Proper Partial Geometries with Singer Groups and Pseudogeometric Partial Difference Sets

Ka Hin Leung Department of Mathematics National University of Singapore 2 Science Drive 2, Singapore 117543 Republic of Singapore matlkh@nus.edu.sg

Siu Lun Ma Department of Mathematics National University of Singapore 2 Science Drive 2, Singapore 117543 Republic of Singapore matmasl@nus.edu.sg

Bernhard Schmidt School of Physical & Mathematical Sciences Nanyang Technological University No. 1 Nanyang Walk, Blk 5, Level 3 Singapore 637616 Republic of Singapore bernhard@ntu.edu.sg

May 4, 2007

Abstract

A partial geometry admitting a Singer group G is equivalent to a partial difference set in G admitting a certain decomposition into cosets of line stabilizers. We develop methods for the classification of these objects, in particular, for the case of abelian Singer groups. As an application, we show that a proper partial geometry $\Pi = pg(s+1,t+1,2)$ with an abelian Singer group G can only exist if t = 2(s+2)and G is an elementary abelian 3-group of order $(s+1)^3$ or Π is the Van Lint-Schrijver partial geometry. As part of the proof, we show that the Diophantine equation $(3^m - 1)/2 = (2^{rw} - 1)/(2^r - 1)$ has no solutions in integers $m, r \ge 1, w \ge 2$, settling a case of Goormaghtigh's Equation.

1 Introduction

A partial geometry $pg(s + 1, t + 1, \alpha)$ is an incidence structure of points and lines with the following properties:

- 1. every line has s + 1 points,
- 2. every point is incident with exactly t + 1 lines,
- 3. through any two points there is at most one line,
- 4. for every line L and every point p not on L there are exactly α lines through p that meet L.

We remark that our notation essentially follows Bose [2]. This notation was also used in [4, 5, 14, 15]. It seems more natural than others since s + 1, t + 1 and α correspond to the objects counted in conditions 1, 2 and 4.

Partial geometries were introduced by Bose [2] in order to unify and generalize certain aspects of the theory of nets, association schemes and designs. The *point graph* of a partial geometry has the points of the geometry as vertices and two points form an edge if and only if they are on a common line. It is well known [2] and straightforward to show that the point graph of a partial geometry is strongly regular. This provides an interesting link between design theory and strongly regular graphs.

Let v, respectively b, be the number of points, respectively lines, of a partial geometry $pg(s+1, t+1, \alpha)$. Elementary counting [2] shows that

$$v = (s+1)(\alpha + st)/\alpha,$$

$$b = (t+1)(\alpha + st)/\alpha.$$

As described in the table below, the notion of partial geometries includes several geometrical structures as special cases.

pg(k, r, k)	Steiner 2-design		
pg(k, r, r)	k, r, r) dual of Steiner 2-design		
pg(k,k,k)	projective plane of order $k-1$		
pg(k, k+1, k)	affine plane of order k		
pg(k, r, r-1)	(k, r)-Bruck net		
$\boxed{\operatorname{pg}(k,r,k-1)}$	transversal design $TD(k, r)$		
pg(k, r, 1)	generalized quadrangle $GQ(k-1, r-1)$		

A proper partial geometry is a partial geometry that does not fall into any of the above categories, i.e. a $pg(s+1,t+1,\alpha)$ with $1 < \alpha < \min\{s,t\}$.

In this paper, we are interested in partial geometries admitting *Singer groups*, i.e. point regular automorphism groups. *Improper* partial geometries with Singer groups exist in abundance. Some prominent instances are cyclic projective planes, affine translation planes and translation nets. However, *proper* partial geometries, in particular those with Singer groups, seem to be extremely rare. The purpose of this paper is to provide some explanation for this phenomenon and to pinpoint certain cases where it might be worth looking for new examples.

A crucial observation for the study of partial geometries with Singer groups is that such a geometry always gives rise to a *partial difference set*: Let G be a Singer group of a $pg(s + 1, t + 1, \alpha)$. We can identify G with the point set of the geometry. Let 1 be the identity element of G. By property 2 of a partial geometry, there are exactly t + 1 lines through the point 1, say L_1, \ldots, L_{t+1} . Let

$$D = \bigcup_{i=1}^{t+1} (L_i \setminus \{1\}).$$

It is straightforward to check that the quotients gh^{-1} , $g, h \in D$, $g \neq h$, cover each element of D the same number of times and cover each element of $G \setminus (D \cup \{1\})$ the same number of times. Such a set D is called a partial difference set. We call such a partial difference set arising from a partial geometry *geometric*. A partial difference set with the same parameters as a potential partial difference set arising from a partial geometry will be called *pseudogeometric*, see Definition 5. Powerful tools are available for the investigation of partial difference sets, see [15, 16, 17, 18]. We will use and extend this machinery to derive new results on pseudogeometric partial geometries with abelian Singer groups.

Let $L_1, ..., L_{t+1} \subset G$ be the lines from above. If G is abelian then by [17, Thm. 3.4], each L_i either is a subgroup of G or does not contain any two elements which are inverses of each other. In the first case, we call L_i a subgroup line, in the second case an orbit line. Following [11], we say the partial geometry is of spread type if all L_i 's are subgroup lines. If there are no subgroup lines, the geometry is said to be of rigid type. In case there are subgroup lines as well as orbit lines, the geometry is said to be of mixed type.

De Winter [11, Remark 5.3] conjectured that no pg(s + 1, t + 1, 2) with abelian Singer group of mixed type exists. We will verify this conjecture except for one exceptional parameter family by proving the following. **Theorem 1** Let $\Pi = pg(s+1,t+1,2)$ be a partial geometry with an abelian Singer group G of mixed type. Then $s+1=3^a$ for some a > 1, $t = 2(3^a+1)$, G is an elementary abelian 3-group of order 3^{3a} , and there are exactly $3^a + 3$ subgroup lines.

Let us summarize the known parameters s+1, t+1, α for which a proper $pg(s+1, t+1, \alpha)$ with an abelian Singer groups exists. An infinite family was discovered by Thas [20, 21]. His construction is based on *PG-reguli* which are defined as follows. Let $n \geq 2$ be an integer and let q be a prime power. By PG(n,q) we denote the desarguesian projective geometry of dimension n over \mathbb{F}_q . Let m < n and let \mathcal{R} be a set of pairwise disjoint m-dimensional subspaces of $\Pi = PG(n,q)$. Then \mathcal{R} is called a PG-regulus if there is a constant $\alpha > 0$ such that the following condition is satisfied.

If U is any m + 1-dimensional subspace of PG(n, q) and an element V of \mathcal{R} is a subspace of U, then U has a point in common with exactly α elements of $\mathcal{R} \setminus \{V\}$.

Given such a PG-regulus \mathcal{R} , a partial geometry can be constructed as follows. Consider Π as embedded in $\Sigma = \mathrm{PG}(n+1,q)$. Let \mathcal{P} be the set of points of Σ which are not in Π and let \mathcal{B} be the set of all m + 1-dimensional subspaces of Σ which intersect Π in an element of \mathcal{R} . Let \mathcal{G} be the geometry with point set \mathcal{P} , line set \mathcal{B} and incidence given by the incidence of Σ . It is straightforward to check that \mathcal{G} is a $\mathrm{pg}(q^{m+1}, |\mathcal{R}|, \alpha)$. Furthermore, the group of elations of Σ with axis Π is a regular automorphism group of \mathcal{G} .

Let r be any positive integer. Denniston [8] constructed maximal $(2^{r+k} - 2^r + 2^k, 2^k)$ -arcs in PG(2, 2^r) for k = 1, ..., r. Such an arc \mathcal{O} is a set of $2^{r+k} - 2^r + 2^k$ points of PG(2, 2^r) which meets every line of PG(2, 2^r) in either 0 or 2^k points. Thus \mathcal{O} is a PG-regulus in PG(2, 2^r) with $\alpha = 2^k - 1$. Hence the construction of Thas shows that for every positive integer r and k = 1, ..., r, there is a pg $(2^r, 2^{r+k} - 2^r + 2^k, 2^k - 1)$ with an abelian Singer group.

Aside from Thas' infinite family, there are two proper partial geometries with abelian Singer groups known: a pg(6, 6, 2) constructed by Van Lint and Schrijver [13] and a pg(9, 21, 2)discovered by Mathon [6]. The partial geometry of Van Lint and Schrijver is of rigid type. To our knowledge, all other known proper partial geometries with Singer groups are of spread type. In particular, no proper partial geometry of mixed type is known.

All known proper partial geometries Π with an abelian Singer group G which are different from the Van Lint-Schrijver geometry have the following properties.

- G is elementary abelian.
- Π is of spread type.

The main thrust of this paper is to investigate whether these two properties must hold for all partial geometries with abelian Singer groups different from the Van Lint-Schrijver geometry.

Some interesting results on this problem are known already: the order of an abelian Singer group of a partial geometry of spread type must be a prime power [17, Thm. 3.6]. This result was strengthened in [9, Thm. 2.5]: Every partial geometry of spread type is isomorphic to a partial geometry obtained by Thas' construction (see above). However, note that this is not a complete classification since PG-reguli have not been classified.

2 Partial Geometries with Singer groups and their Partial Difference Sets

Let G be a Singer group of a partial geometry. As usual, we identify G with the point set of the geometry and let G act by right translation. An element x of G corresponds to the automorphism of the geometry induced by $G \to G, g \mapsto gx$. The G-stabilizer of a line L is denoted by $\operatorname{Stab}_G(L)$, i.e.

$$\operatorname{Stab}_G(L) = \{ x \in G : Lx = L \}.$$

If $|\operatorname{Stab}_G(L)| = 1$ we say that L has a trivial stabilizer.

Loosely speaking, we will show that a partial geometry admitting a Singer group is equivalent to a partial difference set admitting a certain decomposition into cosets of line stabilizers. To make this connection precise, we use the language of group rings.

Let G be a multiplicatively written finite group. The identity element of G will be denoted by 1. We will always identify a subset A of G with the element $\sum_{g \in A} g$ of the integral group ring $\mathbb{Z}[G]$. In particular, we refer to group ring elements with coefficients 0 and 1 only as sets. We write b for a group ring element $b \cdot 1$, $b \in \mathbb{Z}$. For $B = \sum_{g \in G} b_g g \in \mathbb{Z}[G]$ and $r \in \mathbb{Z}$ we write $B^{(r)} := \sum_{g \in G} b_g g^r$ and $|B| := \sum_{g \in G} b_g$. We call $\{g \in G : b_g \neq 0\}$ the support of B. When we write $A \subset B$ for $A, B \in \mathbb{Z}[G]$, this means that the support of A is contained in the support of B. A group homomorphism $G \to H$ is always assumed to be extended to a homomorphism $\mathbb{Z}[G] \to \mathbb{Z}[H]$ by linearity. For $A = \sum_{g \in G} a_g g, B = \sum_{g \in G} b_g g$ and a positive integer n we write $A \equiv B \mod n$ if $a_g \equiv b_g \mod n$ for all $g \in G$.

Denote the order of G by v. A k-subset D of G is called a (v, k, λ, μ) partial difference set in G if the multiset

$$\{gh^{-1}: g, h \in D\}$$

contains each nonidentity element of D with multiplicity λ and each nonidentity element in $G \setminus D$ with multiplicity μ . Throughout this paper, we only consider nonempty partial difference sets, i.e., we assume k > 0. We call a partial difference set D trivial if $D \cup \{1\}$ or $(G \setminus D) \cup \{1\}$ is a subgroup of G. A partial difference set D with $D = D^{(-1)}$ is called reversible. A partial difference set is called regular if it is reversible and it does not contain the identity element. In this paper, we only consider regular partial difference sets. In the group ring language, partial difference sets can be characterized as follows.

Result 2 [15, Thm. 1.3] Let D be a k-subset of a group G of order v such that D does not contain the identity element. Then D is a (v, k, λ, μ) partial difference set in G if and only if in $\mathbb{Z}[G]$ the following equation holds.

$$DD^{(-1)} = (k - \mu) + (\lambda - \mu)D + \mu G.$$
 (1)

Remark 3 Note that applying "(-1)" to both sides of (1) yields $(\lambda - \mu)D = (\lambda - \mu)D^{(-1)}$. Hence every partial difference set with $\lambda \neq \mu$ is reversible. This well known observation is important since, in the abelian case, it allows us to determine the character values of D explicitly, see Result 13. **Theorem 4** Let s, t, α be positive integers and let G be a finite group. The following statements are equivalent.

