TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 356, Number 11, Pages 4343–4358
S 0002-9947(03)03365-8
Article electronically published on August 26, 2003

NONEXISTENCE OF ABELIAN DIFFERENCE SETS: LANDER'S CONJECTURE FOR PRIME POWER ORDERS

KA HIN LEUNG, SIU LUN MA, AND BERNHARD SCHMIDT

ABSTRACT. In 1963 Ryser conjectured that there are no circulant Hadamard matrices of order > 4 and no cyclic difference sets whose order is not coprime to the group order. These conjectures are special cases of Lander's conjecture which asserts that there is no abelian group with a cyclic Sylow p-subgroup containing a difference set of order divisible by p. We verify Lander's conjecture for all difference sets whose order is a power of a prime greater than 3.

1. INTRODUCTION

A (v, k, λ, n)**-difference set** in a finite group G of order v is a k-subset D of G such that every element $g \neq 1$ of G has exactly λ representations $g = d_1 d_2^{-1}$ with $d_1, d_2 \in D$. The positive integer $n := k - \lambda$ is called the **order** of the difference set. A difference set is called **cyclic** (respectively, **abelian**) if the underlying group is cyclic (respectively, abelian). For detailed treatments of difference sets, see [5], [10], [11], [13], [17]. The most obvious application of difference sets is to design theory: a (v, k, λ, n)-difference set in G is equivalent to a design admitting G as a point and block regular automorphism group [7, Thm. VI.1.6].

The theory of difference sets probably started in 1938 with Singer's discovery [21] of the difference sets

$$D := \{x\mathbb{F}_q^* : x \in \mathbb{F}_{q^{d+1}}^*, \mathrm{Tr}(x) = 0\}$$

in $G := \mathbb{F}_{q^{d+1}}^*/\mathbb{F}_q^*$. Here q is a prime power, $d \geq 2$ is an integer, $\mathbb{F}_r^*$ is the multiplicative group of the finite field $\mathbb{F}_r$, and Tr denotes the trace function of $\mathbb{F}_{q^{d+1}}$ relative to $\mathbb{F}_q$.

Until the 1970s, research focussed on *cyclic* difference sets. Note that a cyclic difference set has a constant intersection with all its cyclic shifts. This property is extremely useful for detecting asynchronous shifts in information transmission, and is the basis for applications of difference sets in sequence design and synchronization problems. A variety of such real-world applications can be found in [7, Chapter XII]. An excellent overview of the results on difference sets obtained in the "cyclic period" was given by Baumert [5]. Later the interest shifted to difference sets in general abelian groups and even nonabelian groups (see [7], [13], [15]), mainly because of the connection to design theory.

Though not at all restricted to the cyclic case, the main interest of the present paper is the nonexistence of *cyclic* difference sets, i.e., we return to the study of the

Received by the editors November 13, 2002 and, in revised form, April 10, 2003.
2000 *Mathematics Subject Classification.* Primary 05B10; Secondary 05B20.
Key words and phrases. Difference set, Ryser's conjecture, Lander's conjecture, field descent.

classical difference set problems. One of the longstanding conjectures on difference sets is the following, given in Ryser's influential book [18].

Conjecture 1.1 (Ryser, 1963)**.** *If there is a (v, k, λ, n)-difference set in a cyclic group, then v and n are coprime.*

It is known [7] that a verification of Ryser's conjecture would yield the solution of two further classical combinatorial problems, namely, the nonexistence of Barker sequences of length > 13 and of circulant Hadamard matrices of order > 4.

Turyn [22] was able to prove Ryser's conjecture in special cases where the so-called "self-conjugacy assumption" holds. Baumert [4] later verified Ryser's conjecture for all $k \leq 100$. The following description of the status of Ryser's conjecture from Lander's book [13, p. 224] from 1983 was very much to the point:

"*Despite this evidence, no real progress has been made in settling the conjecture, or even in pinpointing just what property of cyclic groups 'obstructs' such a difference set.*"

To gain more insight in the phenomenon described by Lander was the main motivation for our work [19], [20] and the present paper. It seems we are now finally able to name an obstruction for difference sets in cyclic groups with $(v, n) > 1$: Such difference sets would decompose into two parts with strong algebraic properties; these properties imply that the two parts are too big to be incorporated in a group of order v.

Lander [13, p. 224] proposed the following strengthening of Ryser's conjecture.

Conjecture 1.2 (Lander, 1983)**.** *Let G be an abelian group of order v containing a difference set of order n. If p is a prime dividing v and n, then the Sylow p-subgroup of G cannot be cyclic.*

After a period of near-stagnation for more than three decades, progress on Ryser's conjecture has recently been achieved in [20]. The results of [20] also apply to Lander's conjecture, but in this case they are less conclusive. In summary, Lander's conjecture has been proven for special parameters of difference sets, but no conclusive general result is known yet. In Section 7 we will prove the following.

Theorem 1.3. *Lander's conjecture and thus Ryser's conjecture is true in the case where n is a power of a prime > 3.*

Our result still is restricted to prime power orders. However, this is probably the most important case, since most known difference sets have prime power order or are obtained from such difference sets by product constructions: The parameter series of known difference sets with $\gcd(v, n) > 1$ are the Hadamard, McFarland, Spence and Chen/Davis/Jedwab parameter families; see [19]. With the exception of Hadamard parameters ($(v, k, \lambda, n) = (4u^2, 2u^2 - u, u^2 - u, u^2)$, $u > 0$), n is a prime power in all known constructions for these families. Furthermore, all known Hadamard difference sets have prime power order or are obtained from such difference sets by product constructions [7, Chapter VI].

2. Preliminaries

In this section, we list the definitions and basic facts we need in the rest of the paper. We first fix some notation. Let G be a finite group. We will always identify a subset A of G with the element $\sum_{g \in A} g$ of the integral group ring $\mathbb{Z}[G]$. For

$B = \sum_{g\in G} b_g g \in \mathbb{Z}[G]$ we write $B^{(-1)} := \sum_{g\in G} b_g g^{-1}$ and $|B| := \sum_{g\in G} b_g$. We call $\{g \in G : b_g \neq 0\}$ 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. We will write $o(g)$ for the order of $g \in G$ in G. The exponent of G, i.e., the order of the largest cyclic subgroup of G, will be denoted by $\exp G$. For convenience, we write $\xi_m = e^{2\pi i/m}$ for any integer m.

For an abelian group H we denote the group of complex characters of H by H^*. The character sending all $h \in H$ to 1 is called **trivial**. For a subgroup W of H, we write $W^\perp$ for the subgroup of H^* consisting of all characters which are trivial on W. We repeatedly will make use of the following elementary properties of characters of finite abelian groups. For a proof, see [7, Section VI.3].

Result 2.1. *Let G be a finite abelian group.*

a) *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.

