Rendiconti
Accademia Nazionale delle Scienze detta dei XL
*Memorie di Matematica e Applicazioni*
125° (2009), Vol. XXXI, fasc. 1, pagg. 37-74

DINA GHINELLI(*) – DIETER JUNGNICKEL (**)

# Some Geometric Aspects of Finite Abelian Groups

*In celebration of Professor Beniamino Segre's centennial* (***)

ABSTRACT. — Let $\Pi$ be a finite projective plane admitting a large abelian collineation group. It is well known that this situation may be studied by algebraic means (via a representation by suitable types of difference sets), namely using group rings and algebraic number theory and leading to rather strong nonexistence results. What is less well-known is the fact that the abelian group (and sometimes its group ring) can also be used in a much more geometric way; this will be the topic of the present survey. In one direction, abelian collineation groups may be applied for the construction of interesting geometric objects such as unitals, arcs and (hyper-)ovals, (Baer) subplanes, and projective triangles. On the other hand, this approach makes it sometimes possible to provide simple geometric proofs for non-trivial structural restrictions on the given collineation group, avoiding algebraic machinery.

## 1. - INTRODUCTION

A *projective plane* is a geometry consisting of points and lines such that any two lines meet in exactly one point, any two points are on exactly one common line, and there are four points no three of which are collinear. We usually denote the set of points and the set of lines by $P$ and $\mathcal{L}$, respectively. A standard reference for projective planes is Hughes and Piper [66]; for finite geometries in general, see Dembowski [26] and Beth, Jungnickel and Lenz [7].

(*) Indirizzo dell'Autore: Dina Ghinelli, Dipartimento di Matematica, Università di Roma "La Sapienza", Piazzale Aldo Moro, 2, I-00185 Roma, Italy, e-mail: dina@mat.uniroma1.it

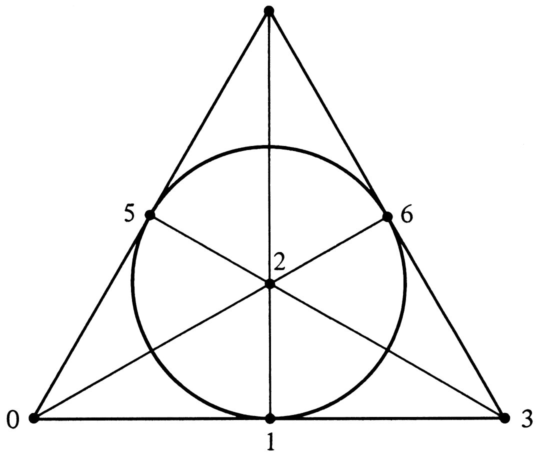
(**) Indirizzo dell'Autore: Dieter Jungnickel, Lehrstuhl für Diskrete Mathematik, Optimierung und Operations Research, Universität Augsburg, D-86135 Augsburg, Germany.

(***) This paper is the extended version of a lecture given by the second author at the conference *Trends in Geometry* (Accademia Nazionale dei Lincei and Università di Roma "La Sapienza", 7-9 June 2004), which was held in memory of Beniamino Segre's (1903-1977) centennial.

A.M.S. Classification: 51E15 - 05B10

In the case of a finite projective plane, it can be shown that the number of points (and also the number of lines) is $n^2 + n + 1$ for some $n \geq 2$ which is called the *order* of the plane. Moreover, each line has $n + 1$ points, and each point is on $n + 1$ lines.

The classical examples are the *Desarguesian planes* $PG(2, q)$ (also called the *classical planes*), where $q$ is a prime power: points and lines are the 1- and 2-dimensional subspaces of the vector space $GF(q)^3$, respectively, and a point is incident with a line if and only if it is a subset of the line. The smallest example is the unique plane of order 2, the so-called *Fano plane*:



Here $P = \mathbb{Z}_7$ and $\mathcal{L} = \{D + x \colon x \in \mathbb{Z}_7\}$, where $D = \{0, 1, 3\}$. One writes $\Pi = \operatorname{dev} D$ for examples of this type.

Projective planes of order $n$ have been constructed for all prime powers $n$, but for no other values of $n$, which motivates the longstanding conjecture that $n$ is necessarily a prime power (*prime power conjecture – PPC*). The nonexistence of a projective plane of order $n$ is known for all $n \equiv 1$ or 2 mod 4 which are not the sum of two squares (Bruck–Ryser theorem [18]), for $n = 10$ (see Lam, Thiel and Swiercz [84]) and for no other values of $n$. Trying to prove the conjecture in general seems hopeless with the present methods of mathematics; thus, it is natural to add extra assumptions. In view of the general philosophy proposed in Felix Klein's *Erlanger Programm*, we will require the existence of a nice collineation group.

Recall that a *collineation* of a projective plane $\Pi$ is a permutation of the point set mapping lines to lines. The set of all collineations of $\Pi$ forms a group Aut $\Pi$ under composition. Any subgroup of Aut $\Pi$ is called a *collineation group* of $\Pi$. Let us mention what is probably the most celebrated result concerning planes with a nice collineation group, namely the seminal Ostrom-Wagner theorem proved in 1959 [90]:

Theorem 1.1 [Ostrom-Wagner theorem]: *Let $\Pi$ be a projective plane of order n admitting a doubly transitive collineation group G. Then $\Pi$ is desarguesian, and $PSL(3, n)$ is a subgroup of G.*

If we weaken the hypothesis of the Ostrom-Wagner theorem somewhat and only require a flag-transitive group, the result should be much the same as before, with two further examples appearing: $G$ may act regularly on flags (and thus be a Frobenius group) for $n \in \{2, 8\}$. Unfortunately – in spite of much effort over several decades – this conjecture still remains open [1].

In the present survey paper, $\Pi$ will be a projective plane of order $n$ admitting a *large* abelian collineation group $G$ in the sense that

$$|G| > \frac{1}{2}(n^2 + n + 1).$$

It is well known that this situation may be studied by algebraic means (via a representation by suitable types of *difference sets*, as in the small example above), namely using group rings and algebraic number theory and leading to rather strong nonexistence results. This is quite technical and has been surveyed by the authors before [47].

What is less well-known is the fact that the abelian group (and sometimes its group ring) can also be used in a much more directly geometric way, which will be the topic of this survey. On one hand, abelian collineation groups may be applied to the construction of interesting geometric objects such as unitals, arcs and (hyper-)ovals, (Baer) subplanes, and projective triangles. On the other hand, this approach makes it sometimes possible to provide simple geometric proofs for non-trivial structural restrictions on the given collineation group, avoiding algebraic machinery. We will provide nice examples for both types of phenomena in this survey. We shall draw freely on our previous survey [47], but present the material from the rather different point of view just outlined, strongly emphasizing the geometric aspects.

## 2. - Preliminaries

We first recall some geometric notions, starting with the most natural subobjects of projective planes, namely subplanes. Let $S$ be a subset of the point set $V$ of a projective plane $\Pi = (V, \mathcal{L})$ with line set $\mathcal{L}$. The lines of $\Pi$ induce a line set on $S$ as follows:

$$\mathcal{L}|_S = \{L \cap S : L \in \mathcal{L}, |L \cap S| \geq 2\}.$$

The incidence structure $\Sigma = (S, \mathcal{L}|_S)$ – and, by abuse of language, also $S$ itself – is said to be a *subplane* if it is itself a projective plane.

In view of the following result of Baer [1] and Bruck [15] a subplane of order $m$ of a projective plane of square order $n = m^2$ is called a *Baer subplane*.

[1] In the case not yet excluded, $G$ would again act regularly on flags, $n$ would be divisible by 8 but not a power of 2, $n^2 + n + 1$ would be a prime $p$ and $\Pi \cong \operatorname{dev} D$, where $D$ consists of the $n$-th powers in $\mathbb{Z}_p^*$. We refer the reader to the excellent survey by Koen Thas [110] for more information and references. We note that the resolution of this case recently claimed in [92] contains a mistake, which unfortunately seems to be beyond repair.

PROPOSITION 2.1: *Let $\Sigma$ be a subplane of order $m$ of a projective plane $\Pi$ of order $n$, where $m < n$. Then $n = m^2$ or $n \geq m^2 + m$. Moreover, $n = m^2$ if and only if each point of $\Pi \setminus \Sigma$ is on a unique line of $\Sigma$ and dually.*

It should be noted that $n$ is a power of $m$ in all known examples of subplanes. For a concrete example, consider the projective plane $PG(2,q)$ over the Galois field $GF(q)$, where $q$ is a proper prime power; then the points and lines with homogeneous coordinates in a prescribed subfield of $GF(q)$ form a subplane. In particular, $GF(q)$ induces a Baer subplane $PG(2,q)$ of $PG(2,q^2)$.

Let $\Pi$ be a projective plane. A subset $A$ of $\Pi$ is called an *arc* if

$$|A \cap L| \leq 2 \quad \text{for each line } L.$$

Sharpening previous results by Bose [13] and Seiden [103], Qvist proved in [98] the following bounds.

LEMMA 2.2: *Let $A$ be an arc in a projective plane of order $n$. Then*

$$|A| \leq \begin{cases} n+2 & \text{for } n \text{ even} \\ n+1 & \text{for } n \text{ odd.} \end{cases}$$

The $(n+1)$-arcs are usually called *ovals*, whereas the $(n+2)$-arcs are called *hyperovals*. We refer the reader to Hirschfeld [58] for background.

The study of ovals and hyperovals in (not necessarily Desarguesian) projective planes has for many years been a topic of considerable interest in finite geometry. For the Desarguesian case, only even orders $q$ need to be considered, as any oval in $PG(2,q)$, $q$ odd, actually is a conic, by the following famous theorem of Segre [100]: □

THEOREM 2.3: *The only ovals in $PG(2,q)$, $q$ odd, are the conics.*

Theorem 2.3 is one of the most celebrated theorems of this great mathematician in finite geometry – an area where his pioneering work is still inspiring a lot of research. We like to mention here, in this paper written for Segre's centennial, at least the third volume of his selected papers [101] were the interested reader can find the full list of his papers, books and lecture notes which, being mainly in Italian, probably are not as well known to the general public as they ought to be.

In the case of even orders, any oval $O$ can be completed to an hyperoval: we may adjoin its *nucleus*, that is, the common point of intersection of all the tangents of $O$. The classification of hyperovals in $PG(2,q)$, $q$ even, is a famous (and very difficult) open problem; we refer the reader to the survey by Cherowitzo [22]. For the non-Desarguesian case, let us just mention a few references, namely the classification of hyperovals in the translation planes of order 16 [21] and the existence of ovals or hyperovals in the Figueroa planes [20, 31] , the Hughes planes [99], in commutative semifield planes [40, 68], and in the Coulter-Matthews planes [30].

Let $\Pi$ be a projective plane of order $q$. A *$(k, n)$-arc $A$* in $\Pi$ is a non-empty proper subset of $k$ points in $\Pi$ such that some line of $\Pi$ meets $A$ in $n$ points, but no line meets $A$ in more than $n$ points. Clearly $(k, 2)$-arcs are the arcs defined above. A $(k, n)$-arc in a projective plane of order $q$ satisfies $k \leq 1 + (q + 1)(n - 1) = qn - q + n$ with equality if and only if every line intersects the arc in 0 or $n$ points; see Barlotti [4]. Arcs realizing the upper bound are called *maximal arcs*; the parameter $n$ is usually called the *degree* of the maximal arc. Equality in the bounds implies that $n$ divides $q$ or $n = q + 1$. If $1 < n < q$, then the maximal arc is said to be *non-trivial.* The known examples of non-trivial maximal arcs in $PG(2, q)$ for $n = 2$ are the hyperovals; for $n > 2$, and $q$ even, Denniston [29] constructed in 1969 maximal arcs in $PG(2, q)$, for every divisor of $q$, starting from a pencil of conics. Apart from an infinite family constructed by Thas [107, 109], these were the only known examples until 2002, when Mathon [88], generalizing Denniston's construction, gave several classes of new examples, again only for $q$ even. Further examples as well as results on the geometric structure and collineation stabilizers were also given in [54] and [55]. In the recent paper [56] this construction method is used to give maximal arcs that are not of Denniston type for all $n$ dividing $q$, $4 < n < q/2$, $q$ even.

For odd $q$, it was conjectured in 1975 ([108]) that maximal arcs do not exist. In [108] this was proved for $(n, q) = (3, 3^h)$. The special case $(3, 9)$ was settled earlier by Cossu [24]. Only in 1997, Ball, Blokhuis and Mazzocca [2] could prove this long-standing conjecture; however, the methods used were difficult to follow and the arguments quite long. Subsequently, a considerably simpler and shorter proof was given by Ball and Blokhuis [3]; this uses only elementary properties of polynomials and is one of the most striking examples of the power of the "polynomial method" in Galois geometry. See, for instance, [58] for more background on maximal arcs. For later use, we include the following well-known result.

PROPOSITION 2.4: *Let $A$ be a maximal arc of degree $n$ in a projective plane $\Pi$ of even order $q$. Then the exterior lines to $A$ (that is, the lines disjoint to $A$) form a maximal arc of degree $q/n$ in the dual plane $\Pi^*$.*

Another interesting geometric application which we shall mention concerns projective triangles. We recall that a *projective triangle of side $k$* in a plane of order $n$ is a set $B$ of $3(k - 1)$ points with the following properties:

- $B$ contains a distinguished triangle $oxy$.
- On each side of $oxy$, there are exactly $k$ points of $B$.
- If the points $q \in ox$ and $r \in oy$ belong to $B$, then $qr \cap xy$ also belongs to $B$.

We will be interested in projective triangles forming small blocking sets. Recall that a *blocking set* is a set of points meeting every line but not containing any line; a blocking set is called *minimal* if no proper subset is again a blocking set. Blocking sets have been extensively studied; see Hirschfeld [58, Chapter 13] or Blokhuis [8] for background.

Next, we define some classes of combinatorial designs which will appear in this survey; see [7] for more background. A $(v, k, \lambda)$*-design* is an incidence structure $\mathcal{D}$ with $v$ points, such that each block contains $k$ points, and any two distinct points are in exactly $\lambda$ blocks. In case $\lambda = 1$, one also speaks of a *Steiner system*; then the notation $S(2, k, v)$ is rather common.

