# Characterization of some 4-gonal configurations of Ahrens-Szekeres type 

Dina Ghinelli<br>Dipartimento di Matematica, Università di Roma "La Sapienza" - Piazzale Aldo Moro, 2, I-00185 Roma, Italy

## ARTICLE INFO

## Article history:

Available online 24 March 2012
To my friend Toni on the occasion of his 70th birthday


#### Abstract

Motivated by the Ahrens-Szekeres Quadrangles, we shall present a variation of the 4 -gonal family method of construction introduced by Kantor in 1980. The relation between generalized quadrangles of order $(s, s)$ and of order $(s-1, s+1)$ has been known for a long time. A geometrical description of this interrelation was given by Payne in 1971 and rests on the notion of regular points or of regular lines. In this paper we wish to develop these connections algebraically in the hope of getting more insight into them from the group-theoretical point of view. In this way we are able to characterize two classes of known 4-gonal configurations.


© 2012 Elsevier Ltd. All rights reserved.

## 1. Introduction

For all notions concerning groups we refer to Gorenstein [12] and in this paper dedicated to Toni Machì we are pleased to refer also to his new book on groups [19] whose translation in English will be published soon. The reader is referred to $[24,25]$ for definitions, results, and references to the vast literature on Generalized Quadrangles (GQs). An excellent survey on this is also [26].

Generalized quadrangles, as a special case of generalized polygons, were introduced by Tits [27] in 1959. There he gave what are considered the classical examples. The first nonclassical examples were also found by Tits in the mid-1960s and appeared first in [5]. Other nonclassical examples were constructed in [1,13,20,22].

In the last fifty years there has been a great activity in the geometric and group-theoretical construction and characterization of generalized quadrangles. Depending on the point of view the main ingredients for these studies were nets or regular elements or flocks (see for instance [10] for nets, [ $8,11,9$ ] for regular elements, [26,2] for flocks and, obviously, all the references in [24,25]).

After 1980, starting with a construction of Kantor [16], several new families have been discovered. As Payne pointed out in the survey [23] "the stories of these discoveries blend in an interesting way,

[^0]connecting the study of translation planes, spreads of the 3-dimensional projective space over a finite field, flocks of a quadratic cone, and even generalized hexagons!".

With the construction in [16], Kantor could obtain all the finite examples known in 1980 of generalized quadrangles but the one with parameters ( $q-1, q+1$ ) (for prime powers $q$ ) due to Ahrens and Szekeres [1] and, independently, to Marshall Hall Jr. [13] for $q$ even, but later included in a more general construction by Payne now known as Payne derivation (see [20,21]).

Motivated by the Ahrens and Szekeres Quadrangles [1,13,20,22] we shall present here a variation of the construction of Kantor [16], by introducing the notion of an $A S$-configuration ( $G, \mathcal{A} \delta$ ). This is a finite group $G$ of order $n^{3}, n \geq 2$, together with a family

$$
\text { A\& : } U_{0}, U_{1}, \ldots, U_{n+1},
$$

of $n+2$ subgroups of $G$, each of order $n$, such that
AS1 $U_{0} \unlhd G$ is a normal subgroup of $G$,
AS2 $U_{i} U_{j} \cap U_{k}=\{1\}$ for pairwise different $i, j, k \geq 0$.
An $A S$-configuration yields a generalized quadrangle admitting an automorphism group acting regularly on the set of points, a theme already studied for instance in [7,4].

The connection between generalized quadrangles of order $(s, s)$ and of order $(s-1, s+1)$ has been known for a long time. A geometrical description of this is given by Payne in [20] and depends on the choice of a particular regular point of a quadrangle of order $s$ or, dualizing the construction in [20], of a particular regular line. In this paper, we will develop this connection algebraically in the hope of getting more insight into it from the group-theoretical point of view. In this way we are able to characterize two classes of known 4-gonal configurations, which are the two extremes of a scale measuring the number of conjugacy classes.

If the underlying group $G$ of an $A S$-configuration is abelian, then clearly the number of conjugacy classes is maximal. In this case, the factors $G / U_{i}, i=0,1, \ldots, n+1$, admit a natural spread describing translation planes. We shall prove in Section 4.1 that the $A S$-configuration is the classical example given by a hyperoval in a desarguesian plane, provided that at least three of the planes given by the spreads in $G / U_{i}, i=0,1, \ldots, n+1$, are desarguesian.

In contrast to the abelian case we study the possibility that the number of conjugacy classes is as small as possible, by assuming that each conjugacy class different from 1 admits a representative in

$$
\bigcup_{j=0}^{n+1}\left(U_{j} \backslash\{1\}\right)
$$

which is a partial difference set for the underlying strongly regular graph. We can prove that this assumption characterizes the classical symplectic 4-gonal configuration.

## 2. 4-gonal configurations of Ahrens-Szekeres type

The following method was introduced by Kantor [16] to construct finite generalized quadrangles admitting a group $G$ of automorphisms fixing a point, say $\infty$, and acting regularly on the set of points at distance 2 from $\infty$.

Let $G$ be a finite group of order $|G|=s^{2} t, s, t>1$, together with two families

$$
\mathcal{G}: A_{1}, \ldots, A_{t+1},
$$

and

$$
g^{\star}: A_{1}^{\star}, \ldots, A_{t+1}^{\star},
$$

of subgroups of $G$ such that
(i) $\left|A_{i}\right|=s,\left|A_{i}^{\star}\right|=s t$ and $A_{i} \leq A_{i}^{\star}$ for $i=1, \ldots, t+1$;
(ii) $A_{i} \cap A_{j}^{\star}=\{1\}$ for $i \neq j$;
(iii) $A_{i} A_{j} \cap A_{k}=\{1\}$ for pairwise different $i, j, k \geq 1$.

We call this a 4-gonal configuration $\left(G, \mathscr{F}, \mathscr{g}^{\star}\right)$. Kantor proved in [16] that a 4-gonal configuration $\left(G, \mathcal{G}, \mathcal{g}^{\star}\right)$ yields a generalized quadrangle with parameters $(s, t)$ having $G$ as a group of automorphisms fixing a uniquely determined point $\infty$ and acting regularly on the set of points at distance 2 from $\infty$.

Definition 1. A 4-gonal configuration ( $G, \mathscr{g}, \mathscr{g}^{\star}$ ) with parameters $(s, t)$ splits (or is said to be splitting), if there is a normal subgroup $N \unlhd G$ of order $t$ such that

$$
A_{i}^{\star}=A_{i} N, \quad i=1, \ldots, t+1 .
$$

We call a splitting 4-gonal configuration with parameters $s=t$ a 4-gonal configuration of Ahrens-Szekeres type, shortly an $A S$-configuration and we denote it ( $G, \mathcal{A} \delta$ ).

In other words, we have the following definition.
Definition 2. An $A S$-configuration ( $G, \mathcal{A} \delta$ ) of order $n$ is a finite group $G$ of order $n^{3}, n \geq 2$, together with a family

$$
\text { A\& : } U_{0}, U_{1}, \ldots, U_{n+1}
$$

of $n+2$ subgroups of $G$, each of order $n$, such that
AS1 $U_{0} \unlhd G$ is a normal subgroup of $G$,
AS2 $U_{i} U_{j} \cap U_{k}=\{1\}$ for pairwise different $i, j, k \geq 0$.
Since $U_{j} \cap U_{k} \subseteq U_{i} U_{j} \cap U_{k}$ and $n \geq 2$, property AS2 implies immediately that

$$
\begin{equation*}
U_{j} \cap U_{k}=\{1\} \quad \text { for } j \neq k . \tag{1}
\end{equation*}
$$

Using the above mentioned method of Kantor [16], an AS-configuration yields a generalized quadrangle with parameters $s=n=t$. In the following theorem we shall prove that it also yields another generalized quadrangle.

