Innovations in Incidence Geometry
Volume 12 (2011), Pages 35–48
ISSN 1781-6475

ACADEMIA PRESS

On polar ovals in abelian projective planes

Kei Yuen Chan Hiu Fai Law Philip P.W. Wong

Abstract

A condition is introduced on the abelian difference set $\mathcal{D}$ of an abelian projective plane of odd order so that the oval $2\mathcal{D}$ is the set of absolute points of a polarity, with the consequence that any such abelian projective plane is Desarguesian.

Keywords: ovals, polarity, cyclic difference sets, projective planes
MSC 2000: 05B10, 05B25, 51E15, 51E21

1 Introduction

A projective plane is *Desarguesian* if any two centrally perspective triangles are axially perspective. It is well-known that a Desarguesian plane can be coordinatized by a division ring. Since any finite division ring is a Galois field, the order of a finite Desarguesian projective plane is a prime power. Although non-Desarguesian planes exist, all known cases have order a prime power. This leads to the following famous long-standing conjecture:

Conjecture 1.1. *Any finite projective plane is of prime power order.*

In terms of number theoretic properties, the most general result about the conjecture is the Bruck-Ryser-Chowla Theorem [7, 8] which states that if a projective plane of order n exists and $n \equiv 1, 2 \pmod 4$, then n is a sum of two squares. The first case not ruled out by the result is order 10. The nonexistence of a projective plane of order 10 has been shown by Lam, Thiel and Swiercz [18] by exhaustive computer search. The next general case, which is 12, remains open.

A *cyclic projective plane* (CPP) is a finite projective plane which admits a cyclic Singer group of collineations, i.e. a collineation group which is sharply transitive on points. Singer [24] has proven that any finite Desarguesian plane is a cyclic projective plane. The converse is another long-standing conjecture:

Conjecture 1.2. *Any cyclic projective plane is Desarguesian.*

This conjecture is equivalent to the combination of two statements (see [5]):

(i) Any cyclic projective plane is of prime power order. (Prime Power Conjecture for CPP.)

(ii) Any cyclic projective plane of prime power order is unique up to isomorphism.

Statement (i) has been verified up to order 2×10^9 in [2, 9]. Statement (ii) has been first verified for the order m and m^2 by Bruck [5], where $m = 2, 3, 5, 7, 8, 9$. Recently, Law and Wong [19] have extended Bruck's result to $m = 11, 16$. Furthermore, Huang and Schmidt [14] have shown that for $n < 41$ and for $n \in \{121, 125, 128, 169, 256, 1024\}$, every CPP of order n is Desarguesian.

More generally, a finite projective plane which admits an abelian Singer group of collineations is called an *abelian projective plane* (APP). In this paper, we isolate a mild necessary and sufficient condition, configurational in nature, for an APP of odd order to be Desarguesian. Essential to our approach is the result of Ott [21] together with its generalization to the abelian case by Ho [13], and the classic characterization of the multiplier group by Bruck [4], which combine to give the conclusion that an APP π with abelian Singer group G is either Desarguesian or G is normal in the full automorphism group $\mathrm{Aut}(\pi)$. We shall construct a polarity on an odd order APP satisfying our condition so that its composition with the Hall polarity associated to an APP defines a collineation which is not in the normalizer of G in $\mathrm{Aut}(\pi)$.

We shall be using the techniques of abelian difference sets. As is well-known, two cyclic projective planes are isomorphic if and only if the associated cyclic difference sets are equivalent. Furthermore, this result extends to abelian groups by Jungnickel [16]. Accordingly, our configurational condition is given in terms of the difference set defining the APP under investigation. Our proofs depend essentially on the classification of points and lines of a plane with respect to ovals and the use of multipliers. For consistency in notation and ease of reference, we have included the discussion of some basic results in the following sections.

2 Arcs and ovals in an abelian projective plane

In this section, we study arcs and ovals and use them to classify the points and lines in an abelian projective plane.

We begin by working in a finite projective plane and then later specialize to an abelian one. Let π be a finite projective plane. An *arc* of lines (respectively points) is a set of lines (respectively points) which are in general position. An *oval* is an arc whose cardinality is the largest among all arcs. Note that this definition of an oval is different from the usual one which is given as $q+1$ lines in general position in a plane of order q (see [15], cfr. also [11].)

Definition 2.1. Given an arc of lines $\mathcal{A}$ of π, a point is called, respectively, a *zero point*, *single point*, *double point* if it is incident on, respectively, $0, 1, 2$ lines in $\mathcal{A}$. The sets of zero points, single points and double points are denoted respectively by Z, S, D.

Definition 2.2. Given an arc of lines $\mathcal{A}$ of π, a line is called, respectively, a *zero line*, *single line*, *double line* if it is incident on, respectively, $0, 1, 2$ single points of $\mathcal{A}$. The sets of zero lines, single lines and double lines are denoted respectively by $\mathcal{Z}, \mathscr{S}, \mathcal{D}$.