Following Gronau and Mullin [51], a design is said to be *super-simple* if any two distinct blocks intersect in at most two points. If it is possible to partition the block set of a design into *parallel classes* (that is, the blocks in each parallel class partition the point set), the design is called *resolvable*.

By *Fisher's inequality* [35], a design with $k > \lambda$ has at least as many blocks as points; in the case of equality, one speaks of a *symmetric design*. The symmetric designs with $\lambda = 1$ are exactly the projective planes; thus their parameters take the form $(n^2 + n + 1, n + 1, 1)$.

A *partially symmetric design* (as introduced by Hughes [65]) is an incidence structure $\mathcal{D}$ with as many points as blocks such that each block contains $k$ points and any two distinct points are in either $\lambda_1$ or $\lambda_2$ blocks; compared to symmetric designs, one allows two different joining numbers. Partially symmetric designs for which one of these two numbers equals 0 are especially interesting. In particular, one speaks of a *divisible semisymmetric design* if there is a partition of the point set into $m$ *point classes* of equal size $c$ such that two distinct points in the same class are not joined, whereas points in distinct point classes are joined by exactly $\lambda$ blocks; and dually. Briefly, such a design is referred to as a divisible $(m, c, k, \lambda)$-SSD. For $c = 1$, this notion reduces to symmetric designs, and for $\lambda = 1$ to *divisible semiplanes* (also called *elliptic semiplanes*).

Finally, we turn our attention to an important method used to describe geometries with a regular group. For the time being, we shall just consider the prototypical case. A $(v, k, \lambda)$*-difference set* (for short a $(v, k, \lambda)$-DS) in a group $G$ of order $v$ is a $k$-subset $D$ of $G$ such that every element $g \neq 0$ of $G$ has exactly $\lambda$ representations $g = d_1 - d_2$ with $d_1, d_2$ in $D$, $d_1 \neq d_2$. The parameter $n = k - \lambda$ is called the *order* of the difference set. This definition also applies if $G$ is written multiplicatively. A difference set $D$ is called *cyclic*, *abelian* etc. if $G$ has the respective property.

For example, the set $D = \{0, 1, 3\}$ in $G = \mathbb{Z}_7$ – already considered in the previous section – is a $(7, 3, 1)$-DS. If $D \neq \emptyset$ is any subset of a finite group $G$, then the incidence structure

$$\operatorname{dev} D \;=\; (G, \boldsymbol{B}, \in) \qquad \text{with} \quad \boldsymbol{B} \;=\; \{D + g \colon g \in G\}$$

is called the *development* of $D$. Obviously $\operatorname{dev} D = \operatorname{dev}(D + a)$ for all $a \in G$.

The development of a $(v, k, \lambda)$-DS in a group $G$ is a symmetric $(v, k, \lambda)$-design admitting $G$ as a regular (i.e. sharply 1-transitive) automorphism group. Conversely, every symmetric $(v, k, \lambda)$-design with a regular automorphism group may be represented in this way. The reader is referred to [7] and [67] for further details.

Difference sets were introduced by Singer [104]; their systematic study, however, only started with the fundamental papers of Hall [53] who considered cyclic difference sets with $\lambda = 1$ and introduced the important concept of multipliers and Bruck [15] who started the investigation of difference sets in general groups. The study of difference sets has developed into a beautiful and quite advanced theory by now; a comprehensive introduction to this area can be found in Chapter VI of Beth, Jungnickel and Lenz [7].

There are several generalizations of the concept of a difference set which allow us also to describe projective planes with other types of abelian groups (not acting regularly): relative difference sets, direct product difference sets, and neo-difference sets. We shall explain these notions later, as they will become necessary.

One of the most important tools in investigating difference sets and their generalizations is the use of the *integral group ring* $\mathbb{Z}G$ of $G$. One advantage of this approach is that subsets and even lists (or submultisets of $G$) can be represented just as elements of the group ring; more important is the fact that it allows one to use algebraic techniques to prove nonexistence results. Indeed, the amazing strength of the approach using various types of difference sets and the machinery of integral group rings was the recurrent theme stressed in our previous survey [47]. But even in the present context, where we emphasize geometric over algebraic aspects, group rings will occasionally be handy.

In order to work with group rings, we have to write $G$ multiplicatively. Then

$$\mathbb{Z}G = \left\{ \sum_{g\in G} a_g g : a_g \in \mathbb{Z} \right\}$$

is the free $\mathbb{Z}$-module with $G$ as basis, equipped with the multiplication

$$\left(\sum_{g\in G} a_g g\right) \cdot \left(\sum_{h\in G} b_h h\right) = \sum_{g,h\in G} a_g b_h gh.$$

We will use the following conventions. For $X = \sum a_g g \in \mathbb{Z}G$, we write $|X| = \sum a_g$ and $[X]_g = a_g$ (the coefficient of $g$ in $X$). For $r \in \mathbb{Z}$ we write $r$ for the group ring element $r1$, and for $S \subseteq G$ we write, by abuse of notation, $S$ instead of $\sum\limits_{g\in S} g$. If $\alpha\colon G \to H$ is any mapping of $G$ into a group $H$, we extend $\alpha$ to a linear mapping from the group ring $\mathbb{Z}G$ into the group ring $\mathbb{Z}H$:

$$X^\alpha = \sum a_g g^\alpha \qquad \text{for} \quad X = \sum a_g g.$$

In the special case $G = H$ and $\alpha\colon g \mapsto g^t$ for some $t \in \mathbb{Z}$, we write $X^{(t)}$ instead of $X^\alpha$, so that $X^{(t)} = \sum a_g g^t$. In particular, $S^{(-1)} = \sum\limits_{g\in S} g^{-1}$. Using these conventions, we immediately obtain the following simple but fundamental lemma.

Lemma 2.5: *Let $G$ be a multiplicative group of order $v$, and let $D$ be a $k$-subset of $G$. Then $D$ is a $(v, k, \lambda)$-difference set of order $n = k - \lambda$ if and only if the following equation holds in $\mathbb{Z}G$:*

$$DD^{(-1)} = n + \lambda G. \tag{2.1}$$

We shall also need another trivial observation, which shows how to compute intersection sizes using the group ring $\mathbb{Z}G$.

LEMMA 2.6: *Let A and B be subsets of a finite group G. Then*

$$|A \cap Bg| \; = \; [B^{(-1)}A]_g.$$

## 3. - THE SEMINAL CASE: SINGER GROUPS

A difference set for a projective plane of order $n$ – that is, an $(n^2+n+1, n+1, 1)$-DS – is called a *planar difference set* of order $n$. As explained in the preceding section, the projective planes admitting a regular collineation group are equivalent to planar difference sets. In view of the following seminal result proved by Singer [104] in 1938, the regular group is usually called a *Singer group*.

THEOREM 3.1 [Singer's theorem]: *The classical projective plane $PG(2,q)$ admits a cyclic regular collineation group; hence it may be represented by a cyclic planar difference set of order $q$.*

One of the central conjectures in finite geometry asserts that the converse of Singer's theorem also holds: a finite projective plane with a Singer group is necessarily classical (at least in the cyclic case). In 1960, Bruck [16] proved that all cyclic planes of order $n$ or $n^2$ with $n \leq 9$ are indeed desarguesian. The best general result towards the converse of Singer's theorem is as follows [91, 60]:

THEOREM 3.2 [Ott-Ho theorem]: *A finite projective plane $\Pi$ is desarguesian if and only if it admits two distinct abelian Singer groups $G_1 \neq G_2$. In other words, if there exists a Singer group which is not normal in the full collineation group* $\mathrm{Aut}\,\Pi$*, then $\Pi$ is desarguesian.*

The representation of a projective plane with a Singer group by a planar difference set $D$ exhibits a regular group of automorphisms; but, of course, the plane may have more automorphisms besides. For instance, the full automorphism group of a desarguesian projective plane is transitive on quadrangles; in particular, it is 2-transitive on the set of points. It is often possible to find some of these other automorphisms in terms of the difference set representation using the notion of multipliers. In the abelian case, a *multiplier* of $D$ can be defined as an automorphism $\alpha$ of the Singer group $G$ which induces an automorphism of $\Delta = \mathrm{dev}\, D$. If $G$ is cyclic, then every multiplier is a *numerical multiplier*, i.e., it is of the form $\alpha : x \mapsto tx$ for some integer $t$ coprime to $|G|$; then the condition for $t$ to be a multiplier is $tD = D + g$ for some $g \in G$. For example, $t = 2$ is a multiplier for the Fano difference set: $2 \cdot \{0,1,3\} = \{0,2,6\} = \{0,1,3\} + 6$.

The importance of the concept of multipliers lies in the fact that very often just the parameters of a hypothetical abelian difference set $D$ force the existence of numerical multipliers, which then may be used to help with either the construction of $D$ or a nonexistence proof. These fundamental ideas are due to Hall [53] who considered them in the special case of cyclic planar difference sets; his result (and proof) admits a rather straightforward generalization to symmetric designs due to Chowla and Ryser [23]. We only state the planar case; a simple proof can be found in our previous survey [47].

Theorem 3.3 [Multiplier theorem]: *Let $D$ be an abelian planar difference set of order $n$. Then every divisor of $n$ is a multiplier of $D$.*

Actually, one may assume $D$ to be fixed by all its multipliers $t$, so that always $tD = D$. The following major result on planar abelian difference sets with an *involutory multiplier* (that is, with a multiplier of order 2) is due to Blokhuis, Brouwer and Wilbrink [9]. We shall include its proof, as it provides a striking example of a situation where a simple geometric proof may be given for a non-trivial structural restriction, avoiding algebraic machinery.

Theorem 3.4: *Let $D$ be a planar difference set in an abelian group $G$. If $D$ admits a multiplier $t$ of order 2, then $n$ is a perfect square, say $n = m^2$, and necessarily $t = m^3$.*

Proof: Define subgroups $A$ and $B$ of $G$ as follows:

$$A = \{g \in G\colon\ tg = -g\} \qquad \text{and} \quad B = \{g \in G\colon\ tg = g\}.$$

Then the mappings $\alpha$ and $\beta$ defined by $g^{\alpha} = (g - tg)/2$ and $g^{\beta} = (g + tg)/2$ are homomorphisms from $G$ to $A$ and $B$, respectively, and $A \cap B = \{0\}$ and $g = g^{\alpha} + g^{\beta}$ for each $g \in G$; thus $G = A \oplus B$. By assumption, $t$ induces an involutory collineation $\tau$ of the projective plane $\Pi = \operatorname{dev} D$. Thus $\tau$ is either an elation (with $n + 1$ fixed points), a homology (with $n + 2$ fixed points), or a Baer involution (with $m^2 + m + 1$ fixed points, where $n = m^2$); see Hughes and Piper [66]. Since the order of $B$ divides that of $G$, the last case must occur, and $B$ is the point set of a Baer subplane $\Pi_0$ of $\Pi$. Thus $n = m^2$ is a square, $B$ has order $m^2 + m + 1$, and $A$ has order $m^2 - m + 1$. As $\gcd(m^2 - m + 1, m^2 + m + 1) = 1$, $G$ has unique subgroups of these two orders; therefore any multiplier of order 2 leads to the same representation $G = A \oplus B$ and acts on $A$ and $B$ in the same way as $t$ does. The result now follows, since $D$ admits the multiplier $m$ and hence also the multiplier $m^3$ of order 2, by Theorem 3.3. □

Theorem 3.4 allows some nice geometric applications to sub-objects of the plane $\Pi = \operatorname{dev} D$ associated with a planar difference set $D$ of order $n = m^2$ in an abelian group $G$. A first application is contained in the proof of Theorem 3.4, where we noted that $\Pi$ contains a Baer subplane $B$. Using the notation in that proof, the cosets of $B$ also yield

Baer subplanes. Thus one can say a lot more, as observed by Bruck [16] for the cyclic case and by the second author [72] in general:

Corollary 3.5: *$\Pi$ admits a partition into Baer subplanes which is invariant under the Singer group $G$.*

In a similar manner, the subgroup $A$ appearing in the proof of Theorem 3.4. also has an interesting geometric meaning: it constitutes an arc in $\Pi$. More precisely, we have the following result:

Corollary 3.6: *$\Pi$ admits a partition into arcs of size $m^2 - m + 1$, which are complete (that is, none of them is contained in any arc of larger size) for $m \neq 2$.*

Proof: We have to show that any line $D + x$ intersects $A$ at most twice. Assume that $a$ is some point of intersection, say $a = d + x$; then $t(d + x) = -d - x$ by the definition of $A$. If $b = d' + x$ is a second point of intersection, we also have $t(d' + x) = -d' - x$. These two equations yield $d' - d = td - td'$ and hence $d' = td$, since $D$ is a difference set with $\lambda = 1$. This shows that $b$ is uniquely determined by $a$, establishing that $A$ is indeed an arc. Then the translates $A + b$, where $b \in B$, partition the point set of $\Pi$ into arcs. Using counting arguments, one can show that these arcs are complete whenever $m \geq 4$; the case $m = 3$ allows the same conclusion, but needs special arguments. □

Corollary 3.6 is due to Blokhuis, Brouwer and Wilbrink [9]; the cyclic case was obtained earlier by Fisher, Hirschfeld and Thas [34] and Boros and Szönyi [11] who only considered the special case $\Pi = PG(2, q^2)$. In this case, the arcs in question had been constructed previously using different methods by Kestenband [81] who, however, did not note their completeness. This completeness is of particular interest, since it shows that a bound of Segre on the size of a complete arc in $PG(2, q^2)$ for $q$ even is best possible; see Hirschfeld [58, Theorem 10.3.3]. We also remark that, more generally, Storme and Van Maldeghem [105], Szönyi [106] and Ho [59] studied the question under which conditions the orbit of a subgroup of a Singer group is an arc.

We now come to a third interesting application of the proof of Theorem 3.4. For this, recall that a polarity of a projective plane of order $m^2$ with exactly $m^3 + 1$ absolute points is called a *unitary polarity*.