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

c) *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 $X \in \mathbb{Z}[G]$.*

Since D is a difference set in G if and only if $G \setminus D$ is a difference set in G, we can restrict our attention to (v, k, λ, n)-difference sets with $k \le v/2$. Counting the number of quotients $d_1 d_2^{-1}$, $d_1, d_2 \in D$, $d_1 \neq d_2$, gives the trivial parameter condition $k(k-1) = \lambda(v-1)$. This implies that $k = v/2$ is impossible. Thus we can assume $k < v/2$. Note that in this case $\lambda < k/2$ and $n > k/2$, since $\lambda = k(k-1)/(v-1) < k^2/v < k/2$. Hence, throughout this paper, we will only consider difference sets with

$$k < \frac{v}{2} \text{ and } \lambda < \frac{k}{2} < n. \tag{1}$$

In the group ring language, difference sets can be characterized as follows [7, Lemma VI.3.2].

Result 2.2. *Let D be a k-subset of a group G of order v. Then D is a (v, k, λ, n)-difference set in G if and only if in $\mathbb{Z}[G]$ the following holds:*

$$DD^{(-1)} = n + \lambda G. \tag{2}$$

By far the most powerful known method for the study of the group ring equation (2) is the use of complex characters: Applying a nontrivial complex character χ of G to (2) yields the equation $|\chi(D)|^2 = n$, where $\chi(D)$ is an element of $\mathbb{Z}[\xi_{\exp G}]$, the ring of algebraic integers of $\mathbb{Q}(\xi_{\exp G})$. This observation together with the Fourier inversion formula leads to the following fundamental result.

Result 2.3. *Let D be a k-subset of an abelian group G. Then D is a (v, k, λ, n)-difference set in G if and only if $|\chi(D)|^2 = n$ for every nontrivial character χ of G.*

Result 2.3 essentially is contained in [22] and has turned out to be a *conditio sine qua non* for the study of difference sets in abelian groups. See [7, Lemma VI.3.12] for a proof.

The significance of the equation $|\chi(D)|^2 = n$ lies in its implications on the behavior of $\chi(D)$ under the Galois automorphisms of $\mathbb{Q}(\xi_{\exp G})$. Any such automorphism which fixes all prime ideals dividing (n) must fix the ideal $(\chi(D))$ of $\mathbb{Z}[\xi_{\exp G}]$. This usually gives strong conditions on the structure of D.

3. The decomposition

A crucial step towards our main result is to show that the character-theoretic method implies a decomposition of a difference set into two parts: one part consisting of an element of a group ring of a "small" subgroup and a second part consisting just of a multiple of a certain subgroup.

An important feature of our decomposition of difference sets is the use of Gauss sums. We recall that a Gauss sum over $\mathbb{F}_p$ is usually defined as $\sum_{x\in\mathbb{F}_p}\chi(x)\xi_p^x$, where χ is a multiplicative character of $\mathbb{F}_p$. By convention, $\chi(0) = 0$. Using a primitive root t mod p, we can rewrite the Gauss sum as $\sum_{i=1}^{p-1}\chi(t)^i\xi_p^{t^i}$. Note that $\chi(t)$ is a complex $(p-1)$st root of unity. In the study of the difference set equation (2) by the character method, Gauss sums arise naturally because of their behavior under Galois automorphisms. The details of this connection can be found in the proof of [14, Thm. 3.4]. The "Gauss sums" we will use are actually *group ring elements* whose character values are Gauss sums:

Definition 3.1. Let G be a finite group, let p be a prime dividing $|G|$ and let t be a primitive root mod p. A **Gauss sum** over G is an element of $\mathbb{Z}[G]$ of the form

$$\mathcal{G}(g,\delta) := \sum_{i=1}^{p-1}(\delta g)^i h^{t^i},$$

where $g, h \in G$ with $o(g)|(p-1)$, $o(h) = p$ and $\delta = \pm 1$.

Notation 3.2. The following notation will be used throughout the rest of the paper.

- G is an abelian group with cyclic Sylow p-subgroup, where p is an odd prime.
- H is a complement of the Sylow p-subgroup of G.
- P is the unique subgroup of G of order p.
- D is a (v,k,λ,n)-difference set in G with $n = p^r$ for some positive integer r.

The following decomposition result is a direct consequence of [14, Thm. 4.1] and is crucial for the present paper. By "up to a translation" we mean that we have to replace D by Df, $f \in G$, if necessary.

Result 3.3. *There are $Y \in \mathbb{Z}[G]$, $D' \in \mathbb{Z}[H]$ and a Gauss sum $\mathcal{G}(g,\delta)$ over G such that up to a translation $D = D'\mathcal{G}(g,\delta) + PY$.*

We remark that results similar to Result 3.3 can be found in various places in the literature, for instance, [1, Lemma 2], [3], [9, Lemma 3.1 (i)], [16, Theorem 2.7]. The most general version of the decomposition can be found in [14, Thm. 3.1] and has some nice applications, such as proving the nonexistence of Barker sequences of

length l with $13 < l \leq 10^{22}$ and the nonexistence of circulant Hadamard matrices of order v with $4 < v \leq 548,964,900$, see [14].

In order to make full use of Result 3.3 it is crucial to find further restrictions on D', g and δ.

Corollary 3.4. *There are a set Y of representatives of distinct cosets of P in G, disjoint subsets of A, B of H and a Gauss sum $\mathcal{G}(g,1)$ over G such that up to a translation*

$$D = (A - B)\mathcal{G}(g,1) + PY. \tag{3}$$

Proof. By Result 3.3 we have $D = D'\mathcal{G}(g,\delta) + PY$ with $Y \in \mathbb{Z}[G]$, $D' \in \mathbb{Z}[H]$.

Claim 1: Y can be chosen as a set of representatives of distinct cosets of P in G.

Proof. In any case, we can choose Y such that no two elements of the support of Y are in the same coset of P. Since D is a subset of G, it has coefficients 0 and 1 as an element of $\mathbb{Z}[G]$. Note that by Definition 3.1 all elements of the support of $D'\mathcal{G}(g,\delta)$ have order exactly divisible by p, since $D' \in \mathbb{Z}[H]$. However, each coset Pa of P contains an element, say a', of order *not* exactly divisible by p. This implies that the coefficient of a' in PY coincides with the coefficient of a' in D, and thus must be 0 or 1. Since we assumed that no two elements of the support of Y are in the same coset of P, this shows that Y has coefficients 0 and 1 only. This proves Claim 1.

Claim 2: D' has coefficients $-1, 0, 1$ only, i.e., $D' = A - B$ for disjoint subsets A, B of H.

Proof. By Result 3.3 we have

$$D = \sum_{i=1}^{p-1} (\delta g)^i D' h^{t^i} + PY, \tag{4}$$

where $g, h \in G$ with $o(g)|(p-1)$, $o(h) = p$ and $\delta = \pm 1$. Note that the supports of $(\delta g)^i D' h^{t^i}$, $i = 1, ..., p-1$, are pairwise disjoint, since the supports of $(\delta g)^i D'$ are contained in H, $\langle h \rangle \cap H = 1$ and t is a primitive root mod p. Hence, if D' has a coefficient $\notin \{-1, 0, 1\}$, then the same is true for $\sum_{i=1}^{p-1} (\delta g)^i D' h^{t^i}$. But then D must have a coefficient $\notin \{0, 1\}$ by (4), since PY has coefficients $0, 1$ only, a contradiction. This shows Claim 2.

Claim 3: If $\delta = -1$ and $D' \neq 0$, then $y := o(g)$ is even.