We have the usual dual version of the above definitions for a given arc of points.

We first discuss the size and content of an oval of lines. However, all results hold if we consider points instead.

Since any line l has $q+1$ points and distinct lines of an arc containing l must intersect l at distinct points, it follows that the cardinality of an oval cannot exceed $q+2$. On the other hand, if there are $q+2$ lines in the oval, then each line in it contains only double points. It follows that a line not in the oval must intersect the lines of the oval in $(q+2)/2$ double points, and so q is even. In fact, it is a remarkable result of Qvist [23] that any arc of $q+1$ lines in a projective plane of even order q can be extended to an oval of $q+2$ lines.

Now suppose $\mathcal{O}$ is an oval of $q+1$ lines in a plane π of odd order. It is easy to see that each line in $\mathcal{O}$ has 1 single point and q double points, and each line outside $\mathcal{O}$ has s single points and d double points where $s+2d = q+1$. In particular, $s \neq 1$ and the set of single lines $\mathscr{S} = \mathcal{O}$. Thus, we may write $\mathcal{O} = \{l_0, l_1, \ldots, l_q\}$, and the set of single points $S = \{P_0, P_1, \ldots, P_q\}$, where P_i is on $l_i, i = 0, 1, \ldots, q$, and l_i is the only single line with respect to $\mathcal{O}$ on P_i. Counting the lines on P_i we conclude that $P_i.P_j$, where $j = 0, 1, \ldots, \hat{i}, \ldots, q$, are q distinct lines, so that S is an arc of points. It follows that any line in π contains at most two single points.

We summarize the above discussion on planes of odd order in the following structure theorem (cfr. [11, 12].)

Theorem 2.3. *Let $\mathcal{O}$ be an oval of $q+1$ lines in a projective plane π of odd order q. The points and lines of π are classified with respect to $\mathcal{O}$ as follows:*

(i) *every point of π is either a zero, a single, or a double point, with* $\mathrm{card}(Z) = q(q-1)/2$, $\mathrm{card}(S) = q+1$, *and* $\mathrm{card}(D) = q(q+1)/2$*; S is an oval;*

(ii) *every line of π is either a zero, a single, or a double line, with* $\mathrm{card}(\mathcal{Z}) = q(q-1)/2$, $\mathrm{card}(\mathscr{S}) = q+1$, *and* $\mathrm{card}(\mathcal{D}) = q(q+1)/2$*; $\mathcal{O} = \mathscr{S}$;*

(iii) *for the pencil of lines through a point P in π:*

(a) *on $P \in Z$, there are $(q+1)/2$ zero lines and $(q+1)/2$ double lines,*

(b) *on $P \in S$, there is 1 single line and there are q double lines,*

(c) *on $P \in D$, there are $(q-1)/2$ zero lines, 2 single lines, and $(q-1)/2$ double lines;*

(iv) *for the points on a line l in π:*

(a) *on $l \in \mathcal{Z}$, there are $(q+1)/2$ zero points and $(q+1)/2$ double points,*

(b) *on $l \in \mathscr{S}$, there is 1 single point and there are q double points,*

(c) *on $l \in \mathcal{D}$, there are $(q-1)/2$ zero points, 2 single points, and $(q-1)/2$ double points.*

We now specialize to abelian projective planes. Let π be an abelian projective plane of order q with points given by an abelian Singer group G of order q^2+q+1 and lines the translates of an abelian difference set $\mathcal{D}_q = \{d_0, d_1, \ldots, d_q\}$ of G. We write $\pi = \pi(\mathcal{D}_q)$. Let $\mathcal{W}(\mathcal{D}_q) = \{\mathcal{D}_q, \mathcal{D}_q+d_1-d_0, \ldots, \mathcal{D}_q+d_q-d_0\}$. Since $\mathcal{D}_q$ is an abelian difference set, $\mathcal{W}(\mathcal{D}_q)$ is an arc of $q+1$ lines. From the discussion above on the size of an oval we note that if $\mathcal{O}$ is an oval of lines in an abelian projective plane $\pi(\mathcal{D}_q)$, then the cardinality of $\mathcal{O}$ is $q+1$ if q is odd, and $q+2$ if q is even.

On the other hand, $-\mathcal{D}_q$ is an arc of $q+1$ points, again since $\mathcal{D}_q$ is an abelian difference set [6, 17]. Indeed, $-d_i$ and $-d_j$ determine uniquely the line $\mathcal{D}_q - d_i - d_j$. If $-d_k \in \mathcal{D}_q - d_i - d_j$, then $-d_k = d_l - d_i - d_j$, contradicting the definition of a difference set. Thus we have the same conclusion on the size of an oval of points in $\pi(\mathcal{D}_q)$.

Note that in case $\mathcal{O}$ is $\mathcal{W}(\mathcal{D}_q)$, where q is odd, $2\mathcal{D}_q$ is an oval of points. Indeed, the single points of $\mathcal{W}(\mathcal{D}_q)$ are given by $2\mathcal{D}_q - d_0$, and the result follows from Theorem 2.3 (cfr. [12].)

