{bmatrix} \in \Sigma^*$, then $b=d$ or $N(b-d)=N(b)$.

2) Since $\begin{bmatrix} 1 \\ 0 \end{bmatrix} \in \Sigma^*$, $a=1$ or $N(a-1)=N(a)$ by 1). Hence $a=\pm 1$ or $\pm\omega-1$.

3) Since $\begin{bmatrix} 1 \\ 0 \end{bmatrix} \in \Sigma^*$ and $\det(\begin{bmatrix} 1 \\ 0 \end{bmatrix} - \begin{bmatrix} 0 \\ b \end{bmatrix}) \neq 0$, $b=\pm\omega\pm 1$.

We use this lemma frequently in the following proofs. By Lemma 4.2, $[-1]$, $[\omega+1]$ and $[\omega]$ have one of the following forms:

$$[-1] = \begin{bmatrix} -1 \\ 0 \end{bmatrix}, \begin{bmatrix} \omega-1 \\ -\omega \end{bmatrix} \text{ or } \begin{bmatrix} -\omega-1 \\ \omega \end{bmatrix},$$
$$[\omega+1] = \begin{bmatrix} \omega+1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ \omega+1 \end{bmatrix}, \begin{bmatrix} -1 \\ \omega-1 \end{bmatrix} \text{ or } \begin{bmatrix} \omega-1 \\ -1 \end{bmatrix},$$
$$[\omega] = \begin{bmatrix} \omega \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ \omega-1 \end{bmatrix}, \begin{bmatrix} -1 \\ \omega+1 \end{bmatrix} \text{ or } \begin{bmatrix} \omega-1 \\ 1 \end{bmatrix},$$

Case 1. $[-1]=\begin{bmatrix} -1 \\ 0 \end{bmatrix}$.

If $\begin{bmatrix} a \\ b \end{bmatrix} \in \Sigma^*$ and $a, b \neq 0$, then $a=\pm 1$ since $\det(\begin{bmatrix} a \\ b \end{bmatrix} - \begin{bmatrix} -1 \\ 0 \end{bmatrix}) \neq 0$. Thus

$$[\omega+1] = \begin{bmatrix} \omega+1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ \omega+1 \end{bmatrix} \text{ or } \begin{bmatrix} -1 \\ \omega-1 \end{bmatrix},$$
$$[\omega] = \begin{bmatrix} \omega \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ \omega-1 \end{bmatrix} \text{ or } \begin{bmatrix} -1 \\ \omega+1 \end{bmatrix}.$$

(1.1) Suppose $[\omega+1]=\begin{bmatrix} \omega+1 \\ 0 \end{bmatrix}$. Then $\begin{bmatrix} 0 \\ b \end{bmatrix} \notin \Sigma^* \setminus \{0\}$. Furthermore if $\begin{bmatrix} a \\ b \end{bmatrix} \in \Sigma^*$ and $a, b \neq 0$, then $a=1$. Thus $\Sigma^* \subseteq \{ \begin{bmatrix} a \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ \pm\omega\pm 1 \end{bmatrix} \mid a \in GF(9)\}$.

(1.1.1) Suppose $[\omega]=\begin{bmatrix} \omega \\ 0 \end{bmatrix}$. Then $\begin{bmatrix} 1 \\ \pm\omega\pm 1 \end{bmatrix} \notin \Sigma^*$. Thus we have the following spread set Σ_1^*:

$$\Sigma_1^* = \{[a] = \begin{bmatrix} a \\ 0 \end{bmatrix} \mid a \in GF(9)\}.$$

Then $Q(2, 9, \Sigma_1^*)$ is isomorphic to $GF(9)$.

(1.1.2) Suppose $[\omega]=\begin{bmatrix}1\\ \omega-1\end{bmatrix}$. If $\begin{bmatrix}a\\0\end{bmatrix}\in\Sigma^*\backslash\{0\}$, then $a=\pm1$ or $\pm\omega+1$. Hence we have the following spread set Σ_2^*.

$$\Sigma_2^*=\left\{\begin{bmatrix}0\\0\end{bmatrix},\begin{bmatrix}\pm1\\0\end{bmatrix},\begin{bmatrix}\pm\omega+1\\0\end{bmatrix},\begin{bmatrix}1\\ \pm\omega\pm1\end{bmatrix}\right\}.$$

Since $\left\{\begin{bmatrix}\pm\omega+1\\0\end{bmatrix},\begin{bmatrix}1\\ \pm\omega\pm1\end{bmatrix}\right\}$ is a conjugate class in G^*, by Theorem A $Q(2,9, \Sigma_2^*)$ is not isomorphic to any $Q(2, 9, \Sigma^*)$ with $\Sigma^*\neq\Sigma_2^*$.