Corollary 3.7: *$\Pi$ admits a unitary polarity.*

Proof: We use the notation introduced in the proof of Theorem 3.4. As noted before, we may assume that $D$ is fixed under the multiplier $t = m^3$. It is easily checked that the correspondence

$$\pi \colon g \leftrightarrow D - tg \tag{3.1}$$

defines a polarity $\pi$ of $\Pi$. Clearly $g$ is an absolute point of $\pi$ if and only if $2g^{\beta} = g + tg \in D$. Since $A$ is the kernel of $\beta$, the set $U$ of absolute points of $\pi$ is given by $U = \{a + b : a \in A, 2b \in D \cap B\}$, and therefore $\pi$ has exactly $(m^2 - m + 1)(m + 1) = = m^3 + 1$ absolute points. □

By a theorem of Seib [102], any unitary polarity of $\Pi$ induces a *unital* $\mathcal{U}$, that is, a resolvable Steiner system $S(2, m + 1, m^3 + 1)$. The point set of $\mathcal{U}$ is the set $U$ of the $m^3 + 1$ absolute points of $\pi$, and the lines are the intersections $U \cap L$, where $L$ is a non-absolute line of $\pi$; all such intersections have cardinality $m + 1$. Moreover, the $m^2$ non-absolute points on an arbitrary absolute line determine a resolution of the line set of $\mathcal{U}$ into parallel classes; see [7, Theorem VIII.5.26] for details. A brief historical survey on unitals, including a listing of important papers with short abstracts, may be found in the appendix of the thesis by Barwick [6].

Corollary 3.7 implies that $\Pi$ contains unitals – a result due to Bose [14] for $\Pi = PG(2, q^2)$, see also Ghinelli [42], and to Blokhuis, Brouwer and Wilbrink [9] in general – and its proof gives an explicit description of the point set $U$ of the unital $\mathcal{U}$ associated with the polarity (3.1). Using Corollary 3.6, this proof shows even more: $U$ can be partitioned into arcs of $\Pi$, namely the translates $A + b$ with $2b \in D \cap B$. On the other hand, using translates of $U$, one also sees that each of the complete arcs in Corollary 3.6. is the intersection of two unitals contained in $\Pi$.

Finally, Blokhuis, Brouwer and Wilbrink [9] used their difference set approach to prove the following beautiful characterization of the classical *Hermitian unitals*, that is, unitals induced by a unitary polarity which can be described by a Hermitian matrix. The proof is considerably more involved than the ones for the preceding corollaries; it exploits the fact that the $\mathbb{Z}_p$-code spanned by the lines of $\Pi$ is nothing but the ideal generated by the difference set $D$ in the group algebra $\mathbb{Z}_p G$.

THEOREM 3.8: *Let $\mathcal{U}$ be a unital embedded in $\Pi = PG(2, q^2)$, where $q = p^r$. Then $\mathcal{U}$ is Hermitian if and only if it is contained in the $\mathbb{Z}_p$-code spanned by the lines of $\Pi$.*

We have now seen that the structural restriction on planes with an abelian Singer group obtained in Theorem 3.4. by geometric means leads to a (probably unexpected) wealth of geometric applications, uniting and generalizing results on the classical planes which were originally obtained by completely different methods. On the other hand, Theorem 3.4. also yields important further structural restrictions, as we shall explain now.

First of all, it implies that the search for a possible counterexample to the PPC for planes with an abelian Singer group can be restricted to non-square orders. To see this, we once more return to the proof of Theorem 3.4. Obviously, $B$ is a Singer group for the Baer subplane $\Pi_0$; actually one may even assume that $\Pi_0$ is represented by the planar difference set $D \cap B$. This establishes the following result due to Ostrom [89] in the cyclic case and to Jungnickel and Vedder [78] in general.

Corollary 3.9: *Assume the existence of a planar abelian difference set of order $n = m^2$ in G. Then there also exists a planar difference set of order m in a subgroup H of G associated with a Baer subplane of* dev *D.*

A second application of Theorem 3.4. was first noted in [47]: one immediately obtains the planar version of the so called Mann test for abelian difference sets due to Mann [87]. The usual proofs first establish the Mann test for difference sets in general and use non-trivial algebraic arguments: either the group ring approach is combined with ideas from algebraic coding theory [85, 94], or a purely computational proof within the group algebra is given [77]. The subsequent specialization to the planar case then also requires some algebraic number theory; see [7, § VI.6]. In contrast, the geometric approach here is considerably simpler and much more elegant.

Theorem 3.10 [Mann test]: *Let D be a planar abelian difference set of order n in G. Then either n is a square or every multiplier of D has odd order modulo the exponent u of G.*

Proof: Let $s$ be a multiplier which has even order modulo $u$, say $2h$. Then $t = s^h$ is a multiplier of order 2, and the general assertion is an immediate consequence of Theorem 3.4. □

The Mann test yields some powerful existence criteria for non-square orders $n$. The following consequence of Theorem 3.10. was proved in [78]; its proof just needs a few standard facts from elementary number theory; see [7, Theorem VI.7.8] for details.

Corollary 3.11: *Let p and q be prime divisors of n and of $v = n^2 + n + 1$, respectively. Then each of the following conditions implies that n is a square:*

- *D has a multiplier which has even order modulo q;*
- *p is a quadratic non-residue modulo q;*
- $n \equiv 4$ *or* $6 \pmod 8$*;*
- $n \equiv 1$ *or* $2 \pmod 8$ *and* $p \equiv 3 \pmod 4$*;*
- $n \equiv m$ *or* $m^2 \pmod{m^2 + m + 1}$ *and p has even order* $(\bmod\, m^2 + m + 1)$.

We conclude this section with some results concerning the application of abelian planar difference sets to the construction of ovals, hyperovals, and maximal arcs. Here the seminal result is the observation by Bruck [17] that $-D$ is an oval whenever $D$ is a cyclic planar difference set. The following more general result is due to Jungnickel and Vedder [78].

Theorem 3.12: *Let D be a planar difference set in an abelian group G. Then the sets $A_g = -D + g$ with $g \in G$ are ovals in the plane $\Pi =$* dev *D, and the lines $D - 2d + g$ with $d \in D$ are tangents to $A_g$ (with $-d + g$ as the tangency point).*

Proof: We first show that any line $D+x$ intersects $A_g$ at most twice. Assume that $a$ is some point of intersection, say

$$a = d + x = -d' + g, \quad \text{hence} \quad d + d' = g - x,$$

with $d, d' \in D$. If $b$ is a second point of intersection, we similarly obtain

$$b = e + x = -e' + g, \quad \text{hence} \quad e + e' = g - x,$$

with $e, e' \in D$. From these two equations, $d - e = e' - d'$ follows, therefore $d = e'$ and $d' = e$, since $D$ is a difference set with $\lambda = 1$. This shows that $b$ is uniquely determined by $a$, proving that $D + x$ intersects $A_g$ at most twice. So, $A_g$ is an arc (and, hence, an oval) in the plane $\Pi = \operatorname{dev} D$. Since we may always rewrite $d + x = -d' + g$ as $d' + x = -d + g$, it is obvious that the line $D + x$ intersects $A_g$ in two points unless $d = d'$. Thus $D + x$ is the (unique) line in $\Pi$ tangent to $A_g$ at the point $-d + g$ if and only if $d = d'$, hence $x = -2d + g$. □

Theorem 3.12. has two interesting consequences also obtained in [78].

Corollary 3.13: *The sets $A_g = -D + g$ with $g \in G$ are $q^2 + q + 1$ ovals which pairwise intersect in a unique point; thus they form the lines of another projective plane (which is isomorphic to $\Pi$) on the point set $G$.*

Corollary 3.14: *Let $n$ be even. Then the sets $(-D + g) \cup \{g\}$ are hyperovals of $D$.*

Proof: We may assume $2D = D$. Then the tangents to $-D + g$ are the lines $D - d + g$ with $d \in D$, which obviously intersect in the point $g$. □

Remark 3.15: By Segre's theorem 2.3, the ovals above are conics for $\Pi = PG(2, q)$ provided that $q$ odd. As noted by Peter Cameron (see [78]), the oval $-D$ is actually the conic with the equation $xz - y^2 + z^2 = 0$ (in suitably chosen homogeneous coordinates), and this also holds for even orders $q$.

The ovals and hyperovals associated with planar difference sets give rise to some reasonably interesting classes of designs; the following three constructions come from [30] and [78]. The first of these results is immediate from Corollary 3.13:

Proposition 3.16: *Let $\Pi$ be a projective plane associated with a planar difference set $D$ of order $q$ in an abelian group $G$. Then the lines $D + g$ and the ovals $-D + g$ together yield a super-simple design with parameters*

$$v = q^2 + q + 1, \ k = q + 1 \ \textit{and} \ \lambda = 2.$$

Proposition 3.17: *Let $D$ be a planar difference set of even order $q$ in an abelian group $G$, and assume, without loss of generality, $2D = D$. Then the hyperovals $(-D + g) \cup \{g\}$ form* *a partially symmetric design with parameters*

$$v = q^2 + q + 1,\ k = q + 2,\ \lambda_1 = 1 \textit{ and } \lambda_2 = 2$$

*admitting G as a regular automorphism group.*

Proof: We use the group ring to prove the desired result; thus we switch to multiplicative notation for $G$, so that the hypothesis $2D = D$ turns into $D^{(2)} = D$. (Note that this hypothesis is justified in view of Theorem 3.3. and the subsequent remarks.) Then the assertion follows from a short computation (using Lemma 2.5.) involving the group ring element $H = 1 + D^{(-1)}$ (which corresponds to the initial hyperoval $-D \cup \{0\}$ in the additive setting):

$$HH^{(-1)} \ = \ (1 + D^{(-1)})(1 + D) \ = \ (q + 1) + G + (D + D^{(-1)}).$$

Now note that $1 \notin D$ which, together with $D^{(2)} = D$, implies that $D$ and $D^{(-1)}$ are disjoint subsets of $G$. □

For the third example, it is simpler to actually state (not only to check) the construction in terms of group rings; we shall omit the proof.

Proposition 3.18: *Let D be a planar difference set of even order q in an abelian group G (written multiplicatively), and assume, without loss of generality, $D^{(2)} = D$. Then the element $S = \frac{1}{2}(D^2 - D) \in \mathbb{Z}G$ gives rise to a partially symmetric design with parameters*

$$v = q^2 + q + 1,\ k = \frac{q(q+1)}{2},\ \lambda_1 = \frac{q^2}{4} \textit{ and } \lambda_2 = \frac{q(q+1)}{4}$$

*admitting G as a regular automorphism group.*

As a fourth application to designs, we mention the following result from [32]; the proof is a little more difficult and will be omitted; we just note that it also involves an argument using the ovals associated with the difference set in question.

Theorem 3.19: *Assume the existence of a planar difference set S of order n in an abelian group G, where $n \equiv 1 \bmod 3$. Then there exists a partially symmetric design with parameters*

$$v = (n^2 + n + 1)/3,\ k = n - 1,\ \lambda_1 = 1 \textit{ and } \lambda_2 = 3$$

*admitting G as a regular automorphism group.*

Next we present a new construction which is inspired by a similar result obtained in [30] (see Theorem 6.5). By Proposition 2.4, the exterior lines to a hyperoval $H$ in a projective plane $\Pi$ of even order $q$ form a maximal arc of degree $q/2$ in the dual plane $\Pi^*$. It is well-known that planes with an abelian Singer group are self-dual; hence, the existence of hyperovals in $\Pi$ for even orders $q$ also implies that of maximal arcs of degree $q/2$ in $\Pi$. The following result gives an explicit description of such a maximal arc in terms of the underlying planar difference set $D$ (using group ring notation).

THEOREM 3.20: *Let $\Pi$ be a projective plane of even order $q = 2^b$ admitting an abelian Singer group $G$, and let $D$ be an associated planar difference set. Write $G$ multiplicatively and assume, without loss of generality, that $D$ is fixed by the multiplier 2. Then the element $M \in \mathbb{Z}G$ defined by*

$$M \;=\; G - \frac{1}{2}(D^2 + D) \tag{3.2}$$

*is a maximal arc of degree $2^{b-1}$ in $\Pi$.*

PROOF: We first check that $M$ indeed defines a subset of $G$, that is, that $M$ has coefficients 0 and 1 only. For $d, e \in D$ with $d \neq e$, the element $g = de = ed \in G$ appears with coefficient 1 in $\frac{1}{2}(D^2 + D)$, as $de = d'e'$ implies $d(d')^{-1} = e'e^{-1}$, and thus $e' = d$ and $d' = e$ because of $\lambda = 1$. For $d \in D$, the elements $d^2$ appearing in $D^2$ form a permutation of the elements of $D$, as $D^{(2)} = D$ by hypothesis; hence the elements of $D$ also appear with coefficient 1 in $\frac{1}{2}(D^2 + D)$.

It remains to verify that $M$ is a maximal arc; thus we have to show that each line of $\Pi$ either is an exterior line or meets $M$ in exactly $2^{b-1} = q/2$ points. We can apply Lemma 2.6. to compute the intersection sizes with lines, using Lemma 2.5. and the obvious fact $GD^{(-1)} = GD = (q+1)G$:

$$MD^{(-1)} \;=\; GD^{(-1)} - \frac{1}{2}(q + G)(D + 1) \;=\; \frac{q}{2}(G - D - 1).$$

Thus the exterior lines to $M$ are precisely the lines $Dg$ with $g \in D \cup \{1\}$, whereas all other lines of $\Pi$ intersect $M$ in $q/2$ points. □

Finally, we mention a result due to Pott [95] which solves a conjecture of Assmus and Key concerning the code generated by the hyperovals of $\mathrm{PG}(2, q)$. Its proof makes essential use of the fact that the code $C$ may be viewed as the ideal generated by the associated difference set $D$ in the group algebra $\mathbb{Z}_2G$ and that $-D$ yields a hyperoval, as above. In addition, it needs some arguments involving characters.