3 Ovals, polarities, and polar ovals

We begin by summarizing some standard facts about polarities and ovals in a finite projective plane which can be found in Hughes and Piper [15]. Recall that a correlation α of a projective plane π is a one-to-one mapping of the points onto the lines and the lines onto the points such that P is on l if and only if l^α is on P^α. Thus a projective plane admits a correlation if and only if it is self-dual. A polarity is a correlation of order two and it is not known whether a self-dual plane must admit a polarity. However, by Hall [10], a cyclic projective plane $\pi(\mathcal{D}_q)$ is self-dual and it always admits the polarity α given by

$$\alpha\colon x \longleftrightarrow \mathcal{D}_q - x. \tag{1}$$

More generally, we consider the case of an abelian projective plane $\pi(\mathcal{D}_q)$, and the polarity α given by (1) will be called the *Hall polarity*.

If α is a polarity of a projective plane π then a point P (line l) is called *absolute* if P is on P^α (l^α is on l). For example, the absolute points of the Hall polarity is the set $\frac{1}{2}\mathcal{D}_q$, where $\frac{1}{2}(x) = ((q^2+q+2)/2)x$ for $x \in \pi(\mathcal{D}_q)$. The next result shows the configuration of absolute points and absolute lines.

Lemma 3.1 ([15, Lemma 12.1]). *Let α be a polarity of a projective plane π. Then every absolute point of α is on a unique absolute line and, dually, every absolute line contains a unique absolute point.*

The next result shows that the set of absolute points $\frac{1}{2}\mathcal{D}_q$ are in general position and is therefore an oval if q is odd. Since this oval is the absolute points of a polarity α, we call such an oval a *polar oval* with respect to α.

Lemma 3.2 ([15, Theorem 12.6]). *Let α be a polarity of a finite projective plane of odd order q. If α has exactly $q+1$ absolute points then the absolute points of α are in general position.*

In the rest of this section we shall be concerned with an abelian projective plane $\pi = \pi(\mathcal{D}_q)$, of odd order q, as described in Section 2, and without loss of generality we may assume that $d_0 = 0$; otherwise the insignificant term $-d_0$ will appear and complicate the notations. Recall that $2\mathcal{D}_q$ is an oval of single points with respect to the oval of single lines $\mathcal{W}(\mathcal{D}_q)$. We study the question of whether the oval $2\mathcal{D}_q$ is a polar oval.

Suppose $2\mathcal{D}_q$ is a polar oval. Let β be a polarity of π such that the absolute points of β are $2D_q$. Since the lines on each $2d_i$ of $2\mathcal{D}_q$ are all double lines except for the single line $\mathcal{D}_q + d_i$ (Theorem 2.3; this result will be used freely below and no further specific reference will be made of it), it follows from Lemma 3.1 that the absolute lines of β are the single lines. Thus the single points and single lines must correspond under β, i.e.

$$\beta\colon 2d_i \longleftrightarrow \mathcal{D}_q + d_i \tag{2}$$

for $i = 0, 1, \ldots, q$.

As for the double points and double lines, they must also correspond in a one-to-one manner under β. Indeed, the double point $d_i + d_j$ is the intersection of the single lines $\mathcal{D}_q + d_i$ and $\mathcal{D}_q + d_j$, and since β is a correlation, $(d_i + d_j)^\beta = (\mathcal{D}_q + d_i)^\beta.(\mathcal{D}_q + d_j)^\beta = 2d_i.2d_j$, which is a double line. Thus, under the polarity β, the double points and double lines correspond as follows:

$$\beta\colon d_i + d_j \longleftrightarrow 2d_i.2d_j \tag{3}$$

for $i, j = 0, 1, \ldots, q, i \neq j$. Note that the correspondence is one-to-one since $2\mathcal{D}_q$ is an oval.

Now let Z be a zero point. We study the line Z^β. Consider the pencil of lines on Z. Since β is a correlation, the $v = (q+1)/2$ double lines $2d_{i'}.2d_{i''}, i = 1, 2, \ldots, v$, on Z must correspond under β to the double points $d_{i'} + d_{i''}, i = 1, 2, \ldots, v$, on Z^β. Since all the single points have been accounted for, these double points are all the double points on Z^β, and so Z^β must be a zero line. If Z' is another zero point, then Z'^β cannot be the same as Z^β as all double points on Z^β have been occupied by the images under β of the double lines on Z. Therefore the zero points and zero lines are also in one-to-one correspondence under β given by

$$\beta\colon Z \longleftrightarrow (2d_{1'}.2d_{1''})^\beta. \ \ldots \ .(2d_{v'}.2d_{v''})^\beta \tag{4}$$

where $2d_{i'}.2d_{i''}, i = 1, 2, \ldots, v$, are the double lines on Z.