Theorem 1. Let $(G, A \&)$ be an AS-configuration of order $n$. Then the coset geometry of

$$
\text { AS: } U_{0}, U_{1}, \ldots, U_{n+1},
$$

that is, by definition, the geometry with points the elements of G , lines the left cosets (or the right cosets) of the subgroups $U_{j}, j=0, \ldots, n+1$ and incidence given by inclusion, is a generalized quadrangle with parameters ( $n-1, n+1$ ).

Proof. The proof of the theorem is divided in two parts. We start proving that

$$
\Delta(A \mathcal{A})=\Delta=\bigcup_{i=0}^{n+1}\left(U_{i} \backslash\{1\}\right)
$$

is a partial difference set in $G$ with parameters $\lambda=n-2$ and $\mu=n+2$. By definition of partial difference set (see for instance [3]), we must show that every element $g \neq 1$ of $G$ has exactly $\lambda$ (respectively $\mu$ ) representations of the form

$$
g=y^{-1} x \text { for } g \in \Delta(\text { respectively } g \notin \Delta)
$$

with $(x, y) \in \Delta \times \Delta$, provided that

$$
x \in \Delta \Longleftrightarrow x^{-1} \in \Delta
$$

In our case, the last condition is trivially satisfied. Let

$$
\begin{equation*}
V_{j}=U_{0} U_{j}, \quad j=1, \ldots, n+1, \tag{2}
\end{equation*}
$$

and note that $V_{j}$ is a subgroup of $G$ of order $n^{2}$. We use property AS2 to prove that

$$
\begin{align*}
& V_{i} \cap V_{j}=U_{0} \quad \text { for } i \neq j,  \tag{3}\\
& \bigcup_{i=1}^{n+1} V_{i}=G . \tag{4}
\end{align*}
$$

By (2), $U_{0} \leq V_{i} \cap V_{j}$. On the other hand, each element $x \in V_{i} \cap V_{j}$ is represented as $x=z_{i} x_{i}=z_{j} x_{j}$ with $z_{i}, z_{j} \in U_{0}$ and $x_{i} \in U_{i}, x_{j} \in U_{j}$. Using AS2, we obtain that $z_{i}^{-1} z_{j}=x_{i} x_{j}^{-1} \in U_{0} \cap U_{i} U_{j}=\{1\}$, hence $x_{i}=x_{j}$, and Eq. (1) gives $x_{i}=x_{j}=1$. Thus $x=z_{i}=z_{j} \in U_{0}$, as desired.

Then we have

$$
\begin{aligned}
\left|\bigcup_{i=1}^{n+1} V_{i}\right| & =\left|U_{0}\right|+\sum_{i=1}^{n+1}\left|V_{i} \backslash U_{0}\right| \\
& =n+(n+1)\left(n^{2}-n\right) \\
& =n^{3},
\end{aligned}
$$

which proves (4).
Now, property AS2 yields

$$
\begin{equation*}
V_{i} U_{j}=U_{0} U_{i} U_{j}=G, \quad \text { for } 0 \neq i, j \text { and } i \neq j . \tag{5}
\end{equation*}
$$

We intend to compute the number of representations of the form

$$
g=x y, \quad x, y \in \Delta,
$$

for a given $1 \neq g \in G$.
If $g \in \Delta$, Eq. (1) yields a unique index $i$ such that

$$
g \in U_{i} \subseteq \Delta,
$$

so that, choosing an arbitrary $x \in U_{i}$ different from 1 and $g$, there are at least $n-2$ such representations for $g$. On the other hand, if $x \notin U_{i}$ or $y \notin U_{i}$, (1) implies $x \in U_{s}, y \in U_{t}$ with pairwise different indexes $i, s, t$, which contradicts property AS2 and we get the required result $\lambda=n-2$.

Next, suppose that

$$
g \notin \Delta .
$$

By (4), there is an $s$ such that

$$
g \in V_{s}
$$

and $s$ is uniquely determined, because $g \notin U_{0}$. Thus $g \in U_{0} U_{s}=U_{s} U_{0}$, but $g \notin U_{0}$, and we already obtain two representations

$$
g=z_{1} x_{1}=x_{2} z_{2} \quad \text { with } 1 \neq z_{1}, z_{2} \in U_{0}, 1 \neq x_{1}, x_{2} \in U_{s} .
$$

We want to prove that these two representations are the only representations of the form $g=x y$ such that $x \in U_{0} \cup U_{s}$ or $y \in U_{0} \cup U_{s}$.

If $x \in U_{0}$ (respectively $x \in U_{s}$ ), we obtain that $y=x^{-1} z_{1} x_{1} \in U_{0} U_{s}$. But then AS2 yields $y \in U_{0} \cup U_{s}$. Since $g \notin \Delta$, it follows $y \in U_{s}$ (respectively $y \in U_{0}$ ) and therefore $x^{-1} z_{1}=y x_{1}^{-1} \in U_{0} \cap U_{s}$ (respectively $y z_{2}^{-1}=x^{-1} x_{2} \in U_{0} \cap U_{s}$ ). By (1), we conclude that $x=z_{1}, y=x_{1}$ (respectively $x=x_{2}, y=z_{2}$ ), as required. The remaining case $y \in U_{0} \cup U_{s}$ is treated by almost the same argument.

Thus, apart from the two given representations, for every other representation there exists an index $i \neq 0, s$ with $x \in U_{i}$. We claim that
( $\star$ ) For $1 \leq i \leq n+1$ and $i \neq s$ there is exactly one representation of the form $g=x y \quad$ with $x \in U_{i}$ and $y \in \Delta$.

Indeed, if $x y=x^{\prime} y^{\prime}$ with $x, x^{\prime} \in U_{i}$ and $y, y^{\prime} \in \Delta$, then $x^{-1} x^{\prime}=y\left(y^{\prime}\right)^{-1} \in U_{i}$ and again using AS2 we conclude that $x=x^{\prime}, y=y^{\prime}$. Therefore there exists at most one representation of such a form.

Now denote by $\mu(g)$ the number of representations of the form $g=x y$ with $x, y \in \Delta$ and $x \notin U_{0} \cup U_{s}$. As we have just seen $\mu(g) \leq n$. Counting yields

$$
\begin{aligned}
\sum_{g \notin \Delta} \mu(g) & =\sum_{i \neq j, i, j \neq 0}\left|\left(U_{i} \backslash\{1\}\right)\left(U_{j} \backslash\{1\}\right)\right| \\
& =(n+1) n(n-1)^{2} \\
& =|\{g \mid g \notin \Delta\}| n \\
& =\sum_{g \notin \Delta} n
\end{aligned}
$$

which implies that $\mu(g)=n$. Then we find exactly $n+2$ representations for $g$.
Thus we have found a partial difference set, which gives a strongly regular graph with parameters

$$
v=n^{3}, \quad k=(n-1)(n+2), \quad \lambda=n-2, \quad \mu=n+2 .
$$

We construct next a generalized quadrangle. Points are the group elements, lines are the left cosets (or the right cosets) of the subgroups $U_{j}, j=0, \ldots, n+1$ and incidence is given by inclusion. Obviously, $G$ acts as a regular automorphism group on the point set.

Clearly, each point is incident with exactly $n+2$ lines, and so we find $t=n+1$. By definition, each line has exactly $n$ points, thus $s=n-1$. Suppose that

$$
\left|x U_{i} \cap y U_{j}\right| \geq 2
$$

for two lines $x U_{i}$ and $y U_{j}$. Since $G$ acts as a group of automorphisms, we may assume that $x U_{i}=U_{i}$. So $U_{i}$ contains two different elements in $y U_{j}$, say $y x_{j} \neq y x_{j}^{\prime} \in U_{i}$. But then $1 \neq x_{j}^{-1} x_{j}^{\prime} \in U_{i} \cap U_{j}$. Using (1), we obtain $i=j$, and so $U_{i}=y U_{j}$. Therefore two distinct points (lines) are incident with at most one line (point).