Proof. If $\delta = -1$, then

$$D = \sum_{i=1}^{p-1} (-g)^i D' h^{t^i} + PY.$$

Recall that $p \geq 3$ and $y = o(g)$ divides $p - 1$. Now assume that y is odd. Since $D' \neq 0$, there is $a \in H$ such that ah has coefficient $c \neq 0$ in $(-g)^{p-1} D' h^{t^{p-1}} = D'h$. Then ah^{t^y} has coefficient $-c$ in $(-g)^y D' h^{t^y} = -D' h^{t^y}$. Recall that the supports of $(\delta g)^i D' h^{t^i}$, $i = 1, ..., p-1$, are pairwise disjoint. Hence one of the elements ah or ah^{t^y} has a negative coefficient in $\sum_{i=1}^{p-1} (-g)^i D' h^{t^i}$ and the other one has a positive coefficient. Since both ah and ah^{t^y} are contained in Pa and since D has nonnegative coefficients only, it follows that every element of Pa has coefficient > 0 in PY. However, this implies that either the coefficient of ah or that of ah^{t^y} in D is greater than 1, a contradiction. This shows Claim 3.

Claim 4: $\delta = 1$.

Proof. Note that δ is irrelevant if $D' = 0$. Thus we can assume $D' \neq 0$. Now suppose $\delta = -1$. Then by Claim 3 the order of g is even. In particular, $v = |G|$ is even. Hence by Schützenberger's theorem [7, Cor. II.3.9] the order n of D is a square. Now let χ be a character of G which is trivial on H and nontrivial on P. Then $\chi(P) = 0$ [7, Lemma VI.3.4], and $\chi(D') = |D'|$ since the support of D' is contained in H. Hence $\chi(D) = |D'| \sum_{i=1}^{p-1} (-1)^i \chi(h)^{t^i}$. Note that $\chi(h)$ is a primitive pth root of unity. Thus $\sum_{i=1}^{p-1} (-1)^i \chi(h)^{t^i}$ is a quadratic Gauss sum of absolute value $\sqrt{p}$ [23, Lemma 6.1]. By Result 2.3 we have $|\chi(D)|^2 = n$ and thus $|D'|^2 = n/p$, which is impossible since n is a square. This shows Claim 4.

Corollary 3.4 follows from Claims 1, 2 and 4. □

The following is an improved version of [9, Lemma 3.2 (i)].

Lemma 3.5. *Let A, B be the sets from Corollary 3.4. Then*

$$(A - B)(A - B)^{(-1)} = \frac{n}{p} + \frac{n(p-1)}{o(g)p}\langle g \rangle.$$

Proof. Write $X := \frac{n}{p} + \frac{n(p-1)}{o(g)p}\langle g \rangle$. By Result 2.1 it suffices to show that

$$\chi((A - B)(A - B)^{(-1)}) = \chi(X)$$

for every character χ of H. Let χ be an arbitrary character of H. Let τ be a character of G with $\tau|_H = \chi$ and $\tau \notin P^\perp$. By Result 2.3 and (3) we have

$$n = |\tau(D)|^2 = \left| \chi(A - B) \sum_{i=1}^{p-1} \chi(g)^i \tau(h)^{t^i} \right|^2. \tag{5}$$

Note that $\chi(g)$ is a $(p-1)$th root of unity and $\tau(h)$ is a primitive pth root of unity.

Case 1: $\chi \in \langle g \rangle^\perp$. Then $\sum_{i=1}^{p-1} \chi(g)^i \tau(h)^{t^i} = \sum_{i=1}^{p-1} \tau(h)^{t^i} = \sum_{j=1}^{p-1} \tau(h)^j = -1$, and thus (5) implies $\chi((A-B)(A-B)^{(-1)}) = |\chi(A-B)|^2 = n$. On the other hand, we have $\chi(X) = n/p + n(p-1)/p = n$ since $\chi \in \langle g \rangle^\perp$.

Case 2: $\chi \notin \langle g \rangle^\perp$. Then $|\sum_{i=1}^{p-1} \chi(g)^i \tau(h)^{t^i}|^2 = p$ by [23, Lemma 6.1], and thus (5) implies $\chi((A-B)(A-B)^{(-1)}) = n/p$. On the other hand, we have $\chi(X) = n/p$ since $\chi \notin \langle g \rangle^\perp$.

Hence $\chi((A - B)(A - B)^{(-1)}) = \chi(X)$ for all $\chi \in H^*$, concluding the proof. □

Lemma 3.6. *Let A, B, Y be the sets from Corollary 3.4. The supports of the following group ring elements are disjoint.*

(a) *$A\mathcal{G}(g, 1)$ and $B\mathcal{G}(g, 1)$,*
(b) *$A\langle g \rangle$ and PY,*
(c) *$A\langle g \rangle$ and $B\langle g \rangle$.*

Proof. If the supports of $A\mathcal{G}(g, 1)$ and $B\mathcal{G}(g, 1)$ have a common element, then there are $a \in A$, $b \in B$ and $i, j \in \mathbb{Z}$ with $ag^i h^{t^i} = bg^j h^{t^j}$. As $(p, |H|) = 1$, $h^{t^i} = h^{t^j}$. Since t is a primitive element mod p and $1 \leq i, j \leq p - 1$, we conclude that $i = j$ and thus $a = b$, contradicting $A \cap B = \emptyset$. This proves (a).

For (b), we assume that the supports of $A\langle g \rangle$ and PY have a common element. Then the supports of $A\mathcal{G}(g, 1)$ and PY also have a common element, since $h \in P$. Since all nonzero coefficients of $A\mathcal{G}(g, 1)$ and PY are 1, we conclude from (a) that

the coefficient of those common elements in D must be 2. This is impossible, and we have thus proved (b).

Finally, if (c) is not true, then there is $b \in B \cap A\langle g\rangle$. By (a), the coefficient of $bg^{p-1}h^{t^{p-1}} = bh$ in $(A-B)\mathcal{G}(g,1)$ is -1. Because of (a) and since D has nonnegative coefficients only, this implies $Pb \subset PY$. But then $b \in A\langle g\rangle \cap PY$, contradicting (b). □

4. The order of g and an upper bound for v

Now that we have obtained the crucial equation $D = (A-B)\mathcal{G}(g,1) + PY$ and derived some basic properties of the sets A, B and Y, we need to determine the order of the element g. We will also show that n is a square and derive an upper bound for v in terms of n.

Lemma 3.6 (a) implies that the set $B\mathcal{G}(g,1)$ is contained in PY, since D has only nonnegative coefficients. Since $h \in P$, we deduce that the support of $B\langle g\rangle P$ is also contained in PY. Let

$$C := \left(\bigcup_{b\in B} P\langle g\rangle b\right) - B\mathcal{G}(g,1).$$

Then C is a subset of G, and since the support of $B\langle g\rangle P$ is contained in PY, we can write

$$D = A\mathcal{G}(g,1) + C + PZ \tag{6}$$

for some subset Z of Y. Note that we can choose Z to consist of representatives of distinct cosets of P in G, since the same is true for Y.