We return to the oval $2\mathcal{D}_q$. We have shown that if there is a polarity β whose absolute points are $2\mathcal{D}_q$, then β must be defined by (2), (3), and (4). In particular, this imposes the following condition on the configuration of double points and double lines, given in terms of the difference set $\mathcal{D}_q$:

Condition D. *If the double lines $2d_i.2d_j,\ 2d_k.2d_l, and\ 2d_m.2d_n$ are concurrent, then the double points $d_i + d_j,\ d_k + d_l, and\ d_m + d_n$ are collinear.*

Condition **D** is therefore a necessary condition for the oval $2\mathcal{D}_q$ to be polar. We shall assume that the odd order abelian projective plane $\pi(\mathcal{D}_q)$ satisfies Condition **D**, define β as above, and proceed to study whether β thus defined is a polarity. Since by definition β is order 2, we need only check whether β is a correlation. It turns out that a further necessary condition is required. Finally, we must also check that the set of absolute points of β is indeed $2\mathcal{D}_q$.

Let P be a point and consider its pencil of lines. With respect to β, we say that a line l in the pencil is *well-behaved* if $l^\beta \in P^\beta$. Dually, let l be a line and consider its points. We say that a point P on the line is *well-behaved* if $P^\beta \ni l^\beta$. If lines on points and points on lines are always well-behaved then β is (by definition) a correlation.

We shall also say that a pair of point P and line l is *well-behaved* with respect to β if $P \in l$ and $P^\beta \ni l^\beta$.

Lemma 3.3. *The following lines on points and points on lines are well-behaved with respect to β:*

(i) *lines on a single point, and points on a single line,*

(ii) *single and zero lines on a double point, and single and zero points on a double line,*

(iii) *double lines on a zero point, and double points on a zero line.*

Proof. Immediate consequences of the definition. To illustrate, consider the case of a zero line z_i on a double point $d_a + d_b$. We show ${z_i}^\beta \in (d_a + d_b)^\beta = 2d_a.2d_b$. Now ${z_i}^\beta$ is by definition the zero point where the images under β of the double lines on it define by their collinearity the line z_i. Since the double point $d_a + d_b$ is on z_i, the double line $2d_a.2d_b$ must be on ${z_i}^\beta$, as we wished. □

Lemma 3.4. *The double lines on a double point are well-behaved with respect to β.*

Proof. Let $u = (q-1)/2$. Let $2d_{i'}.2d_{i''}, i = 1, 2, \dots, u$, be the double lines on the double point $d_a + d_b$. We show $(2d_{i'}.2d_{i''})^\beta \in (d_a + d_b)^\beta$ for each i, i.e. $d_{i'} + d_{i''} \in 2d_a.2d_b$. By Condition **D**, $d_{i'} + d_{i''}, i = 1, 2, \dots, u$, are collinear on a line l. If l is a double line, then it must be $2d_a.2d_b$, since all the remaining $2u = q-1$ single points have been accounted for by the u double points $d_{i'} + d_{i''}$ on l, and we are done. It remains to show that l can neither be a single nor a zero line. If l were a single line, then the single point on it must be either $2d_a$ or $2d_b$ by counting as before, so that l is either $\mathcal{D}_q + d_a$ or $\mathcal{D}_q + d_b$. By comparing the double points on l with those on these two single lines it is clear that l can be neither of these two. If l were a zero line, then l corresponds under β to the zero point whose double lines must include those corresponding to $d_{i'} + d_{i''}, i = 1, 2, \dots, u$, i.e. $2d_{i'}.2d_{i''}, i = 1, 2, \dots, u$. But these lines are concurrent on a double point, namely, $d_a + d_b$. So l cannot be a zero line either. □

Lemma 3.5 (Converse of Condition **D**). *If the double points $d_i + d_j,\ d_k + d_l, and\ d_m + d_n$ are collinear, then the double lines $2d_i.2d_j,\ 2d_k.2d_l, and\ 2d_m.2d_n$ are concurrent.*

Proof. Let l be the line of collinearity of the double points $d_i + d_j,\ d_k + d_l$ and $d_m + d_n$. Suppose l is a double line, say, $2d_a.2d_b$. Consider the double point $(2d_a.2d_b)^\beta = d_a + d_b$. Let $2d_{p'}.2d_{p''}, p = 1, 2, \dots, u$, be the double lines on

d_a+d_b. By Condition **D**, the images under β of these double lines are the double points on $2d_a.2d_b$. Furthermore, by Lemma 3.4, for each p, $(2d_{p'}.2d_{p''})^\beta \in (d_a+d_b)^\beta$, i.e. $d_{p'}+d_{p''} \in 2d_a.2d_b$. Since $d_i+d_j,\ d_k+d_l, and\ d_m+d_n$ are among these $d_{p'}+d_{p''}, p=1,2,\dots,u$, their images under β are concurrent. Next suppose l is a zero line. Then $l=Z^\beta$ where Z is the zero point for which the images under β of its double lines are collinear by Condition **D** and define the double points of l. Since $d_i+d_j,\ d_k+d_l, and\ d_m+d_n$ are among these double points, their images under β are concurrent. Finally suppose l is a single line, say, $\mathcal{D}_q+d_a$. Then $d_i+d_j,\ d_k+d_l,\ d_m+d_n$ and $2d_a$ are collinear, and so $2d_i.2d_j,\ 2d_k.2d_l, and\ 2d_m.2d_n$ are concurrent on $2d_a$. □