(i) There is a partial geometry $pg(s+1, t+1, \alpha)$ admitting G as a Singer group.

(ii) There are a set \mathcal{U} of subgroups of G and subsets R_U of G, $U \in \mathcal{U}$, satisfying the following conditions.

- $1 \in R_U$ for all $U \in \mathcal{U}$.
- $|U||R_U| = s + 1$ for all $U \in \mathcal{U}$.
- The element

$$D = -(t+1) + \sum_{U \in \mathcal{U}} R_U U R_U^{(-1)}$$
(2)

of $\mathbb{Z}[G]$ is a partial difference set in G with parameters

$$v = (s+1)(st+\alpha)/\alpha,$$

$$k = s(t+1),$$

$$\lambda = s + (\alpha - 1)t - 1,$$

$$\mu = \alpha(t+1).$$
(3)

Proof (i) \Rightarrow (ii): Assume that a pg $(s + 1, t + 1, \alpha)$ with an abelian Singer group G exists. Let L_1, \dots, L_{t+1} be the lines which contain 1. By [17, Thm. 2.3], the set

$$D = -(t+1) + \sum_{i=1}^{t+1} L_i$$

is a partial difference set in G with parameters (3). We have to show that D can be written in the form (2).

Let L be any line containing 1 and let $U = \operatorname{Stab}_G(L)$. Then Lu = L for every $u \in U$, i.e. L is a union of left cosets of U, say

$$L = \sum_{i=1}^{r} g_i U$$

where $g_i \in L$ and r|U| = s + 1. Since L contains 1, we can assume that one of the g_i 's is 1. Note that a line $Lg, g \in G$, contains 1 if and only if $g^{-1} \in L$. Hence the lines through 1 which are in the same G-orbit as L are exactly $Lg^{-1}, g \in L$. Hence the set

$$\bigcup_{g \in L} Lg^{-1} = \bigcup_{i,j=1}^r g_i Ug_j^{-1}$$

is contained in *D*. Using the group ring notation and letting $R_U = \sum_{i=1}^r g_i$, this means that $-r + R_U U R_U^{(-1)}$ is contained in *D*. This shows that *D* has the form (2).

(ii) \Rightarrow (i): Assume that *D* defined by (2) is a partial difference set in *G* with the given parameters. In particular, this implies that *D* is a *set*, i.e., has coefficients 0 and 1 only. We

have to show that a $pg(s + 1, t + 1, \alpha)$ with G as a Singer group exists. We take G as the point set of the geometry and

$$\{R_U Ug: U \in \mathcal{U}, g \in G\}$$

as the line set.

We first show that two lines $R_U Ug$ and $R_W Wh$, $U, W \in \mathcal{U}$, $g, h \in G$, are identical only if U = W and Ug = Wh. Assume $R_U Ug = R_W Wh$. Since R_U and R_W contain 1, this implies $gh^{-1} \in R_W W$ and $hg^{-1} \in R_U U$. Hence $gh^{-1} \in R_W W \cap UR_U^{(-1)}$. If $g \neq h$ and $U \neq W$, then this would imply that $gh^{-1} \neq 1$ has coefficient ≥ 2 in D, a contradiction. Thus g = h or U = W. But g = h and $U \neq W$ is not possible since then $R_U U = R_W W$ and every nonidentity element of $R_U U$ would have coefficient ≥ 2 in D. This shows U = W. Hence $R_U Ug = R_U Uh$. This implies $gh^{-1} \in R_U U$, say $gh^{-1} = ru$ with $r \in R_U$, $u \in U$. Thus $R_U U = R_U Uhg^{-1} = R_U Uu^{-1}r^{-1} = R_U Ur^{-1}$. If $r \neq 1$, then there would be nonidentity elements with coefficient ≥ 2 in $R_U UR_U^{(-1)}$, a contradiction. Hence r = 1 and $gh^{-1} = u$. This shows Ug = Uh. In summary, we have shown that two lines $R_U Ug$ and $R_W Wh$, $U, W \in \mathcal{U}, g, h \in G$, are identical only if U = W and Ug = Wh.

It is obvious that every line has exactly s + 1 points. Now let $h \in G$ be any point. We have to show that there are exactly t + 1 lines through h. For each $U \in \mathcal{U}$ and every $r \in R_U$ there is exactly one right coset Ug of U such that $h \in rUg$. Hence, for every $U \in \mathcal{U}$, there are exactly $|R_U|$ lines $R_U Ug$ which contain h. Thus the total number of lines containing his $\sum_{U \in \mathcal{U}} |R_U|$. On the other hand, counting the number of elements of D gives

$$s(t+1) = k = -(t+1) + \sum_{U \in \mathcal{U}} |R_U|^2 |U| = -(t+1) + (s+1) \sum_{U \in \mathcal{U}} |R_U|$$

Hence $\sum_{U \in \mathcal{U}} |R_U| = t + 1$. This shows that there are exactly t + 1 lines through each point.

We now show that all lines containing 1 are contained in $D \cup \{1\}$. Let $1 \in R_U Ug, U \in \mathcal{U}$, $g \in G$. Then $g^{-1} \in R_U U$, say $g^{-1} = ru$, $r \in R_U$, $u \in U$. Hence $R_U Ug = R_U Uu^{-1}r = R_U Ur \subset R_U UR_U^{(-1)}$ is contained in $D \cup \{1\}$. This shows that all lines containing 1 are contained in $D \cup \{1\}$.

To show that any two lines intersect in at most one point, assume that $|L \cap M| \ge 2$ for distinct lines L, M. Choose $g \in L \cap M$. Then Lg^{-1} and Mg^{-1} are distinct lines containing 1 which contain a further common point, say h. But then h has coefficient ≥ 2 in D, a contradiction.

It remains to show that for every line L and every point g not on L, there are exactly α lines through g which meet L. First let L be a line containing 1, i.e., a line contained in $D \cup \{1\}$. We claim that

$$DL = sL + \alpha(G - L). \tag{4}$$

For the proof of (4), let

$$T = [(D - s + \alpha)L]^{(-1)}[(D - s + \alpha)L].$$

Note that $D = D^{(-1)}$ and

$$D^{2} = \alpha(t+1)G + (s - \alpha - t - 1)D + (t+1)(s - \alpha)$$

by Result 2. We compute

$$T = L^{(-1)}(D + \alpha - s)(D + \alpha - s)L$$

= $L^{(-1)} \left[D^2 + 2(\alpha - s)D + (\alpha - s)^2 \right] L$
= $L^{(-1)} \left[\alpha(t+1)G + (\alpha - s - t - 1)D + (t + s - \alpha + 1)(s - \alpha) \right] L.$

The coefficient of 1 in $L^{(-1)}GL = |L|^2 G$ is $|L|^2 = (s+1)^2$, and the coefficient of 1 in $L^{(-1)}L$ is |L| = s+1. We also need to compute the coefficient of 1 in $L^{(-1)}DL$. Since L is a line, we have $L = R_U U r^{-1}$ for some $U \in \mathcal{U}$, $r \in R_U$. The coefficient of 1 in $L^{(-1)}DL$ is the number of solutions of

$$1 = (r_1 u_1 r^{-1})^{-1} d(r_2 u_2 r^{-1}), \qquad r_1, r_2 \in R_U, \ d \in D, u_1, u_2 \in U,$$

i.e. of

$$d = r_1 u_1 u_2^{-1} r_2^{-1}, \qquad r_1, r_2 \in R_U, \ d \in D, u_1, u_2 \in U.$$
(5)

By (2) and since D has coefficients 0 and 1 only, there are exactly |U| solutions of (5) if $d \in R_U U R_U^{(-1)}$ and $d \neq 1$, and no solutions otherwise. Note that the number of nonidentity elements in $R_U U R_U^{(-1)}$ is $|R_U U R_U^{(-1)}| - |R_U|$. Hence the coefficient of 1 in $L^{(-1)}DL$ is

$$(|R_U U R_U^{(-1)}| - |R_U|)|U| = (|R_U||U|)^2 - (|R_U||U|) = (s+1)^2 - (s+1) = s(s+1).$$

By what we have shown, the coefficient of 1 in T is

$$\alpha(t+1)(s+1)^2 + (\alpha - s - t - 1)s(s+1) + (t + s - \alpha + 1)(s - \alpha)(s+1)$$

= $\alpha(s+1)(st + \alpha).$

Write $(D + \alpha - s)L = \sum_{g \in G} a_g g$ with $a_g \in \mathbb{Z}$. Then

$$\sum_{g \in G} a_g = |D + \alpha - s||L| = (k + \alpha - s)(s + 1) = (s + 1)(st + \alpha)$$

The coefficient of 1 in T is $\sum_{q \in G} a_q^2$. Hence

$$\sum_{g \in G} a_g^2 = \alpha(s+1)(st+\alpha).$$

Since $|G| = (s+1)(st+\alpha)/\alpha$, this implies $a_g = \alpha$ for all $g \in G$ and hence

$$(D + \alpha - s)L = \alpha G.$$

This proves (4).

Now let g be any element such that Lg is a line not containing 1. Then $g^{-1} \notin L$ and by (4) the coefficient of g^{-1} in in DL is α . But this coefficient equals $|Lg \cap D|$, so $|Lg \cap D| = \alpha$. Hence there are exactly α lines containing 1 which intersect Lg.

Now let g be any point and let L be any line not containing g. Then Lg^{-1} does not contain 1. By what we have shown, there are exactly α lines trough 1 meeting Lg^{-1} . Hence there are exactly α lines containing g and intersecting L. Q.E.D.

Definition 5 We call the set D from Theorem 4 a geometric partial difference set. Any regular partial difference set with parameters (3) for positive integers s, t, α will be called *pseudogeometric*.

Lemma 6 Let D be a partial difference set corresponding to a proper partial geometry. Then D is nontrivial.

Proof By [15, Prop. 1.2], a regular (v, k, λ, μ) partial difference set is nontrivial if and only if

$$-\sqrt{\Delta} < \lambda - \mu < \sqrt{\Delta} - 2 \tag{6}$$

where $\Delta = (\lambda - \mu)^2 + 4(k - \mu)$. Since *D* has parameters (3), we get $\lambda - \mu = s - t - \alpha - 1$ and $\sqrt{\Delta} = s + t - \alpha + 1$. Since the partial geometry is proper, we have $s > \alpha$ and t > 0. This implies (6). Q.E.D.

Corollary 7 Using the notation of Theorem 4, let $L = R_U U$ be a line of the partial geometry admitting G as a Singer group. Then

$$\operatorname{Stab}_G(L) = U.$$

Furthermore, if U is a normal subgroup of G, then $|U| \in \{1, s+1\}$.

Proof Since $L = R_U U$, we have $U \subset \operatorname{Stab}_G(L)$. Assume that there is $g \in \operatorname{Stab}_G(L) \setminus U$. Then $R_U U g^{-1} = R_U U g = R_U U$ and hence $g^{-1} = ru$ for some $r \in R_U$, $u \in U$. Note $r \notin U$. But then $R_U U = R_U U g = R_U U u^{-1} r^{-1} = R_U U r^{-1}$ which in view of (2) implies that every element of $R_U U$ has coefficient ≥ 2 in D, a contradiction. This shows $\operatorname{Stab}_G(L) = U$.

If U is a normal subgroup of G and $|U| \notin \{1, s+1\}$, then there is a nonidentity element of G with coefficient ≥ 2 in $R_U U R_U^{(-1)} = R_U R_U^{(-1)} U$, contradiction. Q.E.D.

Since we are mainly interested in the case of *abelian* Singer groups, we state this case separately. The following follows directly from Theorem 4 and Corollary 7.

Corollary 8 Let s, t, α be positive integers and let G be a finite abelian group. Then following statements are equivalent.

(i) There is a partial geometry $pg(s+1,t+1,\alpha)$ admitting G as a Singer group.

(ii) There are a set \mathcal{U} of subgroups of order s + 1 of G and a set \mathcal{L} of (s + 1)-subsets of G such that

$$D = -(t+1) + \sum_{U \in \mathcal{U}} U + \sum_{L \in \mathcal{L}} LL^{(-1)}$$
(7)

is a partial difference set in G with parameters (3).

Notation 9 We call the elements of \mathcal{U} in Corollary 8 subgroup lines. For $L \in \mathcal{L}$ all the sets Lg^{-1} , $g \in L$, are distinct lines of the geometry which pass through 1. We call these lines orbit lines.

The following observation is useful.

Lemma 10 Orbit lines do not contain any elements of order 2.