(1.2) Suppose $[\omega+1]=\begin{bmatrix}0\\ \omega+1\end{bmatrix}$. Then $\Sigma^*\subseteqq\left\{\begin{bmatrix}0\\0\end{bmatrix},\begin{bmatrix}\pm1\\0\end{bmatrix},\begin{bmatrix}\pm\omega\\0\end{bmatrix},\begin{bmatrix}0\\ \pm\omega\pm1\end{bmatrix},\begin{bmatrix}\pm1\\ \pm(\omega+1)\end{bmatrix}\right\}$.

(1.2.1) Suppose $[\omega]=\begin{bmatrix}\omega\\0\end{bmatrix}$. Then $\begin{bmatrix}\pm1\\ \pm(\omega+1)\end{bmatrix}\notin\Sigma^*$. Hence we have the following spread set Σ_3^*:

$$\Sigma_3^*=\left\{\begin{bmatrix}0\\0\end{bmatrix},\begin{bmatrix}\pm1\\0\end{bmatrix},\begin{bmatrix}\pm\omega\\0\end{bmatrix},\begin{bmatrix}0\\ \pm\omega\pm1\end{bmatrix}\right\}.$$

Then $Q(2, 9, \Sigma_3^*)$ is a Dickson nearfield.

(1.2.2) Suppose $[\omega]=\begin{bmatrix}-1\\ \omega+1\end{bmatrix}$. Then

$$\Sigma^*=\left\{\begin{bmatrix}0\\0\end{bmatrix},\begin{bmatrix}\pm1\\0\end{bmatrix},\begin{bmatrix}0\\ \pm(\omega+1)\end{bmatrix},\begin{bmatrix}\pm1\\ \pm(\omega+1)\end{bmatrix}\right\}.$$

Take $\begin{bmatrix}-\omega+1\\ \omega\end{bmatrix}\in G^*$. Then since $\begin{bmatrix}-\omega+1\\ \omega\end{bmatrix}^{-1}\begin{bmatrix}1\\ \omega+1\end{bmatrix}\begin{bmatrix}-\omega+1\\ \omega\end{bmatrix}=\begin{bmatrix}\omega+1\\0\end{bmatrix}$, $\begin{bmatrix}-\omega+1\\ \omega\end{bmatrix}^{-1}\begin{bmatrix}0\\ \omega+1\end{bmatrix}\begin{bmatrix}-\omega+1\\ \omega\end{bmatrix}=\begin{bmatrix}\omega\\0\end{bmatrix}$ and $((1))\begin{bmatrix}-\omega+1\\ \omega\end{bmatrix}=((1))$, the quasifield with this spread set is isomorphic to $GF(9)$ by Theorem A.

(1.3) Suppose $[\omega+1]=\begin{bmatrix}-1\\ \omega-1\end{bmatrix}$. Then $\Sigma^*\subseteqq\left\{\begin{bmatrix}0\\0\end{bmatrix},\begin{bmatrix}\pm1\\0\end{bmatrix},\begin{bmatrix}-1\\ \pm\omega\pm1\end{bmatrix},\begin{bmatrix}1\\ \pm(\omega-1)\end{bmatrix},\begin{bmatrix}\pm\omega-1\\0\end{bmatrix},\begin{bmatrix}0\\ \pm(\omega-1)\end{bmatrix}\right\}$.

(1.3.1) Suppose $[\omega]=\begin{bmatrix}1\\ \omega-1\end{bmatrix}$. Take $\begin{bmatrix}\omega+1\\ -\omega\end{bmatrix}\in G^*$. Then $\begin{bmatrix}\omega+1\\ -\omega\end{bmatrix}^{-1}$ $\begin{bmatrix}1\\ \omega-1\end{bmatrix}\begin{bmatrix}\omega+1\\ -\omega\end{bmatrix}=\begin{bmatrix}\omega+1\\0\end{bmatrix}$ and $((1))\begin{bmatrix}\omega+1\\ -\omega\end{bmatrix}=((1))$. Hence this case is included in the case (1.1).