Lemma 3.6. *The double points on a double line are well-behaved with respect to β.*

Proof. This is the dual version of Lemma 3.4, so the dual version of its proof applies with Lemma 3.5 providing the dual of Condition **D**. □

It remains to study the behaviour of the zero points and zero lines under β.

Lemma 3.7. *Let Z be a zero point. Any two lines in the pencil of Z correspond under β to two points collinear on a zero line.*

Proof. By definition, all $v=(q+1)/2$ double lines on Z are mapped by β to collinear double points on the zero line Z^β. So we only need to check the cases where the lines are not both double lines. Consider a double line $2d_{i'}.2d_{i''}$, and a zero line z_j, on Z. Let $l=(2d_{i'}.2d_{i''})^\beta.{z_j}^\beta=(d_{i'}+d_{i''}).{z_j}^\beta$. Since a single line does not contain any zero point, l is either a double or a zero line. If l were a double line, say, $2d_a.2d_b$, then by definition of β, d_a+d_b has to be a double point on z_j. On the other hand, by the well-behaviour of a double line $(2d_a.2d_b)$ on a double point $(d_{i'}+d_{i''})$, we have $d_a+d_b \in 2d_{i'}.2d_{i''}$. Thus $2d_{i'}.2d_{i''}=z_j$, which is impossible. A similar argument applies to the case of two zero lines and will not be repeated here. □

Lemma 3.8. *Let Z be a zero point and $z_i, i=1,2,\dots,v=(q+1)/2$, the zero lines on Z. If ${z_i}^\beta \in Z^\beta$ for some i, then ${z_i}^\beta \in Z^\beta$ for all i.*

Proof. Suppose for some $j \neq i$, ${z_j}^\beta \notin Z^\beta$. Then the $v+1$ lines joining ${z_j}^\beta$ to the v double points and the zero point ${z_i}^\beta$ on Z^β are distinct, so one of them must be a double line. This contradicts Lemma 3.7. □

Remark 3.9. There are of course the dual versions of Lemmas 3.7 and 3.8.

Lemma 3.10. *The following conditions are equivalent:*

(i) *There exists a zero point Z and a zero line z such that $Z \in z$ and $Z^\beta \ni z^\beta$.*

(ii) *For every zero point Z and every zero line z, $Z \in z$ if and only if $Z^\beta \ni z^\beta$.*

Proof. (i) $\Rightarrow$ (ii). Let $Z_i, i = 1, 2, \ldots, v = (q+1)/2$, be the zero points on z, with $Z_1 = Z$. Since $z^\beta \in Z^\beta = {Z_1}^\beta$, $z^\beta \in {Z_i}^\beta$ for all i by the dual version of Lemma 3.8. Next we consider, for each $i = 1, 2, \ldots, v$, the zero lines $z_{ij}, j = 1, 2, \ldots, v$, on Z_i, with $z_{i1} = z$. Since ${z_{i1}}^\beta = z^\beta \in {Z_i}^\beta$, ${z_{ij}}^\beta \in {Z_i}^\beta$ for all j by Lemma 3.8. In other words, if one zero point Z is well-behaved on a zero line z, then all the zero points Z_i on z are well-behaved, and all the zero lines z_{ij} on each zero point Z_i are well-behaved.

The above argument can be applied to the zero points $Z_{ijk}, k = 1, 2, \ldots, v$, of the zero line z_{ij} through Z_i, with $Z_{ij1} = Z_i$. Indeed, as we have shown above that ${Z_{ij1}}^\beta = {Z_i}^\beta \ni {z_{i_j}}^\beta$, it follows for the same reason given above that ${Z_{ijk}}^\beta \ni {z_{ij}}^\beta$ for all k. Thus, the zero points Z_{ijk} on the zero lines z_{ij} are well-behaved. Then it follows that the zero lines z_{ijkl} on the zero points Z_{ijk} are well-behaved. This process can therefore be repeated to generate zero points and zero lines satisfying condition (ii).