If $A$ is a point and $l$ is a line not incident with $A$, then we need to show that there is a unique line through $A$ meeting $l$. By the transitivity of $G$, we may assume that $A=1$. Setting

$$
l=g U_{j}, \quad 0 \leq j \leq n+1,
$$

then $g \notin U_{j}$ and we shall prove that there is a uniquely determined subgroup $U_{i}(0 \leq i \leq n+1)$ such that

$$
g U_{j} \cap U_{i} \neq \emptyset .
$$

First, we would like to see that $U_{i}$ is uniquely determined. Suppose on the contrary that it is not; then

$$
g U_{j} \cap U_{i_{1}}, \quad g U_{j} \cap U_{i_{2}} \neq \emptyset,
$$

for $i_{1} \neq i_{2}$. Thus $g x_{j}=x_{i_{1}}$ and $g x_{j}^{\prime}=x_{i_{2}}$ with $x_{j}, x_{j}^{\prime} \in U_{j}$ and $x_{i_{1}} \in U_{i_{1}}, x_{i_{2}} \in U_{i_{2}}$, which gives immediately that $x_{j}^{-1} x_{j}^{\prime}=x_{i_{1}}^{-1} x_{i_{2}} \in U_{j} \cap U_{i_{1}} U_{i_{2}}$. Since $g \notin U_{j}$, we find $j \neq i_{1}$, $i_{2}$. Now AS2 yields $x_{i_{1}}=x_{i_{2}}$, a contradiction.

If $g \in \Delta$ then $g \in U_{i}$ for a suitable $i$ and the statement is trivial. Therefore we may assume that $g \notin \Delta$. In order to prove the existence of $U_{i}$, we use property ( $\star$ ) holding for $g \notin \Delta$. But by (4), $g \in V_{s}$ for a suitable $s \geq 1$. When $j \neq 0, s$, then $(\star)$ says that there exists an $i$ such that

$$
g \in U_{j} U_{i}
$$

But this means that $U_{i} \cap g U_{j} \neq \emptyset$. We are left just with the cases $j=0$ or $j=s$. If $j=0$, then $U_{s} \cap g U_{0} \neq \emptyset$. If $j=s$, then $U_{0} \cap g U_{s} \neq \emptyset$, as desired.

An $A S$-configuration

$$
\text { AS: } U_{0}, U_{1}, \ldots, U_{n+1},
$$

of an abelian group $G$ is called an abelian $A S$-configuration. In this case we denote by
the set of all endomorphisms $\sigma: x \mapsto x^{\sigma}$ of $G$ satisfying

$$
U_{i}^{\sigma} \leq U_{i}, \quad i=0, \ldots, n+1 .
$$

We call $K(\mathcal{A} f)$ the kernel of the 4 -gonal $A S$-configuration.
Lemma 1. Let $\sigma \neq 0$ be in the kernel of the abelian AS-configuration

$$
U_{0}, U_{1}, \ldots, U_{n+1} .
$$

Then $\sigma$ is an automorphism. In particular, we find that the kernel of the configuration is a field.
Proof. Suppose that $1 \neq x \in \operatorname{ker} \sigma$ and that $\sigma$ is not the trivial endomorphism. By (4), we get

$$
x \in V_{s},
$$

for a suitable $1 \leq s \leq n+1$. Clearly, we may assume that $s=1$.
We claim that there is an index $i \geq 2$ such that $\sigma$ is not trivial on $U_{i}$. By contradiction, assume that $U_{i}^{\sigma}=1$ for all $i \geq 2$. Since $G / U_{j}(j=0,1)$ is generated by $U_{2}, U_{3}$, we see that $\sigma$ induces the trivial endomorphism on $G / U_{j}, j=0,1$; but then $G^{\sigma} \leq U_{0} \cap U_{1}=1$, which contradicts the assumption that $\sigma$ is not trivial. Therefore we can choose $y \in U_{i}, i \geq 2$ such that

$$
y^{\sigma} \neq 1
$$

There exists a suitable $j$ such that $y x \in V_{j}$. We have

$$
y^{\sigma}=y^{\sigma} x^{\sigma}=(y x)^{\sigma} \in V_{i}^{\sigma} \cap V_{j}^{\sigma}=V_{i} \cap V_{j} .
$$

If $V_{i} \neq V_{j}$, then $y^{\sigma} \in U_{0}$, a contradiction to $1 \neq y^{\sigma} \in U_{i}^{\sigma} \leq U_{i}$. Thus $V_{i}=V_{j}$. But then $y, y x \in V_{i}$ gives immediately that $x \in V_{i}$. Since $y \notin V_{s}$, we have $i \neq s$, which implies in turn that $x \in V_{i} \cap V_{s}=U_{0}$. Thus ker $\sigma \leq U_{0}$.

Since the configuration is abelian, we can exchange the role of $U_{0}$ and $U_{1}$, and then (1) yields the statement.

## 3. Structure of an $A S$-configuration

In the following $(G, \mathcal{A} \delta)$ denotes an $A S$-configuration of order $n$. Let us remind that a partition $\pi$ of a finite group $H$ is called a spread, if $H=A B$ for all $A, B \in \pi$ with $A \neq B$. Let us consider the homomorphism

$$
G \rightarrow \bar{G}=G / U_{0}, \quad g \mapsto \bar{g}=g U_{0}
$$

We claim that

$$
\begin{equation*}
\overline{U_{i}}, \quad i=1, \ldots, n+1, \tag{7}
\end{equation*}
$$

is a spread of $\bar{G}$. Now, $\bar{g} \in \overline{U_{i}} \cap \overline{U_{j}}, i \neq j$ implies that $g \in U_{i} U_{0} \cap U_{j} U_{0}$. By relation (3) it follows that $g \in U_{0}$, and so $\bar{g}=1$, as desired. Using (5), we find $G=U_{i} U_{j} U_{0}$ for $i, j \neq 0$ and $i \neq j$. Thus

$$
\bar{G}=\overline{U_{i} U_{j}},
$$

as desired. Given a spread in a finite group $H$, it is well known that the coset geometry of the spread yields an affine translation plane, whose translation group is isomorphic to $H$. Thus we obtain the following two results (see [5]).

Theorem 2. The coset geometry given by the partition (7) is an affine plane of order $n$.

Corollary 1. $G$ is a p-group. In particular, $G / U_{0}$ is an elementary abelian group and

$$
[G, G], \quad \Phi(G) \leq U_{0} .
$$

Another consequence is

$$
\begin{equation*}
U_{i}^{g} \leq U_{i} U_{0} \unlhd G, \quad g \in G . \tag{8}
\end{equation*}
$$

Using the above results, we have the following.
Theorem 3. If $(G, A \not f)$ is an abelian AS-configuration, then $G$ is an elementary abelian 2-group.
Proof. Since $G$ is abelian, we can replace the role of $U_{0}$ by $U_{1}$ and Corollary 1 gives $\Phi(G)=1$, hence $G$ is an elementary abelian $p$-group. We have to show that $p=2$.

To begin with, let $Q$ be a subgroup of order $p$, not contained in a component of the $A S$-configuration. Fix $0 \leq i \leq n+1$. Since $G / U_{i}$ admits the above mentioned spread, there is a uniquely determined $f(i)$ such that

$$
Q \leq U_{i}+U_{f(i)} .
$$

Clearly, $f(f(i))=i$. Thus $f$ is a bijection of $\{0,1, \ldots, n+1\}$. By the choice of $Q$, we have $f(i) \neq i$. Hence $f$ is an involution without fixed points. It follows that

$$
n+2 \equiv 0(\bmod 2)
$$

and this yields the statement.
For conjugacy classes we shall need the following.

## Lemma 2. We have

(i) Each coset of $U_{0}$ is an invariant complex.
(ii) An element $x u \in U_{0} u$ is conjugate to $u$ if and only if there exists a $g \in G$ such that $x=\left[g, u^{-1}\right]$.