Proof Let Lg^{-1} be an orbit line, $L \in \mathcal{L}$, $g \in L$. Assume that Lg^{-1} contains an element h of order 2, say $h = lg^{-1}$ with $l \in L$. But since $h = h^{-1} = gl^{-1}$, we conclude that h has coefficient ≥ 2 in $LL^{(-1)}$ and hence in D, a contradiction. Q.E.D.

3 Partial Difference Sets and Characters

Complex characters of abelian groups are an indispensable tool for the study of partial difference sets. Let G be a finite abelian group. We denote the group of complex characters of G by G^* . The character sending all $g \in G$ to 1 is called **trivial** and denoted by χ_0 . For a subgroup W of G, we write W^{\perp} for the subgroup of G^* consisting of all characters which are trivial on W. We will repeatedly make use of the following elementary properties of characters of finite abelian groups. For a proof, see [1, Section VI.3].

Result 11 Let G be a finite abelian group. (i) Let $D = \sum_{g \in G} d_g g \in \mathbb{C}[G]$. Then

$$d_g = \frac{1}{|G|} \sum_{\chi \in G^*} \chi(Dg^{-1})$$

for all $g \in G$ (Fourier Inversion Formula). In particular, two elements of $\mathbb{C}[G]$ are equal if and only if all their character values are equal.

(ii) If $\chi \in G^*$ is nontrivial on a subgroup U of G, then $\chi(U) = 0$.

(iii) If H is a subgroup of G and $A, B \in \mathbb{Z}[G]$ with $\chi(A) = \chi(B)$ for all $\chi \in G^* \setminus H^{\perp}$, then A = B + XH for some $X \in \mathbb{Z}[G]$.

(iv) G^{**} is isomorphic to G and an isomorphism $G \to G^{**}$ is given by $g \mapsto \tau_g$ where τ_g is the character of G^* defined by $\tau_g(\chi) = \chi(g), \ \chi \in G^*$.

Corollary 12 Let G be a finite abelian group, let U be a subgroup and let S be a subset of G. Then

$$|S \cap U| = \frac{|U|}{|G|} \sum_{\chi \in U^{\perp}} \chi(S).$$

Proof Let $\rho: G \to G/U$ be the canonical epimorphism. The set of characters of G/U can be identified with U^{\perp} such that $\chi(X) = \chi(\rho(X))$ for all $X \in \mathbb{Z}[G]$ and all $\chi \in U^{\perp}$. Note that $|S \cap U|$ is the coefficient of 1 in $\rho(S)$. Hence

$$|S \cap U| = \frac{1}{|G/U|} \sum_{\chi \in (G/U)^*} \chi(\rho(S)) = \frac{|U|}{|G|} \sum_{\chi \in U^{\perp}} \chi(S)$$

by Result 11(i).

Recall that a partial difference set D is called regular if $D = D^{(-1)}$ and $1 \notin D$. Part (i) of Result 11 leads to the following.

Result 13 [15, Cor. 3.3] Let G be an abelian group of order v. A k-subset D of G with $1 \notin D$ is a regular (v, k, λ, μ) partial difference set in G if and only if

$$\chi(D) = \frac{\lambda - \mu \pm \sqrt{(\lambda - \mu)^2 + 4(k - \mu)}}{2} \tag{8}$$

for every nontrivial character χ of G.

Notation 14 Result 13 indicates that the parameter $\Delta := (\lambda - \mu)^2 + 4(k - \mu)$ plays an important role in the study of regular partial difference sets. We will use this parameter throughout this paper.

An essential tool for the study of partial difference sets is *duality*. It was developed by Delsarte in his PhD thesis [7]. Let D be a regular (v, k, λ, μ) partial difference set in an abelian group G. The *dual* of D is defined as

$$D^* = \{ \chi \in G^* : \chi \neq \chi_0, \ \chi(D) = (\lambda - \mu - \sqrt{\Delta})/2 \}.$$

Delsarte [7] proved that the dual of a partial difference set again is a partial difference set. Since Delsarte's result is formulated in a different framework, we sketch a proof here for the convenience of the reader.

Result 15 [7] Let G be an abelian group and let $D \neq G \setminus \{1\}$ be a regular (v, k, λ, μ) partial difference set. Then the dual D^* is a regular $(v, k^*, \lambda^*, \mu^*)$ partial difference set in G^* with parameters

$$k^* = \frac{2k + (v-1)(\lambda - \mu + \sqrt{\Delta})}{2\sqrt{\Delta}}$$
$$\mu^* = \frac{2k + (v-1)(\lambda - \mu + \sqrt{\Delta})}{2\sqrt{\Delta}} + \frac{-v^2 + (\lambda - \mu + v - 2k + \sqrt{\Delta})^2}{4\Delta}$$
$$\lambda^* = \mu^* - \frac{\lambda - \mu + v - 2k + \sqrt{\Delta}}{\sqrt{\Delta}}$$

Proof Since $1 \notin D$, we have $\sum_{\chi \in G^*} \chi(D) = 0$ by Result 11(i). This implies

$$k + |D^*|(\lambda - \mu - \sqrt{\Delta})/2 + (v - |D^*| - 1)(\lambda - \mu + \sqrt{\Delta})/2 = 0.$$

Hence

$$|D^*| = [2k + (v - 1)(\lambda - \mu + \sqrt{\Delta})]/(2\sqrt{\Delta}) = k^*.$$

In the following, we will use the canonical isomorphism between G and $(G^*)^*$ given by $g \mapsto (G^* \to \mathbb{C}, \ \chi \mapsto \chi(g))$. In particular, for $g \in G$ and $Y = \sum_{\chi \in G^*} a_{\chi}\chi \in \mathbb{Z}[G^*]$, we write $g(Y) := \sum_{\chi \in G^*} a_{\chi}\chi(g)$. We also use the Fourier transforms

$$\begin{split} f: \mathbb{Z}[G] \to \mathbb{Z}[G^*], \ X \mapsto \sum_{\chi \in G^*} \chi(X) \chi \\ F: \mathbb{Z}[G^*] \to \mathbb{Z}[G], \ Y \mapsto \sum_{g \in G} g(Y) g. \end{split}$$

It is well known and follows easily from Result 11 that

$$F(f(X)) = vX^{(-1)}$$
 (9)

for every $X \in \mathbb{C}[G]$. By Result 13 we have

$$f(D) = k\chi_0 + \left(\frac{\lambda - \mu - \sqrt{\Delta}}{2}\right)D^* + \left(\frac{\lambda - \mu + \sqrt{\Delta}}{2}\right)(G^* - D^* - \chi_0).$$
(10)

Using $1 \notin D$, $D^{(-1)} = D$, (9), (10), and Result 11 we get

$$2vD = 2F(f(D)) = \sum_{g \in G, g \neq 1} \left[2k - \lambda + \mu - \sqrt{\Delta} - 2\sqrt{\Delta} g(D^*) \right] g.$$
(11)

Hence

$$g(D^*) = \begin{cases} \frac{2k - \lambda + \mu - \sqrt{\Delta}}{2\sqrt{\Delta}} & \text{if } g \notin D\\ \frac{-2v + 2k - \lambda + \mu - \sqrt{\Delta}}{2\sqrt{\Delta}} & \text{if } g \in D \end{cases}$$
(12)

Q.E.D.

Now the assertion follows from Result 13.

4 Results on Partial Difference Sets

In this section, we recall some basic results on partial difference sets in abelian groups and prove several new results. These tools will be very helpful in the investigation of partial geometries with abelian Singer groups in the following sections.

Let D be a regular (v, k, λ, μ) partial difference set in an abelian group G. The following parameters are usually associated with D.

$$\beta = \lambda - \mu$$

$$\Delta = (\lambda - \mu)^2 + 4(k - \mu)$$

$$\delta = \sqrt{\Delta}$$
(13)

It is known that "usually" the parameter Δ is a square, i.e. that δ is a positive integer (see [15] for the case that Δ is not a square).

Using (1) one finds the identity

$$2k = v + \beta \pm \sqrt{(v+\beta)^2 - (\Delta - \beta^2)(v-1)}.$$
(14)

In particular, $(v + \beta)^2 - (\Delta - \beta^2)(v - 1)$ is a square. By Result 15,

$$D^* = \{ \chi \in G^* : \chi \neq \chi_0, \ \chi(D) = (\beta - \delta)/2 \}.$$

is a regular $(v^*,k^*,\lambda^*,\mu^*)$ partial difference set in G^* with

$$v^{*} = v,$$

$$k^{*} = \frac{2k + (\beta + \delta)(v - 1)}{2\delta},$$

$$\beta^{*} = -\left(\frac{v - 2k + \beta + \delta}{\delta}\right),$$

$$\delta^{*} = \sqrt{(\beta^{*})^{2} + 4(k^{*} - \mu^{*})} = \frac{v}{\delta},$$

$$\mu^{*} = k^{*} - \left(\frac{(\delta^{*})^{2} - (\beta^{*})^{2}}{4}\right),$$

$$\lambda^{*} = \beta^{*} + \mu^{*}.$$
(15)

Lemma 16 Using the notation from above, if Δ is a square, the following hold.

- (a) β and δ have the same parity.
- (b) D is nontrivial if and only if $-\delta < \beta < \delta 2$.
- (c) If $D \neq G \setminus \{1\}$, then $v \equiv (2k \beta + \delta)/2 \equiv 0 \mod \delta$.
- (d) If D is nontrivial, then v, δ, δ^* have the same prime divisors.
- (e) $D^{(t)} = D$ for all t relatively prime to v.

Proof (a), (b), (d), (e) and $v \equiv 0 \mod \delta$ in (c) are well-known, see e.g. [15]. By (15), we have

$$k^* + 1 = \frac{2k - \beta + \delta}{2\delta} + \left(\frac{\delta + \beta}{2}\right)\delta^*.$$

Since k^* , δ^* are integers and β , δ have the same parity, $(2k - \beta + \delta)/2 \equiv 0 \mod \delta$. Q.E.D.

Corollary 17 Let p be a prime and let D be a regular partial difference set in an abelian group $G = H \times P$ where P is a p-group and |H| is not divisible by p. Suppose the parameter Δ is a square. Let $h \in H$. Then

$$|D \cap Ph| \equiv \begin{cases} 1 \mod (p-1) & \text{if } h \in D\\ 0 \mod (p-1) & \text{if } h \notin D. \end{cases}$$
(16)

Proof Assume $gh \in D$ where $g \in P$. Since P is a p-group, the order of g in G is a power of p, say p^a , $a \ge 0$. By Lemma 16 (e), we have $D = D^{(t)}$ for all t relatively prime to |G|. Using the Chinese remainder theorem, we conclude $g^ih \in D$ for all i relatively prime to p. The number of these elements g^ih is $(p-1)p^{a-1}$. Hence $D \cap Ph$ can be decomposed into sets of cardinality divisible by p-1 and possibly the single element set $\{h\}$. The latter set occurs in the decomposition if and only if $h \in D$. Q.E.D.

Partial difference sets in abelian groups G have the amazing property that in many cases certain subgroups of G also contain partial difference sets. This "sub-difference set property" was discovered in [19, 16] and is one of the major tools for the investigation of partial difference sets. We quote this result in the form given in [15, Thm. 7.1].

Result 18 Let D be a nontrivial regular (v, k, λ, μ) partial difference set in an abelian group G. Suppose Δ is a square. Let N be a subgroup of G such that |N| and |G/N| are coprime and |G/N| is odd. Let

$$\pi := (|N|, \delta) \quad and \quad \theta := \left\lfloor \frac{\beta + \pi}{2\pi} \right\rfloor.$$

Then $D \cap N$ is a regular (v', k', λ', μ') partial difference set in N with v' = |N| and

$$\beta' = \lambda' - \mu' = \beta - 2\pi\theta \Delta' = (\beta')^2 + 4(k' - \mu') = \pi^2.$$
(17)

Remark 19 Note that the parameters k', λ' , μ' of the partial difference set $D \cap N$ can be expressed in terms of v', β , π , and θ using (14) and (17).

Lemma 20 Assume that a nontrivial regular (v, k, λ, μ) partial difference set exists. If Δ is a square, then $k^2 + k \ge 2(v - 1)$.

Proof For a nontrivial partial difference set, $\mu \ge 1$. By [18, Theorem 5.1], μ must be even if Δ is a square. Hence $\mu \ge 2$. By counting the number of quotients $gh^{-1} \in G \setminus (D \cup \{1\})$, $g, h \in D$, we obtain $k^2 - k \ge \mu(v - k - 1)$ and hence $k^2 + k \ge 2(v - 1)$. Q.E.D.