It remains to show that any zero point (and dually any zero line) is generated in the above process. Let Z' be a zero point. If $Z'.Z_i$ is a zero line for some i, then we are done. So we may assume that $Z'.Z_i$ are double lines for all i. Now $Z'.Z_1$ contains $u-2$ zero points other than Z' and Z_1. Since $v - 1 > u - 2 = (q-1)/2 - 2$, $Z'.Z_1$ intersects z_{2j} at a double point for some $j \neq 1$. Consider the intersections between $Z'.Z_i$ and z_{2j} for $i = 2, \ldots, v$. As these intersections use up at most $v-1$ zero points on z_{2j}, there is a zero point Z'' on z_{2j} outside of these intersections. The line $Z'.Z''$ is a zero line z'' as all v double lines on Z' have been accounted for by the $Z'.Z_i$'s. Thus Z' is a zero point on a zero line z'' through a zero point Z'' on a zero line z_{2j} through the zero point Z_2 on the zero line z, as we wished.

(ii) $\Rightarrow$ (i). This is clear. $\square$

With Lemma 3.10 we can now conclude that if there is a pair of zero point and zero line well-behaved under β, then β is a correlation. We summarize the results obtained in this section in the following theorem:

Theorem 3.11. *Let $\pi(\mathcal{D}_q)$ be a projective plane of odd order q defined by an abelian difference set $\mathcal{D}_q = \{0, d_1, d_2, \ldots, d_q\}$. Let β be defined by* (2)*,* (3) *and* (4)*. Suppose Condition* **D** *holds, and there exists a pair of zero point and zero line well-behaved with respect to β. Then β is a polarity whose set of absolute points contains the oval $2\mathcal{D}_q$.*

4 Multipliers, conics, and Desarguesian planes

In this section we show that an abelian projective plane satisfying the hypotheses of Theorem 3.11 is Desarguesian. We shall deduce this from the result of Ott [21] with its generalization by Ho [13], and the classic characterization of the multiplier group by Bruck [4], using the polarity β provided by Theorem 3.11. Furthermore, we shall use the fact that in a Desarguesian plane of odd order q, a classical unital can never contain a conic. It follows that the set of absolute points of the polarity β, which contains the oval $2\mathcal{D}_q$ (hence a conic by Segre's Theorem, [25]), is equal to $2\mathcal{D}_q$.

Let $\pi(\mathcal{D}_q)$ be an abelian projective plane of odd order q, with abelian Singer group G and abelian difference set $\mathcal{D}_q = \{0, d_1, d_2, \dots, d_q\}$ of G. Suppose the conditions of Theorem 3.11 are satisfied, so that we have a polarity β satisfying (2), (3), and (4). Let α be the Hall polarity given by (1), and consider the collineation $\alpha\beta$.

Lemma 4.1. *The collineation $\alpha\beta$ is not in the normalizer $N(G)$ of G in the full automorphism group $\mathrm{Aut}(\pi(\mathcal{D}_q))$.*

Proof. Suppose $\alpha\beta \in N(G)$. Let $d_i \in \mathcal{D}_q\backslash\{0\}$. Then $\alpha\beta d_i(\alpha\beta)^{-1} = h_i$ for some $h_i \in G$. Since α and β are polarities, we have $\alpha\beta {d_i}^2\beta\alpha = {h_i}^2$. Evaluating at 0 we obtain from the definitions that $-d_i = \alpha(\mathcal{D}_q + d_i) = \alpha\beta(2d_i) = 2h_i$. So $h_i = -d_i/2$. Returning to the original equation and evaluating at 0 we obtain $\alpha\beta d_i\beta\alpha(0) = \alpha\beta(d_i) = -d_i/2$. By the definition of α this gives $\beta(d_i) = \mathcal{D}_q + d_i/2$. Since $\beta(d_i) = \beta(0 + d_i)$ is by definition the line $0.2d_i$, there exist $d_j, d_k \in \mathcal{D}_q$ such that $0 = d_j + d_i/2$ and $2d_i = d_k + d_i/2$. So $-d_i/2, 3d_i/2 \in \mathcal{D}_q$. But then $0-(-d_i/2) = 3d_i/2-d_i$, giving two expressions for $d_i/2$ as differences of elements of $\mathcal{D}_q$ and contradicting the definition of a difference set. □

In view of Theorem 4.3 given below, Lemma 4.1 implies that $\pi(\mathcal{D}_q)$ is Desarguesian. Before stating the result formally, we wish to describe an alternate approach in which more emphasis is put on the role played by the multipliers. We shall need the following results.

Theorem 4.2 ([4]). *Let $\pi(\mathcal{D}_q)$ be an abelian projective plane with an abelian Singer group G. Denote by M the group of all multipliers of $\mathcal{D}_q$. Then $MG = N(G)$, where $N(G)$ is the normalizer of G in the full automorphism group of $\pi(D_q)$. Moreover, $N(G)/G$ is isomorphic to M.*

Theorem 4.3 ([13], [3, Theorem VI 7.4]). *Let $\pi(\mathcal{D}_q)$ be an abelian projective plane with an abelian Singer group G. Then either $\pi(\mathcal{D}_q)$ is Desarguesian or G is a normal subgroup of the full automorphism group of $\pi(\mathcal{D}_q)$.*

Note that Theorem 4.3 is a consequence of Theorem 4.2 and the result of Ho [13], which states that an abelian projective plane is Desarguesian if it admits another abelian Singer group. Indeed, since $N(G) = MG$ by Theorem 4.2, if $\pi(\mathcal{D}_q)$ is Desarguesian then it has elations and these are clearly not in $N(G)$ and so G is not normal in $\mathrm{Aut}(\pi(\mathcal{D}_q))$. On the other hand, if $\gamma \in \mathrm{Aut}(\pi(\mathcal{D}_q))\backslash G$, then $\gamma G \gamma^{-1} \neq G$ and by the result of Ho [13], $\pi(\mathcal{D}_q)$ is Desarguesian.