Proof. By Corollary $1,[G, G] \leq U_{0}$. It follows that

$$
\left(U_{0} x\right)^{y}=U_{0} x^{y}=U_{0} x^{y} x^{-1} x=U_{0} x,
$$

since $x^{y} x^{-1}=\left[y, x^{-1}\right] \in U_{0}$, and (i) is proved.
Clearly, $u$ is conjugate to $x u$ if and only if there is a $g \in G$ with $u^{g}=x u$, which is equivalent to

$$
x=u^{g} u^{-1}=\left[g, u^{-1}\right],
$$

and the lemma is proved.

## 4. Examples and characterizations

The two known classes of $A S$-configurations are the two extremes of a scale measuring the number of conjugacy classes. Let us begin with the maximal number of conjugacy classes.

### 4.1. Abelian examples

Example 1. The classical example is given by a hyperoval in a projective plane over $K=\mathbb{F}_{q}$, where $q$ is a power of a 2 : the plane is represented by the nontrivial subspaces of $K^{3}$. A hyperoval $\mathscr{H}$ is a set of $q+2$ subspaces of dimension 1 , each three of which generate $K^{3}$, which is equivalent to the fact that $\left(K^{3}, \mathscr{H}\right)$ is an AS-configuration.

By Theorem 3, we can regard the group of an abelian AS-configuration

$$
\text { A\& : } U_{0}, U_{1}, \ldots, U_{n+1},
$$

as a vector space $V=G$ of dimension $n^{3}$ over $\mathbb{F}_{2}$. But by Lemma 1 , we may regard $V$ also as a vector space over the kernel $K=K(A \not \&)$. Setting

$$
|K|=q \quad \text { and } \quad \operatorname{dim}_{K} U_{j}=m, \quad j=0,1, \ldots, n+1,
$$

we have

$$
n=q^{m}, \quad \operatorname{dim}_{K} V=3 m .
$$

Obviously, the condition that the subspaces $U_{0}, U_{1}, \ldots, U_{q^{m}+1}$ of dimension $m$ form an $A S$ configuration in $V$ is equivalent to the fact that every three of them generate $V$. Thus for every $K$-linear bijection $\Lambda: V \rightarrow V, x \mapsto x \Lambda$, the images

$$
\mathcal{A} \& \Lambda: U_{0} \Lambda, U_{1} \Lambda, \ldots, U_{q^{m}+1} \Lambda,
$$

form also an $A S$-configuration in $V$. Now by (5),

$$
V=U_{0} \oplus U_{1} \oplus U_{2} .
$$

Identifying $U_{0}, U_{1}, U_{2}$ with $K^{m}$, we have $V=K^{3 m}$ and

$$
U_{0}=\left\{(x, 0,0) \mid x \in K^{m}\right\}, \quad U_{1}=\left\{(0, x, 0) \mid x \in K^{m}\right\} \quad U_{2}=\left\{(0,0, x) \mid x \in K^{m}\right\} .
$$

Moreover, each of the subspaces $U_{j}, j \geq 3$ is represented as

$$
U_{j}=\left\{\left(x, x \Sigma_{j}, x \Theta_{j}\right) \mid x \in U_{0}=K^{m}\right\}, \quad j=3, \ldots, q^{m}+1,
$$

where $\Sigma_{j}, \Theta_{j}: U_{0} \rightarrow U_{0}$ are $K$-linear bijections or regular $m \times m$-matrices over $K$. Setting $\Lambda=$ $1_{K^{m}} \oplus \Sigma_{3}^{-1} \oplus \Theta_{3}^{-1}$ and replacing $\mathcal{A} \&$ by $A \& ~ \Lambda$, we may assume that $\Sigma_{3}=\Theta_{3}=1_{K^{m}}$. In other words

$$
U_{3}=\left\{(x, x, x) \mid x \in K^{m}\right\} .
$$

Since the given $A S$-configuration induces a translation plane $\Pi_{1}$ (respectively $\Pi_{2}$ ) in $V / U_{1}$ (respectively $V / U_{2}$ ), the sets

$$
\Sigma=\left\{\Sigma_{j} \mid j=3, \ldots, q^{m}+1\right\} \text { and } \Theta=\left\{\Theta_{j} \mid j=3, \ldots, q^{m}+1\right\}
$$

are so called spreads of matrices (see [15]). For the convenience of the reader we remind that a spread $\Gamma$ of $m \times m$-matrices over $K$ is a set of regular matrices such that
(i) If $\alpha, \beta \in \Gamma$ with $\alpha \neq \beta$ then $\alpha-\beta$ is nonsingular.
(ii) Given $a, b \in K^{m} \backslash\{0\}$ there exists an $\alpha \in \Gamma$ such that $a \alpha=b$.

Again, there is an induced translation plane $\Pi_{0}$ in $V / U_{0}$. Thus

$$
\Gamma=\left\{\Gamma_{j}=\Sigma_{j}^{-1} \Theta_{j} \mid j=3, \ldots, q^{m}+1\right\}
$$

yields also a spread of matrices.
Our classification Theorem 4 will be proved using some group theoretical theorems. Thus we begin with the following lemma.

Lemma 3. With the above notation, if $\Sigma, \Theta, \Gamma$ are groups. Then

$$
\Xi=\Sigma \Theta=\Theta \Gamma=\Gamma \Sigma,
$$

is a subgroup of $\operatorname{GL}(m, q)$.

Proof. To prove that $\Sigma \Theta$ is a subgroup of $G L(m, q)$ it is sufficient to show that $\Sigma \Theta=\Theta \Sigma$. Now $\Gamma$ is a group, hence

$$
\Sigma_{i}^{-1} \Theta_{i} \Sigma_{j}^{-1} \Theta_{j} \in \Gamma \subseteq \Sigma \Theta
$$

It follows that

$$
\Theta_{i} \Sigma_{j}^{-1} \in \Sigma_{i} \Sigma \Theta \Theta_{j}^{-1}=\Sigma \Theta,
$$

since $\Gamma, \Theta$ are groups. But then
$\Theta \Sigma \subseteq \Sigma \Theta$.
Taking inverse elements, we get

$$
\Sigma \Theta \subseteq \Theta \Sigma
$$

Thus $\Sigma \Theta=\Theta \Sigma$, as desired.
Similarly, one shows that $\Theta \Lambda$ and $\Lambda \Sigma$ are subgroups of $G L(m, q)$. Since

$$
\Sigma, \Theta, \Gamma \leq \Sigma \Theta, \Theta \Lambda, \Lambda \Sigma
$$

it follows that

$$
\langle\Sigma, \Theta, \Gamma\rangle=\Sigma \Theta=\Theta \Lambda=\Lambda \Sigma,
$$

which proves the lemma.
We remark that $\Sigma$ is a group if and only if the corresponding translation plane $\Pi_{1}$ is coordinatized by a (regular) DICKSON nearfield (see [5] or [15,6]). Moreover, the proof of the following characterization rests on the well known result that $\Pi_{1}$ is a desarguesian plane if and only if $\Sigma$ is an abelian group, and under this assumption $\Sigma^{\diamond}=\Sigma \cup\{0\}$ is even a field, which means in particular that $\Sigma$ is a cyclic group (see for instance [15]).

The next theorem shows that it seems difficult to find abelian $A S$-configurations that are not hyperovals.

Theorem 4. With the above notation suppose that three of the planes given by the spreads in $G / U_{i}, i=$ $0,1, \ldots, n+1$ are desarguesian. Then the AS-configuration is isomorphic to the hyperoval given in Example 1.