The following is an improved version of [18, Theorem 2.2]. For a prime p and positive integers b, z, we write $p^{b}||z$ if p^{b} divides z and p^{b+1} does not divide z.

Theorem 21 Let D be a regular (v, k, λ, μ) partial difference set in an abelian group G. Suppose $D \neq G \setminus \{1\}$ and Δ is a square. If p is a prime divisor of v such that $p^m || v$ and $p^r || \delta$, then

$$k \le \frac{\mu(p^m - 1) + \xi}{p^r - 1}$$

where

$$\xi = \begin{cases} 0 & \text{if } \beta \le -p^r, \\ (\beta + p^r)^2/4 & \text{if } -p^r < \beta \le 2p^m - p^r - 2, \\ (\beta - p^m + p^r + 1)(p^m - 1) & \text{if } \beta > 2p^m - p^r - 2. \end{cases}$$

Proof For $\chi \in G^*$,

$$\chi(D) - \left(\frac{\beta - \delta}{2}\right) = \begin{cases} (2k - \beta + \delta)/2 & \text{if } \chi \text{ is trivial} \\ 0 & \text{or } \delta & \text{otherwise} \end{cases}$$
$$\equiv 0 \mod \delta.$$

Let P be the Sylow p-subgroup of G and $\rho: G \to G/P$ the natural epimorphism. Then

$$\rho(D) = a + p^r \sum_{g \in G/P \setminus \{1\}} b_g g$$

where a, b_g are integers and $0 \le a \le p^m - 1$. The result follows by the same arguments as in the proof of [18, Theorem 2.2]. Q.E.D.

In certain cases, it is possible to strengthen the bound on k from Theorem 21 considerably by a finer analysis. The following is a result of this type which will be very helpful for the study of pseudogeometric partial difference sets in the next section.

Theorem 22 Assume that there is a nontrivial regular (v, k, λ, μ) partial difference set Din an abelian group G such that Δ is a square and $\beta = \lambda - \mu \leq 0$. Let p be an odd prime dividing v and let m, r be positive integers such that $p^m || v$, and p^r divides each of k, δ , and β . Then

$$(p^{r+1} - p^r - 1)k \le \mu(p^m - 1) + \frac{1}{2} \left[(p-2)p^{2r} \left(\beta + \delta + \frac{2k - \beta - \delta}{p^m} \right) \right].$$

Proof Write $G = P \times H$ with $|P| = p^m$ and (p, |H|) = 1. By Result 13 we have $\chi(D) = (\beta \pm \delta)/2$ and hence $\chi(D) \leq (\beta + \delta)/2$ for all nontrivial characters χ of G. Using Corollary 12, we get

$$|D \cap H| = \frac{1}{p^m} \sum_{\chi \in H^\perp} \chi(D)$$

$$\leq \frac{1}{p^m} \left(k + \frac{(p^m - 1)(\beta + \delta)}{2} \right)$$

$$= \frac{1}{2} \left(\beta + \delta + \frac{2k - \beta - \delta}{p^m} \right).$$
(18)

Now let $\rho: G \to G/P$ be the canonical epimorphism. Applying ρ to (1) yields

$$\rho(D)\rho(D)^{(-1)} = \mu p^m(G/P) + \beta \rho(D) + k - \mu.$$
(19)

Let C be the coefficient of the identity in $\rho(D)\rho(D)^{(-1)}$. Since $\beta \leq 0$ we have

$$C \le \mu(p^m - 1) + k \tag{20}$$

by (19). From the assumptions, we have $\chi(D) \equiv 0 \mod p^r$ for all characters χ of G. Since |G/P| is not divisible by p, this implies

$$\rho(D) \equiv 0 \bmod p^r \tag{21}$$

Now let $h \in H$ be arbitrary. Corollary 17 yields $|D \cap Ph| \equiv 1 \mod (p-1)$ if $h \in D$ and $|D \cap Ph| \equiv 0 \mod (p-1)$ if $h \notin D$. If $|D \cap Ph| \equiv 1 \mod (p-1)$, then by (21) we have $|D \cap Ph| = p^r + (p-1)p^r u$ for some u. Let $X = \{Ph : h \in D \cap H\}$. By what we have shown, we can write

$$\rho(D) = p^r X + (p-1)p^r X_1 + (p-1)p^r Y$$
(22)

where $X, X_1, Y \in \mathbb{Z}[G/P]$ have nonnegative coefficients, the support of X_1 is contained in X and the support of Y is disjoint from X. Now assume that some $g \in X$ has coefficient $c \geq 0$ in X_1 . Then the coefficient of g in $\rho(D)$ is $p^r[1 + c(p-1)]$ and thus the contribution of this coefficient to C is

$$p^{2r}[1+c(p-1)]^2 \ge p^{2r}+cp^{2r}(p-1)^2.$$

Hence the contribution of $p^r X + (p-1)p^r X_1$ to C is at least

$$p^{2r}|X| + p^{2r}(p-1)^2|X_1|.$$

Since $|X_1| + |Y| = (k - p^r |X|) / [(p - 1)p^r]$ we get

$$C \ge -(p-2)p^{2r}|X| + (p-1)p^rk$$
(23)

from (22). By (18) we have

$$|X| \le \frac{1}{2} \left(\beta + \delta + \frac{2k - \beta - \delta}{p^m} \right).$$
(24)

Combining (20), (23) and (24) gives the assertion.

Theorem 23 There are no regular (v, k, λ, μ) partial difference sets with parameters satisfying $v = zw^2$, $\Delta = w^2$ and $\beta = w - 6$ where w and z are any integers with $z \ge w \ge 4$.

Proof Suppose there exists such a partial difference set D in a group G. Since $-\sqrt{\Delta} < \beta < \sqrt{\Delta} - 2$, the partial difference set is nontrivial by Lemma 16 (b). By (14) we have

$$k = \frac{1}{2} \left(v + \beta \pm \sqrt{(v + \beta)^2 - (\Delta - \beta^2)(v - 1)} \right)$$

= $\frac{1}{2} \left(zw^2 + w - 6 \pm w\sqrt{z^2w^2 - 10zw + 24z + 1} \right)$

and $(v + \beta)^2 - (\Delta - \beta^2)(v - 1)$ is a square.

We first consider the case $z \ge 5$. Let $X = (10zw - 24z - 1)/(z^2w^2)$. Note that $0 < X < 10/(zw) \le 1/2$. By Taylor's theorem we have

$$\sqrt{1-X} = 1 - \frac{1}{2}X - \frac{1}{8}(1-X_1)^{-3/2}X^2,$$

Q.E.D.

for some X_1 with $0 < X_1 < X$. Note that $zw^2X = 10w - 24 - 1/z < 10w - 24$ and X < 10/(zw). Also recall $z \ge 4$. Hence

$$w\sqrt{z^2w^2 - 10zw + 24z + 1}$$

= $zw^2\sqrt{1-X}$
> $zw^2\left[1 - \frac{1}{2}X - \frac{1}{8}\left(1 - \frac{1}{2}\right)^{-3/2}X^2\right]$
> $zw^2 - \frac{1}{2}(10w - 24) - \frac{1}{\sqrt{8}}\left(\frac{10}{zw}\right)(10w - 24)$
> $zw^2 - 5w + 12 - \frac{100}{z\sqrt{8}}$
> $zw^2 - 5w.$

So either k < 3w or k > v - 2w - 3. If k < 3w, then by Lemma 20, we have

$$z \le \frac{9}{2} + \frac{3}{2w} + \frac{1}{w^2} < 5,$$

a contradiction. If k > v - 2w - 3, then v - k - 1 < 2w + 2 and we have the same result by applying Lemma 20 to $G \setminus (D \cup \{1\})$. Finally, for z = w = 4, we have $(v + \beta)^2 - (\Delta - \beta^2)(v - 1) = z^2w^2 - 10zw + 24z + 1 = 193$ which is not a square, a contradiction. Q.E.D.

Theorem 24 Assume that there exists a regular partial difference set D in an abelian group with parameters $v = u^3$, $\Delta = (3u)^2$ and $\beta = -u - 6$ where u is a positive integer. Then u = 6 or $u = 3^n$ with $n \ge 1$.

Proof Since v and Δ have the same odd prime divisors by Lemma 16 (d), we have $u = 3^n w$ where $n, w \ge 1$ and gcd(3, w) = 1. First assume $w \ge 4$. We apply Result 18 with $|N| = w^3$. Then $\pi = w$ and

$$\theta = \left\lfloor \frac{\beta + \pi}{2\pi} \right\rfloor = \left\lfloor -\frac{3^n - 1}{2} - \frac{3}{w} \right\rfloor = -\frac{3^n + 1}{2}$$

Hence, by Result 18, there exists a partial difference set with parameters $v' = w^3$, $\Delta' = w^2$ and $\beta' = \beta - 2\pi\theta = w - 6$. But this is impossible by Theorem 23. So w = 1 or 2.

It remains to show that n = 1 if w = 2. Thus assume w = 2 and $n \ge 2$. Write $x = 3^n$. We use (13) and (14) to calculate the parameters of D and obtain the following two possible cases.

v	k	λ	μ	β	Δ
$8x^3$	$8x^2 + 2x - 3$	6x	8x + 6	-2x - 6	$36x^2$
$8x^3$	$8x^3 - 8x^2 - 4x - 3$	$8x^3 - 16x^2$	$8x^3 - 16x^2 + 2x + 6$	-2x - 6	$36x^2$

For the first case, Lemma 21 implies $k \leq 7\mu$ contradicting n = 2. For the second case, the parameters of the complementary partial difference set $G \setminus (D \cup \{1\})$ are as follows.

v	k	λ	μ	β	Δ
$8x^3$	$8x^2 + 4x + 2$	10x + 10	8x + 6	2x + 4	$36x^2$

We apply Lemma 21 with p = 2. Note that $\xi = (\beta - 8 + 2 + 1)(8 - 1) = 7(\beta - 5)$ since $\beta \ge 2 \cdot 3^2 + 4 = 22$. Hence $k \le 7(\mu + \beta - 5)$ by Lemma 21, i.e. $8x^2 + 4x + 2 \le 7(10x + 5)$. This implies x < 9 and hence n < 2, a contradiction. Q.E.D.

5 Pseudogeometric Partial Difference Sets

In this section, we obtain several new results on pseudogeometric partial difference sets. First let us fix some notation which we will use in the rest of this section. Let D be a pseudogeometric partial difference set in an abelian group G. Recall that the parameters of D are given by (3). Using the notation of Section 4, we have

$$v = (s+1)(st+\alpha)/\alpha,$$

$$k = s(t+1),$$

$$\lambda = s + (\alpha - 1)t - 1,$$

$$\mu = \alpha(t+1),$$

$$\beta = \lambda - \mu = s - \alpha - t - 1,$$

$$\delta = \sqrt{\beta^2 + 4(k-\mu)} = s - \alpha + t + 1.$$
(25)

Furthermore, by (15), the dual partial difference set D^* has parameters

$$v^* = \frac{(s+1)(st+\alpha)}{\alpha},$$

$$k^* = \frac{s(s-\alpha+1)(st+\alpha)}{\alpha(s-\alpha+t+1)},$$

$$\mu^* = \frac{(s+1)(s-\alpha)(s-\alpha+1)(st+\alpha)}{\alpha(s-\alpha+t+1)^2},$$

$$\delta^* = \frac{(s+1)(st+\alpha)}{\alpha(s-\alpha+t+1)},$$

$$\beta^* = -\frac{(s-2\alpha+1)(st+\alpha)}{\alpha(s-\alpha+t+1)}.$$

(26)

Note that $D = G \setminus \{1\}$ if and only if k = v - 1, i.e., if $\alpha = s + 1$.

Theorem 25 Let $D \neq G \setminus \{1\}$ be a pseudogeometric partial difference set with parameters (25) in an abelian group G. Then

$$(s+1)(t+1) \equiv 0 \mod \delta. \tag{27}$$

Furthermore, let p be a prime divisor of δ and define m, r by $p^m ||v|$ and $p^r ||\delta$.