The significance of (6) lies in the fact that all terms on the right hand side have coefficients 0 and 1 only. In particular, since D has coefficients 0 and 1 only, the supports of the three terms on the right hand side of (6) are pairwise disjoint. Hence we can get useful lower bounds on $k = |D|$ from (6). It turns out that lower bounds on $|Z|$ are especially desirable. We now list some basic properties of the sets A, B, C, and Z.

Let $\rho : G \to G/P$ be the canonical epimorphism. Write $\rho(Z) = \sum Z_i w_i$, where $Z_i \subset \rho(\langle g\rangle)$ and the w_i are representatives of distinct cosets of $\rho(\langle g\rangle)$ in G/P.

Lemma 4.1. (a) *The supports of $A\langle g\rangle$, $B\langle g\rangle$ and $PZ\langle g\rangle$ are pairwise disjoint.*
(b) $|C| \geq |B|$.
(c)

$$\sum Z_i Z_i^{(-1)} = \frac{n}{p^2} + c\rho(\langle g\rangle) \tag{7}$$

in $\mathbb{Z}[G/P]$, where c is a nonnegative integer. In particular, $|Z| \geq n/p^2$.

Proof. (a) By Lemma 3.6 (c), the supports of $A\langle g\rangle$ and $B\langle g\rangle$ are disjoint. Furthermore, $B\langle g\rangle$ and $PZ\langle g\rangle$ have disjoint supports by the definition of C. Since $Z \subset Y$, the supports of $A\langle g\rangle$ and $PZ\langle g\rangle$ are disjoint by Lemma 3.6 (b).

(b) Observe that $B \subset H$. Therefore no two elements in B are in the same coset of P. So, the number of $P\langle g\rangle$-cosets in $\bigcup_{b\in B} P\langle g\rangle b$ is at least $|B|/o(g)$. Hence, $|\bigcup_{b\in B} P\langle g\rangle b| \geq p|B|$. Recall that $C = \left(\bigcup_{b\in B} P\langle g\rangle b\right) - B\mathcal{G}(g,1)$ and $|\mathcal{G}(g,1)| = p-1$. Thus, we have $|C| \geq p|B| - (p-1)B = |B|$.

(c) We claim that

$$\rho(Z)\rho(Z)^{(-1)} = \frac{n}{p^2} + E\rho(\langle g\rangle) \tag{8}$$

for some $E \in \mathbb{Z}[G/P]$. Note that the characters of G/P can be identified with the characters of G which are trivial on P. Let χ be any character of G which is nontrivial on $\langle g\rangle$ and trivial on P. Then $\chi(\rho(Z)\rho(Z)^{(-1)}) = \chi(ZZ^{(-1)}) = \chi(DD^{(-1)})/p^2 = n^2/p^2$ by (6) and Result 2.3, since $\chi(\mathcal{G}(g,1)) = \sum_{i=1}^{p-1}\chi(g)^i = 0$. Now Result 2.1 implies (8). Equation (7) follows from (8) by restricting it to $\mathbb{Z}[\rho(\langle g\rangle)]$. Since each nonzero coefficient of Z_i is 1, c is a nonnegative integer. □

Theorem 4.2. *n is a square and $o(g) = (p-1)/2$. Moreover, if $r \geq 4$, then the following hold.*

(a) $v \leq 9n/2$,
(b) $p||v$,
(c) $p||\lambda$ *or* $p^{r-1}||\lambda$.

Proof. Let $s := (p-1)/o(g)$. Lemma 3.5 gives

$$(A-B)(A-B)^{(-1)} = \frac{n}{p} + \frac{ns}{p}\langle g\rangle. \tag{9}$$

Applying the trivial character to (9) gives $|A| - |B| = \pm\sqrt{n}$. In particular, n is a square. On the other hand, comparing the coefficient of 1 in (9) yields $|A| + |B| = (1+s)n/p$. Hence

$$|A| = \frac{(1+s)(n/p) \pm \sqrt{n}}{2} \text{ and } |B| = \frac{(1+s)(n/p) \mp \sqrt{n}}{2}. \tag{10}$$

Since n is odd and $|A|$ is an integer, s is even. Recall that any nonzero coefficient of A, C, Z is 1 in (6). Hence (6), Lemma 4.1 and (10) imply

$$\begin{aligned} k = |D| &\geq (p-1)|A| + |B| + p|Z| \\ &\geq \frac{p-1}{2}\left[\frac{(1+s)n}{p} \pm \sqrt{n}\right] + \frac{1}{2}\left[\frac{(1+s)n}{p} \mp \sqrt{n}\right] + \frac{n}{p} \\ &= \frac{(1+s)n}{2} \pm \frac{(p-2)\sqrt{n}}{2} + \frac{n}{p}. \end{aligned} \tag{11}$$

As $n \geq p^2$, $(p-2)\sqrt{n}/2 < n/2$. Hence $k > sn/2$. Recall that $k < 2n$ by (1). Thus $s < 4$. Since s is even, we conclude that $s = 2$ and thus $o(g) = (p-1)/2$.

From now on, we assume $r \geq 4$. In that case, $(p-2)\sqrt{n}/2 < n/p$. Hence $k > 3n/2 - n/p + n/p = 3n/2$. Thus $\lambda = k - n > n/2$. Since $\lambda < n$ by (1), we have $\lambda/n \in (1/2, 1)$. Moreover, $k^2 = n + \lambda v$ and thus $(n+\lambda)^2 = k^2 > \lambda v$. Hence

$$v \leq n(1 + \frac{\lambda}{n})(\frac{n}{\lambda} + 1) = n(2 + \frac{\lambda}{n} + \frac{n}{\lambda}). \tag{12}$$

For $n/\lambda \in (1/2, 1)$ we have $(\lambda/n + n/\lambda) < 5/2$, and thus we get $v \leq 9n/2$.

Suppose p^2 divides v. Then by [2, Cor. 4], we get $4(p-1)n \leq v$. Hence $4(p-1)n \leq v \leq 9n/2$. This is impossible when $p \geq 3$. This proves (b).

Recall that $n = p^r$. We have $(n+\lambda)^2 = n + \lambda v$, and hence

$$\lambda^2 + 2\lambda p^r + p^{2r} - p^r = \lambda v. \tag{13}$$

We define β by $p^\beta||\lambda$. Since $\lambda < n$, we have $\beta < r$. Observe that

$$p^{2\beta}||\lambda^2,\ p^{\beta+r}||\lambda p^r,\ p^r||(p^{2r}-p^r),\ \text{and}\ p^{\beta+1}||\lambda v.$$

Hence either $\beta = 1$ or $r = \beta + 1$ by (13). □

5. A lower bound for λ/n

For the rest of this article, we assume $p \geq 5$. Note that by Lemma 4.2 we can also assume $o(g) = (p-1)/2$.

Consider the decompositions $D = (A-B)\mathcal{G}(g,1) + PY = A\mathcal{G}(g,1) + C + PZ$. The key idea of our proof of Theorem 1.3 is that the algebraic property of the sets A, B obtained in Lemma 3.5 forces the sets A, B and Z to touch too many cosets of $P\langle g\rangle$ in G. On one hand, we obtain lower bounds on $|A|$, $|C|$ and $|Z|$ from Lemma 3.5. It turns out that this corresponds to a lower bound on λ/n. On the other hand, the number of cosets of $P\langle g\rangle$ touched by A, B and Z trivially cannot exceed the total number of cosets of $P\langle g\rangle$ in G. Together with lower bounds obtained from Lemma 3.5 this gives an upper bound on λ/n irreconcilable with its lower bound thus showing that no such difference set can exist.

