1996

# Exponent Bounds for a Family of Abelian Difference Sets

K. T. Arasu

James A. Davis
*University of Richmond*, jdavis@richmond.edu

Jonathan Jedwab

Siu Lun Ma

Robert L. McFarland



## Recommended Citation

Arasu, K. T., James A. Davis, Jonathan Jedwab, Siu Lun Ma, and Robert L. McFarland. "Exponent Bounds for a Family of Abelian Difference Sets." In *Groups, Difference Sets, and the Monster: Proceedings of a Special Research Quarter at the Ohio State University, Spring 1993*, edited by K. T. Arasu, J. F. Dillon, K. Harada, S. Sehgal, and R. Solomon, 129-43. Ohio State University Mathematical Research Institute Publications. New York: Walter De Gruyter, 1996.

# Exponent bounds for a family of abelian difference sets

*K.T. Arasu*[1], *James A. Davis*[2], *Jonathan Jedwab*,
*Siu Lun Ma*, and *Robert L. McFarland*

**Abstract.** Which groups $G$ contain difference sets with the parameters $(v, k, \lambda) = (q^3 + 2q^2, q^2 + q, q)$, where $q$ is a power of a prime $p$? Constructions of K. Takeuchi, R.L. McFarland, and J.F. Dillon together yield difference sets with these parameters if $G$ contains an elementary abelian group of order $q^2$ in its center. A result of R.J. Turyn implies that if $G$ is abelian and $p$ is self-conjugate modulo the exponent of $G$, then a necessary condition for existence is that the exponent of the Sylow $p$-subgroup of $G$ be at most $2q$ when $p = 2$ and at most $q$ if $p$ is an odd prime. In this paper we lower these exponent bounds when $q \neq p$ by showing that a difference set cannot exist for the bounding exponent values of $2q$ and $q$. Thus if there exists an abelian $(96, 20, 4)$-difference set, then the exponent of the Sylow 2-subgroup is at most 4. We also obtain some nonexistence results for a more general family of $(v, k, \lambda)$-parameter values.

## 1. Introduction

A $k$-element subset $D$ of a finite multiplicative group $G$ of order $v$ is called a $(v, k, \lambda)$-*difference set* in $G$ provided that the "differences" $d_1 d_2^{-1}$ for $d_1, d_2 \in D$, $d_1 \neq d_2$, yield every nonidentity element of $G$ exactly $\lambda$ times. We call $v, k, \lambda$ and $n = k - \lambda$ the *parameters* of the difference set. We call $G$ the *group* of the difference set. If the group $G$ is abelian, then we call $D$ an *abelian* difference set.

The *exponent* of a finite abelian group $G$, written $\exp G$, is the order of the largest cyclic subgroup of $G$.

A prime $p$ is said to be *semiprimitive* modulo $w$ if $p^i \equiv -1 \pmod{w}$ for some integer $i$. An integer $m$ is said to be *self-conjugate* modulo $w$ if every prime divisor $p$ of $m$ is semiprimitive modulo $w_p$, where $w_p$ is the largest divisor of $w$ that is not divisible by $p$.

In this paper we obtain improved exponent bounds necessary for the existence of abelian difference sets with the parameters

$$(v, k, \lambda, n) = (q^3 + 2q^2, q^2 + q, q, q^2), \tag{1.1}$$

1 This work is partially supported by NSA grant # MDA 904-94-H-2042 and by NSF grant #NCR-9200265. The author thanks the Mathematics Department, Royal Holloway College, University of London for its hospitality during the time of this research.

2 This work is partially supported by NSA grant # MDA 904-92-H-3067

where $q$ is a prime power that is not a prime and $q$ is self-conjugate modulo the exponent of the group of the difference set.

The parameters (1.1) are a special case $(d = 1)$ of the parameters

$$\begin{aligned} v &= q^{d+1}(\frac{q^{d+1}-1}{q-1}+1) = q^{d+1}(q^d + q^{d-1} + \cdots + q + 2), \\ k &= q^d(\frac{q^{d+1}-1}{q-1}) = q^d(q^d + q^{d-1} + \cdots + q + 1), \\ \lambda &= q^d(\frac{q^d-1}{q-1}) = q^d(q^{d-1} + q^{d-2} + \cdots + q + 1), \\ n &= q^{2d}. \end{aligned} \tag{1.2}$$

Takeuchi **[13]** gave the first construction for difference sets with parameters (1.1) for every prime power $q$. McFarland **[12]** constructs difference sets with parameters (1.2) with $q$ a prime power in any group $G$ (not necessarily abelian) of the specified order $v$ that contains an elementary abelian group of order $q^{d+1}$ as a direct factor. Dillon **[7]** shows that McFarland's construction is valid under the weaker hypothesis that $G$ contain an elementary abelian group of order $q^{d+1}$ in its center. Note that if $G$ is abelian, Dillon's result extends McFarland's construction when $q$ is a power of 2.