(i) If $\beta < 0$, then

$$\frac{s-1}{\alpha} < \frac{p^m - 1}{p^r - 1}.$$
(28)

(ii) If $\beta \leq -p^r$, then

$$\frac{s}{\alpha} \le \frac{p^m - 1}{p^r - 1}.\tag{29}$$

(iii) If $\beta < 0$ and $\beta^* < 0$, then

$$\frac{\delta}{p^r} < \frac{(s+1)(s-\alpha)}{s-\alpha-1}.$$
(30)

(iv) If $\beta \leq -p^r$ and $\beta^* \leq -p^{m-r}$, then

$$\frac{\delta}{p^r} \le s+1 \quad and \quad \frac{v}{p^m} \le (s+1)^2. \tag{31}$$

Proof We get (27) directly from Lemma 16 (c). For (ii), if $\beta \leq -p^r$, applying Theorem 21 to D yields $s/\alpha \leq (p^m - 1)/(p^r - 1)$. For (i), suppose $\beta < 0$. Then by Theorem 21,

$$s \le \alpha \left(\frac{p^m - 1}{p^r - 1}\right) + \frac{\xi}{(t+1)(p^r - 1)}$$

where $0 \le 4\xi \le (\beta + p^r)^2 \le p^{2r}$. Since $\beta = s - \alpha - t - 1 < 0$, $s - \alpha < t + 1$. Thus $p^r \le \delta = s - \alpha + t + 1 < 2(t + 1)$ and

$$0 \le \frac{\xi}{(t+1)(p^r-1)} < \frac{p^r}{2(p^r-1)} \le 1.$$

Now we first study (iv), i.e. $\beta \leq -p^r$ and $\beta^* \leq -p^{m-r}$. Note that $p^{m-r} ||\delta^*$. Applying Theorem 21 to D^* yields

$$\frac{s\delta}{(s-\alpha)(s+1)} \le \frac{p^m - 1}{p^{m-r} - 1}.$$
(32)

Combining (29) and (32), we get

$$\left(\frac{p^r}{\delta}\right)\frac{(s-\alpha)(s+1)}{s} \ge \frac{p^m - p^r}{p^m - 1} = 1 - \frac{p^r - 1}{p^m - 1} \ge 1 - \frac{\alpha}{s}.$$

Hence $\delta/p^r \leq s+1$ and

$$v = \frac{(s+1)(st+\alpha)}{\alpha}$$

= $(s+1)\left[\frac{s\delta - (s+1)(s-\alpha)}{\alpha}\right]$
= $(s+1)\left[\frac{s}{\alpha}(\delta - s - 1) + s + 1\right]$
 $\leq (s+1)\left[\frac{p^m - 1}{p^r - 1}\{p^r(s+1) - s - 1\} + s + 1\right]$
= $(s+1)^2p^m$.

This completes the proof of (31).

Finally, for (iii), we have $\beta < 0$ and $\beta^* < 0$. Define $A = (st + \alpha)/(s - \alpha + t + 1)$ and $B = (s - \alpha + 1)(st + \alpha)/[\alpha(s - \alpha + t + 1)]$. Note that $\beta^* = A - B$ and $\delta^* = A + B$. Applying Theorem 21 to D^* yields

$$s \le \frac{(s+1)(s-\alpha)}{\delta} \left(\frac{p^m - 1}{p^{m-r} - 1}\right) + \frac{\xi^*}{B(p^{m-r} - 1)}$$

where $0 \leq 4\xi^* \leq p^{2(m-r)}$. By the same argument as the proof of (i), we get

$$\frac{(s-1)\delta}{(s-\alpha)(s+1)} < \frac{p^m - 1}{p^{m-r} - 1}.$$
(33)

Combining (28) and (33), we get (30)

Corollary 26 Let D be a pseudogeometric partial difference set with parameters (25) in an abelian group G. Let p be a prime divisor of δ and define m, r by $p^m ||v|$ and $p^r ||\delta$. If $s > 2\alpha - 1$, $\beta < 0$ and p does not divide s + 1, then

$$\delta/p^r \le s+1$$
 and $v/p^m \le (s+1)^2$.

Proof Since $\alpha \neq s + 1$, we have $D \neq G \setminus \{1\}$. Hence $(s+1)(t+1) \equiv 0 \mod \delta$ by (27). This implies $t+1 \equiv 0 \mod p^r$ and $\beta = \delta - 2(t+1) \equiv 0 \mod p^r$. So $\beta \leq -p^r$. Note that $\beta^* = -(s-2\alpha+1)v/[\delta(s+1)] < 0$ since $s > 2\alpha - 1$. On the other hand, p^{m-r} divides β^* and hence $\beta^* \leq -p^{m-r}$. Now the assertion follows from Theorem 25. Q.E.D.

In Section 6 we will show that most geometric partial difference sets satisfy the condition $t = x(s+1) + \alpha$ for some positive integer x. Note that in this case, the parameters of the partial difference set take the following form.

$$v = (s+1)^{2}(sx+\alpha)/\alpha,$$

$$\delta = (s+1)(x+1),$$

$$k = s[(s+1)x+\alpha+1],$$

$$\beta = -(s+1)(x-1) - 2\alpha - 2,$$

$$\mu = \alpha[(s+1)x+\alpha+1].$$

(34)

Moreover, if $t = x(s+1) + \alpha$ the parameters of the dual partial difference sets are given by

$$v^* = (s+1)^2 (sx+\alpha)/\alpha,$$

$$k^* = \frac{s(sx+\alpha)(s-\alpha+1)}{\alpha(x+1)},$$

$$\delta^* = \frac{(s+1)(sx+\alpha)}{\alpha(x+1)} = \frac{v}{\delta},$$

$$\beta^* = -\frac{(sx+\alpha)(s-2\alpha+1)}{\alpha(x+1)},$$

$$\mu^* = \frac{(sx+\alpha)(s-\alpha+1)(s-\alpha)}{\alpha(x+1)^2}.$$

(35)

Q.E.D.

From Theorem 22 we can derive the following restriction on partial difference sets with parameters (34).

Theorem 27 Assume that there is a pseudogeometric partial difference set with parameters (34) in an abelian group such that $s \ge 2\alpha - 1$, $x + 1 = p^r$ and $(sx + \alpha)/\alpha = p^m$ for some prime p and m > r. Then p = 2.

Proof Assume $p \ge 3$. We apply Theorem 22 to the dual of D. Note $p^m || v$ and that all of k^* , β^* , and δ^* are divisible by p^{m-r} . Also note that

$$\frac{1}{2}\left(\beta^* + \delta^* + \frac{2k^* - \beta^* - \delta^*}{p^m}\right) = p^{-r}s(s - \alpha + x + 1).$$

Furthermore,

$$(p^{m-r+1} - p^{m-r} - 1)k^* - \mu^*(p^m - 1) = (p-2)p^{2m-2r}(s - \alpha + 1)s.$$

Hence Theorem 22 implies

$$s - \alpha + 1 \le p^{-r}(s - \alpha + x + 1) = s - \alpha p^{m-r} + 1$$

and hence m = r, a contradiction.

6 General Results on Proper Partial Geometries with Abelian Singer Groups

First let us fix some notation which we will use in the rest of this section. Suppose there exists a proper partial geometry $\Pi = pg(s + 1, t + 1, \alpha)$ with an abelian Singer group G. By Corollary 8, the partial difference set D in G arising from the partial geometry has parameters (25) and its dual has parameters (26). Recall that by Corollary 8, we have

$$D = -(t+1) + \sum_{U \in \mathcal{U}} U + \sum_{L \in \mathcal{L}} LL^{(-1)}$$

and that the elements of \mathcal{U} are called subgroup lines and the elements of \mathcal{L} are called orbit lines. If there are no subgroup lines, the geometry is said to be of rigid type.

Lemma 28 For any nontrivial character χ of G,

$$\chi(D) = -(t-1) \text{ or } s - \alpha.$$

Furthermore, if $\chi(D) = -(t+1)$, then $\chi(S) = 0$ for all $S \in \mathcal{U} \cup \mathcal{L}$.

Proof The first part is the consequence of Result 13. By (4),

$$DS = (s - \alpha)S + \alpha G$$

for all $S \in \mathcal{U} \cup \mathcal{L}$. Thus, $[\chi(D) - (s - \alpha)]\chi(S) = 0$. If $\chi(D) = -(t + 1)$, then $\chi(S) = 0$. Q.E.D.

Q.E.D.

Lemma 29 Let p be a prime divisor of s + 1 such that $p^m || v$ and $p^r || (s + 1)$. Then

$$|\mathcal{U}|(p^r - 1) \le p^m - 1.$$
(36)

Proof The lemma follows because each subgroup line contains a subgroup of order p^r . Q.E.D.

The following direct consequence of Lemma 16 (c) was proved in [11].

Lemma 30 If a proper $pg(s + 1, t + 1, \alpha)$ with admitting an abelian Singer group exists, then

$$v \equiv (s+1)(t+1) \equiv 0 \mod \delta.$$

Here v and δ are given by (25).

Corollary 31 Suppose that Π is of rigid type with $s > 2\alpha - 1$. Then every prime divisor of δ must divide s + 1.

Proof Suppose there is a prime divisor p of δ such that p does not divide s + 1. Suppose $p^r || \delta$. By Corollary 26,

$$\frac{\delta}{p^r} \le s+1.$$

Recall $\delta = s - \alpha + t + 1$. Since the geometry is of rigid type, we have t + 1 = (s+1)x for some positive integer x. As $(s+1)(t+1) \equiv 0 \mod \delta$, we have $x \equiv 0 \mod p^r$ and hence $x \geq p^r$. Thus

$$\frac{s-\alpha+(s+1)x}{x} = \frac{\delta}{p^r} \le \frac{\delta}{x} \le s+1.$$

This implies $s \leq \alpha$. But this is impossible since we assumed that the partial geometry Π is proper. Q.E.D.

In the following, we investigate the case with at least two subgroup lines in more depth.

Theorem 32 Suppose that Π has at least two subgroup lines. We have the following:

(i) There exists a positive integer x such that

$$t = (s+1)x + \alpha.$$

In particular, there are at least $\alpha + 1$ subgroup lines.

(ii) The partial difference set associated with Π has parameters (34) and its dual has parameters (35). Furthermore, $sx \equiv 0 \mod \alpha$ and there exists a positive integer w such that

$$s - \alpha = (x + 1)w.$$

(iii) $(sx + \alpha)/\alpha \equiv 0 \mod (x + 1)$ and $wx \equiv 0 \mod \alpha$.

Proof (i) Let U_1 and U_2 be two subgroup lines. Then $U_1 \cap U_2 = \{1\}$ since otherwise there would be coefficients ≥ 2 in D. Thus U_1U_2 is a subgroup of G of order $(s+1)^2$. Hence $(s+1)^2$ divides $v = (s+1)(st+\alpha)/\alpha$ which implies $-t + \alpha \equiv st + \alpha \equiv 0 \mod (s+1)$. So we can write $t = (s+1)x + \alpha$ for some $x \geq 1$. Since there are exactly t+1 lines through 1 and since the number of orbit lines is divisible by s+1, the number of subgroup lines is at least $\alpha + 1$. This proves (i).

(ii) Substituting $t = (s+1)x + \alpha$ into (25), we deduce that the parameters have the form (34). Since $(s+1)^2$ divides v, we conclude that $(sx + \alpha)/\alpha$ is an integer, i.e. $sx \equiv 0 \mod \alpha$. Note that D is nontrivial by Lemma 6. Hence $\delta = (s+1)(x+1)$ divides $(2k - \beta + \delta)/2 = (s+1)(t+1)$ by Lemma 16 (c). This implies $s - \alpha \equiv 0 \mod (x+1)$.

(iii) We write x + 1 = XY where all prime factors of X are prime factors of s + 1 and gcd(Y, s+1) = 1. Since $s+1-(\alpha+1) = (x+1)w$ for an integer w, every prime factor of X is a prime factor of $\alpha + 1$. Hence, X and α are coprime. It follows that $(sx + \alpha)/\alpha \equiv 0 \mod X$. On the other hand, as x + 1 divides v, we conclude that Y divides v. Since Y and s + 1 are relatively prime, $(sx + \alpha)/\alpha \equiv 0 \mod Y$ also. As X and Y are relatively prime we have $(sx+\alpha)/\alpha \equiv 0 \mod XY$. Finally, $(sx+\alpha)/\alpha \equiv 0 \mod (x+1)$ implies $sx+\alpha \equiv 0 \mod (x+1)\alpha$. Since $sx + \alpha = [(x + 1)w + \alpha]x + \alpha = (x + 1)(wx + \alpha)$, we see that $wx \equiv 0 \mod \alpha$. Q.E.D.

Corollary 33 If Π has at least two subgroup lines, then $s > 2\alpha$.

Proof Theorem 32 (iii) implies that $(x + 1)\alpha$ divides $(sx - \alpha) - (x + 1)\alpha = x(s - \alpha)$. As $s > \alpha$, we conclude that $x(s - \alpha) \ge (x + 1)\alpha > x\alpha$. This shows $s > 2\alpha$. Q.E.D.