Proof. By the preparation for this theorem, we may assume that $\Pi_{j}, j=0,1,2$, are desarguesian. We need to show that $1=m=\operatorname{dim}_{K} U_{j}$. For convenience we set $\Lambda_{0}=\Gamma, \Lambda_{1}=\Sigma, \Lambda_{2}=\Theta$ and

$$
G=\Lambda_{0} \Lambda_{1}=\Lambda_{1} \Lambda_{2}=\Lambda_{2} \Lambda_{0} .
$$

We wish to show that $\Lambda_{0}=\Lambda_{1}=\Lambda_{2}$. By contradiction, suppose that this is false. Since all three subgroups have the same order, it follows that the three subgroups are pairwise different. In particular, for each permutation $i, j, k$ of $0,1,2$

$$
\Delta_{k}=\Lambda_{i} \cap \Lambda_{j},
$$

is a proper subgroup of $\Lambda_{i}$ and $\Lambda_{j}$. Since $\left[\Delta_{k}, \Lambda_{i}\right]=\left[\Delta_{k}, \Lambda_{j}\right]=1$, the subgroup $\Delta_{k}$ lies in the center $Z(G)$ of $G$.

By the above remark, $\Lambda_{i}^{\diamond}$ is a field and $\Lambda_{i}^{\diamond} \cong \mathbb{F}_{q^{m}}$. We find immediately that

$$
\begin{equation*}
C_{G L(m, q)}\left(\Lambda_{i}\right)=\Lambda_{i}, \quad i=0,1,2 . \tag{9}
\end{equation*}
$$

It follows that

$$
\begin{equation*}
Z(G)=\Delta_{0}=\Delta_{1}=\Delta_{2} . \tag{10}
\end{equation*}
$$

A theorem of Kegel ([18], Folgerung 2) states that a finite trifactorized group

$$
H=A B=B C=C A,
$$

with nilpotent subgroups $A, B, C \leq H$ is itself nilpotent. Thus $G$ is nilpotent. Since $G / Z(G)$ is a product of two cyclic groups, then Theorem 24a in [14] yields that at least one of the two factors contains a nontrivial normal subgroup, which itself is cyclic of course. Therefore we may assume that there is a normal subgroup $N$ of $G$ such that

$$
Z(G)<N \leq \Lambda_{0} \quad \text { and } \quad[N: Z(G)]=p,
$$

with a certain prime $p$. Clearly, $N$ is cyclic and $\Lambda_{1}$ acts by conjugation on $N$ as a group of automorphisms with kernel $C_{\Lambda_{1}}(N)$. By (9), $C_{\Lambda_{1}}(N) \neq \Lambda_{1}$, because $N$ is not contained in $\Lambda_{1}$. Since $N \Lambda_{1}$ is nilpotent $Z(G) \leq \Lambda_{1}$, and because $[N: Z(G)]=p$, we have that $\Lambda_{1} / C_{\Lambda_{1}}(N)$ is a nontrivial $p$-group. On the other hand, $N$ is cyclic and therefore the cyclic $p$-Sylow subgroup $P=\langle x\rangle$ of $N$ has at least order $p^{2}$. We find

$$
\begin{equation*}
p||Z(G)||\left|C_{\Lambda_{1}}(N)\right| . \tag{11}
\end{equation*}
$$

Since $\Lambda_{1}$ acts trivially on $x^{p} \in Z(G)$, we conclude that $\Lambda_{1} / C_{\Lambda_{1}}(N)$ has order $p$. Thus

$$
p=\frac{q^{m}-1}{\left|C_{\Lambda_{1}}(N)\right|} .
$$

Now $C_{\Lambda_{1}}(N) \cup\{0\}$ is closed under addition, so it is a subfield of $\Lambda_{1}^{\diamond}$. We find $\left|C_{\Lambda_{1}}(N)\right|=q^{a}-1$ with $m=a b, 1<a<m$ and $p \mid q^{a}-1$ by (11). So

$$
p=\frac{q^{m}-1}{q^{a}-1}=1+q^{a}+q^{2 a}+\cdots+q^{(b-1) a}>q^{a}>p
$$

a contradiction. Therefore we have proved that $G=\Sigma=\Theta=\Lambda$.
Now we claim that for $g \in \Sigma$ the $K$-linear map $\Xi_{g}$ defined by the rule

$$
(x, y, z) \Xi_{g}=(x g, y g, z g),
$$

is in the kernel of the $A S$-configuration. Indeed, $\Xi_{g}$ leaves $U_{0}, U_{1}, U_{2}$ invariant. And since $\Sigma$ is abelian, for $j \geq 3$

$$
\begin{aligned}
U_{j} \Xi_{g} & =\left\{\left(x g, x \Sigma_{j} g, x \Theta_{j} g\right), \mid x \in K^{m}\right\} \\
& =\left\{\left(x g, x g \Sigma_{j}, x g \Theta_{j}\right), \mid x \in K^{m}\right\} \\
& =U_{j} .
\end{aligned}
$$

Looking at the restriction of $\Sigma$ to $U_{0}$ we see that $K$ acts transitively on $U_{0} \backslash\{0\}$, because $\Sigma$ is a spread. But then $\operatorname{dim}_{K} U_{0}=1$, as desired, and the theorem is proved.

### 4.2. The other extremal case

In contrast to the abelian case we study here the possibility that the number of conjugacy classes is as small as possible. So we assume in the following that

$$
\text { A\& : } U_{0}, U_{1}, \ldots, U_{n+1},
$$

is an $A S$-configuration for the group $G$ satisfying the
Hypothesis. Each conjugacy class different from $\{1\}$ has a representative in

$$
\Delta(\mathcal{A} f)=\bigcup_{j=0}^{n+1}\left(U_{j} \backslash\{1\}\right) .
$$

We call this a symplectic AS-configuration. We describe in some detail the only known class of symplectic $A S$-configurations.

Example 2. Let $q$ be an odd prime power and $G=\mathbb{F}_{q}^{3}$. Furthermore, let $M$ be a $2 \times 2$-matrix over $\mathbb{F}_{q}$. With respect to the multiplication

$$
(\alpha, z)(\beta, w)=\left(\alpha+\beta, z+w+\alpha M \beta^{\top}\right), \quad \alpha, \beta \in \mathbb{F}_{q}^{2}, z, w \in \mathbb{F}_{q},
$$

$G$ becomes a group, denoted by $G_{M}$.
One easily verifies that

$$
M+M^{\top} \text { is regular } \Longrightarrow Z\left(G_{M}\right)=\left\{(0,0, z) \mid z \in \mathbb{F}_{q}\right\} .
$$

Now, let $G_{M_{1}}, G_{M_{2}}$ be two such groups and suppose that there exists a regular matrix $M$ such that

$$
N=M M_{2} M^{\top}-M_{1}
$$

is a symmetric matrix and set $2 Q(\alpha)=\alpha N \alpha^{\top}$. Then the application $\tau$ from $G_{M_{1}}$ onto $G_{M_{2}}$ defined by

$$
(\alpha, z)^{\tau}=(\alpha M, z+Q(\alpha))
$$

is an isomorphism. In fact, we have

$$
\begin{aligned}
((\alpha, z)(\beta, w))^{\tau} & =\left(\alpha+\beta, z+w+\alpha M_{1} \beta^{\top}\right)^{\tau} \\
& =\left(\alpha M+\beta M, z+w+\alpha M_{1} \beta^{\top}+Q(\alpha+\beta)\right) \\
& =\left(\alpha M+\beta M, z+w+\alpha M_{1} \beta^{\top}+Q(\alpha)+Q(\beta)+\alpha N \beta^{\top}\right),
\end{aligned}
$$

and

$$
\begin{aligned}
(\alpha, z)^{\tau}(\beta, w)^{\tau} & =(\alpha M, z+Q(\alpha))(\beta M, w+Q(\beta)) \\
& =\left(\alpha M+\beta M, z+w+Q(\alpha)+Q(\beta)+\alpha M M_{2}(\beta M)^{\top}\right) \\
& =\left(\alpha M+\beta M, z+w+Q(\alpha)+Q(\beta)+\alpha M M_{2} M^{\top} \beta^{\top}\right) \\
& =\left(\alpha M+\beta M, z+w+Q(\alpha)+Q(\beta)+\alpha\left(N+M_{1}\right) \beta^{\top}\right) .
\end{aligned}
$$