(1.3.2) Suppore $[\omega]=\begin{bmatrix}-1\\ \omega+1\end{bmatrix}$. Then $\begin{bmatrix}1\\ \pm(\omega-1)\end{bmatrix}$ and $\begin{bmatrix}1\\ \pm(\omega-1)\end{bmatrix}\notin\Sigma^*$. Hence we have the following spread set Σ_4^*.

$$\Sigma_4^* = \{\begin{bmatrix}0\\0\end{bmatrix}, \begin{bmatrix}\pm 1\\0\end{bmatrix}, \begin{bmatrix}\pm\omega-1\\0\end{bmatrix}, \begin{bmatrix}-1\\\pm\omega\pm 1\end{bmatrix}\}.$$

Similarly to the case (1.1.2), $\{\begin{bmatrix}\pm\omega-1\\0\end{bmatrix}, \begin{bmatrix}-1\\\pm\omega+1\end{bmatrix}\}$ is a conjugate class in G^* and so $Q(2, 9, \Sigma_4^*)$ is not isomorphic to any $Q(2, 9, \Sigma^*)$ with $\Sigma^* \neq \Sigma_4^*$.

Case 2. $[-1]=\begin{bmatrix}\omega-1\\-\omega\end{bmatrix}$.

Then $\Sigma^* \subseteq \{\begin{bmatrix}0\\0\end{bmatrix}, \begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}-\omega\\0\end{bmatrix}, \begin{bmatrix}\pm(\omega-1)\\0\end{bmatrix}, \begin{bmatrix}0\\-\omega\pm 1\end{bmatrix}, \begin{bmatrix}1\\-\omega\pm 1\end{bmatrix}, \begin{bmatrix}-1\\\omega\pm 1\end{bmatrix}, \begin{bmatrix}\omega-1\\\pm 1\end{bmatrix}, \begin{bmatrix}\omega-1\\\pm\omega\end{bmatrix}, \begin{bmatrix}-\omega-1\\\pm 1\end{bmatrix}, \begin{bmatrix}-\omega-1\\-\omega\end{bmatrix}\}$. Then

$$[\omega+1] = \begin{bmatrix}\omega-1\\-1\end{bmatrix} \text{ or } \begin{bmatrix}-1\\\omega-1\end{bmatrix},$$

$$[\omega] = \begin{bmatrix}\omega-1\\1\end{bmatrix} \text{ or } \begin{bmatrix}-1\\\omega+1\end{bmatrix}.$$

(2.1) Suppose $[\omega+1]=\begin{bmatrix}\omega-1\\-1\end{bmatrix}$. Then $\Sigma^* \subseteq \{\begin{bmatrix}0\\0\end{bmatrix}, \begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}-\omega\\0\end{bmatrix}, \begin{bmatrix}\pm(\omega-1)\\0\end{bmatrix}, \begin{bmatrix}0\\-\omega-1\end{bmatrix}, \begin{bmatrix}1\\-\omega-1\end{bmatrix}, \begin{bmatrix}-1\\\omega+1\end{bmatrix}, \begin{bmatrix}\omega-1\\\pm 1\end{bmatrix}, \begin{bmatrix}\omega-1\\\pm\omega\end{bmatrix}, \begin{bmatrix}-\omega-1\\-1\end{bmatrix}, \begin{bmatrix}-\omega-1\\-\omega\end{bmatrix}\}$.

(2.1.1) Suppose $[\omega]=\begin{bmatrix}\omega-1\\1\end{bmatrix}$. Then $\Sigma^* \subseteq \{\begin{bmatrix}0\\0\end{bmatrix}, \begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}-\omega\\0\end{bmatrix}, \begin{bmatrix}\pm(\omega-1)\\0\end{bmatrix}, \begin{bmatrix}\omega-1\\\pm 1\end{bmatrix}, \begin{bmatrix}\omega-1\\\pm\omega\end{bmatrix}, \begin{bmatrix}-\omega-1\\-\omega\end{bmatrix}\}$. Since $\det(\begin{bmatrix}-\omega-1\\-\omega\end{bmatrix}-\begin{bmatrix}-\omega\\0\end{bmatrix})=\det(\begin{bmatrix}-\omega-1\\-\omega\end{bmatrix}-\begin{bmatrix}\omega-1\\0\end{bmatrix})=0$, we have the following spread set Σ_5^*.

$$\Sigma_5^* = \{\begin{bmatrix}0\\0\end{bmatrix}, \begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}-\omega\\0\end{bmatrix}, \begin{bmatrix}\pm(\omega-1)\\0\end{bmatrix}, \begin{bmatrix}\omega-1\\\pm 1\end{bmatrix}, \begin{bmatrix}\omega-1\\\pm\omega\end{bmatrix}\}.$$

Since $\begin{bmatrix}-1\\0\end{bmatrix} \notin \Sigma_5^*$, the quasifield with Σ_5^* is not isomorphic to any quasifield with Σ_i^*, $i=1, 2, 3, 4$.