THEOREM 3.21: *Let $\Pi$ be a projective plane of even order with an abelian Singer group $G$. Then the hyperovals in $\Pi$ generate the dual of the $\mathbb{Z}_2$-code $C$ determined by the lines of $\Pi$.*

## 4. - THE DEMBOWSKI-PIPER CLASSIFICATION

Let $\Pi$ be a projective plane of order $n$ with a *quasiregular* collineation group $G$, that is, a group inducing a regular action on each orbit: each group element fixes either none or all elements in the orbit. Clearly, this condition is satisfied in our case, where $G$ is assumed to be abelian: it is easy to prove that all permutation representations of a group $G$ are quasiregular if and only if every subgroup of $G$ is normal. If a quasiregular group $G$ is *large* in the sense that

$$|G| > \frac{1}{2}(n^2 + n + 1),$$

then there are unique faithful point and/or line orbits; see [26], p.181. Let us also recall that the number of point orbits of a collineation group agrees with the number of line orbits by the *orbit theorem*; see [66, Theorem 13.4]. Dembowski and Piper classified planes of this type into the following eight cases.

THEOREM 4.1 [Dembowski-Piper theorem]: *Let $G$ be a collineation group acting quasiregularly on the points and lines of a projective plane of order $n$, and assume $|G| > \frac{1}{2}(n^2 + n + 1)$. Let $t$ denote the number of point orbits, and let $F$ be the incidence structure consisting of the fixed points and fixed lines. Then one of the following holds.*

(a) $|G| = n^2 + n + 1,\ t = 1,\ F = \emptyset$. *Here $G$ is transitive.*
(b) $|G| = n^2,\ t = 3$, *$F$ is a flag, that is, an incident point-line pair $(\infty, L_\infty)$.*
(c) $|G| = n^2,\ t = n + 2$, *$F$ is either a line and all its points or, dually, a point together with all its lines.*
(d) $|G| = n^2 - 1,\ t = 3$, *$F$ is an antiflag, that is, a non-incident point line pair $(\infty, L_\infty)$.*
(e) $|G| = n^2 - \sqrt{n},\ t = 2,\ F = \emptyset$. *In this case one of the point orbits is precisely the set of points of a Baer subplane $\Pi_0$ of $\Pi$.*
(f) $|G| = n^2 - n,\ t = 5$, *$F$ consists of two points, the line joining them, and another line through one of the two points.*
(g) $|G| = n^2 - 2n + 1,\ t = 7$, *$F$ consists of the vertices and sides of a triangle.*
(h) $|G| = (n^2 - \sqrt{n} + 1)^2,\ t = 2\sqrt{n} + 1,\ F = \emptyset$. *In this case there are $t - 1$ disjoint subplanes of order $\sqrt{n} - 1$ whose point sets constitute $t - 1$ orbits, each of length $n - \sqrt{n} + 1$.*

Case (c) – translation planes and dual translation planes – is atypical and of no interest in the present context. In our previous survey [47] we presented most known results concerning the remaining cases (a), (b), and (d)–(h), concentrating on the status of the PPC for planes of these types. In all these cases, one has – as for the case (a) of Singer groups – a sort of difference set associated with the plane. We now recall the relevant definitions.

A $k$-subset $D$ of an additively written group $G$ of order $v = mc$ is called a *relative difference set* with parameters $(m, c, k, \lambda)$ (for short, an $(m, c, k, \lambda)$-RDS ) provided that the list of differences $(d - d' \colon d, d' \in D, d \neq d')$ covers every element in $G \setminus N$ exactly $\lambda$ times, and the elements in $N \setminus \{0\}$ not at all; here $N$ is a specified subgroup of $G$ of order $c$, usually called the *forbidden subgroup*. A relative difference set $D$ is called *cyclic* or *abelian* if $G$ has the respective property. If $c = 1$, the relative difference set becomes a *difference set* in the usual sense.

Relative difference sets first appear in the work of Bose [12], although he was only concerned with a special case and did not use this term which was introduced by Butson [19]. The first systematic investigations are in Elliott and Butson [33] and Lam [83]. For further results and references see the excellent survey on relative difference sets by Pott [97]. There is also a close connection to balanced generalized weighing matrices; see [75, 76].

The main motivation for studying relative difference sets is provided by the fact that the existence of an $(m, c, k, \lambda)$-RDS in $G$ is equivalent to the existence of a divisible semisymmetric design with the same parameters admitting $G$ as a regular automorphism group. As in the special case of difference sets and symmetric designs, the group $G$ is called a *Singer group* for the SSD. The following basic result is due to the second author [69].

THEOREM 4.2: *Assume the existence of an* $(m, c, k, \lambda)$*-RDS* $D$ *in a group* $G$ *relative to a subgroup* $N$*. Then the incidence structure*

$$\operatorname{dev} D = (G, \boldsymbol{B}, \in) \qquad \textit{with} \quad \boldsymbol{B} = \{D + g \colon g \in G\}$$

*is a divisible* $(m, c, k, \lambda)$-SSD *admitting* $G$ *as a Singer group, where* $N$ *acts as the stabilizer of the point class of* 0*. Moreover, any* SSD *with a Singer group* $G$ *may be represented in this way. Finally,* $N$ *is a normal subgroup of* $G$ *if and only if it acts regularly on each point class of* $\operatorname{dev} D$*.*

The reader is referred to Ghinelli [43, 44, 45, 46], Hughes [65] and Jungnickel [69] for more details on semisymmetric designs and relative difference sets. For our purposes, $G$ is abelian; hence $N$ is normal and thus acts as a *class regular* automorphism group of $\operatorname{dev} D$.

Four of the eight cases in the Dembowski-Piper theorem are connected to relative difference sets with $\lambda = 1$, as shown by Ganley and Spence [39]. If we are in one of the cases (a), (b), (d), and (e) of Theorem 4.1, then the faithful point and line orbit of $G$ form a divisible semiplane $\varDelta$, and if $p$ and $L$ are a point and line in these orbits, respectively, then $D = \{g \in G \colon p^g \in L\}$ is an $(m, c, k, 1)$-RDS and $\varDelta \cong \operatorname{dev} D$; of course, $D$ depends on the choice of the *base point* $p$ and the *base line* $L$. More precisely, [39, Lemma 2.2] gives the following cases:

- **Type (a)** Here $D$ is a planar difference set of order $n$, and $\varDelta = \varPi$.
- **Type (b)** Here $D$ has parameters $(n, n, n, 1)$, and the forbidden subgroup $N$ is the pointwise stabilizer of the fixed line $L_\infty$. The associated divisible semiplane $\varDelta$ is a special case of a *symmetric net*; see [7] for background on such structures.
- **Type (d)** Here $D$ has parameters $(n + 1, n - 1, n, 1)$, and the forbidden subgroup $N$ is the pointwise stabilizer of the fixed line $L_\infty$; one usually calls $D$ an *affine difference set* of order $n$. The associated divisible semiplane $\varDelta$ is sometimes called a *biaffine plane* of order $n$.

- **Type (e)** Here $D$ has parameters $(n+\sqrt{n}+1, n^2-\sqrt{n}, n, 1)$, and the forbidden subgroup $N$ is the stabilizer of a Baer subplane $\Pi_0$. The associated divisible semiplane $\Delta$ is often called a *Baer semiplane* of order $n$. The only known abelian example for this case occurs when $n=4$, and it is conjectured that there are no further examples; hence we shall ignore this case.

As noted before, integral group rings are an important tool for investigating relative difference sets. Using the convention introduced in Section 2, we obtain in this case the following lemma.

LEMMA 4.3: *Let $G$ be a multiplicatively written group of order $mc$, let $N$ be a normal subgroup of $G$ of order $c$, and let $D \in \mathbb{Z}G$. Then $D$ is an $(m, c, k, \lambda)$-RDS in $G$ relative to $N$ if and only if the following equation holds in $\mathbb{Z}G$:*

$$DD^{(-1)} = k + \lambda(G - N). \tag{4.1}$$

Later we will also require two variants of relative difference sets in order to deal with the types (f) and (g); these will be defined below. Once a difference set condition is translated into a group ring equation, such as (4.1), these objects can be studied in a purely algebraic setting, which was the main theme of our previous survey [47]. There is also a similar approach for case (h), and this has been used to show that this case is truly sporadic, even for quasiregular groups in general: the only example occurs when $n=4$, by a result of Ganley and McFarland [38].

Planes of type (f) may be represented by the *direct product difference sets* (DPDS) introduced by Ganley [37]. Using group ring notation, a DPDS of order $n$ may be defined to be a subset $D$ of a group $G$ of order $n(n-1)$ with two normal subgroups $A$ and $B$ of orders $n$ and $n-1$, respectively, which satisfies the equation

$$DD^{(-1)} = n + G - A - B \tag{4.2}$$

in $\mathbb{Z}G$. Thus every element not in the union of the two *forbidden subgroups* $A$ and $B$ has a unique "difference representation" from $D$. Note that $G = A \times B$ under our assumptions.

Finally, planes of type (g) are represented by the abelian neo-difference sets of order $n$ considered by the authors in [48, 49, 50]. We note that this type of difference set was first introduced by Hughes [62, 63, 64]; in his terminology, it is a *partial difference set for a partially transitive plane of type (3)*. Using group ring notation, a *neo-difference set* of order $n$ may be defined to be a subset $D$ of a group $G$ of order $(n-1)^2$ with three pairwise disjoint subgroups $X$, $Y$, and $Z$ of order $n-1$ which satisfies the equation

$$DD^{(-1)} = n + G - X - Y - Z \tag{4.3}$$

in $\mathbb{Z}G$; thus every element $\gamma$ not in the union $N$ of the three *forbidden subgroups* $X$, $Y$, and $Z$ has a unique "difference representation" $\gamma = \delta\varepsilon^{-1}$ with $\delta, \varepsilon \in D$.

## 5. - Affine Singer groups

In this section $\Pi$ will denote a plane of type (d), that is, a projective plane with an abelian automorphism group $G$ of order $n^2 - 1$ fixing an antiflag $(\infty, L_\infty)$ and with three point (and three line) orbits. By omitting from $\Pi$ the line $L_\infty$ with all its points and the point $\infty$ with all the lines through it, we obtain a *biaffine plane* $\Delta$: the $n^2 - 1$ points of $\Delta$ split into $n + 1$ point classes of $n - 1$ points each given by the lines through $\infty$, and a line class consists of the lines through a point on $L_\infty$. Note that $\Delta$ is the structure consisting of the faithful point and line orbits, hence the group $G$ is a Singer group for $\Delta$. Therefore $\Delta$ may be represented by an affine difference set $D$ of order $n$, as explained in Section 4. Conversely, given in an abelian group $G$ of order $n^2 - 1$ an affine difference set $D$ relative to the subgroup $N$, we can construct a projective plane $\Pi$ from $D$ as follows:

1. Adjoin an element $\infty \notin G$.
2. Take as lines all $D + g$ and all $(N + g) \cup \{\infty\}$.
3. This gives an affine plane $\Sigma$ of order $n$, which may be completed to a projective plane, as usual.

We note that planes of type (d) are $(\infty, L_\infty)$-*transitive* for the antiflag $(\infty, L_\infty)$, that is, for any two points $p, p' \neq \infty$ and $p, p' \notin L_\infty$ on a line through $\infty$ there is a collineation $\varphi$ fixing $\infty$ and $L_\infty$ pointwise such that $\varphi(p) = p'$. In other words, the forbidden subgroup $N$ is always a group of $(\infty, L_\infty)$-*homologies*.

A fundamental result of Bose [12] provides the classical example, namely $AG(2, q)$ *punctured* in its origin $(0, 0)$: that is, $\Delta = AG(2, q) \setminus \{(0, 0)\}$ with the $n + 1$ lines through $(0, 0)$ deleted. We note that the special choice of the origin does not affect the result of puncturing, as $AG(2, q)$ has a point-transitive group.

Theorem 5.1: *The classical projective plane $PG(2, q)$ admits a cyclic collineation group $G$ of order $q^2 - 1$. This is a cyclic Singer group for $AG(2, q)$ punctured in its origin. Thus there exists an affine difference set of order $q$ in $\mathbb{Z}_{q^2-1}$ for every prime power $q$.*

The proof of Theorem 5.1 is analogous to the standard proof of Singer's Theorem 3.1 [104]. This result of Bose [12] was the starting point for the investigation of *cyclic affine planes*, that is, those affine planes of order $n$ which admit a cyclic group of order $n^2 - 1$; they have been studied extensively beginning with the work of Hoffman [61] who already stated the PPC for this case. The two papers of Bose [12] and of Hoffman [61] started the theory of affine difference sets in much the same way as the work of Singer [104], followed by that of Hall [53], started the theory of planar difference sets. Interestingly, the results – and to a considerable extent also the methods – for both the affine and the planar case of the PPC are quite parallel. A systematic study of affine difference sets was given by Jungnickel [74] who concentrated on nonexistence results giving some evidence for the validity of the PPC.

As with planar difference sets, multipliers are a central tool in the theory of affine difference sets. Hoffman [61] proved the affine analogue of Hall's multiplier theorem for planar difference sets: every prime divisor $p$ of $n$ is a multiplier of every cyclic affine difference set of order $n$. This result remains true for abelian affine difference sets, as a special case of the multiplier theorem of Elliott and Butson [33] for relative difference sets. Using the group ring setting, we presented in [47] a very simple and transparent proof. There also is an affine analogue of the Mann test (see Theorem 3.10.), but it seems that a geometric proof similar to the one given for that result is unfortunately not possible. Hence we will not even state the affine result and refer to [47] instead.

We proceed to discuss geometric applications of affine difference sets; some interesting families of ovals and hyperovals can be obtained also in this case. Again, planes of even order yield the most interesting configurations. In [70] the second author obtained the following theorem; its proof is analogous to that of Theorem 3.12.

THEOREM 5.2: *Let $D$ be an affine difference set in an abelian group $G$. Then the sets $-D+g$ are $n$-arcs in the plane $\Pi$ associated with* dev $D$*; each of these arcs extends to an oval $O_g$ by adjoining $\infty$.*

REMARK 5.3: In the classical case, the oval $-D \cup \{\infty\}$ can be obtained as the affine conic with the equation

$$dx^2 + y^2 + xy + x = 0,$$

where $x^2 + x + d$ is a primitive polynomial over $GF(q)$.

The following (more involved) result was proved by the second author in [73].