We are interested in

$$
M_{1}=\left(\begin{array}{cc}
0 & 0 \\
-1 & 0
\end{array}\right),
$$

hence

$$
(x, y, z)(a, b, c)=(x+a, y+b, z+c-y a) .
$$

It is not difficult to show that $G=G_{M_{1}}$ is isomorphic to the semidirect product of the translation group of the affine plane corresponding to $G / Z(G) \cong \mathbb{F}_{q}^{2}$ with the group of shears having a fixed center. Moreover, the commutator $[\alpha, \beta]$ is well defined on $G / Z(G)$. We have

$$
[\alpha, \beta]=a_{2} b_{1}-a_{1} b_{2}=\alpha\left(\begin{array}{cc}
0 & -1 \\
1 & 0
\end{array}\right) \beta^{\top}=\alpha M_{2} \beta^{\top},
$$

for $\alpha=\left(a_{1}, a_{2}\right)$ and $\beta=\left(b_{1}, b_{2}\right)$. We find that the group

$$
G / Z(G) \oplus Z(G)=G_{M_{2}}
$$

is the group given by Kantor in [17], A.3.4. Setting

$$
M=\left(\begin{array}{cc}
1 & 0 \\
0 & -1 / 2
\end{array}\right),
$$

we have

$$
M M_{2} M^{\top}-M_{1}=\left(\begin{array}{cc}
0 & 1 / 2 \\
1 / 2 & 0
\end{array}\right)
$$

hence the two groups are isomorphic under the above mentioned isomorphism. In accordance with [17], A.3.4, this isomorphism yields the following $A S$-configuration for $G_{M_{1}}$.

$$
U_{0}=Z(G), \quad U_{1}=\left\{(0, z, 0) \mid z \in \mathbb{F}_{q}\right\}, \quad U_{2}=\left\{(z, 0,0) \mid z \in \mathbb{F}_{q}\right\} .
$$

Modulo $Z(G)$, the remaining components of the configuration are the lines (not equal to $\{(0, x) \mid x \in$ $\left.\mathbb{F}_{q}\right\}$ ) through the origin of the affine plane given by $G / Z(G)$, namely

$$
W_{c}=\left\{\left(x, x c, x^{2} c / 2\right) \mid x \in \mathbb{F}_{q}\right\}, \quad c \in \mathbb{F}_{q} .
$$

In order to show that the hypothesis in Section 4.2 holds, we need to show that the conjugacy classes laying in $V_{j} \backslash U_{0}=U_{0} U_{j} \backslash U_{0},(j=1, \ldots, n+1)$ are represented by the elements in $U_{j}$. By Lemma 2 this will follow if we can show that for some $1 \leq i \neq j \leq n+1$,

$$
\left[u, U_{i}\right]=U_{0} \quad \text { for each } 1 \neq u \in U_{j}, j=1, \ldots, n+1,
$$

and this is a straightforward computing argument.
Lemma 4. Each conjugacy class of the given AS-configuration is a subset of $U_{0}$ or a coset of the form

$$
U_{0} u \quad \text { with } u \in \bigcup_{j=1}^{n+1}\left(U_{j} \backslash\{1\}\right)=\Delta^{\star} .
$$

In particular, we have

$$
\left|C_{G}(u)\right|=n^{2}, \quad u \in \Delta^{\star} .
$$

Moreover, for each $u \in \Delta^{\star}$ the set

$$
[u, G]=\{[u, g] \mid g \in G\}
$$

of commutators equals $U_{0}$, thus $U_{0}=[u, G]$.
Proof. By hypothesis, each conjugacy class not contained in $U_{0}$ is of the form $u^{G}$ with $u \in \Delta^{\star}$. So Lemma 2 yields

$$
u^{G} \subseteq U_{0} u
$$

But $u$ is the only element of $\Delta^{\star}$ in $U_{0} u$. Therefore the hypothesis implies that $u^{G}=U_{0} u$, as desired.
Now let $1 \neq u \in U_{1}$. As we have just seen, for $u_{0} \in U_{0}$ the element $u_{0} u$ is conjugate to $u$. But then there is a $g \in G$ such that $u^{g}=u_{0} u$, which is $\left[g, u^{-1}\right]=u_{0}$. Thus $[u, G]=U_{0}$.

As an immediate consequence we find the following.
Corollary 2. The center of $G$ is a subgroup of $U_{0}$ :

$$
Z(G) \leq U_{0} .
$$

Since $G / U_{0}$ is elementary abelian, the above Lemma 4 implies that

$$
U_{0}=[G, G]=\Phi(G) .
$$

Corollary 3. For $i, j \geq 1$ and $i \neq j$, we have

$$
\left\langle U_{i}, U_{j}\right\rangle=G .
$$

Proof. If this is false there is a maximal subgroup $M$ such that $\left\langle U_{i}, U_{j}\right\rangle \leq M<G$. Since $U_{0}=\Phi(G)$, we have $U_{0} \leq M$. But $G=U_{0} U_{i} U_{j}$ and this is a contradiction.

Next we prove the following lemma.
Lemma 5. Let $i \geq 1$. Then

$$
N_{G}\left(U_{i}\right)=C_{G}\left(U_{i}\right) \leq U_{0} U_{i}=V_{i}
$$

Proof. Clearly, $C_{G}\left(U_{i}\right) \leq N_{G}\left(U_{i}\right)$. Conversely, let $g \in N_{G}\left(U_{i}\right)$. For each $x \in U_{i}$ it follows that

$$
x^{-1} x^{g}=[x, g] \in U_{i} \cap U_{0} .
$$

Since $U_{i} \cap U_{0}=\{1\}$ we get $x=x^{g}, x \in U_{i}$. Thus $g \in C_{G}\left(U_{i}\right)$, as desired.
Now suppose that there exists an element $g \in N_{G}\left(U_{i}\right) \backslash U_{0} U_{i}=C_{G}\left(U_{i}\right) \backslash V_{i}$. But then $g \in V_{j}, 1 \leq$ $j \neq i$, say $1 \neq g=u_{0} u_{j}$ with $u_{0} \in U_{0}, u_{j} \in U_{j}$. By Lemma $4, g$ is conjugate to $u_{j}$. Thus we find an element $h \in G$ such that $u_{j} \in C_{G}\left(U_{i}^{h}\right)$, hence

$$
1 \neq u_{j} \in C_{G}\left(U_{i}^{h}\right), \quad C_{G}\left(U_{j}\right) .
$$

Since $U_{i}^{h} \leq V_{i}, U_{j} \leq V_{j}$ and $V_{i} \cap V_{j}=U_{0}$, it follows that $U_{i}^{h} \cap U_{j}=\{1\}$ and so

$$
\left|U_{i}^{h} U_{j}\right|=n^{2} .
$$

Using Lemma 4 we obtain

$$
C_{G}\left(u_{j}\right)=U_{j} U_{i}^{h} .
$$

Choose $1 \neq u_{0} \in Z(G) \leq U_{0}$. Thus $u_{0} \in U_{j} U_{i}^{h}$, hence

$$
u_{0}=x y^{h} \quad \text { with } x \in U_{j}, y \in U_{i},
$$

and $x y=u_{0}\left(y^{-1} y^{h}\right)^{-1} \in U_{j} U_{i} \cap U_{0}=\{1\}$. But then $x=y^{-1} \in U_{i} \cap U_{j}=\{1\}$, and therefore $x=y=1$. We conclude $u_{0}=1$, a contradiction to the choice of $u_{0}$ and the lemma is proved.