(2.1.2) Suppose $[\omega]=\begin{bmatrix}-1\\\omega+1\end{bmatrix}$. Then $\Sigma^* \subseteq \{\begin{bmatrix}0\\0\end{bmatrix}, \begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}\omega-1\\0\end{bmatrix}, \begin{bmatrix}0\\-\omega-1\end{bmatrix}, \begin{bmatrix}1\\-\omega-1\end{bmatrix}, \begin{bmatrix}-1\\\omega+1\end{bmatrix}, \begin{bmatrix}\pm\omega-1\\-1\end{bmatrix}, \begin{bmatrix}\pm\omega-1\\-\omega\end{bmatrix}\}$. Since $\det(\begin{bmatrix}\omega-1\\0\end{bmatrix}-\begin{bmatrix}0\\-\omega-1\end{bmatrix})=\det(\begin{bmatrix}\omega-1\\0\end{bmatrix}-\begin{bmatrix}1\\-\omega-1\end{bmatrix})=0$, $\Sigma^*=\{\begin{bmatrix}0\\0\end{bmatrix}, \begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}0\\-\omega-1\end{bmatrix}, \begin{bmatrix}1\\-\omega-1\end{bmatrix}, \begin{bmatrix}-1\\\omega+1\end{bmatrix}, \begin{bmatrix}\pm\omega-1\\-1\end{bmatrix}, \begin{bmatrix}\pm\omega-1\\-\omega\end{bmatrix}\}$. Then $\begin{bmatrix}-\omega+1\\\omega\end{bmatrix}^{-1}\Sigma^*\begin{bmatrix}-\omega+1\\\omega\end{bmatrix}=\Sigma_5^*$ and $((1))\begin{bmatrix}-\omega+1\\\omega\end{bmatrix}=((1))$. Hence the quasifield with this spread set is isomorphic to the quasifield with Σ_5^* by Theorem A.

(2.2) Suppose $[\omega+1]=\begin{bmatrix}-1\\\omega-1\end{bmatrix}$. Then $\Sigma^* \subseteq \{\begin{bmatrix}0\\0\end{bmatrix}, \begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}\omega-1\\0\end{bmatrix}, \begin{bmatrix}0\\-\omega+1\end{bmatrix},$

$\begin{bmatrix} 1 \\ -\omega+1 \end{bmatrix}, \begin{bmatrix} -1 \\ \omega\pm1 \end{bmatrix}, \begin{bmatrix} \pm\omega-1 \\ 1 \end{bmatrix}, \begin{bmatrix} \pm\omega-1 \\ -\omega \end{bmatrix}\}$.

(2.2.1) Suppose $[\omega]=\begin{bmatrix} \omega-1 \\ 1 \end{bmatrix}$. Then $\Sigma^* \subseteqq \{\begin{bmatrix} 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} \omega-1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ -\omega+1 \end{bmatrix}, \begin{bmatrix} 1 \\ -\omega+1 \end{bmatrix}, \begin{bmatrix} -1 \\ \omega-1 \end{bmatrix}, \begin{bmatrix} \pm\omega-1 \\ 1 \end{bmatrix}, \begin{bmatrix} \pm\omega-1 \\ -\omega \end{bmatrix}\}$. Since $\det(\begin{bmatrix} \omega-1 \\ 0 \end{bmatrix}-\begin{bmatrix} 1 \\ -\omega+1 \end{bmatrix})=\det(\begin{bmatrix} \omega-1 \\ 0 \end{bmatrix}-\begin{bmatrix} -\omega-1 \\ 1 \end{bmatrix})=0$, $\Sigma^*=\{\begin{bmatrix} 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ -\omega+1 \end{bmatrix}, \begin{bmatrix} 1 \\ -\omega+1 \end{bmatrix}, \begin{bmatrix} -1 \\ \omega-1 \end{bmatrix}, \begin{bmatrix} \pm\omega-1 \\ 1 \end{bmatrix}, \begin{bmatrix} \pm\omega-1 \\ -\omega \end{bmatrix}\}$. Then $\begin{bmatrix} \omega+1 \\ -\omega \end{bmatrix}^{-1} \Sigma^* \begin{bmatrix} \omega+1 \\ -\omega \end{bmatrix}=\Sigma_5^*$ and $((1)) \begin{bmatrix} \omega+1 \\ -\omega \end{bmatrix}=((1))$. Hence the quasifield with this spread set is isomorphic to the quasifield with Σ_5^* by Theorem A.