Corollary 34 Suppose that Π has at least two subgroup lines. If L is an orbit line in Π , then $\langle L \rangle = G$ (here $\langle L \rangle$ denotes that smallest subgroup of G containing L).

Proof If $\langle L \rangle \neq G$, then there exists a character χ of G which is trivial on $\langle L \rangle$ but nontrivial on G. Then $\chi(D) \geq -(t+1) + |\chi(L)|^2 = -(t+1) + (s+1)^2 = (s+1)(s+1-x) - \alpha - 1$. But by Lemma 28, $\chi(D) = s - \alpha$. So $x \geq s+1$. This contradicts $s - \alpha = (x+1)w$ for some positive integer w. Q.E.D.

In view of the above corollary, we only need to deal with the case $s > 2\alpha$ whenever Π is proper and it has at least two subgroups lines.

Theorem 35 Suppose that Π has at least two subgroup lines. Let x be the integer defined by (34). If there is a prime divisor p of x + 1 such that p does not divide s + 1, then p = 2, $x + 1 = 2^r$ and $(sx + \alpha)/\alpha = 2^m$ for some positive integers m, r.

Proof By Theorem 32, the parameters of the partial difference set associated with Π are given by (34). Let p be a prime divisor of x+1 such that p does not divide s+1. Define m and r by $p^m ||(sx + \alpha)/\alpha$ and $p^r ||x+1$. By (34) and Corollary 33, we have $\beta < 0$ and $s \ge 2\alpha + 1$. Hence we have $(s+1)(x+1) = \delta \le p^r(s+1)$ and $v = (s+1)^2(sx+\alpha)/\alpha \le p^m(s+1)^2$ by Corollary 26. This shows $x+1 = p^r$ and $(sx + \alpha)/\alpha = p^m$.

It remains to show p = 2. Since $s > \alpha$, we have $(sx + \alpha)/\alpha > x + 1$ and hence m > r. Thus p = 2 by Theorem 27. Q.E.D.

Theorem 36 Suppose that Π has at least two subgroup lines. Let x be the integer defined by (34). Then s + 1 can have at most one prime divisor which does not divide $(sx + \alpha)/\alpha$. Furthermore, this potential prime divisor cannot be larger than $\alpha + 1$.

Proof Assume s+1 has at least two prime divisors, say q_1 , q_2 , which do not divide $(sx+\alpha)/\alpha$. Let $q_i^{s_i}||(s+1)$ for i = 1, 2. Then by (34) we have $q_i^{2s_i}||v$ and $q_i^{s_i}||\delta$ for each *i*. Using (28) we conclude $s - 1 < \alpha(q_i^{s_i} + 1)$ and hence

$$s \le \alpha (q_i^{s_i} + 1)$$

for all i. Now (36) implies

$$(\alpha + 1)(q_i^{s_i} - 1) \le q^{2s_i} - 1$$

and hence $\alpha \leq q_i^{s_i}$ for all *i*. Combining the two inequalities, we deduce that $s \leq (q_i^{s_i} + 1)q_i^{s_i}$. Without loss of generality, we may assume $q_1^{s_1} \geq q_2^{s_2} + 1$. We then have

$$s+1 \ge q_1^{s_1}q_2^{s_2} \ge (q_2^{s_2}+1)q_2^{s_2} \ge s.$$

This is impossible unless $s + 1 = q_1^{s_1} q_2^{s_2}$. But then $\alpha \ge s/(q_2^{s_2} + 1) > q_1^{s_1} - 1$. Thus, $\alpha \ge q_1^{s_1} > q_2^{s_2}$. This is also impossible.

Now let q be any prime divisor of s + 1 which does not divide $(sx + \alpha)/\alpha$. It remains to show $q \leq \alpha + 1$. Assume $q > \alpha + 1$. Let U be a subgroup line of II. Recall that |U| = s + 1. Since q does not divide $(sx + \alpha)/\alpha$, there is $g \in G \setminus U$ such that the order of g in G in not divisible by q. Choose $h \in U$ such that the order of h in G is q. By Lemma 16 (d) and the Chinese Remainder Theorem, we have $h^i g \in D$ for i = 1, ..., q - 1. Recall that D consists exactly of the points $\neq 1$ which are collinear with 1. Note that the line Ug does not contain 1. But it contains at least q - 1 points collinear with 1, namely, $h^i g$, i = 1, ..., q - 1. Since $q - 1 > \alpha$, this contradicts property 4 of a partial geometry. Q.E.D.

By Corollary 33, Theorem 35 and Theorem 36, we have the following result.

Corollary 37 Suppose that Π has at least two subgroup lines. Let x be the integer defined by (34). If there exists a prime divisor p of x + 1 such that p does not divide s + 1, then $s + 1 = q^u$, $x + 1 = 2^r$ and $(sx + \alpha)/\alpha = 2^m$ where q is an odd prime and u, r and m are positive integers. Furthermore, $q \leq \alpha + 1$.

Theorem 38 Suppose that Π has at least two subgroup lines. Then s + 1 has at most three prime factors.

Proof Suppose s + 1 has r prime factors with r > 3. By Corollary 37 and Lemma 16 (d), all prime divisors of v must be prime divisors of s + 1. Let $s + 1 = \prod_{j=1}^{r} q_i^{s_i}$ where q_1, q_2, \ldots, q_r are distinct primes and $s_i \ge 1$. For each i, let $q_i^{x_i}||(x+1)$ and $q_i^{v_i}||v$ where

 $x_i \ge 0$ and $v_i \ge 1$. Note that $\delta = (s+1)(x+1) = \prod_{i=1}^r q_i^{s_i+x_i}$. By (28), for each *i*, we have $(s-1)/\alpha < (q_i^{v_i}-1)/(q_i^{s_i+x_i}-1)$. Hence

$$\left(\frac{s-1}{\alpha}\right)^r < \prod_{i=1}^r \frac{q_i^{v_i} - 1}{q_i^{s_i + x_i} - 1} \le \prod_{i=1}^r q_i^{v_i - s_i - x_i} \frac{q_i^{s_i}}{q_i^{s_i} - 1} = \frac{v}{(s+1)(x+1)} \prod_{i=1}^r \frac{q_i^{s_i}}{q_i^{s_i} - 1} \le \frac{s}{\alpha}(s+1) \prod_{i=1}^r \frac{q_i}{q_i - 1} \le \frac{s}{\alpha}(s+1)$$

Simplifying, we get

$$\frac{(s-1)^{r-1}}{s+1} < \frac{(s-1)^r}{s(s+1)} < \alpha^{r-1} \prod_{i=1}^r \frac{q_i}{q_i-1}.$$
(37)

By Lemma 36 we have $\alpha(q_i^{s_i} - 1) \leq q_i^{v_i} - 1$ for all *i*. Hence

$$\alpha^{r} \leq \prod_{i=1}^{r} \frac{q_{i}^{v_{i}} - 1}{q_{i}^{s_{i}} - 1} \leq \prod_{i=1}^{r} q_{i}^{v_{i} - s_{i}} \frac{q_{i}}{q_{i} - 1} = \frac{v}{s+1} \prod_{i=1}^{r} \frac{q_{i}}{q_{i} - 1} \leq \frac{(s+1)(sx+\alpha)}{\alpha} \prod_{i=1}^{r} \frac{q_{i}}{q_{i} - 1}$$

and

$$\alpha^{r+1} \le (s+1)(sx+\alpha) \prod_{i=1}^r \frac{q_i}{q_i-1} \le (s+1)^2(x+1) \prod_{i=1}^r \frac{q_i}{q_i-1}.$$
(38)

By Theorem 25 (iii) we have $\delta(s - \alpha - 1)/(s - \alpha) < q_i^{s_i + x_i}(s + 1)$ for all *i*. Substituting $\delta = (s+1)(x+1)$ and $s - \alpha = (x+1)w$, we have $x+1 - (1/w) < q_i^{s_i + x_i}$ and hence $x+1 \leq q_i^{s_i + x_i}$. Therefore $(x + 1)^r \leq \prod_{i=1}^r q_i^{s_i + x_i} = (s + 1)(x + 1)$ which implies $x + 1 \leq (s + 1)^{1/(r-1)}$. Substituting this into (38), we have

$$\alpha^{r+1} \le (s+1)^{\frac{2r-1}{r-1}} \prod_{i=1}^{r} \frac{q_i}{q_i - 1}.$$
(39)

Combined with inequalities (37) and (39), we get

$$\frac{(s-1)^{\frac{(r+1)(r-1)}{r}}}{(s+1)^3} \le \left(\prod_{i=1}^r \frac{q_i}{q_i-1}\right)^2.$$

As $r \ge 4$, we get

$$\left(\frac{s-1}{s+1}\right)^{5} (s+1) \le \left(\prod_{i=1}^{r} \frac{q_i}{q_i - 1}\right)^{\frac{5}{3}}.$$
(40)

Note that $r \ge 4$ implies $s + 1 \ge 210$. Thus $[(s - 1)/(s + 1)]^5 \ge 2/3$. It is obvious that $q_i \ge [q_i/(q_i - 1)]^{8/3}$ when $q_i \ge 5$. On the other hand,

$$\frac{2}{3} \cdot 2 \cdot 3 \cdot 5 \cdot 7 \ge \left(\frac{2}{1} \cdot \frac{3}{2} \cdot \frac{5}{4} \cdot \frac{7}{6}\right)^{\frac{8}{3}}$$

This contradicts (40). Hence we have proved $r \leq 3$.

Q.E.D.

7 The Case $\alpha = 2$

In this section, we begin with the proof Theorem 1. The proof will be completed in the following sections. The following result is the consequence of [11, Corollary 2.3 and Lemma 5.2].

Lemma 39 Let Π be a proper pg(s + 1, t + 1, 2) with an abelian Singer group G of mixed type and let D be the partial difference set in G associated to Π . Then there is a positive integer x such that

$$t + 1 = (s + 1)x + 3 \tag{41}$$

and

$$s - 2 \equiv 0 \mod (x+1). \tag{42}$$

Furthermore, (sx + 2)/(2(x + 1)) is an integer and the parameters of D are given by

$$v = (s+1)^{2}(x+1) \left[\frac{sx+2}{2(x+1)} \right],$$

$$\delta = (s+1)(x+1),$$

$$k = s(t+1),$$

$$\beta = -(s+1)(x-1) - 6,$$

$$\mu = 2(t+1)$$

(43)

Proof By [11, Lemma 5.1], the geometry must have at least two subgroup lines. Hence (41), (42) and (43) follow from Theorem 32. Q.E.D.

Note that by (35), the parameters of the dual D^* of the partial difference D in Lemma 39 take the following form.

$$v^{*} = (s+1)^{2}(x+1) \left[\frac{sx+2}{2(x+1)} \right],$$

$$k^{*} = s(s-1) \left[\frac{sx+2}{2(x+1)} \right],$$

$$\beta^{*} = -(s-3) \left[\frac{sx+2}{2(x+1)} \right],$$

$$\delta^{*} = (s+1) \left[\frac{sx+2}{2(x+1)} \right],$$

$$\mu^{*} = (s-1) \left(\frac{s-2}{x+1} \right) \left[\frac{sx+2}{2(x+1)} \right].$$
(44)

Lemma 40 In the situation of Lemma 39, let p be a divisor of x + 1, say, $p^r ||x + 1$ for some $r \ge 1$.

- (a) If $p \neq 3$, then $s + 1 = 3^u$, $x + 1 = 2^r$ and $(sx + 2)/[2(x + 1)] = 2^n$ for some positive integers u, r, n.
- (b) If p = 3 and $r \ge 2$, then $x + 1 = 3^r$ and $(sx + 2)/[2(x + 1)] = 3^n$ or $2 \cdot 3^n$ for some $n \ge 0$.

Proof Since $s + 1 \equiv 3 \mod (x+1)$, we have (s+1, x+1) = 1 or 3. So, if $p \neq 3$ then p does not divide s + 1. Thus part (a) follows from Corollary 37.

Now assume p = 3 and $r \ge 2$. By part (a), we have $x+1 = 3^r$. Since $s+1 \equiv 3 \mod (x+1)$, we have 3||s+1 (note that this conclusion would be false if r = 1 which is the reason why the case r = 1, i.e. x = 2, is a different story). Write $(sx+2)/(2(x+1)) = 3^n z$ where z is not divisible by 3. Using Theorem 21, we get

$$2 \cdot 3^{n} z = \frac{sx+2}{x+1} < s \le \frac{2(3^{r+n+2}-1)}{3^{r+1}-1} \quad \Rightarrow \quad z < 3 + \frac{3^{n+1}-1}{3^{n}(3^{r+1}-1)}.$$

Q.E.D.