We set $U=U_{1}$ and

$$
\Omega=\left\{g \in G \mid g \notin \bigcup_{1 \neq u \in U} C_{G}(u)\right\} .
$$

Since $C_{G}(U) \leq C_{G}(u), u \in U$, we have

$$
\bigcup_{1 \neq u \in U} C_{G}(u) \subseteq \bigcup_{1 \neq u \in U}\left(C_{G}(u) \backslash C_{G}(U)\right) \cup C_{G}(U),
$$

which implies

$$
\begin{aligned}
\left|\bigcup_{1 \neq u \in U} C_{G}(u)\right| & \leq\left|\bigcup_{1 \neq u \in U}\left(C_{G}(u) \backslash C_{G}(U)\right)\right|+\left|C_{G}(U)\right| \\
& \leq(n-1)\left(n^{2}-\left|C_{G}(U)\right|\right)+\left|C_{G}(U)\right| \\
& \leq n^{3}-n^{2}-(n-1)\left|C_{G}(U)\right|+\left|C_{G}(U)\right| \\
& \leq n^{3}-n^{2}-(n-2)\left|C_{G}(U)\right|,
\end{aligned}
$$

and therefore

$$
\begin{equation*}
|\Omega| \geq n^{3}-n^{3}+n^{2}+(n-2)\left|C_{G}(U)\right|=n^{2}+(n-2)\left|C_{G}(U)\right| . \tag{12}
\end{equation*}
$$

Since $U$ is abelian, $C_{G}(U)$ acts as a permutation group on $\Omega$ via left multiplication. Denote by $\Omega^{\star}$ the set of orbits of $C_{G}(U)$ on $\Omega$ and let

$$
g_{1}, \ldots, g_{N}
$$

be a set of representatives of the orbits in $\Omega^{\star}$. Formally, we set $g_{0}=1$. By (12), we find

$$
\begin{equation*}
|N| \geq \frac{n^{2}+(n-2)\left|C_{G}(U)\right|}{\left|C_{G}(U)\right|} \geq n-2+\frac{n^{2}}{\left|C_{G}(U)\right|} \geq n-1 . \tag{13}
\end{equation*}
$$

Lemma 6. Let $0<i<j \leq N$. Then

$$
U^{g_{i}} \cap U^{g_{j}}=\{1\} \text { and } U_{0} \cap U^{g_{i}}=\{1\} .
$$

Proof. The proof rests on the following property:

$$
U^{h} \cap U^{g} \neq\{1\} \Rightarrow C_{G}(U) g=C_{G}(u) h .
$$

Indeed, the assumption implies $\mathrm{hg}^{-1} \in N_{G}(U)$, then Lemma 5 gives $g h^{-1} \in C_{G}(U)$, thus $C_{G}(U) g=$ $C_{G}(U) h$, as desired. It remains to show that

$$
U_{0} \cap U^{g_{i}}=\{1\} .
$$

But $U_{0} \cap U^{g_{i}}=U_{0}^{g_{i}^{-1}} \cap U_{1}=U_{0} \cap U_{1}=\{1\}$.
Since $U^{g} \leq V_{1}$ for $g \in G$, Lemma 6 and (13) imply that

$$
\begin{align*}
n^{2} & \geq\left|U_{0}\right|+\sum_{j=0}^{N}\left(\left|U^{g_{j}}\right|-1\right) \\
& \geq n+(N+1)(n-1) \\
& \geq n+n(n-1) \\
& \geq n^{2} . \tag{14}
\end{align*}
$$

Setting

$$
\Gamma=\left\{U_{0}\right\} \cup\left\{U^{g_{i}} \mid i=0,1, \ldots, N\right\},
$$

we obtain the following results.
Corollary 4. With the above notation we have
(1) $N+1=n$.
(2) $\Gamma$ is a spread of $V_{1}$.
(3) $V_{1}$ is elementary abelian.
(4) $C_{G}(u)=V_{1}$ for each $1 \neq u \in U$.
(5) We can choose $U_{2}$ as the set $g_{0}, g_{1}, \ldots, g_{N}=g_{n-1}$ of representatives.
(6) $\Gamma \backslash\left\{U_{0}\right\}$ is the conjugacy class of $U$.

Proof. By (14), it follows immediately that $N+1=n$. Thus $|\Gamma|=n+1$ and Lemma 6 shows that $\Gamma$ is a spread of $V_{1}$. But then $V_{1}$ is the translation group of the corresponding affine plane, and this proves (3).

From (3) we deduce $C_{G}(u) \geq V_{1}$ and Lemma 4 yields (4).
For (5), we need to show that an element $1 \neq u_{2} \in U_{2}$ does not commute with $1 \neq u \in U$. Now, $C_{G}(u) \cap U_{2}=V_{1} \cap U_{2}=U_{0} U_{1} \cap U_{2}=\{1\}$.

Finally, claim (5) together with the fact that $N_{G}(U)=C_{G}(U)=V_{1}$ yields (6).
Let us denote by $\mathcal{A}$ the affine plane corresponding to the spread of $V_{1}$. Then, by definition, $V_{1}$ acts as a translation group on $\mathcal{A}$. Furthermore by claim (6) of Corollary 4, an element $u_{2} \in U_{2}$ acts as an automorphism on $\mathscr{A}$ via the action

$$
\sigma_{u_{2}}: V_{1} \rightarrow V_{1}, \quad x \mapsto x^{u_{2}}=u_{2}^{-1} x u_{2} .
$$

Since $\sigma_{u_{2}}$ fixes $U_{0}$ pointwise, and also fixes each line in the parallel class of $U_{0}$, because

$$
\left(U_{0} g\right)^{u_{2}}=U_{0} g^{u_{2}}=U_{0}\left[u_{2}, g^{-1}\right] g=U_{0},
$$

the group $U_{2}$ acts as a (linear) transitive group of shears (affine elations) with axes $U_{0}$. In other words, $\mathcal{A}$ is a semifield plane, coordinatized by a semifield $\mathbb{S}$ (see for instance [5] or [15]). In particular, we have identified our group $G$ : it is the semidirect product of the translation group with the group of
shears of a semifield plane. Thus $\mathbb{S}$ is a semifield with $q$ elements and $\mathcal{A}=\mathbb{S}^{2}$. The translations are the mappings of the form

$$
\tau_{(a, b)}:(x, y) \mapsto(x+a, y+b) \quad \text { for }(a, b) \in \mathbb{S}^{2},
$$

and the affine elations are

$$
\delta_{a}:(x, y) \mapsto(x, x a+y) \quad \text { for } a \in \mathbb{S} .
$$

Setting

$$
\gamma(a, c, b)=\tau_{(a, b)} \delta_{c}:(x, y) \mapsto(x+a,(x+a) c+y+b)
$$

we find

$$
\begin{aligned}
(x, y) \gamma(a, c, b) \gamma(u, w, v) & =(x+a, x c+a c+y+b) \gamma(v, w, u) \\
& =(x+a+u,(x+a+u) w+(x+a) c+y+b+v),
\end{aligned}
$$

and

$$
\begin{aligned}
(x, y) \gamma(a+u, c+w, b+v-u c) & =(x+a+u,(x+a+u)(c+w)+y+b+v-u c) \\
& =(x+a+u,(x+a+u) w+(x+a) c+y+b+v) .
\end{aligned}
$$

We consider the group of order $q^{3}$

$$
G=\mathbb{S}^{3}
$$

with the multiplication given by

$$
(x, y, z)(u, v, w)=(x+u, y+v, z+w-u y) .
$$

With this identification the three subgroups $U_{i}, i=0,1,2$, of order $q$ are

$$
U_{0}=\{(0,0, z) \mid z \in \mathbb{S}\}, \quad U_{1}=\{(x, 0,0) \mid x \in \mathbb{S}\}, \quad U_{2}=\{(0, y, 0) \mid y \in \mathbb{S}\}
$$