(2.2.2) Suppose $[\omega]=\begin{bmatrix} -1 \\ \omega+1 \end{bmatrix}$. Then $\Sigma^* \subseteqq \{\begin{bmatrix} 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} \omega-1 \\ 0 \end{bmatrix}, \begin{bmatrix} -1 \\ \omega\pm1 \end{bmatrix}, \begin{bmatrix} \pm\omega-1 \\ -\omega \end{bmatrix}\}$, which consists of seven matrices. Hence this case does not occur.

Case 3. $[-1]=\begin{bmatrix} -\omega-1 \\ \omega \end{bmatrix}$.

Since $\begin{bmatrix} 0 \\ 1 \end{bmatrix}^{-1}\begin{bmatrix} -\omega-1 \\ \omega \end{bmatrix}\begin{bmatrix} 0 \\ 1 \end{bmatrix}=\begin{bmatrix} \omega-1 \\ -\omega \end{bmatrix}$ and $((1)) \begin{bmatrix} 0 \\ 1 \end{bmatrix}=((1))$, this case is reduced to the case 2.

M. Hall has proved that there exist up to isomorphism exactly two translation planes of order 9 [3].

We prove this theorem using the spread sets Σ_i^*, $i=1, 2, 3, 4, 5$. Since $\Sigma_3^*=\{[a]+\begin{bmatrix} -1 \\ 0 \end{bmatrix} \mid [a]\in\Sigma_2^*\}=\{[a]+\begin{bmatrix} 1 \\ 0 \end{bmatrix} \mid [a]\in\Sigma_4^*\}=\{\begin{bmatrix} 0 \\ 1 \end{bmatrix}[a]+\begin{bmatrix} 0 \\ -\omega+1 \end{bmatrix} \mid [a]\in\Sigma_5^*\}$, the translation plane coordinatized by the quasifield with Σ_i^*, $i=2$, 4 or 5 is isomorphic to the translation plane coordinatized by the Dickson nearfield $Q(2, 9, \Sigma_3^*)$ by Theorem B.

(V) Hall quasifields

Let $Q=Q(2, q^2, \Sigma^*)$ be a quasifield. If Q satisfies the following conditions, then Q is called a Hall quasifield [3]:

1) Let $f(x)=x^2-rx-s$ be an irreducible polynomial over $GF(q)$. Every element ξ of Q not in $GF(q)$ satisfies the quadratic equation $f(\xi)=0$.

2) Every element of $GF(q)$ commutes with all elements of Q.

Now we determine the spread set Σ^* of a Hall quasifield $Q(2, q^2, \Sigma^*)$.

Theorem 3. *Let ω be the element of $GF(q^2)$ such that $f(\omega)=\omega^2-r\omega-s=0$.*

Case 1. *Assume that q is a power of 2. Then Σ^* consists of the following matrices*:

$$[k]=\begin{bmatrix} k \\ 0 \end{bmatrix} \qquad \textit{for } k\in GF(q),$$

$$[a\omega+b]=\begin{bmatrix}\omega+\tau(a,b)\\(a+1)\omega+b+\tau(a,b)\end{bmatrix}\qquad \textit{for } a\neq 0, \textit{ where}$$
$$\tau(a,b)=r^{-1}(as+br+a^{-1}f(b)).$$

The multiplication in $Q(2, q^2, \Sigma^*)$ *is as follows*:

$$(a\omega+b)\circ(c\omega+d)=\begin{cases} ad\omega+bd & \textit{if } c=0\\ (bc-ad+ar)\omega+bd-ac^{-1}f(d) & \textit{if } c\neq 0\,.\end{cases}$$