This implies z = 1 or 2.

Corollary 41 In the situation of Lemma 39, one of the following cases must occur.

- **A:** $s + 1 = 3 \cdot 2^m$, $x + 1 = 3^r$ and $(sx + 2)/[2(x + 1)] = 3^n$ or $2 \cdot 3^n$ for some positive integers m, r and n with $r \ge 2$.
- **B**: $s + 1 = 3^u$, $x + 1 = 2^r$ and $(sx + 2)/[2(x + 1)] = 2^n$ for some positive integers u, r, n. **C**: x = 2.

Proof If x + 1 has a prime divisor different from 3, then case **B** holds by Lemma 40. Now let x + 1 be a power of 3, say $x + 1 = 3^r$, $r \ge 2$. Then $(sx + 2)/[2(x + 1)] = 3^n$ or $2 \cdot 3^n$ by Lemma 40. It remains to show that $s + 1 = 3 \cdot 2^m$ for some positive integer m. We have seen in the proof of Lemma 40 that 3||s + 1, say s + 1 = 3z where gcd(z, 3) = 1. By Theorem 36, there can only be one prime divisor q of s + 1 apart from 3 and $q \le \alpha + 1 = 3$. This shows that z is a power of 2. Q.E.D.

In the following sections, we work on the cases **A-C** stated in Corollary 41 in order to complete the proof of Theorem 1.

8 Case A

Lemma 42 Case A of Corollary 41 is impossible.

Proof Assume $s + 1 = 3 \cdot 2^m$, $x + 1 = 3^r$, $r \ge 3$, and $(sx + 2)/[2(x + 1)] = 3^n$ or $2 \cdot 3^n$. Then

$$3 \cdot 2^m - 1 = \frac{2(2^{\epsilon} \cdot 3^{r+n} - 1)}{3^r - 1} \tag{45}$$

where $\epsilon \in \{0, 1\}$. First assume $\epsilon = 0$. If r would not divide n, then

$$gcd(3^{n+r}-1, 3^r-1) = 3^{(n+r,r)} - 1 = 3^{(n,r)} - 1 \le 3^{r-1} - 1.$$

But since $3^r - 1$ divides $2(3^{n+r} - 1)$, we have

$$gcd(3^{n+r}-1, 3^r-1) \ge \frac{1}{2}gcd(2(3^{n+r}-1), 3^r-1) = \frac{1}{2}(3^r-1),$$

a contradiction. Hence r divides n. This shows that, for $\epsilon = 0$, the right hand side of (45) is even while the left hand side is odd, a contradiction. Hence $\epsilon = 0$ is impossible.

Now let $\epsilon = 1$. Since $2 \cdot 3^{r+n} - 1$ is odd, $2||3^r - 1$ and hence $3^r \equiv 3 \mod 8$. Then

 $(3 \cdot 2^m - 1)(3^r - 1) = 2(2 \cdot 3^{r+n} - 1) \implies 3 \cdot 2^m \equiv 2 \cdot 3^{r+n} \mod 4.$

This implies m = 1 and s + 1 = 6. But then $3 = s - 2 \equiv 0 \mod (x + 1)$ contradicting $x + 1 = 3^r$ with $r \ge 2$. Q.E.D.

9 Case B and Goormaghtigh's Equation

The Diophantine equation

$$\frac{x^m-1}{x-1} = \frac{y^w-1}{y-1}, \ y > x > 1, \ m, w > 2$$

is called *Goormaghtigh's Equation*. It has been studied in several papers, see [3] for a reference. The only known solutions are (x, y, m, w) = (2, 5, 5, 2) and (2, 90, 13, 3) and it is conjectured that there are no other solutions. In order to deal with Case **B** of Corollary 41, we prove the following new result on Goormaghtigh's equation.

Theorem 43 The equation

$$\frac{3^m - 1}{2} = \frac{2^{rw} - 1}{2^r - 1}$$

has no solution in positive integers m, r, w with w > 1.

Proof Assume that there is a solution. Then we have

$$(3m - 1)(2r - 1) = 2(2wr - 1)$$
(46)

Considering (46) mod 8 we see that r > 1. Taking (46) mod 4 we see that m is odd. Since, for $r \ge 3$, the order of 3 mod 2^r is 2^{r-2} , we get $r \le 74$ from [3, Lemma 2].

Now consider the values p_i and n_i defined in the following table.

i	1	2	3	4	5	6	7
p_i	3	5	7	11	13	17	23
n_i	7	31031	2097151	453277445	14672749	632388379	12667487

It is straightforward to check by computer that for i = 1, 2, ..., 7 all solutions (m, r, w) of

$$(3^m - 1)(2^r - 1) \equiv 2(2^{wr} - 1) \mod n_i, \quad m \equiv 1 \mod 2$$

have the property that

$$gcd(m-1, w-1)r \equiv 0 \mod p_i$$

Since r < 75, this implies

$$gcd(m-1, w-1) > 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 23/75 = 78278.2.$$

In particular, we have w - 1 > 78278.2. Using (46) we get $3^{m-1} < 3^m - 1 < 2^{r(w-1)+2}$. Since w - 1 > 78278.2 and r < 75, this implies

$$\frac{m-1}{w-1} \le \frac{\log 2}{\log 3} \left(r + \frac{2}{n-1} \right) < 47.$$

Hence we can take $\alpha = 47$ in [3, Lemma 4] and get

$$gcd(m-1, w-1) \le 743\left(47 + \frac{1}{2}\right) = 35292.5,$$

a contradiction.

Corollary 44 Case B of Corollary 41 is impossible.

Proof In case **B** of Corollary 41 we have $s+1 = 3^u$, $x+1 = 2^r$ and $(sx+2)/(2(x+1)) = 2^n$. Hence

$$\frac{3^u - 1}{2} = \frac{2^{n+r} - 1}{2^r - 1}.$$
(47)

Q.E.D.

Note that r divides n since $(2^{n+r} - 1, 2^r - 1) = 2^{(n,r)} - 1$. This contradicts Theorem 43. Q.E.D.

10 Case C

Now we consider the case x = 2 in Corollary 41, i.e. partial geometries pg(s + 1, 2(s + 1) + 3, 2) with abelian Singer groups of mixed type. Let G be the Singer group. Recall that by (13), the associated partial difference set D in G has parameters

$$v = (s + 1)^{3},$$

$$\delta = 3(s + 1),$$

$$k = s[2(s + 1) + 3],$$

$$\beta = -(s + 1) - 6,$$

$$\mu = 2[2(s + 1) + 3].$$

(48)

Recall that

$$D = -(t+1) + \sum_{U \in \mathcal{U}} U + \sum_{L \in \mathcal{L}} LL^{(-1)}.$$
(49)

Corollary 45 If a proper partial geometry pg(s + 1, 2(s + 1) + 3, 2) with an abelian Singer group of mixed type exists, then $s + 1 = 3^n$ for some integer $n \ge 2$.

Proof In view of (48) and Theorem 24, we have s + 1 = 6 or $s + 1 = 3^n$ with $n \ge 1$. For the latter case, n = 1 is not possible since the partial geometry is assumed to be proper. Now suppose s + 1 = 6. Then $v = 2^3 \cdot 3^3$, $\delta = 2 \cdot 3^2$, $\beta = -12$ and $\beta^* = -4$. Applying Theorem 25 (iv) with $p^r = 2$, we have $9 = \delta/p^r \le s + 1 = 6$, a contradiction. Q.E.D.

Now we begin with the investigation of the case $s + 1 = 3^n$ in Corollary 45.

Lemma 46 Let $s+1 = 3^n$ for some $n \ge 2$ and let D be given by (49). Let $L \in \mathcal{L}$ be arbitrary and $g \in L$. Define $L^* := \{h_1h_2^{-1} : h_1, h_2 \in L \text{ and } h_1 \ne h_2\} \subset G$. Then the following hold.

- (a) If $o(g) \ge 27$, then L^* contains at most 6 nonidentity elements of $\langle g \rangle$.
- (b) If o(g) = 9, then L^* contains at most 2 elements of $\langle g \rangle$.

Proof First, we write $L = A_1 + A_2 u_2 \cdots + A_f u_f$ such that A_i are nonempty subsets of $\langle g \rangle$ and $\langle g \rangle u_i$ are distinct $\langle g \rangle$ -cosets not equal to $\langle g \rangle$.

We claim $|A_i| = 1$ if $i \neq 1$. Otherwise, without loss of generality, we may assume $\{1, g^a\} \subset A_2$ where $g^a \neq 1$. Since u_2 and $g^a u_2$ are in L, both Lu_2^{-1} and $L(g^a u_2)^{-1}$ are lines that contain 1 but are distinct from L. Since $g^a \in Lu_2^{-1}$ and $g^{-a} \in L(g^a u_2)^{-1}$, both g^a and g^{-a} are in $D \setminus L$. Therefore, Lg^a and Lg^{-a} are lines that do not contain 1 and hence $|Lg^a \cap D| = |Lg^{-a} \cap D| = 2$. On the other hand, $\{g^a, g^{a+1}, g^a u_2\} \subset Lg^a$ and $\{g^{-a}, g^{-a+1}, u_2\} \subset Lg^{-a}$. Since g^a, g^{-a}, u_2 and $g^a u_2$ are in D, both g^{a+1} and g^{-a+1} are not in D. However, as o(g) is a power of 3, either $o(g) = o(g^{a+1})$ or $o(g) = o(g^{-a+1})$ and by Lemma 16 (e), this implies either g^{a+1} or g^{-a+1} is in D, a contradiction.

Since $|A_i| = 1$ for $i \neq 1$, we have $L^* \cap \langle g \rangle = A_1 A_1^{-1} \setminus \{1\}$. Now, let us write

$$A_1 = B_1 \cup B_2 g \cup B_3 g^2$$

where $B_i \subset \langle g^3 \rangle$ for each *i*. Recall that DL = sL + 2(G - L) by (4) and $g\langle g^3 \rangle + g^2 \langle g^3 \rangle \subset D$ by Lemma 16 (e). In DL, the coefficient of elements in $\langle g^3 \rangle$, $g\langle g^3 \rangle$ and $g^2 \langle g^3 \rangle$ are at least $|B_2| + |B_3|$, $|B_1| + |B_3|$ and $|B_1| + |B_2|$ respectively. As $o(g) \ge 9$, it is not possible that L contains a $\langle g^3 \rangle$ -coset. Therefore, each of $|B_2| + |B_3|$, $|B_1| + |B_3|$ and $|B_1| + |B_2|$ must be at most 2. It follows that $|B_1| + |B_2| + |B_3| \le 3$ and in case $|B_1| + |B_2| + |B_3| = 3$, $|B_1| = |B_2| = |B_3| = 1$. Now (a) is clear as $|A_1| \le 3$.

For (b), we have o(g) = 9 and it suffices to show $|A_1| \leq 2$. If $|A_1| \geq 3$, we may assume $\{1, g, g^{2+3r}\} \subset L$ for some r. As $g^{-1} \notin L$, we have $r \neq 2$. When r = 0, we consider the line Lg^{-1} . Note that $\{1, g\} \subset Lg^{-1} \cap L$ but $Lg^{-1} \neq L$ as $g^{-1} \notin L$. This is impossible. When r = 1, we consider $Lg^{-4} \neq L$. Again, $\{g, g^5\} \subset Lg^{-4} \cap L$ and this is impossible. Hence, $|A_1| \leq 2$.

Theorem 47 Assume that a proper pg(s + 1, 2(s + 1) + 3, 2) admitting an abelian Singer group G exists. Then G is an elementary abelian 3-group.

Proof By Corollary 45, we have $s + 1 = 3^n$ for some $n \ge 2$. Let D be the partial difference set in G corresponding to the geometry and recall that D has the form (49). Note that $|\mathcal{L}| = 1$ or 2. We claim that $\bigcup_{L \in \mathcal{L}} LL^{(-1)}$ contains elements of order 3 only. Then by Corollary 34, the group G must be elementary abelian.

Suppose there exists $g \in L_1$ for some $L_1 \in \mathcal{L}$ such that $o(g) \geq 9$. Observe that, by Lemma 16 (e), we have $M = \{g^i : \gcd(3, i) = 1\} \subset \bigcup_{L \in \mathcal{L}} LL^{(-1)}$ as $g \notin U$ for any $U \in \mathcal{U}$. If o(g) = 9, then by Lemma 46 (b), there can be at most 4 elements of M in $\bigcup_{L \in \mathcal{L}} LL^{(-1)}$. This contradicts $|M| \geq 6$ in this case. Hence $o(g) \geq 27$. However, by Lemma 46 (a), there can be at most 12 elements of M in $\bigcup_{L \in \mathcal{L}} LL^{(-1)}$. This is impossible since $|M| \geq 18$ in this case. Q.E.D.