Our strategy to get the lower bound for λ/n is as follows. In order to make use of the key equation $D = A\mathcal{G}(g,1) + C + PZ$ we first derive a lower bound on $|Z|$ from Lemma 3.5. Along the way we derive lower bounds on the number of cosets of $\langle g\rangle$ touched by A and B (respectively, Z) which will be useful for obtaining an upper bound on λ/n. The lower bound on $|Z|$ together with the key equation gives a lower bound on $k = |D|$, since we know $|A|$ and $|B|$ from (10). Since $k - n = \lambda$, the lower bound on k gives also a lower bound on λ and hence on λ/n.

Recall that

$$D = (A-B)\mathcal{G}(g,1) + PY = A\mathcal{G}(g,1) + C + PZ \tag{14}$$

by (3) and (6). Furthermore, (11) becomes

$$(A-B)(A-B)^{(-1)} = \frac{n}{p} + \frac{2n}{p}\langle g\rangle, \tag{15}$$

since $o(g) = (p-1)/2$.

Notation 5.1. By l we denote the number of cosets of $\langle g\rangle$ in H which have nonempty intersection with A or B. In view of Lemma 3.6 (c), we can write

$$A - B = \sum_{i=1}^{l} \pm e_i U_i,$$

where $e_1, ..., e_l$ are representatives of distinct cosets of $\langle g\rangle$ in H and $U_1, ..., U_l$ are subsets of $\langle g\rangle$.

Lemma 5.2.

$$\frac{9n}{p^2} < l \leq \frac{2v}{p(p-1)}$$

Proof. Since $|H| \leq v/p$ there are at most $2v/[p(p-1)]$ cosets of $\langle g\rangle$ in H. Hence $l \leq 2v/[p(p-1)]$. Comparing the coefficient of 1 in (15) gives $\sum_{i=1}^{l} |U_i| = 3n/p$.

On the other hand, comparing the sum of the coefficients of all elements of $\langle g\rangle$ in (15) gives $\sum_{i=1}^{l}|U_i|^2 = n$. Cauchy's inequality yields

$$l\sum_{i=1}^{l}|U_i|^2 \geq (\sum_{i=1}^{l}|U_i|)^2,$$

and thus $l \geq 9n/p^2$. Note that equality occurs if and only if all $|U_i|$'s are equal. In this case, $l = 9n/p^2$ divides $3n/p = \sum_{i=1}^{l}|U_i|$. But this is impossible, as $p > 3$. □

Lemma 5.2 together with Lemma 4.2(a) shows that $A \cup B$ has common elements with "almost all" cosets of $\langle g\rangle$ in H. Our goal now is to show that there is not enough space left for the set Z from (14).

Notation 5.3. By m we denote the number of cosets of $\langle g\rangle$ in G which have a common element with Z.

Lemma 5.4. (a) $m \geq 4n/[p^2(p-1)]$.

(b) *If* $r \geq 4$, *then* $|Z| \geq (9n/4p^2)\left(1 - \frac{1}{3}\sqrt{1+\frac{16}{p-1}}\right)$.

Proof. As in Lemma 4.1, write $\rho(Z) = \sum_{i=1}^{m} Z_i w_i$, where the w_i are representatives of distinct cosets of $\rho(\langle g\rangle)$ in G/P. Recall that

$$\sum_{i=1}^{m} Z_i Z_i^{(-1)} = \frac{n}{p^2} + c\rho(\langle g\rangle),$$

where c is a nonnegative integer by Lemma 4.1. Let $T_i := Z_i$ if $|Z_i| \leq (p-1)/4$ and $T_i := \rho(\langle g\rangle) - Z_i$ if $|Z_i| > (p-1)/4$. Then

$$\sum_{i=1}^{m} T_i T_i^{(-1)} = \frac{n}{p^2} + d\rho(\langle g\rangle) \tag{16}$$

for some nonnegative integer d. Comparing the coefficient of 1 in (16) gives $\sum_{i=1}^{m}|T_i| \geq n/p^2$. On the other hand, since $|T_i| \leq (p-1)/4$ by definition, we have $\sum_{i=1}^{m}|T_i| \leq m(p-1)/4$. Hence $m \geq 4n/[p^2(p-1)]$.

By the definition of l, exactly l cosets of $P\langle g\rangle$ have a common element with A or B. Since the group ring elements $A\langle g\rangle$, $B\langle g\rangle$ and $PZ\langle g\rangle$ have pairwise disjoint supports by Lemma 4.1, this implies $m \leq 2v/[p(p-1)] - l$. By Lemmas 4.2 and 5.2, we have $v \leq 9n/2$ and $l > 9n/p^2$. Thus $m < 9n/[p(p-1)] - 9n/p^2 = 9n/[p^2(p-1)]$.

Comparing the sum of all coefficients of nonidentity elements in (16), we get $\sum_{i=1}^{m}|T_i|(|T_i|-1) = d(p-3)/2$. Comparing the coefficient of 1 in (16) gives

$$\sum_{i=1}^{m}|T_i| = \frac{n}{p^2} + d = \frac{n}{p^2} + \frac{2\sum_{i=1}^{m}|T_i|(|T_i|-1)}{p-3}.$$

Rearranging this equation yields

$$\frac{n(p-3)}{p^2} = (p-1)(\sum_{i=1}^{m}|T_i|) - 2\sum_{i=1}^{m}|T_i|^2. \tag{17}$$

By Cauchy's inequality, we have

$$m\sum_{i=1}^{m}|T_i|^2 \geq \left(\sum_{i=1}^{m}|T_i|\right)^2.$$

Since $m < 9n/[p^2(p-1)]$, we get

$$\sum_{i=1}^{m} |T_i|^2 \geq \frac{p^2(p-1)(\sum_{i=1}^{m} |T_i|)^2}{9n}.$$

Thus (17) implies

$$\frac{n(p-3)}{p^2} \leq (p-1)(\sum_{i=1}^{m} |T_i|) - \frac{2p^2(p-1)(\sum_{i=1}^{m} |T_i|)^2}{9n}.$$

Substituting $\gamma := p^2(\sum_{i=1}^{m} |T_i|)/n$, we get

$$p - 3 \leq (p-1)\gamma - \frac{2(p-1)}{9}\gamma^2.$$

It is straightforward to show that this implies $\gamma \geq \frac{9}{4}\left(1 - \frac{1}{3}\sqrt{1 + \frac{16}{p-1}}\right)$, completing the proof. □

Corollary 5.5. *Recall that $n = p^r$. Assume $r \geq 4$. Then $\frac{\lambda}{n} \geq f(p,n)$, where*

$$f(p,n) = \frac{1}{2} - \frac{p-2}{2\sqrt{n}} + \frac{9}{4p}\left(1 - \frac{1}{3}\sqrt{1 + \frac{16}{p-1}}\right).$$