Case 2. *Assume that* q *is a power of an odd prime. Set* $\lambda=\omega-\varpi$. *Then* Σ^* *consists of the following matrices*:

$$[k]=\begin{bmatrix}k\\0\end{bmatrix}\qquad \textit{for } k\in G(q)\,,$$
$$[a\lambda+b]=\begin{bmatrix}\left(\frac{1}{2}a-\tau(a,b)\right)\lambda+\frac{1}{2}r\\ \left(\frac{1}{2}a+\tau(a,b)\right)\lambda-\frac{1}{2}r+b\end{bmatrix}\qquad \textit{for } a\neq 0, \textit{ where}$$
$$\tau(a,b)=(2a(r^2+4s))^{-1}f(b)\,.$$

The multiplication in $Q(2, q^2, \Sigma^*)$ *is as follows*:

$$(a\lambda+b)\circ(c\lambda+d)=\begin{cases} ad\lambda+bd & \textit{if } c=0\\ (bc-ad+ar)\lambda+bd-ac^{-1}f(d) & \textit{if } c\neq 0\,.\end{cases}$$

Proof. Case 1. q is a power of 2.

Since $f(\omega)=\omega^2+r\omega+s=0$, $\omega^2=r\omega+s$, $\omega+\varpi=r$ and $\omega\varpi=s$. Set $GF(q^2)=\{a\omega+b\,|\,a, b\in GF(q)\}$. Let $[k]=\begin{bmatrix}a\omega+k'\\a\omega+k'+k\end{bmatrix}$ for $k\in GF(q)$. Since $k\circ\omega=\omega\circ k$ by the assumption 2), we have

$$k\circ\omega=k\omega\,,$$
$$\omega\circ k=\widehat{(\omega,\varpi)}\begin{bmatrix}a\omega+k'\\a\omega+k'+k\end{bmatrix}=a\omega^2+k'\omega+a\omega\varpi+(k+k')\varpi$$
$$=a(r\omega+s)+k'\omega+as+(k+k')(r+\omega)$$
$$=(ar+k'+k+k')\omega+as+as+(k+k')r=(ar+k)\omega+(k+k')r\,.$$

Hence $a=0$ and $k=k'$. Thus $[k]=\begin{bmatrix}k\\0\end{bmatrix}$.

Let $[a\omega+b]=\begin{bmatrix}a'\omega+b'\\(a+a')\omega+b'+b\end{bmatrix}$, $a\neq 0$. Then

$$(a\omega+b)\circ(a\omega+b)=\widehat{(a\omega+b, a\varpi+b)}\begin{bmatrix}a'\omega+b'\\(a+a')\omega+b+b'\end{bmatrix}$$
$$=aa'\omega^2+ab'\omega+a'b\omega+bb'+a(a+a')\omega\varpi+a(b+b')\varpi+b(a+a')\omega+b(b+b')$$

$$= aa'(r\omega+s)+ab'\omega+a'b\omega+bb'+a(a+a')s+a(b+b')(\omega+r)+b(a+a')\omega$$
$$+b(b+b')$$
$$= aa'r\omega+a^2s+a(b+b')r+b^2.$$

Then since $f(a\omega+b)=0$ in Q,

$$aa'r\omega+a^2s+a(b+b')r+b^2+ar\omega+br+s$$
$$= (aa'r+ar)\omega+a^2s+a(b+b')r+f(b) = 0\,.$$

Hence $a'+1=0$ and so $a'=1$. Furthermore $b'=r^{-1}(as+br+a^{-1}f(b))$. Thus

$$[a\omega+b] = \begin{bmatrix} \omega+r^{-1}(as+br+a^{-1}f(b)) \\ (a+1)\omega+b+r^{-1}(as+br+a^{-1}f(b)) \end{bmatrix}.$$

By computation, $\det[a\omega+b]=s\neq 0$, $\det([a\omega+b]-[k])=f(k)\neq 0$ and $\det([a\omega+b]-[a'\omega+b'])=(aa')^{-1}((ab'+a'b)+(a+a')\omega)((ab'+a'b)+(a+a')\varpi)\neq 0$, where a, $a'\neq 0$. Thus we have a spread set.

Furthermore we have

$$(a\omega+b)\circ(c\omega+d) = \widehat{\langle\!\langle a\omega+b\rangle\!\rangle}\begin{bmatrix} \omega+\tau(c,\,d) \\ (c+1)\omega+\tau(c,\,d)+d \end{bmatrix}$$
$$= (bc+ad+ar)\omega+bd+ac^{-1}f(d)\,, \qquad \text{for } c\neq 0\,.$$

Case 2. q is a power of an odd prime.