Lemma 48 Let n be non-negative integer, $\eta = \exp \frac{2\pi i}{3}$ and $X, Y \in \mathbb{Z}[\eta]$.

- (a) If $|X|^2 + |Y|^2 = 3^n$ then X = 0 or Y = 0.
- (b) If $|X|^2 + |Y|^2 = 2 \cdot 3^n$ then $|X|^2 = |Y|^2 = 3^n$.

Proof For $Z = e + f\eta \in \mathbb{Z}[\eta]$ we have $|Z|^2 = e^2 + f^2 - ef$ and hence

$$|Z|^2 \equiv 0, 1, 3, 4, \text{ or } 7 \mod 9 \text{ and}$$
(50)

$$Z|^2 \notin \{2, 5, 6\} \tag{51}$$

Write $X = a + b\eta$ and $Y = c + d\eta$ with $a, b, c, d \in \mathbb{Z}$.

(a) We prove part (a) by induction on n. By (51), the assertion is true for $n \leq 1$. Now assume $n \geq 2$. In view of (50), $|X|^2 + |Y|^2 \equiv 0 \mod 9$ implies $|X|^2 \equiv 0 \mod 9$ and $|Y|^2 \equiv 0 \mod 9$. It is straightforward to check that, in turn, this implies $a \equiv b \equiv c \equiv d \equiv 0 \mod 3$. Hence $X/3 \in \mathbb{Z}[\eta], Y/3 \in \mathbb{Z}[\eta], |X/3|^2 + |Y/3|^2 = 3^{n-2}$ and the assertion follows by induction.

(b) Again, we use induction on n. By (51), the assertion is true for $n \leq 1$. Now, the same argument as in the proof of part (a) completes the proof. Q.E.D.

Lemma 49 Let G be an abelian group of order $(s + 1)^3$ for some positive integer s. Let S be a subset of G such that |S| = s + 1 and in $SS^{(-1)}$ all nonidentity elements of G have coefficient 0 or 1. Furthermore, assume $|\chi(S)|^2 \in \{0, s + 1, 3(s + 1)\}$ for all characters χ of G. Let

$$x = |\{\chi \in G^* : \chi \neq \chi_0, \ |\chi(S)|^2 = s + 1\}|,$$

$$y = |\{\chi \in G^* : \chi \neq \chi_0, \ |\chi(S)|^2 = 3(s + 1)\}|.$$

Then

$$x = \frac{1}{2}(s+1)(s^2+4s),$$
$$y = \frac{1}{6}s^2(s+1)$$

Proof The coefficient of 1 in $SS^{(-1)}$ is s+1. Hence by Result 11 (i), we have $\sum_{\chi \in G^*} |\chi(S)|^2 = (s+1)^4$. Since |S| = s+1, this implies $\sum_{\chi \neq \chi_0} |\chi(S)|^2 = (s+1)^4 - (s+1)^2$, i.e.

$$x(s+1) + 3y(s+1) = (s+1)^4 - (s+1)^2.$$
(52)

The coefficient of 1 in $(SS^{(-1)})(SS^{(-1)})^{(-1)}$ equals the sum of the squares of the coefficients of $SS^{(-1)}$ and thus is $(s+1)^2 + s(s+1) = (2s+1)(s+1)$. Using Result 11 (i), we get $\sum_{\chi \in G^*} |\chi(S)|^4 = (2s+1)(s+1)^4$. Hence $\sum_{\chi \neq \chi_0} |\chi(S)|^4 = (2s+1)(s+1)^4 - (s+1)^4 = 2s(s+1)^4$ and thus

$$x(s+1)^{2} + 9y(s+1)^{2} = 2s(s+1)^{4}.$$
(53)

Solving the equations (52) and (53) gives the assertion.

Q.E.D.

Theorem 50 A proper pg(s+1, 2(s+1)+3, 2) with an abelian Singer group and exactly 2(s+1) orbit lines does not exist.

Proof Assume that such a partial geometry exists. By Corollary 45, we have $s + 1 = 3^n$ for some $n \ge 2$. By Theorem 47, the group G must be an elementary abelian 3-group. By (49), we have

$$D = -[2(s+1)+3] + U_1 + U_2 + U_3 + SS^{(-1)} + TT^{(-1)}$$

where the U_i 's are subgroups of G of order s + 1 and S, T are distinct orbit lines. Note that $\chi(D) = -[2(s+1)+3]$ or s-2 for all nontrivial characters χ of G. By Lemma 28, we have $|\chi(S)|^2 + |\chi(T)|^2 \in \{0, s+1, 2(s+1), 3(s+1)\}$. Using Lemma 48, we conclude $|\chi(S)|^2 \in \{0, s+1, 3(s+1)\}$ and $|\chi(T)|^2 \in \{0, s+1, 3(s+1)\}$. Let D^* be the dual of D, i.e.

$$D^* = \{ \chi \in G^* : \chi \neq \chi_0, \, \chi(D) = -[2(s+1)+3] \}.$$

Then $|D^*| = (s-1)s(s+1)/3$ by (44). Let

$$X = \{ \chi \in G^* : \chi \neq \chi_0, |\chi(S)|^2 = s+1 \}, Y = \{ \chi \in G^* : \chi \neq \chi_0, |\chi(S)|^2 = 3(s+1) \}, Z = \{ \chi \in G^* : \chi \neq \chi_0, |\chi(T)|^2 = 3(s+1) \}.$$

Then $|X| = \frac{1}{2}(s+1)(s^2+4s)$ and $|Y| = |Z| = \frac{1}{6}s^2(s+1)$ by Lemma 49. Furthermore, the sets D^* , X, Y, Z are pairwise disjoint. This implies

$$|D^*| + |X| + |Y| + |Z| \le (s+1)^3 - 1.$$

Substituting the values for $|D^*|$, |X|, |Y|, |Z| gives $-s^3 + s^2 + 4s \ge 0$ and thus n < 2, a contradiction. Q.E.D.

Proposition 51 For s + 1 = 9, a pg(s + 1, 2(s + 1) + 3, 2) with an abelian Singer group G and exactly s + 1 orbit lines does not exist.

Proof Assume the contrary and let $D \subset G$ be the associated partial difference set. Then $|G| = 3^6$ and $D = -21 + \sum_{i=1}^{12} U_i + SS^{(-1)}$ where the U_i 's are subgroups of G of order 9 and S is an orbit line. By Theorem 47, the group G is elementary abelian. Furthermore, $|\chi(S)|^2 \in \{0, 9, 27\}$ for all nontrivial characters χ of G. From Corollary 34 we conclude that S contains a set $\{g_1, ..., g_6\}$ such that $\langle g_1, ..., g_6 \rangle = G$. In particular, $g_i \neq 1$ for i = 1, ..., 6. Hence

$$S = \{1, g_1, \dots, g_6, a, b\}$$

for some $a, b \in G$, $a \neq b$. Now let $\eta = \exp 2\pi i/3$ and let χ_i be the character of G with $\chi_i(g_i) = \eta$ and $\chi_i(g_j) = 1$ for $i \neq j$. Then

$$\chi_i(S) = 6 + \eta + \chi_i(a+b).$$

Since $|\chi_i(S)|^2 \equiv 0 \mod 9$, we know that $\chi_i(S)$ is divisible by 3. Hence

$$\eta + \chi_i(a+b) \equiv 0 \mod 3.$$

This is only possible if $\chi_i(a) = \chi_i(b) = \eta$ or $\chi_i(a+b) = 1 + \eta^2$. But $\chi_i(a+b) = 1 + \eta^2$ is impossible since $|\chi_i(S)|^2 = 36$ in this case. Hence

$$\chi_i(a) = \chi_i(b) \text{ for } i = 1, ..., 6.$$
 (54)

Since the g_i generate G, we can write

$$a = \prod_{i=1}^{6} g_i^{a_i}$$
$$b = \prod_{i=1}^{6} g_i^{b_i}$$

for some integers a_i , b_i with $0 \le a_i \le 2$, $0 \le b_i \le 2$. By (54) we get

$$\gamma^{a_i} = \chi_i(a) = \chi_i(b) = \eta^{b_i}, \ i = 1, ..., 6.$$

Hence $a_i = b_i$ for all *i*. This implies a = b, a contradiction.

11 Proof of Theorem 1

Theorem 1 follows directly from Corollary 41, Lemma 42, Corollaries 44 and 45, Theorems 47, 50, and Proposition 51. If a proper pg(s + 1, t + 1, 2) with an abelian Singer group G of spread type exists, then $|G| = (s + 1)^3$, t = 2(s + 2), and G is an elementary abelian 3-group by [11, Thm. 4.1]. Furthermore, by [11, Cor. 6.12], the only pg(s + 1, t + 1, 2) with an abelian Singer group of rigid type is the Van Lint-Schrijver geometry [13]. Together with Theorem 1 this implies the following.

Corollary 52 Let Π by a proper partial geometry pg(s + 1, t + 1, 2) with an abelian Singer group G. Then G is an elementary abelian 3-group of order $(s + 1)^3$ and t = 2(s + 2) or Π is the Van Lint-Schrijver partial geometry.

Q.E.D.

References

- T. Beth, D. Jungnickel, H. Lenz: *Design Theory* (2nd edition). Cambridge University Press 1999.
- [2] R.C. Bose: Strongly regular graphs, partial geometries and partially balanced designs. *Pacific J. Math.* 13 (1963), 389-419.
- [3] Y. Bugeaud, T.N. Shorey, On the Diophantine equation $\frac{x^m-1}{x-1} = \frac{y^n-1}{y-1}$. Pacific J. Math. **207** (2002), 61-75.
- [4] P.J. Cameron, J.H. van Lint: On the Partial Geometry pg(6, 6, 2). J. Combin. Theory Ser. A. 32 (1982), 252-255.
- [5] P.J. Cameron, J.H. van Lint: Designs, graphs, codes and their links. London Mathematical Society Student Texts 22. Cambridge University Press 1991.
- [6] F. De Clerck, M. Delanote, N. Hamilton, R. Mathon: Perp-Systems and partial geometries. Adv. Geom. 2 (2002), 1-12.
- [7] P. Delsarte: An algebraic approach to the association schemes of coding theory. Philips Res. Rep. Suppl. No. 10 (1973).
- [8] R.H.F. Denniston: Some maximal arcs in finite projective planes. J. Combin. Theory Ser. A. 6 (1969), 317-319.
- [9] S. De Winter: Elation and translation semipartial geometries. J. Combin. Theory Ser. A. 108 (2004), 313-330.
- [10] S. De Winter, K. Thas: Generalized quadrangles with an abelian Singer group. Des. Codes. Crypt. 39 (2006), 81-87.
- [11] S. De Winter: Partial geometries pg(s, t, 2) with an abelian Singer group and a characterization of the van Lint-Schrijver partial geometry. J. Alg. Combin. 24 (2006), 285-297.
- [12] D. Hachenberger, D. Jungnickel: Translation nets: a survey. Discrete Math. 106/107 (1992), 231-242.
- [13] J.H. van Lint, A. Schrijver: Construction of strongly regular graphs, two-weight codes and partial geometries by finite fields. *Combinatorica.* 1 (1981), 63-73.
- [14] J.H. van Lint, R.M. Wilson: A course in combinatorics. Second edition. Cambridge University Press 2001.
- [15] S.L. Ma, A Survey of partial difference sets. Des. Codes. Crypt. 4 (1994), 221-261.
- [16] S.L. Ma, On subsets of partial difference sets. Discrete Math. 125 (1994), 263-272.
- [17] S.L. Ma, Regular automorphism groups on partial geometries. J. Stat. Planning and Inference. 51 (1996), 215-222.

- [18] S.L. Ma, Some necessary conditions on the parameters of partial difference sets. J. Stat. Planning and Inference. 62 (1997), 47-56.
- [19] R.L. McFarland: Sub-Difference Sets of Hadamard Difference Sets. J. Combin. Theory Ser. A. 54 (1990), 112-122.
- [20] J.A. Thas: Construction of maximal arcs and partial geometries. Geom. Dedicata. 3 (1974), 61-64.
- [21] J.A. Thas: Semipartial geometries and spreads of classical polar spaces. J. Combin. Theory Ser. A. 35 (1983), 58-66.