PROPOSITION 5.4: *Let $\Pi$ be a projective plane of type (d) associated with an affine difference set $D$ of even order $n$ in an abelian group $G$, and assume $2D = D$. Then the sets $O_g = (-D+g) \cup \{g\}$ with $g \in G$ are $n^2-1$ ovals with common nucleus $\infty$ which can be partitioned into $n+1$ families of $n-1$ ovals each such that any two ovals from different families meet in exactly one point, whereas the ovals in any of the $n+1$ families partition the point set of the divisible semiplane $\Delta$, that is, the set of affine points $\neq \infty$.*

*Moreover, the group $G$ splits into a direct sum $G = H \oplus N$ for a suitable subgroup $H$ of order $n+1$, as $(n-1, n+1) = 1$. The $n-1$ sets $H+h$ with $h \in N$ constitute a further family $\mathcal{O}(H)$ of $n-1$ ovals with common nucleus $\infty$ which partition the set of affine points other than $\infty$. The group $H$ acts regularly on each of these ovals, and $N$ acts regularly on $\mathcal{O}(H)$.*

## 6. - SEMIREGULAR DIFFERENCE SETS

In this section $\Pi$ will denote a plane of type (b), that is a projective plane of order $n$ with an abelian automorphism group $G$ of order $n^2$ fixing a flag $(\infty, L_\infty)$ and with three point (and line) orbits. By omitting from $\Pi$ the line $L_\infty$ with all its points and the point $\infty$ with all the lines through it, we obtain a symmetric net $\Delta$: the $n^2$ points of $\Delta$ split into $n$ point classes of $n$ points each given by the lines through $\infty$, and a line class consists of the lines through a point on $L_\infty$. As $\Delta$ is the structure consisting of the faithful point and line orbit, the group $G$ is a Singer group for $\Delta$. Therefore $\Delta$ – and hence $\Pi$ – may be represented by a relative difference set $D$ with parameters $(n, n, n, 1)$, as explained in Section 4.

Conversely, given in an abelian group $G$ of order $n^2$ a *semiregular difference set* $D$ of order $n$ (i.e. an RDS of parameters $(n, n, n, 1)$, relative to a subgroup $N$), we may construct a projective plane $\Pi$ from $D$ by taking as lines all $D + g$ and all $N + g$, and by completing the resulting affine plane.

We note that planes of type (b) are $(\infty, L_\infty)$-*transitive* for the flag $(\infty, L_\infty)$, that is, for any two points $p, p' \notin L_\infty$ on a line through $\infty$ there is a collineation $\varphi$ fixing $L_\infty$ pointwise such that $\varphi(p) = p'$. In other words, the forbidden subgroup $N$ is always a group of $(\infty, L_\infty)$-*elations*.

The classical example is given by discarding one parallel class from $AG(2, q)$. More generally, semifields and planar functions also give rise to planes of type (b).

Loosely speaking, a proper semifield may be thought of as a (not necessarily commutative) field with non-associative multiplication. To be precise, a finite *semifield* is a finite set $S$ on which two operations, addition and multiplication $(\cdot)$, are defined with the following properties:

(S1) $(S, +)$ is an abelian group with identity 0.

(S2) $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(a + b) \cdot c = a \cdot c + b \cdot c$ for all $a$, $b$, $c \in S$.

(S3) There is an element $1 \neq 0$ with $1 \cdot a = a = a \cdot 1$ for all $a \in S$.

(S4) If $a \cdot b = 0$, then $a = 0$ or $b = 0$.

A *proper semifield* – that is, a semifield which is not a field – of order $q = p^r$ exists if and only if $r \geq 3$ for $p \neq 2$ and $r \geq 4$ for $p = 2$, even if we require the multiplication to be commutative; see [26, p.244]. For a detailed discussion of semifields, we refer the reader to Dembowski [26] and Hughes and Piper [66], where the term *division ring* is used instead.

In order to construct a $(q, q, q, 1)$-RDS associated with the projective semifield plane $\Pi$ of order $q = p^r$ determined by $S$, we need an explicit description of the corresponding affine semifield plane $\Sigma$; see Hughes and Piper [66]. The points of $\Sigma$ are the pairs $(x, y)$ with $x, y \in S$, and the lines are all point sets

$$[m, k] = \{(x, y) : mx + y = k\} \quad \text{with } m, k \in S$$

and all

$$[k] = \{(k, y) : y \in S\} \quad \text{with } k \in S.$$

The divisible semiplane $\Delta$ is obtained by deleting the parallel class of lines $[k]$ which corresponds to the special point $\infty$ on the line $L_\infty$ of $\Pi$. Then the $q^2$ bijections

$$\alpha_{ab} \colon (x, y) \mapsto (x + a, y + ax + b) \quad \text{with } a, b \in S \tag{6.1}$$

are collineations of $\Sigma$; indeed,

$$\alpha_{ab}\colon [m,k] \mapsto [m-a, k+ma+b-a^2] \quad \textit{and} \quad [k] \mapsto [k+a].$$

These collineations form a group $G$ acting regularly on the points and lines of $\Delta$, as $\alpha_{ab}\alpha_{a'b'} = \alpha_{a+a',b+b'+a'a}$. To simplify notation, we identify $\alpha_{ab}$ with the ordered pair $(a,b)$ and consider $G$ to be defined on $S \times S$ by

$$(6.2) \qquad (a,b) * (a',b') \;=\; (a+a', b+b'+a'a).$$

Note that $G$ is abelian if and only if $S$ is a commutative semifield; we now assume this to be the case. Using (6.2), it is easy to show by induction on $m$ that

$$(6.3) \qquad (a,b)^m \;=\; \left(ma, mb + \frac{m(m-1)}{2}a^2\right) \qquad \text{in } (G,*).$$

Thus $(a,b)$ has order $p$ for all $(a,b) \neq (0,0)$ if $p$ is odd; and for $p=2$, the element $(a,b)$ has order 2 whenever $a=0$ and $b \neq 0$ and order 4 for $a \neq 0$.

Finally, we write down a corresponding $(q,q,q,1)$-RDS $D$ explicitly. To do so, we choose the point (0,0) as base point and the line $\{(x,x)\colon x \in R\} = [-1,0]$ as base line. By (6.1), the unique element of $G$ mapping (0,0) to $(a,b)$ is $\alpha_{ab}$; hence

$$(6.4) \qquad D \;=\; \{(x,x)\colon x \in S\} \;\subset\; G.$$

The preceding observations lead to the following theorem essentially due to Hughes [64]; see also Dembowski [26] and Jungnickel [69] for more details.

THEOREM 6.1: *Let $S$ be a semifield of order $q = p^r$. Then the set $S \times S$ together with the operation* (6.2) *is a group $G$ which acts as a quasiregular group of type (b) on the semifield plane associated with $S$, and a corresponding* $(q,q,q,1)$*-RDS is given by* (6.4). *Moreover, $G$ is abelian if and only if $S$ is commutative; in this case, $G$ is elementary abelian if $p$ is odd, and a direct product of cyclic groups of order* 4 *if $p=2$.*

By the results of [36] and [10], an abelian relative difference set with parameters $(n,n,n,1)$ exists if and only if $n$ is a prime power; see also [47, §4] for an exposition of this result. If $n$ is odd, *all* known abelian $(n,n,n,1)$-RDS occur in elementary abelian groups, and we have just seen an abundance of examples. On the theoretical side, the results of [10] only guarantee that $G$ has rank at least $b+1$, where $n = p^b$ for the odd prime $b$. It would be very nice if one could show that $G$ has to be elementary abelian.

As far as we are aware, the only known examples of planes of even order with an abelian collineation group of type (b) are those defined over a commutative semifield of even order; it is an interesting (but probably rather difficult) problem to decide if there are any other examples. In the odd order case, the situation is different. To see this, we require the notion of a planar function as introduced by Dembowski and Ostrom [27].

Let $H$ and $K$ be additively written (for our purposes, abelian) groups of order $n$. A *planar function* of *order n* is a mapping $f\colon H \to K$ such that for every $h \in H \setminus \{0\}$ the induced mapping $f_h\colon x \mapsto f(h+x) - f(x)$ is a bijection. Every planar function gives rise to a projective plane; this is due to Dembowski and Ostrom [27]. We mention in passing that planar functions on cyclic groups have important applications in information theory and the communication sciences; see [82].

If a planar function from $H$ to $K$ exists, then $G = H \oplus K$ is a group of type (b); in fact, $D = \{(x, f(x)) \colon x \in H\}$ is easily seen to be an $(n, n, n, 1)$-RDS in $G = H \oplus K$ relative to $N = \{0\} \oplus K$. Conversely, every *splitting* $(n, n, n, 1)$*-RDS* – that is, every RDS for which the forbidden subgroup $N$ is a direct factor of the underlying group $G$ – is of this type; see Kumar [82] and Pott [97]. In particular, in view of Theorem 6.1, any commutative semifield plane of odd order can be described by a planar function; see Dembowski [26, p245] for a more detailed discussion and some explicit examples. In [57], Hiramine characterized the planar functions over $(GF(q), +)$ corresponding to semifield planes.

Coulter and Matthews [25] proved that the polynomial

$$f(X) = X^{(3^a+1)/2} \tag{6.5}$$

is planar over $GF(3^e)$ provided that $a$ is odd and $(a, e) = 1$. The corresponding projective planes are not translation planes but of Lenz-Barlotti type II.1 [2]. It is an interesting open problem whether or not there are similar constructions in the case of a characteristic other than 3. The Coulter-Matthews planes are of particular interest, as they are associated with the only known planar functions which do not give rise to translation planes.

We now turn to geometric applications of abelian groups of type (b), as studied in [30]. The basic result is as follows; it is essentially due to the second author [71]. Again, the proof is similar to that of Theorem 3.12.

THEOREM 6.2: *Let $D$ be an RDS with parameters $(n, n, n, 1)$ in an abelian group $G$. Then the sets $-D + g$ are $n$-arcs in the projective plane $\Pi$ associated with* $\operatorname{dev} D$*; each of these arcs extends to an oval $O_g$ by adjoining the infinite point $\infty$ associated with the parallel class determined by the forbidden subgroup.*

In particular, the preceding result provides a simple alternative proof for the existence of ovals in commutative semifield planes [40, 68]. Even more interesting is the fact that it also yields the first known examples of ovals in planes of Lenz-Barlotti class II.1, namely in the Coulter-Matthews planes discussed before.

[2] In the *Lenz-Barlotti classification*, collineation groups of projective planes are classified according to the configuration $F$ formed by the point-line pairs $(p, L)$ for which the given group $G$ is $(p, L)$-transitive; in the special case $G = \operatorname{Aut} \Pi$, one speaks of the *Lenz-Barlotti class* of $\Pi$. For a detailed description of this famous classification of projective planes with respect to their central collineations – due to Lenz for elations [86] and to Barlotti [5] for homologies – the reader is referred to Dembowski [26, Section 3.1] and Hughes and Piper [66], or to the survey articles by Yaqub [111] and Ghinelli [41].

Remark 6.3: In the semifield case, the arc $D^{(-1)}$ associated with the RDS $D$ given in equation (6.4) can be realized as the affine conic with equation $y = x^2 + x$ over the underlying commutative semifield $S$.

If $n$ is even, it is necessarily a power of 2, by a result of Ganley [37]; see also [71] for a simpler proof. Of course, the ovals of Theorem 6.2. then extend to hyperovals. If we assume, without loss of generality, $0 \in D$, the nucleus of $O_g$ is the point $\infty_{Ng}$ on the line $L_\infty$ which is determined by the parallel class of lines $D + g + h$, where $h \in N$. Analyzing the intersection properties of the ovals constructed in Theorem 6.2. leads to the following result obtained in [30]:

Theorem 6.4: *Let $\Pi$ be a projective plane of even order $n$ admitting an abelian collineation group $G$ of type (b). Then $\Pi$ contains a $G$-orbit of $n^2$ hyperovals sharing the common point $\infty$ which can be partitioned into $n$ families of $n$ hyperovals each such that any two hyperovals from different families meet in exactly two points (namely, $\infty$ and a further point on the line $L_\infty$), whereas the hyperovals in any of the $n$ families partition the affine plane $\Sigma = \Pi \setminus L_\infty$. Moreover, these $n^2$ hyperovals together with the $n^2 + n$ points $\neq \infty$ of $\Pi$ yield an embedding of the dual affine plane $\Sigma^*$ into $\Pi$.*

Proof: Except for the final assertion, the proof is routine. The intersection properties of the $n^2$ hyperovals which we have constructed show that the incidence structure $\Phi$ formed by these hyperovals (as lines) and the $n^2 + n$ points $\neq \infty$ of $\Pi$ is a dual affine plane of order $n$; note that $\Phi$ can also be obtained as the unique completion of the divisible semiplane $\Delta = \operatorname{dev} D$ to a dual affine plane. As the relative difference sets $D$ and $-D$ lead to isomorphic divisible semiplanes, it is clear that $\Phi$ is isomorphic to the dual affine plane $\Phi'$ obtained from $\Pi$ by removing the point $\infty$. Now it is well-known that planes with an abelian collineation group of type (b) are self-dual [36]; explicitly, the map $\pi\colon g \mapsto D - g$ is a polarity of $\Delta = \operatorname{dev} D$, cf. [7, Proposition I.4.11], and this clearly extends to a polarity of $\Pi$ which interchanges $\infty$ and $L_\infty$. Therefore, the dual affine plane $\Phi'$ is isomorphic to the dual of the affine plane $\Sigma$, proving the final assertion. □

The following theorem concerning the existence of maximal arcs in planes with an abelian group of type (b) was also proved in [30]; cf. Theorem 3.20.

Theorem 6.5: *Let $D$ be an $(n, n, n, 1)$-RDS in a group $G$, where $n = 2^b$. Write $G$ multiplicatively and assume, without loss of generality, $1 \in D$. Then the element $M \in \mathbb{Z}G$ defined by*

$$M = G - \frac{1}{2}(D^2 + N)$$

*belongs to a maximal arc of degree $n/2$ in $\Pi$. Moreover, the affine points together with the*

*$n^2$ translates $Mg$ of $M$ (as blocks) form a symmetric design with parameters*

$$(2^{2b}, 2^{2b-1} - 2^{b-1}, 2^{2b-2} - 2^{b-1}) \tag{6.6}$$

*admitting $G$ as a regular automorphism group.*

Proof: We first check that $M$ indeed determines a subset of $G$, that is, that $M$ has coefficients 0 and 1 only. Now the sum of the entries $d^2$ contained in the formal sum $D^2$ is just the group ring element $N$, as the hypothesis $1 \in D$ guarantees $D^{(2)} = N$ by a result in [71]; thus $\frac{1}{2}(D^2 + N)$ contains each element of $N$ with coefficient 1. If $d, e \in D$ with $d \neq e$, then the element $g = de \in G \setminus N$ also appears with coefficient 1 in $\frac{1}{2}(D^2 + N)$, as in the proof of Theorem 3.20.