Let $\lambda=\omega-\varpi$. Then $\bar{\lambda}=-\lambda$ and $\lambda^2=r^2+4s$. Set $GF(q^2)=\{a\lambda+b\,|\,a,\,b\in GF(q)\}$. Similarly to the case 1, $[k]=\begin{bmatrix} k \\ 0 \end{bmatrix}$ for $k\in GF(q)$.

Let $[a\lambda+b]=\begin{bmatrix} a'\lambda+b' \\ (a-a')\lambda+b-b' \end{bmatrix}$, $a\neq 0$. Then

$$(a\lambda+b)\circ(a\lambda+b) = \widehat{\langle\!\langle a\lambda+b\rangle\!\rangle}\begin{bmatrix} a'\lambda+b' \\ (a-a')\lambda+b-b' \end{bmatrix}$$
$$= aa'\lambda^2+ab'\lambda+a'b\lambda+bb'-a(a-a')\lambda^2-a(b-b')\lambda+b(a-a')\lambda+b(b-b')$$
$$= 2ab'\lambda+(2aa'-a^2)\,(r^2+4s)+b^2\,.$$

Then since $f(a\lambda+b)=0$ in Q,

$$2ab'\lambda+a(2a'-a)(r^2+4s)+b^2-r(a\lambda+b)-s = 0\,.$$

Hence $2ab'-ar=0$ so $b'=\frac{1}{2}r$. Furthermore $a(2a'-a)(r^2+4s)+f(b)=0$ so $a'=-(2a(r^2+4s))^{-1}f(b)+\frac{1}{2}a$. Set $\tau(a,\,b)=(2a(r^2+4s))^{-1}f(b)$. Then we have

$$[a\lambda+b] = \begin{bmatrix} \left(\frac{1}{2}a-\tau(a,b)\right)\lambda+\frac{1}{2}r \\ \left(\frac{1}{2}a+\tau(a,b)\right)\lambda+b-\frac{1}{2}r \end{bmatrix}.$$

By computation, $\det[a\lambda+b]=-s\neq 0$, $\det([a\lambda+b]-[k])=f(k)\neq 0$ and $\det([a\lambda+b]-[a'\lambda+b'])=(2^{-1}(a-a')\lambda+ab'-a'b-2^{-1}r(a-a'))(-2^{-1}(a-a')\lambda+ab'-a'b-2^{-1}r(a-a'))\neq 0$, where $a, a'\neq 0$.

Furthermore we have

$$(a\lambda+b)\circ(c\lambda+d)=(bc-ad+ra)\lambda+bd-ac^{-1}f(d) \qquad \text{for } c\neq 0\,.$$

Moreover since $\lambda=2\omega-r$, we have also

$$(a\omega+b)\circ(c\omega+d)=(bc-ad+ra)\omega+bd-ac^{-1}f(d) \qquad \text{for } c\neq 0\,.$$

(VI) Walker quasifields

A quasifield $Q=Q(2, q^2, \Sigma^*)$ with $q\equiv -1 \pmod 6$ is called a Walker quasifield, if Q has the following multiplication:

$$(a\omega+b)\circ(c\omega+d)=(a(d-c^2)+bc)\omega-\frac{1}{3}ac^3+bo\,,$$

where $GF(q^2)=\{a\omega+b\,|\,a, b\in GF(q)\}$ (see [4], p. 72).

Now we determine the spread set Σ^* of a Walker quasifield. Since $q\equiv -1 \pmod 6$, $f(x)=x^2+3$ is an irreducible polynomial over $GF(q)$. Hence let ω and $-\omega$ be elements of $GF(q^2)$ such that $f(\omega)=f(-\omega)=\omega^2+3=0$.

Set $[a\omega+b]=\begin{bmatrix} a'\omega+b' \\ (a-a')\omega+b-b' \end{bmatrix}$. Then

$$\begin{aligned}\omega\circ(a\omega+b) &= \widehat{(\omega, -\omega)}\begin{bmatrix} a'\omega+b' \\ (a-a')\omega+b-b' \end{bmatrix} \\ &= a'\omega^2+b'\omega-(a-a')\omega^2-(b-b')\omega \\ &= (2b'-b)\omega+3(a-2a')\,.\end{aligned}$$

On the other hand by the definition of the multiplication,

$$\omega\circ(a\omega+b)=(b-a^2)\omega-\frac{1}{3}a^3.$$

Hence $2b'-b=b-a^2$ so $b'=b-\frac{1}{2}a^2$, and $3(a-2a')=-\frac{1}{3}a^3$ so $a'=\frac{1}{2}a+\frac{1}{18}a^3$. Then we have

$$[a\omega+b]=\begin{bmatrix} \left(\frac{1}{2}a+\frac{1}{18}a^3\right)\omega+b-\frac{1}{2}a^2 \\ \left(\frac{1}{2}a-\frac{1}{18}a^3\right)\omega+\frac{1}{2}a^2 \end{bmatrix}.$$

Furthermore by computation, we can show that $\{[a\omega+b]\,|\,a, b\in GF(q)\}$ satisfies the condition of a spread set.