We saw in Section 2 that $-\mathcal{D}_q$ is always an arc, and if q is odd then $2\mathcal{D}_q$ is an oval. Thus -1 is never a multiplier, nor is 2 for q odd. On the other hand, by the Multiplier Theorem [10, 22], 2 is a multiplier for q even. We next study -2.

Lemma 4.4. *-2 is not a multiplier for any abelian difference set $\mathcal{D}_q$ of arbitrary order q.*

Proof. First suppose q is even. Since 2 is a multiplier, $-2\mathcal{D}_q = -\mathcal{D}_q + g$ for some $g \in G$, which is an arc, and so -2 is not a multiplier. Next suppose q is odd. Take $d_i \in \mathcal{D}_q$ such that $d_i \neq 0$. If -2 were a multiplier, we may assume that $\mathcal{D}_q$ is invariant under -2 ([20]). Then $-2\mathcal{D}_q = \mathcal{D}_q$, so that $-2d_i = d_j$ and $-2d_k = d_i$ for some $d_j, d_k \in \mathcal{D}_q$. Then $d_i + d_j = 2d_k$. Now $d_j \neq d_i$ since $d_i \neq 0$, and so $d_i + d_j$ is a double point. However, $2d_k$ is a single point, giving a contradiction. $\square$

We are now ready to put the significance of the existence of the polarity β of Section 3 in the following light.

Lemma 4.5. *Let q be odd. An abelian projective plane $\pi(\mathcal{D}_q)$ with an abelian group G is Desarguesian if and only if it admits a polarity satisfying* (2).

Proof. If $\pi(D_q)$ is Desarguesian, then since $2\mathcal{D}_q$ is an oval and q is odd, $2\mathcal{D}_q$ is a conic by Segre's Theorem [25]. Hence, $2\mathcal{D}_q$ is the set of absolute points of an orthogonal polarity. Conversely, we assume the contrary and obtain a contradiction. Suppose $\pi(\mathcal{D}_q)$ is not Desarguesian, and let β be a polarity satisfying the hypothesis. Consider the collineation $\alpha\beta$, where α is the Hall polarity given by (1). By Theorem 4.3, $\mathrm{Aut}(\pi(\mathcal{D}_q)) \subset N(G)$ and so $\alpha\beta \in N(G)$, where $N(G)$ is the normalizer of G in the automorphism group $\mathrm{Aut}(\pi(\mathcal{D}_q))$ of $\pi(\mathcal{D}_q)$. Then Theorem 4.2 implies $\alpha\beta \in MG$ and so for $x \in \pi(\mathcal{D}_q)$, $\alpha\beta(x) = a(x) + g$, for some multiplier $a \in M$ and $g \in G$. Since $\alpha\beta(2d_i) = \alpha(\mathcal{D}_q + d_i) = -d_i$ for all i, it follows that $a(2d_i - 2d_j) = a(2d_i) - a(2d_j) = \alpha\beta(2d_i) - \alpha\beta(2d_j) = d_j - d_i$ for all distinct pairs i, j. This covers every element of G and so $a = -\frac{1}{2}$, which is not a multiplier by Lemma 4.4. We have a contradiction and this proves the lemma. $\square$

For our purpose, Lemma 4.5 is an alternative to Lemma 4.1. In other words, with either Lemma, we can add that $\pi(\mathcal{D}_q)$ is Desarguesian to the conclusion in Theorem 3.11.

We have yet to prove that the set of absolute points of β is exactly $2\mathcal{D}_q$. However, now that the plane in question is Desarguesian, if the set of absolute points of β is larger than $2\mathcal{D}_q$, then β is a unitary polarity, its set of absolute points is the set of points of a classical unital $\mathcal{U}$, and the order q of the plane is a square. We now have an oval $2\mathcal{D}_q$, which is a conic, contained in $\mathcal{U}$, in a Desarguesian plane. This is impossible, by the following classical result.

Lemma 4.6. *In the Desarguesian plane $PG(2, q^2)$, where q is odd, a conic is not a subset of a classical unital.*

Proof. See, for example, [1, Corollary 4.20, p.79]. □

We have now proven the following result.