In order to verify that $M$ is a maximal arc, we show that each line of $\Pi$ either is an exterior line or meets $M$ in exactly $n/2$ points. By definition, $L_\infty$ is an exterior line. We now apply Lemma 2.6. to compute the intersection sizes for lines of the form $Ng$ and $Dg$, respectively, with the help of Lemma 4.3. and the fact $DN = D^{(-1)}N = G$, which is obvious from the definition of an $(n, n, n, 1)$-RDS:

$$MD^{(-1)} \;=\; nG - \frac{1}{2}\Big((n + G - N)D + G\Big) \;=\; \frac{n}{2}(G - D)$$

and

$$MN^{(-1)} \;=\; MN \;=\; nG - \frac{1}{2}(nG + nN) \;=\; \frac{n}{2}(G - N).$$

Thus the exterior lines to $M$ are precisely the lines $Dg$ with $g \in D$ and the lines $N$ and $L_\infty$, whereas all other lines of $\Pi$ intersect $M$ in $n/2$ points.

In order to prove the final assertion, it suffices to show that $M$ is a difference set with parameters (6.6) in $G$. Using Lemma 4.3, this follows from another short computation:

$$\begin{aligned} MM^{(-1)} &= \Big(G - \frac{1}{2}(D^2 + N)\Big)\Big(G - \frac{1}{2}\Big((D^2)^{(-1)} + N\Big)\Big) \\ &= n^2G - (n^2 + n)G + \frac{1}{4}\Big((n + G - N)^2 + 2nG + nN\Big) \\ &= \frac{n^2}{4} + \frac{n^2 - 2n}{4}\, G. \end{aligned}$$

□

In this context, one should also mention a result due to Kantor [80] which has some similarity to Theorem 6.5, though the point sets considered there are probably somewhat less interesting than maximal arcs. Recall that a *line oval* in a projective plane of order $n$ is the dual notion of an oval: it consists of $n + 1$ lines, no three if which are concurrent.

Theorem 6.6: *Let $\Pi$ be an affine translation plane of order $n = 2^b$, and let $O$ be a line oval containing one line of each of the $n + 1$ parallel classes. Then the union of the $n + 1$ lines of $O$ forms a difference set with parameters* (6.6).

Finally, we once again look at the special case where $\Pi$ is defined over a commutative semifield $R$ of order $q$. As noted before, the affine arc $D^{(-1)}$ is the conic of $\Sigma$ with the equation $y = x^2 + x$. Now the translation group $T$ of $\Sigma$ consists of all collineations

$$\tau_{ab}\colon (x,y) \mapsto (x+a, y+b) \quad \text{with } a,b \in R,$$

and thus the arc $D^{(-1)}$ is obtained from the base point (0,0) by applying all translations $\tau_{-x,-x+x^2}$ with $x \in R$. As $R$ has characteristic 2, these translations form a subgroup of $T$ of order $q$. This proves that the arc $D^{(-1)}$ is a *translation oval* as defined by Cherowitzo [21]. It is easily checked that actually all the affine arcs $A_g$ constructed in Theorem 6.2. are translation ovals in the case under consideration. Hence one obtains a partition of the affine semifield plane $\Sigma$ into translation ovals; this considerably strengthens a result of Jha and Wene [68] who constructed $q-1$ pairwise disjoint translation ovals in affine plane defined over a special class of commutative semifields of even order $q^n$ (namely those with middle nucleus of order $q$).

## 7. - Direct product difference sets

In this section, we consider planes admitting an abelian collineation group of type (f). Such planes may be represented using the direct product difference sets defined in Section 4. We now give an explicit description for the associated projective plane $\Pi$ which may be obtained from the semiplane $\Delta = \operatorname{dev} D$; this is rather more involved than the corresponding constructions for affine difference sets and semiregular relative difference sets.

Let $D$ be a DPDS of order $n$ in the abelian group $G$ (multiplicatively written) with respect to the forbidden subgroups $A$ and $B$. In view of equation (4.2), $D$ meets every coset of $A$ and all but one coset of $B$ exactly once. In particular, we may assume $D \cap B = \emptyset$. Under this assumption, we can give the following simplified variant of the construction in Ganley [37], which is due to de Resmini and the present authors [30]. The points of $\Pi$ are

- the $n(n-1)$ group elements $g \in G$;
- a point $\infty_A$ and $n$ points $(a)$, where $a \in A$;
- a point $\infty_B$ and $n-1$ points $((b))$, where $b \in B$.

The lines of $\Pi$ are

- $n(n-1)$ lines $[a,b] = Dab \cup \{(a), ((b))\}$, where $a \in A$ and $b \in B$;
- a line $L_\infty$ containing $\infty_A$, $\infty_B$ and the $n-1$ points $((b))$, where $b \in B$;
- a line $L_A$ containing $\infty_A$ and the $n$ points $(a)$, where $a \in A$;
- $n-1$ lines $[Ab] = Ab \cup \{\infty_A\}$, where $b \in B$;
- $n$ lines $[Ba] = Ba \cup \{\infty_B, (a)\}$, where $a \in A$.

It is somewhat tedious (but not really difficult) to check that this indeed defines a projective plane $\Pi$ of order $n$. Note that $\Pi$ is both $(\infty_A, L_\infty)$- and $(\infty_B, L_A)$-transitive and therefore at least in Lenz-Barlotti class II.2. Any plane admitting two such transitivities is of type (f) and can be described by a DPDS; see [96]. The only known examples are provided by the Desarguesian planes $PG(2, q)$.

We now turn to geometric properties of abelian groups of type (f), as studied in [30]. The proof of the following result is again similar to that of Theorem 3.12.

Proposition 7.1: *Let $\Pi$ be a projective plane of order $n$ admitting an abelian collineation group $G = A \times B$ of type (f), and let $D$ denote an associated DPDS such that $D \cap B = \emptyset$. Then the $(n-1)$-sets $D^{-1}g$ are arcs in $\Delta = \operatorname{dev} D$, and the $n-1$ lines $Dd^{-2}g$ with $d \in D$ are tangents to $D^{-1}g$ (with $d^{-1}g$ as the tangency point). Moreover, the lines of $\Pi$ corresponding to the cosets of $A$ and $B$, respectively, cannot be secants; hence, $D^{-1}g$ may be extended to an oval $O_g = D^{-1}g \cup \{\infty_A, \infty_B\}$ of $\Pi$.*

Remark 7.2: In the classical case $\Pi = PG(2, q)$, the plane may be represented by a direct product difference set $D$ in $G = EA(q) \times \mathbb{Z}_{q-1}$ for which the arc $D^{-1}$ is the affine hyperbola with the equation $y = -1/x$.

Using Proposition 7.1, we can provide a further example for a situation where a simple geometric argument may be given for a non-trivial structural restriction, avoiding algebraic machinery; we shall prove the following result due to Ganley [37] for even orders and to Pott [96] for odd orders, respectively.

Theorem 7.3: *Let $\Pi$ be a projective plane of order $n$ admitting an abelian collineation group $G = A \times B$ of type (f). If $n$ is even, then $n$ is a power of 2 and the Sylow 2-subgroup $A$ of $G$ is elementary abelian; and if $n$ is odd, the Sylow 2-subgroup of $G$ is cyclic.*

Proof: Consider the intersections of the tangents to $D^{-1}$ with the special line $L_A$. By Proposition 7.1, each point $d = ab \in D$ leads to the tangent $[a^{-2}, b^{-2}]$ of $O = O_1$, which intersects $L_A$ in the point $(a^{-2})$. If $n$ is even, all the tangents are concurrent in the nucleus of $O$; as $O$ meets $L_A$ exactly once (namely in the point $\infty_A$), the nucleus has to be on $L_A$. Therefore, all the values $(a^{-2})$ with $a \in A$, $a \neq 1$, coincide (as $D$ meets all cosets of $B$ except $B$ itself). But $A$ is of even order and hence contains an involution, so the common value is necessarily 1. Thus $A$ is an elementary abelian 2-group in this case, and the nucleus of $O$ is the point $(1)$. On the other hand, if $n$ is odd, no point can be on more than two tangents, and a similar reasoning shows that $A$ contains a unique involution which implies that the Sylow 2-subgroup of $G$ is cyclic. □

The above argument about the nucleus of the oval $O$ generalizes to the following result:

Corollary 7.4: *Under the hypotheses of Proposition* 7.1, *assume that $n$ is even. Let $g \in G$, say $g = ab$ with $a \in A$ and $b \in B$. Then the nucleus of the oval $O_g$ is the point* $(a) \in L_A$.

On the purely geometric side, we may again obtain rather nice families of hyperovals, whereas the odd order case seems a little less interesting (and will not be stated).

Theorem 7.5: *Let $\Pi$ be a projective plane of even order $n$ admitting an abelian collineation group $G$ of type (f). Then $\Pi$ contains a $G$-orbit of* $n(n-1)$ *hyperovals sharing two common points $\infty_A$ and $\infty_B$ which can be partitioned into $n-1$ families of $n$ hyperovals each such that any two hyperovals from different families meet in exactly three points (namely, $\infty_A$, $\infty_B$ and a further point neither on $L_\infty$ nor on $L_A$), whereas the hyperovals in any of the $n-1$ families partition the affine plane $\Sigma = \Pi \setminus L_\infty$.*

As in Theorems 3.20 and 6.5, one can also give an explicit construction for maximal arcs in terms of the underlying direct product difference set $D$ (using group ring notation):

Proposition 7.6: *Let $\Pi$ be a projective plane of even order $n$ admitting an abelian collineation group $G = A \times B$ of type (f), and let $D$ be an associated DPDS. Write $G$ multiplicatively and assume, without loss of generality, $D \cap B = \emptyset$. Then the element $M \in \mathbb{Z}G$ defined by*

$$M = G - \frac{1}{2}(D^2 + B) \tag{7.1}$$

*corresponds to a maximal arc of degree $n/2$ in $\Pi$.*

## 8. - Neo-difference sets

In this final section, we consider projective planes admitting an abelian group $G$ of type (g). Such a group $G$ is of Lenz-Barlotti type I.4, that is, the configuration $F$ formed by the point-line pairs $(p, L)$ for which $G$ is $(p, L)$-transitive consists of the vertices and the opposite sides of a triangle. The associated plane $\Pi$ may be represented using an abelian neo-difference set as defined in Section 4. We now give an explicit description for $\Pi$; as in the case of direct product difference sets, this is somewhat involved. The following results are taken from our papers [48, 49]; they were inspired on one hand by the work of Hughes, cf. [64, pp. 660-662], with some simplifications made possible by the more special situation we consider, and on the other hand, by the more usual representation of planes with a group of type I.4 by *neofields* – an approach which we shall not discuss here, as it is not needed for our purposes.

Let $D$ be a neo-difference set of order $n$ in the abelian group $G$ (multiplicatively written) with respect to the forbidden subgroups $X$, $Y$, and $Z$. These three subgroups are necessarily isomorphic, and hence one may assume $G = X \times X$. Then the forbidden subgroups turn into $U_1 = X \times \{1\}$, $U_2 = \{1\} \times X$, and $U_3 = \{(\xi, \xi) : \xi \in X\}$, and the defining group ring equation (4.3) becomes

$$DD^{(-1)} \;=\; n + G - U_1 - U_2 - U_3. \tag{8.1}$$

As shown in [48], one may assume that both $U_1$ and $U_2$ are disjoint from $D$ and that the unique coset of $U_3$ missing $D$ is $U_3(1, \theta)$, where $\theta$ is an (in fact, the unique) involution in $X$ if $n$ is odd, and $\theta = 1$ otherwise. With these assumptions, we may write

$$D \;=\; \sum_{\xi \in X \setminus \{1\}} \Big(\xi, g(\xi)\Big), \tag{8.2}$$

where $g \colon X \setminus \{1\} \to X \setminus \{1\}$ is a bijection. Note that the element $(\xi, g(\xi))$ is in the coset $U_3(1, \xi^{-1}g(\xi))$, and therefore

$$\{\xi^{-1}g(\xi) \colon \xi \in X\} \;=\; X \setminus \{\theta\}. \tag{8.3}$$

Later, we shall need the following simple restriction on the structure of $X$ which was first proved by Paige [93] in the context of neofields.

LEMMA 8.1: *The group $X$ contains at most one involution.*

PROOF: Let $\gamma$ be an involution of $G$, and assume $\gamma \notin N = U_1 \cup U_2 \cup U_3$. Then there is a representation $\gamma = \delta\varepsilon^{-1}$ with $\delta, \varepsilon \in D$. But this implies the second representation $\gamma = \gamma^{-1} = \varepsilon\delta^{-1}$, a contradiction. Therefore all involutions of $G$ are contained in $N$. Now let $\kappa$ and $\lambda$ be involutions of $X$. Then $(\kappa, \lambda)$ is an involution of $G$, and hence lies in $N$; this is only possible if $\kappa = \lambda$. □

In order to give an explicit description of the desired projective plane $\Pi = \Pi(D)$ in terms of $D$, we choose an element $0 \notin X$ and embed $X$ into the semigroup $\overline{X} = X \cup \{0\}$, where $0\xi = \xi 0 = 0$ for all $\xi \in X$. Moreover, let $\infty$ be some symbol not in $\overline{X}$. Now the points of $\Pi$ are

- the $n^2$ elements $(\xi, \psi) \in \overline{G} = \overline{X} \times \overline{X}$ (for $(\xi, \psi) \in G$, we speak of *ordinary points*);
- $n$ points $(\xi)$, where $\xi \in \overline{X}$, and a point $(\infty)$;

  and the lines of $\Pi$ are
- $(n-1)^2$ lines $[\xi, \psi] \;=\; D(\xi, \psi) \cup \{(\xi, 0), (0, \psi), (\theta\psi\xi^{-1})\}$, where $\xi, \psi \in X$;
- $n$ lines $[U_1\psi] = \{(\xi, \psi) : \xi \in \overline{X}\} \cup \{(0)\}$, where $\psi \in \overline{X}$;
- $n$ lines $[U_2\xi] = \{(\xi, \psi) : \psi \in \overline{X}\} \cup \{(\infty)\}$, where $\xi \in \overline{X}$;
- $n - 1$ lines $[U_3\psi] = \{(\xi, \xi\psi) : \xi \in \overline{X}\} \cup \{(\psi)\}$, where $\psi \in X$;
- a line $[\infty] = \{(\xi) : \xi \in \overline{X}\} \cup (\infty)$.