(VII) Lüneburg quasifields

A quasifield $Q=Q(2, (2^{2s+1})^2, \Sigma^{**})$ with $2s+1>1$ is called a Lüneburg quasifield, if Q has the following multiplication:

$$(a\omega+b)\circ(c\omega+d) = (a(c^\sigma+dd^\sigma)+bo)\omega+ac+bd\,,$$

where σ is the automorphism of $GF(2^{2s+1})$ such that $x^\sigma=x^{2s+1}$ for all $x\in GF(2^{2s+1})$ and $GF((2^{2s+1})^2)=\{a\omega+b\,|\,a,\ b\in GF(2^{2s+1})\}$.

Now we determine the spread set Σ^* of a Lüenburg quasifield. Since $GF(2^{2s+1})$ is a field extension of odd dimension of $GF(2)$, $f(x)=x^2+x+1$ is an irreducible polynomial over $GF(2^{2s+1})$. Hence let ω and ϖ be elements of $GF((2^{2s+1})^2)$ such that $f(\omega)=f(\varpi)=0$. Then $\omega+\varpi=1$, $\omega\varpi=1$ and $\omega^2=\omega+1$.

Set $[a\omega+b]=\begin{bmatrix} a'\omega+b' \\ (a+a')\omega+b+b' \end{bmatrix}$. Then

$$\begin{aligned}\omega\circ(a\omega+b) &= (\omega,\ \varpi)\begin{bmatrix} a'\omega+b \\ (a+a')\omega+b+b' \end{bmatrix}\\ &= a'\omega^2+b'\omega+(a+a')\omega\varpi+(b+b')\varpi\\ &= (a'+b)\omega+a+b+b'\,.\end{aligned}$$

On the other hand by the definition of the multiplication,

$$\omega\circ(a\omega+b) = (a^\sigma+bb^\sigma)\omega+a\,.$$

Hence $a'=a^\sigma+b+bb^\sigma$ and $b'=b$. Thus we have

$$[a\omega+b] = \begin{vmatrix} (a^\sigma+b+bb^\sigma)\omega+b \\ (a+a^\sigma+b+bb^\sigma)\omega \end{vmatrix}.$$

Furthermore by computation, we can show that $\{[a\omega+b]\,|\,a,\ b\in GF(2^{2s+})\}$ satisfies the condition of a spread set.

Appendix. M. Matsumoto has showed the following:

A quasifield $Q=Q(2, q^2, \Sigma^*)$ is a Hall quasifield if and only if Σ^* consists of $\{[k\ 0]\,|\,k\in GF(q)\}$ and a conjugate class of G^* containing $\begin{bmatrix}\omega\\0\end{bmatrix}$, where ω is a element of $GF(q^2)\backslash GF(q)$.

References

[1] J. André: *Über nicht-Desarguesche Ebenen mit transitiver Translationgruppe,* Math. Z. **60** (1954), 156–186.

[2] E. Ellers and H. Karzel: *Endliche Inzidenzgruppen,* Abh. Math. Sem. Hamburg **27** (1964), 250–264.

[3] M. Hall: *Projective palnes,* Trans. Amer. Math. Soc. **54** (1943), 229–277.

[4] M. Kallaher: Affine planes with transitive collineation groups, North-Holland, 1982.

[5] H. Lüneburg: Die Suzukigruppen und ihre Geometrien, Lecture Notes in Math. 10, Springer, 1965.

[6] H. Lüneburg: Translation planes, Springer, 1980.

[7] D.M. Maduram: *Matrix representation of translation planes,* Geom. Dedicata **4** (1975), 485–497.

[8] F. Sherk: *Indicator sets in an affine space of any dimension,* Canad. J. Math. **31** (1979), 211–224.

Department of Mathematics
Osaka Kyoiku University
Tennoji, Osaka 543
Japan