Theorem 4.7. *Let $\pi(\mathcal{D}_q)$ be an abelian projective plane of odd order q defined by an abelian difference set $\mathcal{D}_q = \{0, d_1, d_2, \ldots, d_q\}$. Let β be defined by* (2)*,* (3) *and* (4)*. Suppose Condition* **D** *holds, and there exists a pair of zero point and zero line well-behaved with respect to β. Then $2\mathcal{D}_q$ is a polar oval with respect to β, and $\pi(\mathcal{D}_q)$ is Desarguesian.*

Remark 4.8. The sufficient conditions in Theorem 4.7 are all satisfied by a Desarguesian plane and are therefore necessary conditions.

Remark 4.9. Unlike the odd order case, where the single points with respect to an oval of lines themselves form an oval, in the case of a plane of even order n, the single points with respect to an arc of $n + 1$ lines are collinear. Hence, the study of the analogous problem for the even order case requires the discovery of a different approach. In this connection, in addition to ovals, it is of interest, for planes of square order of both parities, to study the existence and types of unitals embedded in a CPP/APP.

Acknowledgment. The authors would like to thank the referees for their comments and suggestions which led to an improvement of the results.

References

[1] **S. Barwick** and **G. Ebert**, *Unitals in projective planes* (2008), Springer-Verlag, New York.

[2] **L.D. Baumert** and **D.M. Gordon**, On the existence of cyclic difference sets with small parameters. *In: High Primes and Misdemeanours: Lectures in Honour of the 60th Birthday of Hugh Cowie Williams. Fields Inst. Commun.* **41** (2004), 61–68.

[3] **T. Beth**, **D. Jungnickel** and **H. Lenz**, *Design theory (second edition)* (1999), Cambridge University Press, Cambridge.

[4] **R.H. Bruck**, Difference sets in finite groups, *Trans. Amer. Math. Soc.* **78** (1955), 464–481.

[5] ______, Quadratic extensions of cyclic planes, *Combinatorial Analysis, Proceedings of Symposia in Applied Mathematics X* (1960), 15–44. American Mathematical Society, Providence, Rhode Island.

[6] ______, Circle geometry in higher dimensions. II. *Geom. Ded.* **2** (1973), 133–188.

[7] **R.H. Bruck** and **H.J. Ryser**, The non-existence of certain finite projective planes, *Canadian J. Math.* **1** (1949), 88–93.

[8] **S. Chowla** and **H.J. Ryser**, Combinatorial problems. *Canad. J. Math.* **2** (1950), 93–99.

[9] **D.M. Gordon**, The prime power conjecture is true for $n < 2,000,000$. *Electron. J. Comb.* **1** (1994), R6, 7pp.

[10] **M. Jr. Hall**, Cyclic projective planes, *Duke Math. J.* **14** (1947), 1079–1090.

[11] **J.W.P. Hirschfeld**, *Projective geometries over finite fields (second edition)* (1998), Clarendon Press, Oxford.

[12] **C.Y. Ho**, Some remarks on orders of projective planes, planar difference sets and multipliers, *Des. Codes Cryptogr.* **1** (1991), 69–75.

[13] ______, Finite projective planes with transitive abelian collineation groups. *J. Algebra* **208** (1998), 533–550.

[14] **Y. Huang** and **B. Schmidt**, Uniqueness of some cyclic projective planes, *Des. Codes Cryptogr.* **50** (2009), 253–266.

[15] **D.R. Hughes** and **F.C. Piper**, *Projective Planes* (1973), Springer-Verlag, New York.

[16] **D. Jungnickel**, The isomorphism problem for abelian projective planes. *AAECC* **19** (2008), 195-200.

[17] **D. Jungnickel** and **K. Vedder**, On the geometry of planar difference sets, *European J. Comb.* **5** (1984), 143–148.

[18] **C.W.H. Lam**, **L.H. Thiel** and **S. Swiercz**, The non-existence of finite projective planes of order 10, *Canad. J. Math.* **41** (1989), 1117–1123.

[19] **H.F. Law** and **P.P.W. Wong**, On quadratic extensions of cyclic projective planes, *Algebraic geometry and its applications, Series on Number Theory and Its Applications* **5** (2008), 434–466, World Scientific, Singapore.

[20] **R.L. McFarland** and **H.B. Mann**, On multipliers of difference sets. *Canad. J. Math.* **17** (1965), 541–542.

[21] **U. Ott**, Endliche zyklische Ebenen, *Math. Z.* **144** (1975), 195–215.

[22] **A. Pott**, Applications of the DFT to abelian difference sets. *Arch. Math.* **51** (1988), 283–288.

[23] **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 pp.

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

[25] **B. Segre**, Ovals in a finite projective plane, *Canad. J. Math.* **7** (1955), 414–416.

Kei Yuen Chan
DEPARTMENT OF MATHEMATICS, UNIVERSITY OF HONG KONG, HK

Hiu Fai Law
MATHEMATICAL INSTITUTE, OXFORD UNIVERSITY, UK

Philip P.W. Wong
DEPARTMENT OF MATHEMATICS, UNIVERSITY OF HONG KONG, HK
e-mail: `ppwwong@maths.hku.hk`