Again, it is somewhat involved to check that this indeed defines a projective plane $\Pi$ of order $n$. We remark that the vertices of the special triangle mentioned above are the points $o = (0,0)$, $x = (0)$, and $y = (\infty)$. The only known examples are provided by the classical planes $PG(2,q)$. With $K = GF(q)$, the set

$$D \; = \; \{(\xi,\psi) \in K^* \times K^* \colon \; \xi + \psi = 1\}$$

is an abelian neo-difference set of order $n$ in $G = K^* \times K^*$; this is easily checked directly.

As with planar difference sets, multipliers are again a central tool in studying neo-difference sets. Hughes [63] proved the neo-analogue of Hall's multiplier theorem for planar difference sets: every prime divisor $p$ of $n$ is a multiplier of every abelian neo-difference set of order $n$. Using the group ring setting, we presented in [48] a considerably simpler and more transparent proof. As for affine difference sets, there is an analogue of the Mann test (essentially due to Kantor [79]), and here we even have a simple geometric proof similar to the one given for Theorem 3.10. Hence we will include the relevant results from our paper [48].

THEOREM 8.2: *Let D be an abelian neo-difference set of order n in* $G = X \times X$. *If D admits a multiplier t of order* 2, *then n is a perfect square, say* $n = m^2$, *and necessarily* $t = m$.

PROOF: Let $t$ be any multiplier of order 2 of $D$, and denote the induced collineation of the associated projective plane $\Pi$ by $\pi$. Then $\pi$ is an involution whose set of fixed points contains the quadrangle $oxyu$, where $u = (1,1)$. Thus $\pi$ is a Baer involution, that is, the fixed elements of $\pi$ form a Baer subplane $\Pi_0$; see Hughes and Piper [66]. In particular, $n$ must be a square, say $n = m^2$. We now define subgroups $A$ and $B$ of $X$ as follows:

$$A \; = \; \{\xi \in X \colon \; \xi^t = \xi^{-1}\} \quad \text{and} \quad B \; = \; \{\xi \in X \colon \; \xi^t = \xi\}.$$

Then the mappings $\alpha$ and $\beta$ defined by $\xi^\alpha = \xi^{1-t}$ and $\xi^\beta = \xi^{1+t}$ are homomorphisms from $X$ to $A$ and $B$, respectively, and $\xi^\alpha \xi^\beta \; = \; \xi^2$ for each $\xi \in X$; thus $AB$ contains $X^\square$, the set of squares in $X$. Hence $AB$ is a subgroup of index at most 2, by Lemma 8.1. The same lemma also shows that the Sylow 2-subgroup of $X$ is cyclic, which implies that $X$ contains unique subgroups of orders $m-1$ and $m+1$, respectively.

Note that the ordinary points of $\Pi_0$ are simply the pairs $(\xi,\psi)$ with $\xi, \psi \in B$; therefore $B$ is the subgroup of order $m-1$ of $X$. Also, $A$ has to contain the subgroup $A_1$ of order $m+1$ of $X$, as $AB$ is a subgroup of index at most 2 in $X$. (It can be shown that actually $A = A_1$ and $AB = X^\square$, but we do not really need these facts.)

The preceding arguments show that any multiplier of order 2 leads to the same subgroups $A_1$ and $B$ and acts on them in the same way as the given multiplier $t$ does. In particular, this holds for the multiplier $m$ of order 2 whose existence is guaranteed by the multiplier theorem mentioned before. Therefore the collineations induced by $t$ and $m$ certainly agree on all ordinary points $(\xi,\psi)$ with $\xi, \psi \in X^\square$, which suffices to show that $tm^{-1}$ must be the identity.

Corollary 8.3: *Assume the existence of an abelian neo-difference set of square order $n$ in $G$, say $n = m^2$. Then there also exists an abelian neo-difference set of order $m$.*

Proof: One may assume that the given neo-difference set $D$ is fixed by the multiplier $m$ of order 2. Hence – using the same notation as in the proof of Theorem 8.2. – $D$ belongs to the Baer subplane $\Pi_0$ formed by the fixed elements of the collineation $\pi$ induced by $m$. Thus $D \cap B$ is an $(m-1)$-subset of $B \times B$ which is easily seen to be a sub-neo-difference set of $D$. □

Theorem 8.4 [Mann test]: *Let $D$ be an abelian neo-difference set of order $n$ in $G = X \times X$. Then either $n$ is a square or every multiplier of $D$ has odd order modulo* exp $G$. *In particular, each of the following conditions implies that $n$ is a square:*

- *$D$ has a multiplier which has even order modulo $q$, where $q$ divides $n-1$ and either $q = 4$ or $q$ is an odd prime*;
- *$p$ is a quadratic non-residue modulo $q$, where $p$ and $q$ are prime divisors of $n$ and of $n-1$, respectively*;
- *$n \equiv 4$ or $6 \pmod 8$*;
- *$tp^f \equiv -1 \pmod q$ for some prime $p$ dividing $n$, a suitable non-negative integer $f$ and some multiplier $t$ of $D$, where $q$ divides $n-1$ and either $q = 4$ or $q$ is an odd prime*;
- *$(t+1, n-1) \geq 3$ for some multiplier $t$ of $D$.*

Proof: If $t$ has even order, a suitable power of $t$ has order 2, and thus the first assertion is an immediate consequence of Theorem 8.2. The remaining assertions follow using some elementary number theory; see [48]. □

We conclude this section with some results concerning the application of abelian neo-difference sets to the construction of ovals, hyperovals, and projective triangles, all taken from [48]. The proof of the following result is again similar to that of Theorem 3.12, though a little more involved.

Proposition 8.5: *Let $\Pi$ be a projective plane of order $n$ represented by a neo-difference set $D$ in an abelian group $G$, and let $D$ have the form (8.2). Then the $(n-2)$-sets $A_\gamma = D^{(-1)}\gamma$ with $\gamma = (\alpha, \beta) \in G$ are arcs in $\Pi$, and the line $[\xi^{-2}\alpha, g(\xi)^{-2}\beta]$ is the tangent to $A_\gamma$ with $(\xi, g(\xi))^{-1}\gamma$ as the tangency point. Moreover, the $(n-2)$-arc $A_\gamma$ may be extended to an oval of $\Pi$, namely $O_\gamma = A_\gamma \cup \{(0,0),(0),(\infty)\}$. Finally, if $n$ is even, the nucleus of $O_\gamma$ is the ordinary point $\gamma$.*

Let us note an interesting consequence of Proposition 8.5, which was originally proved by Kantor [79] in a different way.

Corollary 8.6: *Under the assumptions of Proposition* 8.5, *let* $n \neq 2$ *be even. Then n is a multiple of* 4.

Proof: Note that $D$ is disjoint from any translate of the form $D\gamma$ with $1 \neq \gamma \in N$. For such a $\gamma$, the hyperovals completing $O_{(1,1)}$ and $O_\gamma$ intersect precisely in the three special points $(0,0)$, $(0)$ and $(\infty)$. But in a plane of order $n \equiv 2 \pmod 4$, any two hyperovals intersect in an even number of points; see, for instance, [78, Lemma 3.3]. □

We also mention the following configuration result which is immediate from Proposition 8.5.

Corollary 8.7: *Let $\Pi$ be a projective plane of order n represented by a neo-difference set D in an abelian group G; in particular, we may take $\Pi = PG(2,n)$. Then $\Pi$ contains a family $\mathcal{O}$ of $(n-1)^2$ ovals all of which contain the special triangle oxy and have pairwise at most one further point of intersection.*

Our final application concerns projective triangles, see Section 2.

Proposition 8.8: *Let $\Pi$ be a projective plane of odd order n represented by a neo-difference set D in an abelian group G. Let O denote the oval $D^{(-1)} \cup \{o,x,y\}$, where $o = (0,0)$, $x = (0)$, and $y = (\infty)$ (see Proposition* 8.5*). Now define B as the set of all points which arise as the intersection of some side of oxy with some tangent of O. Then B is a projective triangle of side $\frac{1}{2}(n+3)$; moreover, B is a minimal blocking set for $\Pi$.*

Proof: By Proposition 8.5, the line $L_\xi = [\xi^{-2}, g(\xi)^{-2}]$ is the unique tangent of $O$ in the point $(\xi, g(\xi))$, where $\xi$ runs over $X \setminus \{1\}$. Now the line $L_\xi$ meets the $x$-axis $ox$ in $(\xi^{-2}, 0)$, the $y$-axis $oy$ in $(0, g(\xi)^{-2})$, and the line at infinity $xy$ in $(\theta g(\xi)^{-2}\xi^2)$. Hence, using (8.3),

$$B = \{o,x,y\} \cup \{(\xi,0) \colon \xi \in X^{\square}\} \cup \{(0,\psi) \colon \psi \in X^{\square}\} \cup \{(\theta\eta) \colon \eta \in X^{\square}\},$$

where we write $X^{\square}$ for the set of squares in $X$. By Lemma 8.1, $X$ contains a unique involution, and hence $X^{\square}$ has index 2 in $X$, which shows that each side of $oxy$ contains exactly $\frac{1}{2}(n+3)$ points of $B$. Now consider a point $q = (\xi, 0) \in ox$ and a point $r = (0,\psi) \in oy$. Then $qr$ is the line $[\xi,\psi]$ and thus $z = qr \cap xy = (\theta\psi\xi^{-1})$. It is now immediate that $q, r \in B$ implies $z \in B$, proving that $B$ is indeed a projective triangle. On the other hand, if the line $L = [\xi,\psi]$ intersects neither $ox$ nor $oy$ in a point of $B$, then both $\xi$ and $\psi$ must be non-squares. As $X^{\square}$ has index 2 in $X$, we see that $\psi\xi^{-1}$ is a square. Thus $L$ intersects $xy$ in a point of $B$, so that $B$ is indeed a blocking set, which is obviously minimal. □

In the special case of Desarguesian planes, Proposition 8.8 provides the following synthetic construction for projective triangles (which are usually defined in an algebraic way, using coordinates):

COROLLARY 8.9: *Let $\Pi = PG(2, q)$, where $q$ is odd. Choose any conic $C$ in $\Pi$, and let $oxy$ be a triangle contained in $C$. Now define $B$ as the set of all points which arise as the intersection of some side of $oxy$ with some tangent of $C$. Then $B$ is a projective triangle of side $\frac{1}{2}(q + 3)$; moreover, $B$ is a minimal blocking set for $\Pi$.*

*Acknowledgements*: The authors thank the referee for some helpful suggestions. This work was partially supported by GNSAGA, by the Italian Ministry for University, Research and Technology (project: *Strutture geometriche, combinatoria e loro applicazioni*) and the Università di Roma "La Sapienza" (project: *Gruppi, Grafi e Geometrie*). The paper started while the second author was a Visiting Research Professor at the University of Rome "La Sapienza"; he gratefully acknowledges the hospitality and financial support extended to him.

## REFERENCES

[1] R. BAER, *Projectivities with fixed points on every line of the plane*, Bull. Amer. Math. Soc., **52** (1946), 273-286.

[2] S. BALL - A. BLOKHUIS - F. MAZZOCCA, *Maximal arcs in desarguesian planes of odd order do not exist*, Combinatorica, **17** (1997), 31-41.

[3] S. BALL - A. BLOKHUIS, *An easier proof of the maximal arcs conjecture*, Proc. Amer. Math. Soc., **126** (1998), 3377-3380.

[4] A. BARLOTTI, *Sui $\{k; n\}$-archi di un piano lineare finito*, Boll. Un. Mat. Ital., **11** (1956), 553-556.

[5] A. BARLOTTI, *Le possibili configurazioni del sistema delle coppie punto-retta $(A, a)$ per cui un piano grafico risulta $(A, a)$ transitivo*, Boll. Un. Mat. Ital., **12** (1957), 212-226.

[6] S.G. BARWICK, *Substructures of finite geometries*, Ph. D. thesis, University of London.

[7] T. BETH - D. JUNGNICKEL - H. LENZ, *Design theory (2nd edition)*, Cambridge University Press, Cambridge (1999).

[8] A. BLOKHUIS, *Blocking sets in Desarguesian planes*, In: "Combinatorics. Paul Erdös is eighty", Vol. 2, pp. 133-155. János Bolyai Math. Soc., Budapest (1996).

[9] A. BLOKHUIS - A.E. BROWER - H.A. WILBRINK, *Hermitian unitals are code words*, Discrete Math., **97** (1991), 63-68.

[10] A. BLOKHUIS - D. JUNGNICKEL - B. SCHMIDT, *Proof of the prime power conjecture for projective planes of order $n$ with abelian collineation groups of order $n^2$*, Proc. Amer. Math. Soc., **130** (2002), 1473-1476.

[11] E. BOROS - T. SZÖNYI, *On the sharpness of a theorem of Segre*, Combinatorica, **6** (1986), 261-268.

[12] R.C. BOSE, *An affine analogue of Singer's theorem*, J. Indian Math. Soc., **6** (1942), 1-15.

[13] R.C. BOSE, *Mathematical theory of the symmetrical factorial design*, Sankhyā, **8** (1947), 107-166.

[14] R.C. BOSE, *On the application of finite projective geometry for deriving a certain series of balanced Kirkman arrangements*, In: "Calcutta Math. Soc. golden jubilee commemoration" Vol. II, pp. 341-356 (1958-59).

[15] R.H. BRUCK, *Difference sets in a finite group*, Trans. Amer. Math. Soc. **78** (1955), 464-481.

[16] R.H. BRUCK, *Quadratic extensions of cyclic planes*, Proc. Sympos. Appl. Math. **10** (1960), 15-44.