In particular,

$$\frac{\lambda}{n} > \begin{cases} \frac{1}{2} + \frac{p+2}{2p^2} & if\ r \geq 4\ and\ p \geq 11, \\ \frac{1}{2} + \frac{11}{16p} & if\ r \geq 4\ and\ p \geq 17, \\ \frac{1}{2} + \frac{1}{p} & if\ r \geq 6\ and\ p \geq 11. \end{cases}$$

Proof. By (6), Lemma 4.1 (b) and (10) we have

$$k \geq \frac{3n}{2} - \frac{(p-2)\sqrt{n}}{2} + p|Z|.$$

Subtracting n and using Lemma 5.4, we get

$$\lambda \geq \frac{n}{2} - \frac{(p-2)\sqrt{n}}{2} + \frac{9n}{4p}\left(1 - \frac{1}{3}\sqrt{1 + \frac{16}{p-1}}\right).$$

Dividing by n gives $\frac{\lambda}{n} \geq f(p,n)$. Note that

$$\frac{9}{4}\left(1 - \frac{1}{3}\sqrt{1 + \frac{16}{p-1}}\right) > \begin{cases} 1 & \text{for } p \geq 11, \\ 19/16 & \text{for } p \geq 17. \end{cases}$$

Hence

$$f(p,n) > \frac{1}{2} - \frac{p-2}{2p^2} + \frac{1}{p} = \frac{1}{2} + \frac{p+2}{2p^2}$$

for $r \geq 4$ and $p \geq 11$, and

$$f(p,n) > \frac{1}{2} - \frac{p-2}{2p^2} + \frac{19}{16p} > \frac{1}{2} + \frac{11}{16p}$$

for $r \geq 4$ and $p \geq 17$.

Now let $r \geq 6$. Note that $f(p,n) \geq \frac{1}{2} + \frac{g(p)}{p}$, where

$$g(p) = -\frac{p-2}{2p^2} + \frac{9}{4}\left(1 - \frac{1}{3}\sqrt{1 + \frac{16}{p-1}}\right).$$

But g is an monotonically increasing function on $[11, \infty)$, and thus $g(p) \geq g(11) > 1$ for $p \geq 11$. Hence $\frac{\lambda}{n} \geq f(p,n) > \frac{1}{2} + \frac{1}{p}$ for $p \geq 11$. □

6. An upper bound for λ/n

Recall that l is the number of cosets of $\langle g\rangle$ in H which have nonempty intersection with A or B, and that m is the number of cosets of $\langle g\rangle$ in G which have a common element with Z. In the last section, we obtained lower bounds on l and m. It turns out that these lower bounds imply an upper bound on λ/n, because high values of λ/n imply that there is not enough space in G for A, B and Z. In this way, we get the following result.

Lemma 6.1.

$$\lambda/n < \begin{cases} (p+2)/(2p) & \text{if } p \geq 17, \\ (6-\sqrt{11})/5 & \text{if } p = 5, \\ (17-\sqrt{93})/14 & \text{if } p = 7, \\ (79-\sqrt{1885})/66 & \text{if } p = 11, \\ (31-\sqrt{285})/26 & \text{if } p = 13. \end{cases}$$

Proof. By Lemma 5.4(a), we have $m \geq 4n/[p^2(p-1)]$. Since Z consists of representatives of distinct cosets of P in G, m is also the number of cosets of $P\langle g\rangle$ in G which have a common element with Z. Recall that $l > 9n/p^2$ by Lemma 5.2. Since $H \cap P = \{1\}$, the number of cosets of $P\langle g\rangle$ in G with nonempty intersection with A or B is also l. As the group ring elements $A\langle g\rangle$, $B\langle g\rangle$ and $PZ\langle g\rangle$ have pairwise disjoint supports by Lemma 4.1(a), none of the $2v/[p(p-1)]$ cosets of $P\langle g\rangle$ in G can contribute to both m and l. This implies $m+l \leq 2v/[p(p-1)]$. Using $v\lambda < (n+\lambda)^2$ and writing $\tau := \lambda/n$, we conclude that

$$\frac{p(p-1)(m+l)}{2n} < \frac{(n+\lambda)^2}{\lambda n} = \tau + 2 + \frac{1}{\tau}. \tag{18}$$

Using the lower bounds for l and m, we get $\frac{2}{p} + \frac{9(p-1)}{2p} < \tau + 2 + \frac{1}{\tau}$, and thus

$$\tau + 2 + \frac{1}{\tau} > \frac{9p-5}{2p}.$$

Note that the function $h(s) := s + 2 + \frac{1}{s}$ is monotonically decreasing on $(0, 1]$ and

$$h((p+2)/(2p)) - [(9p-5)/(2p)] = -(p-14)/[2p(p+2)] < 0$$

for $p > 14$. Thus $\tau < (p+2)/(2p)$ for $p \geq 17$.

For $p = 5$, we need to improve our lower bound for l. Recall that $A - B = \sum_{i=1}^{l} \pm e_i U_i$, where $e_1, ..., e_l$ are representatives of distinct cosets of $\langle g\rangle$ in H and $U_1, ..., U_l$ are subsets of $\langle g\rangle$. Since $p = 5$, we have $o(g) = 2$, and thus $|U_i| \in \{1, 2\}$ for all i. Let a and b be the number of i's with $|U_i| = 1$ and $|U_i| = 2$ respectively. By restricting (9) to $\mathbb{Z}[\langle g\rangle]$, we get $\sum_{i=1}^{l} U_i U_i^{(-1)} = (n/5) + (2n/5)\langle g\rangle$. This implies $a = b = n/5$. Thus $l = a + b = 2n/5$. Using (18) and $m \geq 4n/[p^2(p-1)]$, we get $\tau + 2 + 1/\tau > 22/5$. This implies $\tau < (6-\sqrt{11})/5$.

Now let $p \in \{7, 13\}$. For this case, we get a better lower bound for m than in Lemma 5.4 as follows. As before, let $\rho : G \to G/P$ be the canonical epimorphism. Note that $o(g) = (p-1)/2$ is divisible by 3. Let W be the subgroup of order 3 in $\langle g\rangle$. Write $\rho(Z) = \sum W_i v_i$, where the W_i are nonempty subsets of $\rho(W)$ and the v_i are representatives of distinct cosets of $\rho(W)$ in G/P. It is straightforward to check that

$$W_i W_i^{(-1)} = \begin{cases} 1 & \text{if } |W_i| = 1, \\ 1 + W & \text{if } |W_i| = 2, \\ 3W & \text{if } |W_i| = 3. \end{cases} \tag{19}$$

Exactly in the same way as we proved (7), we obtain $\sum W_i W_i^{(-1)} = \frac{n}{p^2} + e\rho(W)$ for some nonnegative integer e. Together with (19) this implies that the number of i's with $|W_i| = 1$ or $|W_i| = 2$ is n/p^2. Thus $m \geq n/p^2$ if $p = 7$ and $m \geq n/(2p^2)$ if $p = 13$. Hence, in both cases, $m \geq 6n/[p^2(p-1)]$. Using (18) and $l > 9n/p^2$, we get

$$\tau + 2 + \frac{1}{\tau} > \frac{9p-3}{2p}.$$

For $p = 13$ this implies $\tau < (31 - \sqrt{285})/26$, as desired.