Moreover, we know that

$$
Z(G)=U_{0} \quad \text { and } \quad G=U_{0} U_{1} U_{2} .
$$

The remaining commutative subgroups of the $A S$-configuration are of the form

$$
U_{j}=\left\{\left(x, f_{j}(x), g_{j}(x)\right) \mid x \in \mathbb{S}\right\}, \quad j=3, \ldots, q+1
$$

where

$$
f_{j}: \mathbb{S} \rightarrow \mathbb{S}, \quad \text { and } \quad g_{j}: \mathbb{S} \rightarrow \mathbb{S}
$$

are two maps. We wish to deduce some relations for these maps. Clearly, $(0,0,0)=\left(0, f_{j}(0), g_{j}(0)\right) \in$ $U_{j}$. So

$$
f_{j}(0)=g_{j}(0)=0, \quad j \geq 3 .
$$

## A straightforward computation yields

$$
\left(x, f_{i}(x), g_{i}(x)\right)\left(y, f_{j}(y), g_{j}(y)\right)=\left(x+y, f_{i}(x)+f_{j}(y), g_{i}(x)+g_{j}(y)-y f_{i}(x)\right)
$$

Since $U_{j}, j \geq 3$, is a commutative group, for $i=j$ it follows that

$$
\begin{align*}
& f_{i}(x)+f_{i}(y)=f_{i}(x+y),  \tag{15}\\
& g_{i}(x)+g_{i}(y)-y f_{i}(x)=g_{i}(x+y),  \tag{16}\\
& y f_{i}(x)=x f_{i}(y) . \tag{17}
\end{align*}
$$

Setting $f_{i}(1)=c_{i}$, Eq. (17) gives

$$
\begin{equation*}
f_{i}(x)=x f_{i}(1)=x c_{i} . \tag{18}
\end{equation*}
$$

Furthermore,

$$
g_{i}(x+y)=g_{i}(x)+g_{i}(y)-x\left(y c_{i}\right) .
$$

Using (17) we obtain

$$
\begin{equation*}
y\left(x c_{i}\right)=x\left(y c_{i}\right) . \tag{19}
\end{equation*}
$$

We claim that the elements $c_{3}, \ldots, c_{q+1}$ are pairwise different, meaning that

$$
\mathbb{S} \backslash\{0\}=\left\{c_{3}, \ldots, c_{q+1}\right\} .
$$

If not, we may assume, without loss of generality, $c_{3}=c_{4}$. We see that

$$
\left(1, c_{3}, g_{3}(1)\right) \in U_{3} \quad \text { and } \quad\left(1, c_{3}, g_{4}(1)\right) \in U_{4}
$$

and conclude $g_{3}(1) \neq g_{4}(1)$, because $U_{3} \cap U_{4}=\{1\}=(0,0,0)$. Now

$$
\left(1, c_{3}, g_{4}(1)\right)\left(0,0,-g_{4}(1)+g_{3}(1)\right)=\left(1, c_{3}, g_{3}(1)\right),
$$

hence

$$
U_{0} \cap U_{4} U_{3} \neq\{1\},
$$

a contradiction. In particular, without loss of generality we may assume that $c_{3}=1$. For $i=3$ Eq.(19) gives now the main conclusion.

Lemma 7. The semifield is commutative, and

$$
y(x z)=x(y z)=x(z y)=z(x y)=(x y) z=(y x) z .
$$

Hence we have the following.
Theorem 5. The semifield is a field.
We conclude that our AS-configuration is exactly the example $G_{M_{1}}$ given in Example 2. Therefore we have proved the following classification theorem.

Theorem 6. An AS-configuration of symplectic type is classical.

## Acknowledgments

This research was supported in part by the Ministero dell'Istruzione, dell'Università e della Ricerca (project: Disegni Combinatori, Grafi e loro Applicazioni, PRIN 2008), the Università di Roma "La Sapienza" (project: Gruppi, Grafi e Geometrie) and G.N.S.A.G.A. of I.N.D.A.M.

## References

[1] R.W. Ahrens, G. Szekeres, On a combinatorial generalization of 27 lines associated with a cubic surface, J. Aust. Math. Soc. 10 (1969) 485-492.
[2] L. Bader, D. Ghinelli, T. Penttila, On monomial flocks, European J. Combin. 22 (2001) 447-454.
[3] T. Beth, D. Jungnickel, H. Lenz, Design Theory, second ed., Cambridge University Press, Cambridge, 1999.
[4] S. de Winter, K. Thas, Generalized quadrangles admitting a sharply transitive Heisenberg group, Des. Codes Cryptogr. 47 (2008) 237-242.
[5] P. Dembowski, Finite Geometries, Springer-Verlag, Berlin, Heidelberg, New York, 1968.
[6] L.E. Dickson, On finite algebras, Nachr. Akad. Wiss. Göttingen (1905) 358-393.
[7] D. Ghinelli, Regular groups on generalized quadrangles and nonabelian difference sets with multiplier-1, Geom. Dedicata 41 (1992) 165-174.
[8] D. Ghinelli, S. Löwe, Generalized quadrangles with a regular point and association schemes, Linear Algebra Appl. 226-228 (1995) 87-104.
[9] D. Ghinelli, S. Löwe, et al., Generalized quadrangles and pencils of quadrics, in: A. Blokhuis (Ed.), Finite Geometries, in: Dev. Math., vol. 3, Kluwer Academic Publishers, Dordrecht, 2001, pp. 147-158.
[10] D. Ghinelli, U. Ott, Nets and generalized quadrangles, Geom. Dedicata 52 (1994) 1-14.
[11] D. Ghinelli, S.E. Payne, The Ghinelli-Loewe construction of generalized quadrangles, European J. Combin. 24 (2003) 511-516.
[12] D. Gorenstein, Finite Groups, second ed., AMS Chelsea Publishing, 1980, Reprinted 2007 by the AMS.
[13] M. Hall Jr., Affine Generalized Quadrilaterals, in: L. Mirsky (Ed.), Studies in Pure Mathematics, Academic Press, 1971, pp. 113-116.
[14] B. Huppert, Über das Produkt von paarweise vertauschbaren zyklischen Gruppen, Math. Z. 58 (1953) 243-264.
[15] M. Kallaher, Translation planes, in: Handbook of Incidence Geometry, Elsevier Science B.V., Amsterdam, 1994, pp. 137-192.
[16] W.M. Kantor, Generalized quadrangles associated with $G_{2}(q)$, J. Combin. Theory Ser. A 29 (1980) 212-219.
[17] W.M. Kantor, Generalized polygons, SCABs and GABs, in: Buildings and the Geometry of Diagrams, Como, 1984, in: Lecture Notes in Mathematics, vol. 1181, Springer, Berlin, 1986, pp. 79-158.
[18] O.H. Kegel, Zur Struktur mehrfach faktorisierter endlicher Gruppen, Math. Z. 87 (1965) 42-48.
[19] A. Machì, Gruppi. Una Introduzione a idee e Metodi della Teoria dei Gruppi, Spriger-Verlag, Italia, Milano, 2007.
[20] S.E. Payne, Nonisomorphic generalized quadrangles, J. Algebra 18 (1971) 201-212.
[21] S.E. Payne, The equivalence of certain generalized quadrangles, J. Combin. Theory Ser. A 10 (1971) 284-289.
[22] S.E. Payne, Quadrangles of order ( $s-1, s+1$ ), J. Algebra 22 (1972) 97-119.
[23] S.E. Payne, A census of generalized quadrangles, in: W.M. Kantor, et al. (Eds.), Finite Geometries, Buildings and Related Topics, Clarendon Press, Oxford, 1990, pp. 29-36.
[24] S.E. Payne, J.A. Thas, Finite Generalized Quadrangles, Pitman, 1984.
[25] S.E. Payne, J.A. Thas, Finite Generalized Quadrangles, second ed., in: EMS Series of Lectures in Mathematics, European Mathematical Society (EMS), Zürich, 2009.
[26] J.A. Thas, Generalized polygons, in: Handbook of Incidence Geometry, North-Holland, Amsterdam, 1995, pp. 383-431.
[27] J. Tits, Sur la trialité et certains groupes qui s'en deduisent, Publ. Math. Inst. Hautes Études Sci. 2 (1959) 14-60.


[^0]:    E-mail address: dina.ghinelli@uniroma1.it.
    0195-6698/\$ - see front matter © 2012 Elsevier Ltd. All rights reserved.
    doi:10.1016/j.ejc.2012.03.018