[17] R.H. BRUCK, *Circle geometry in higher dimensions, II*, Geom. Dedicata, **2** (1973), 133-188.

[18] R.H. BRUCK - H.J. RYSER, *The nonexistence of certain finite projective planes*, Canadian J. Math., **1** (1949), 88-93.

[19] A.T. Butson, *Relations among generalised Hadamard matrices, relative difference sets and maximal length linear recurring sequences*, Canadian J. Math., **15** (1963), 42-48.

[20] W.E. Cherowitzo, *Ovals in Figueroa planes*, J. Geom., **37** (1990), 84-86.

[21] W.E. Cherowitzo, *Hyperovals in the translation planes of order 16*, J. Combin. Math. Combin. Comp., **9** (1991), 39-55.

[22] W.E. Cherowitzo, *Hyperovals in desarguesian planes: An update*, Discrete Math., **155** (1996), 31-38.

[23] S. Chowla - H.J. Ryser, *Combinatorial problems*, Canadian J. Math., **2** (1950), 93-99.

[24] A. Cossu, *Su alcune proprietà dei $\{k; n\}$-archi di un piano proiettivo sopra un corpo finito*, Rend. Mat. e Appl., **20** (1961), 271-277.

[25] R. Coulter - R. Matthews, *Planar functions and planes of Lenz-Barlotti class II*, Designs, Codes and Cryptography, **10** (1997), 167-184.

[26] P. Dembowski, *Finite geometries*, Springer, Berlin (1968, Reprint 1997).

[27] P. Dembowski - T. G. Ostrom, *Planes of order n with collineation groups of order $n^2$*, Math. Z., **103** (1968), 239-258.

[28] P. Dembowski - F.C. Piper, *Quasiregular collineation groups of finite projective planes Math. Z.,* ***99** (1967), 53-75.*

[29] R.H.F. Denniston, *Some maximal arcs in finite projective planes J. Combin. Theory (A),* **6** *(1969), 317-319.*

[30] M.J. de Resmini - D. Ghinelli - D. Jungnickel, *Arcs and ovals from abelian groups*, Designs, Codes and Cryptography, **26** (2002), 213-228.

[31] M.J. de Resmini - N. Hamilton, *Hyperovals and unitals in Figueroa planes*, European J. Combin., **19** (1998), 215-220.

[32] M.J. de Resmini - D. Jungnickel, *Two infinite families of failed symmetric designs*, Discrete Math., **261** (2003), 235-241.

[33] J.E.H. Elliott - A.D. Butson, *Relative difference sets*, Illinois J. Math., **10** (1966), 517-531.

[34] J.C. Fisher - J.W.P. Hirschfeld - J.A. Thas, *Complete arcs in planes of square order*, Ann. Discrete Math., **30** (1986), 243-250.

[35] R.A. Fisher, *An examination of the different possible solutions of a problem in incomplete blocks*, Ann. Eugenics, **10** (1940), 52-75.

[36] M.J. Ganley, *On a paper of Dembowski and Ostrom*, Arch. Math., **27** (1976), 93-98.

[37] M.J. Ganley, *Direct product difference sets*, J. Combin. Theory (A), **23** (1977), 321-332.

[38] M.J. Ganley - R.L. McFarland, *On quasiregular collineation groups*, Arch. Math., **26** (1975), 327-331.

[39] M.J. Ganley - E. Spence, *Relative difference sets and quasiregular collineation groups*, J. Combin. Theory (A), **19** (1975), 134-153.

[40] C.W. Garner, *Von Staudt conics in semifield planes*, Aequationes Math., **11** (1974), 183-188.

[41] D. Ghinelli, *Classificazione di Lenz-Barlotti e problemi aperti inerenti ad essa*, Ist. Mat. "G. Castelnuovo" Roma (1969), 1-30.

[42] D. Ghinelli, *Varietà Hermitiane e strutture finite, I*, Rend. Mat. Appl., (6) **2** (1969), 23-62.

[43] D. Ghinelli(-Smit), *On semisymmetric designs*, Report, Westfield College, University of London (1980).

[44] D. Ghinelli(-Smit), *Nonexistence theorems for automorphism groups of divisible square designs*, Ph.D. Thesis, University of London (1983).

[45] D. Ghinelli(-Smit), *Hall-Ryser type theorems for relative difference sets*, Ann. Discrete Math., **37** (1988), 189-194.

[46] D. Ghinelli, *A rational congruence for a standard orbit decomposition*, European J. Combin., **11** (1990), 105-113.

[47] D. Ghinelli - D. Jungnickel, *Finite projective planes with a large abelian group*, In: "Surveys in Combinatorics (Ed. C.D.Wensley)", pp. 175-237, Cambridge University Press, Cambridge (2003).

[48] D. Ghinelli - D. Jungnickel, *On finite projective planes in Lenz-Barlotti class at least I.3*, Adv. Geom., Special Issue dedicated to A. Barlotti (2003), S28-S48.

[49] D. Ghinelli - D. Jungnickel, *Piani proiettivi finiti e neo-insiemi di differenze*, Quaderni elettronici del Seminario di Geometria Combinatoria, (**13 E**) Febbraio 2004, 1-30. http://www.mat.uniroma1.it/combinatoria/quaderni

[50] D. Ghinelli - D. Jungnickel, *A non-existence result for finite projective planes in Lenz-Barlotti class I.4*, Combinatorica, **27** (2007), 163-166.

[51] H.-D.O.F. Gronau - R.C. Mullin, *On super-simple 2-$(v, k, \lambda)$-designs*, J. Combin. Math. - Combin. Comp., **11** (1992), 113-121.

[52] M. Hall, *Projective planes*, Trans. Amer. Math. Soc., **54** (1943), 229-277.

[53] M. Hall, *Cyclic projective planes*, Duke Math. J., **14** (1947), 1079-1090.

[54] N. Hamilton, *Degree 8 maximal arcs in* PG$(2, 2^h)$*, h odd*, J. Combin. Theory (A), **100** (2002),265-276.

[55] N. Hamilton - R. Mathon, *More maximal arcs in Desarguesian projective planes and their geometric structure*, Adv. Geom., **3**, (2003), 251-261.

[56] N. Hamilton - R. Mathon, *On the spectrum of non-Denniston maximal arcs in* PG$(2, 2^h)$, European J. Combin., **25**, (2004), 415-421.

[57] Y. Hiramine, *On planar functions*, J. Algebra, **133** (1990), 103-110.

[58] J.W.P. Hirschfeld, *Projective geometries over finite fields (2nd edition)*, Oxford University Press, Oxford (1998).

[59] C.Y. Ho, *Arc subgroups of planar Singer groups*, In: "Mostly finite geometries (Ed. N.L. Johnson)." Marcel Dekker, New York, pp. 227-233 (1997).

[60] C.Y. Ho, *Finite projective planes with transitive abelian collineation groups*, J. Algebra **208** (1998), 553-550.

[61] A.J. Hoffmann, *Cyclic affine planes*, Canadian J. Math. **4** (1952), 295-301.

[62] D.R. Hughes, *Planar division neo-rings*, Ph.D. Thesis, University of Wisconsin, Madison (1955).

[63] D.R. Hughes, *Planar division neo-rings*, Trans. Amer. Math. Soc. **80** (1955), 502-527.

[64] D.R. Hughes, *Partial difference sets*, Amer. J. Math. **78** (1956), 650-674.

[65] D.R. Hughes, *On designs*, In: "Geometries and groups" (eds. M. Aigner and D. Jungnickel), pp. 43-67. Springer, Berlin, 1981.

[66] D.R. Hughes - F.C. Piper, *Projective planes (2nd edition)*, Springer, 1982.

[67] D.R. Hughes - F.C. Piper, *Design theory*, Cambridge University Press, Cambridge, 1985.

[68] V. Jha - G. Wene, *An oval partition of the central units of certain semifield planes*, Discrete Math., **155** (1996), 127-134.

[69] D. Jungnickel, *On automorphism groups of divisible designs*, Canadian J. Math., **34** (1982), 257-297.

[70] D. Jungnickel, *A note on affine difference sets*, Arch. Math., **47** (1986), 279-280.

[71] D. Jungnickel, *On a theorem of Ganley*, Graphs Combin., **3** (1987), 141-143.

[72] D. Jungnickel, *Divisible semiplanes, arcs, and relative difference sets*, Canadian J. Math., **39** (1987), 1001-1024.

[73] D. Jungnickel, *On the geometry of affine difference sets of even order*, Arab Gulf J. Scient. Res. Math. Phys. Sci., **A7** (1989), 21-28.

[74] D. Jungnickel, *On affine difference sets*, Sankhyā (A), **54** (1992), 219-240.

[75] D. Jungnickel, *Balanced generalized weighing matrices and related structures*, Quaderni elettronici del Seminario di Geometria Combinatoria **16 E** (Febbraio 2005), 1-39.

[76] D. Jungnickel - H. Kharaghani, *Balanced generalized weighing matrices and their applications*, Le Matematiche, **LIX** (2004), 225-261.

[77] D. Jungnickel - A. Pott, *Two results on difference sets*, Coll. Math. Soc. János Bolyai, **52** (1988), 325-330.

[78] D. JUNGNICKEL - K. VEDDER, *On the geometry of planar difference sets*, European J. Combin., **5** (1984), 143-148.

[79] W. M. KANTOR, *Projective planes of type I-4*, Geom. Dedicata, **3** (1974), 335-346.

[80] W. M. KANTOR, *Symplectic groups, symmetric designs, and line ovals*, J. Algebra, **33** (1975), 43-58.

[81] B. KESTENBAND, *Unital intersections in finite projective planes*, Geom. Dedicata, **11** (1981), 107-117.

[82] P.V. KUMAR, *On the existence of square dot-matrix patterns having a specific three-valued periodic-correlation function*, IEEE Trans. Inform. Theory, **34** (1988), 271-277.

[83] C.W.H. LAM, *On relative difference sets*, Congr. Numer., **20** (1977), 445-474.

[84] C.W.H. LAM - L. THIEL - S. SWIERCZ, *The non-existence of finite projective planes of order 10*, Canadian J. Math., **41** (1989), 1117-1123.

[85] E.S. LANDER, *Symmetric designs: An algebraic approach*, Cambridge University Press, Cambridge, 1983.

[86] H. LENZ, *Kleiner desarguesscher Satz und Dualität in projektiven Ebenen*, Jahresber. - Deutsche Math. Ver., **57** (1954), 20-31.

[87] H.B. MANN, *Balanced incomplete block designs and abelian difference sets*, Illinois J. Math., **8** (1964), 252-261.

[88] R. MATHON, *New maximal arcs in Desarguesian planes*, J. Combin. Theory (A), **97** (2002), 353-368.

[89] T.G. OSTROM, *Concerning difference sets*, Canadian J. Math., **5** (1953), 421-424.

[90] T.G. OSTROM - A. WAGNER, *On projective and affine planes with transitive collineation groups*, Math. Z., **71** (1959), 186-199.

[91] U. OTT, *Endliche zyklische Ebenen*, Math. Z., **144** (1975), 195-215.

[92] U. OTT, *Sharply flag-transitive projective planes and power residue difference sets*, J. Algebra, **276** (2004), 663-673.

[93] L.J. PAIGE, *Neofields.*, Duke Math. J., **16** (1949), 39-60.

[94] A. POTT, *A note on self-orthogonal codes*, Discrete Math., **76** (1989), 283-284.

[95] A. POTT, *On abelian difference set codes*, Designs, Codes and Cryptography, **2** (1992), 263-271.

[96] A. POTT, *On projective planes admitting elations and homologies*, Geom. Dedicata, **52** (1994), 181-193.

[97] A. POTT, *A survey on relative difference sets*, In: “Groups, difference sets and the monster.” (Eds. K.T. Arasu et al.), pp. 195-232. Walter de Gruyter, Berlin, 1996.

[98] B. QVIST, *Some remarks concerning curves of the second degree in a finite plane*, Ann. Acad. Sci. Fennicae. Ser. A. I. Math.-Phys., **134** (1952), 27-48.

[99] T. G. ROOM, *Polarities and ovals in the Hughes plane*, J. Austral. Math. Soc., **13** (1972), 196-204.

[100] B. SEGRE, *Ovals in a finite projective plane*, Canadian J. Math., **7** (1955), 414-416.

[101] B. SEGRE, *Opere scelte. A cura della Unione Matematica Italiana e con il contributo del Consiglio Nazionale delle Ricerche*, Vol. III, Ed. Cremonese, Roma (2000), I -XXII and 863-1297.

[102] G. SEIB, *Unitäre Polaritäten endlicher projektiver Ebenen*, Arch. Math., **21** (1970), 103-112.

[103] E. SEIDEN, *A theorem in finite projective geometry and an application to statistics*, Proc. Amer. Math. Soc., **1** (1950), 282-286.

[104] J. SINGER, *A theorem in finite projective geometry and some applications to number theory*, Trans. Amer. Math. Soc., **43** (1938), 377-385.

[105] L. STORME and H. VAN MALDEGHEM, *Cyclic arcs in $PG(2,q)$.*, J. Algebraic Comb., **3** (1994), 113-128.

[106] T. SZÖNYI, *On cyclic caps in projective spaces*, Designs, Codes and Cryptography **8** (1996), 327-332.

[107] J.A. Thas, *Construction of maximal arcs and partial geometries*, Geom. Dedicata, **3** (1974), 61-64.

[108] J.A. Thas, *Some results concerning* $\{(q+1)(n-1);n\}$*-arcs and* $\{(q+1)(n-1)+1;n\}$*-arcs in finite projective planes of order* $q$, J. Combin. Theory (A), **19** (1975), 228-232.

[109] J.A. Thas, *Construction of maximal arcs and dual ovals in translation planes*, European J. Combin., **1** (1980), 189-192.

[110] K. Thas, *Finite flag-transitive projective planes: a survey and some remarks*, Discrete Math., **266** (2003), 417-429.

[111] J.C.D.S. Yaqub, *The Lenz-Barlotti classification*, Proc. Proj. Geometry Conference, pp. 129-160. Univ. of Illinois, Chicago (1967).

*Direttore responsabile*: Prof. A. Ballio - Autorizz. Trib. di Roma n. 7269 dell'8-12-1959
«Monograf» - Via Collamarini, 5 - Bologna