For $p = 7$, we also need to refine our estimate for l. Writing $A - B = \sum_{i=1}^{l} \pm e_i U_i$ as above, we have $|U_i| \in \{1, 2, 3\}$ for all i, and

$$U_i U_i^{(-1)} = \begin{cases} 1 & \text{if } |U_i| = 1, \\ 1 + \langle g \rangle & \text{if } |U_i| = 2, \\ 3\langle g \rangle & \text{if } |U_i| = 3. \end{cases} \tag{20}$$

Restricting (9) to $\mathbb{Z}[\langle g \rangle]$, we get

$$\sum_{i=1}^{l} U_i U_i^{(-1)} = (n/7) + (2n/7)\langle g \rangle. \tag{21}$$

For $j = 1, 2, 3$ let C_j be the number of i's with $|U_i| = j$ respectively. Comparing the coefficient of 1 in (21) gives $C_1 + 2C_2 + 3C_3 = 3n/7$. Comparing the coefficient of a nonidentity element in (21) and using (20) gives $C_2 + 3C_3 = 2n/7$. Thus $C_1 + C_2 = n/7$ and $C_3 = (-C_2 + 2n/7)/3 \geq n/21$. Hence $l = C_1 + C_2 + C_3 \geq 4n/21$. Combining this with (18) and $m \geq 6n/[p^2(p-1)]$ gives $\tau + 2 + \frac{1}{\tau} > 31/7$. This implies $\tau < (17 - \sqrt{93})/14$ as desired.

Finally, we consider the case $p = 11$. As in Lemma 4.1, write

$$\rho(Z) = \sum_{i=1}^{m} Z_i Z_i^{(-1)}.$$

Recall that

$$\sum_{i=1}^{m} Z_i Z_i^{(-1)} = \frac{n}{p^2} + c\rho(\langle g \rangle) \tag{22}$$

by Lemma 4.1, where c is a nonnegative integer. For $j = 1, ..., 5$ let a_j be the number of Z_i's with j elements respectively. Comparing the coefficient of 1 in (22) gives $a_1 + 2a_2 + 3a_3 + 4a_4 + 5a_5 = (n/p^2) + c$. Comparing the sum of all coefficients of nonidentity elements in (22) yields $c = (2a_2 + 6a_3 + 12a_4 + 20a_5)/4$. Combining the last two equations, we get

$$a_1 + \frac{3}{2}(a_2 + a_3) + a_4 = \frac{n}{p^2}.$$

This implies

$$m = a_1 + a_2 + a_3 + a_4 + a_5 \geq \frac{2}{3}\left[a_1 + \frac{3}{2}(a_2 + a_3) + a_4\right] = \frac{2n}{3p^2}.$$

Combining this with (18) and $l > 9n/p^2$, we get $\tau + 2 + \frac{1}{\tau} > 145/33$. This implies $\tau < (79 - \sqrt{1885})/66$, as desired. □

7. Proof of Theorem 1.3

Recall that $n = p^r$ and that we assume $p \geq 5$.

Lemma 7.1. $r = 2$.

Proof. Recall that by Lemma 4.2, n is a square. Suppose $r \geq 4$. By Corollary 5.5 we have $\frac{\lambda}{n} \geq f(p,n)$. Note that $f(p,n) \geq f(p,p^4)$, since $r \geq 4$. Thus $\lambda/n \geq f(p,p^4)$. For $p = 5, 7, 11, 13$ this contradicts Lemma 6.1, which can checked by straightforward computation. Hence $p \geq 17$. If $r \geq 6$, then $\frac{\lambda}{n} > \frac{1}{2} + \frac{1}{p}$ by Corollary 5.5. This contradicts Lemma 6.1. Hence $r = 4$.

It remains to show that the case $p \geq 17$ and $r = 4$ cannot occur. In this case, we have $p||\lambda$ or $p^3||\lambda$ by Lemma 4.2 (c).

If $p^3||\lambda$, then $\lambda = p^3\lambda_1$, where $1 \leq \lambda_1 < p$ since $\lambda < n = p^4$. By Corollary 5.5 we have $\lambda/n > (1/2) + (p+2)/(2p^2)$ and thus $\lambda_1 > (p+1)/2 + (1/p)$. Since λ_1 is an integer, we get $\lambda_1 \geq (p+3)/2$ and hence $\lambda/n \geq (p+3)/(2p)$. This contradicts Lemma 6.1. Thus $p^3||\lambda$ is impossible.

If $p||\lambda$, write $\lambda = p\lambda_1$ with $(p, \lambda_1) = 1$. It follows from (13) that λ_1 is a divisor of $p^4 - 1$. Thus $p^4 - 1 = \beta\lambda_1$ for some $\beta \in \mathbb{N}$. Note that $(p-1)/2$ divides v since $o(g) = (p-1)/2$. Hence $v = (p-1)v_1/2$ for some $v_1 \in \mathbb{N}$. Dividing (13) by λ, we get

$$\lambda + 2p^4 + \beta p^3 = \frac{p-1}{2} v_1. \tag{23}$$

Observe that $\beta = p(p^4 - 1)/\lambda = p(1 - 1/p^4)(n/\lambda)$. Therefore, Corollary 5.5 and Lemma 6.1 imply

$$p\left(1 - \frac{1}{p^4}\right)\frac{2p}{p+2} < \beta < p\left(1 - \frac{1}{p^4}\right)\frac{16p}{8p+11}. \tag{24}$$

It is straightforward to check that the left hand side of (24) is larger than $2p - 4$ while the right hand side is smaller than $2p - 2$. This implies $\beta = 2p - 3$. As $\beta\lambda_1 = p^4 - 1$ and $(2p - 3, p - 1) = 1$, it follows that $p - 1$ divides λ. Hence (23) implies

$$\lambda + 2p^4 + \beta p^3 \equiv 2 + (2p - 3) \equiv 0 \pmod{\frac{p-1}{2}},$$

a contradiction. □

Proof of Theorem 1.3. In view of Lemma 4.2 and Lemma 7.1, we may assume $o(g) = (p-1)/2$ and $r = 2$. In this case, we have $|A| = (3p \pm p)/2$ and $|B| = (3p \mp p)/2$ by (10).

Using Result 2.3 and applying a character of G which is nontrivial on $\langle g \rangle$ and trivial on P to (6), we see that $|Z| > 0$. Thus (11) implies $k \geq (p-1)|A| + |B| + p$. If $|A| = 2p$, then $k \geq 2p^2 = 2n$, contradicting (1). Thus $|A| = p$ and $|B| = 2p$. Let N be the number of cosets of $P\langle g \rangle$ in G which have a common element with B. Since $B \subset H$, we get $N \geq 2p/[(p-1)/2] > 4$. Hence $N \geq 5$. Recall that

$$C = \left(\bigcup_{b \in B} P\langle g \rangle b\right) - B\mathcal{G}(g, 1).$$

Since $N \geq 5$, we get

$$|C| \geq \frac{5p(p-1)}{2} - |B|(p-1) = \frac{p(p-1)}{2}.$$

Hence (6) implies

$$k = |D| \geq (p-1)|A| + |C| + p \geq (p-1)p + \frac{p(p-1)}{2} + p = \frac{3p^2 - p}{2}.$$

Thus $\lambda \geq (p^2-p)/2$ and $\lambda/n = \lambda/p^2 \geq (p-1)/(2p)$. Using (12) and the fact that the function $f(x) = x + 1/x$ is monotonically decreasing on $(0,1]$, we get

$$v \leq p^2(2 + \frac{\lambda}{n} + \frac{n}{\lambda}) \leq p^2(2 + \frac{p-1}{2p} + \frac{2p}{p-1}) = 4p^2 + \frac{(p-1)p}{2} + 2p + \frac{2p}{p-1}.$$

Hence

$$\frac{v}{p} \leq 4p + 2 + \frac{p-1}{2} = 9\left(\frac{p-1}{2}\right) + 6. \tag{25}$$

Recall that l is the number of cosets of $P\langle g\rangle$ which have a common element with A or B, and that the group ring elements A, B and $P\langle g\rangle Z$ have pairwise disjoint supports by Lemma 4.1. Since $|Z| \geq 1$, the element $P\langle g\rangle Z$ covers at least one coset of $P\langle g\rangle$. Hence $l \leq (2v/(p(p-1))) - 1$. On the other hand, Lemma 5.2 gives $l \geq 10$. This implies

$$\frac{v}{p} \geq 11\left(\frac{p-1}{2}\right). \tag{26}$$

From (25) and (26) we conclude that $p \leq 7$, i.e., $n = 25$ or $n = 49$. But these cases are well known to be impossible, see [4], [8] and [12]. □

8. Further results and some open cases

Recall that we need the assumption $p > 3$ in Theorem 1.3. Nevertheless, for $p = 2, 3$ we also get strong results by our methods. For $p = 3$, only three cases remain which need further investigation. We mention this result without proof, but omit the result for $p = 2$ since we find it too tedious to state here.

Result 8.1. *Let G be an abelian group containing a (v,k,λ,n)-difference set with $n = 3^r$, $3|v$, and assume that the Sylow 3-subgroup of G is cyclic. Then n is a square, and one of the following holds:*

(i) $v = (25n-9)/6$ *and* $3^{r-1}||\lambda$.
(ii) $v = (49n-9)/12$ *and* $3||\lambda$.
(iii) $v = (64n-9)/15$ *and* $3||\lambda$.

We remark that Result 8.1 in particular excludes $(v,k,\lambda,n) = (2691, 270, 27, 243)$, a case listed as open in [6]. To our knowledge, $(v,k,\lambda,n) = (465, 145, 45, 100)$ is the smallest open case of Lander's conjecture. We conclude this paper by listing a few further open cases of Lander's conjecture taken from [6]:

v	k	λ	n
945	177	33	144
5859	203	7	196
2233	217	21	196
1785	224	28	196

Acknowledgment

We thank the anonymous referee for helpful suggestions concerning the exposition of the paper.

References

[1] K.T. Arasu, S.L. Ma: Abelian difference sets without self-conjugacy. *Des. Codes Cryptogr.* **15** (1998), 223-230. MR **2000a:**05040

[2] K.T. Arasu, S.L. Ma: A nonexistence result on difference sets, partial difference sets and divisible difference sets. *J. Stat. Planning and Inference* **95** (2001), 67-73. MR **2002b:**05025

[3] K.T. Arasu, S.L. Ma: Some new results on circulant weighing matrices. *J. Alg. Combin.* **14** (2001), 91-101. MR **2002k:**05045

[4] L.D. Baumert: Difference Sets. *SIAM J. Appl. Math.* **17** (1969), 826-833. MR **41:**80

[5] L.D. Baumert: *Cyclic Difference Sets.* Springer Lecture Notes **182**, Springer 1971. MR **44:**97

[6] L.D. Baumert, D.M. Gordon: On cyclic difference sets. Preprint.

[7] T. Beth, D. Jungnickel, H. Lenz: *Design Theory* Vols. I, II (2nd edition). Cambridge University Press 1999. MR **2000h:**05019; MR **2000j:**05002

[8] M. Hall: A survey of difference sets. *Proc. Amer. Math. Soc.* **7** (1956), 975-986. MR **18:**560h

[9] Z. Jia: New necessary conditions for the existence of difference sets without self-conjugacy. *J. Comb. Theory Ser. A* **98** (2002), 312-327. MR **2003g:**05029

[10] D. Jungnickel: Difference Sets. *Contemporary Design Theory: A Collection of Surveys, eds. J.H. Dinitz, D.R. Stinson.* Wiley 1992, 241-324. MR **94c:**05001

[11] D. Jungnickel, B. Schmidt: Difference Sets: An Update. *Geometry, Combinatorial Designs and Related Structures. Proc. First Pythagorean Conference, eds. J.W.P. Hirschfeld et al.* Cambridge University Press 1997, 89-112. MR **2001a:**05024

[12] L.E. Kopilovich: Difference sets in noncyclic abelian groups. *Kibernetika* (*Kiev*) **1989**, no. 2, 20-23; English transl., *Cybernetics* **25** (1989), 153–157. MR **90g:**05047

[13] E.S. Lander: *Symmetric Designs: An Algebraic Approach.* London Math. Soc. Lect. Notes **75**, Cambridge University Press 1983. MR **85d:**05041

[14] K.H. Leung, B. Schmidt: The field descent method. Submitted. Download from `http://www.math.uni-augsburg.de/opt/bschmidt/download_pub.html`

[15] R.A. Liebler: The inversion formula. *J. Comb. Math. Comb. Comput.* **13**, (1993), 143-160. MR **94f:**20014

[16] S.L. Ma: Planar Functions, Relative Difference Sets and Character Theory. *J. Algebra* **185** (1996), 342-356. MR **98b:**05016

[17] A. Pott: *Finite geometry and character theory.* Springer Lecture Notes **1601**, Springer 1995. MR **98j:**05032

[18] H.J. Ryser: *Combinatorial Mathematics.* Wiley 1963. MR **27:**51

[19] B. Schmidt: Cyclotomic integers and finite geometry. *J. Am. Math. Soc.* **12** (1999), 929-952. MR **2000a:**05042

[20] B. Schmidt: *Characters and cyclotomic fields in finite geometry.* Springer Lecture Notes in Mathematics **1797** (2002).

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

[22] R.J. Turyn: Character sums and difference sets. *Pacific J. Math.* **15** (1965), 319-346. MR **31:**3349

[23] L.C. Washington: *Introduction to Cyclotomic Fields.* 2nd ed., Graduate Texts in Math. 83, Springer, Berlin/Heidelberg/New York 1997. MR **97h:**11130

Department of Mathematics, National University of Singapore, Kent Ridge, Singapore 119260, Republic of Singapore

E-mail address: `matlkh@nus.edu.sg`

Department of Mathematics, National University of Singapore, Kent Ridge, Singapore 119260, Republic of Singapore

E-mail address: `matmasl@nus.edu.sg`

Institut für Mathematik, Universität Augsburg, 86135 Augsburg, Germany

E-mail address: `schmidt@math.uni-augsburg.de`