On the other hand, a fundamental result of Turyn **[14]** yields (as we show at the beginning of the next section) the following exponent bounds:

Suppose that there exists a difference set with the parameters (1.2) in an abelian group $G$, where $q$ is a power of a prime $p$ that is self-conjugate modulo $\exp G$. Let $P$ be the Sylow $p$-subgroup of $G$. Then $\exp P \leq 2q$ if $p = 2$ and $\exp P \leq q$ if $p$ is an odd prime.

The main result of this paper is that these exponent bounds for $P$ cannot be achieved for the parameters (1.1) when the prime power $q$ is not a prime. For example, since $p = 2$ is self-conjugate modulo $v = 96$, there cannot exist a $(96, 20, 4)$-difference set in an abelian group whose Sylow 2-subgroup has exponent $2q = 8$ or larger.

We also obtain some related nonexistence results for $(q[(q+1)^2\alpha - 1], q(q+1)\alpha, q\alpha)$-difference sets, where $\alpha$ is a positive integer.

Difference sets are usually studied in the context of the group ring $Z[G]$ of the multiplicative group $G$ over the ring of integers $Z$. The definition of a $(v, k, \lambda)$-difference set $D$ in $G$ yields the equation $DD^{(-1)} = n + \lambda G$ in $Z[G]$, where we have identified the sets $D, D^{(-1)}, G$ with the respective group ring elements $D = \sum_{d \in D} d$, $D^{(-1)} = \sum_{d \in D} d^{-1}$, $G = \sum_{g \in G} g$, and $n$ denotes the group ring element $n 1_G$, where $1_G$ is the identity of $G$.

The *contraction* of a difference set $D$ in the group $G$ with respect to a normal subgroup $U$ of $G$ is the multiset $D_U = \{Ud : d \in D\}$. We can identify $D_U$ with group ring element $D_U = \sum_{X \in G/U} t_X X$ in $Z[G/U]$, where $t_X = |X \cap D|$ is the number of elements of $D$ in the coset $X$ of $U$. The coefficients of $D_U$, that is the elements of the multiset $\{t_X : X \in G/U\}$, are called the *intersection numbers* of $D$ relative to $U$. Alternatively, we can view $D_U$ as the image of $D$ under the natural group ring epimorphism $Z[G] \to Z[G/U]$ induced by the group epimorphism $G \to G/U$. Applying the epimorphism to the equation $DD^{(-1)} = n + \lambda G$ yields $D_U D_U{}^{(-1)} = n + \lambda |U| G/U$. Comparing the coefficients on the identity of $G/U$ on both sides of this last equation yields

$$\sum_{X \in G/U} t_X{}^2 = n + \lambda |U|.$$

Clearly,

$$\sum_{X \in G/U} t_X = k.$$

These last two equations are called the *intersection number equations* for $D$ relative to $U$.

Let $G$ be a finite abelian group. Then a *character* $\chi$ of $G$ is a homomorphism of $G$ into the multiplicative group of complex roots of unity. It is well known that under pointwise multiplication the set of all characters of $G$ form a group that is isomorphic to $G$. The identity of this group is the *principal character*, $\chi_0$, that maps every element of $G$ to 1. If $D_U$ is the contraction of a difference set $D$ in $G$ with respect to a (normal) subgroup $U$ of $G$, then $D_U D_U^{(-1)} = n + \lambda |U| G/U$ implies that $\chi(D_U D_U^{(-1)}) \equiv 0 \pmod{n}$ for all nonprincipal characters $\chi$ of $G/U$.

## 2. Main results

We begin with a result of Turyn [**14**, Corollary 1, p. 332], although we state it in a slightly more general form as given by Lander [**10**, Theorem 4.33, pp. 168–174].

**Theorem 2.1.** *Let $D$ be a $(v, k, \lambda)$-difference set in an abelian group $G$. Let $H$ be a subgroup of index $u$ in $G$. Suppose that there is an integer $m$ satisfying:*
1) *$m^2$ divides $k - \lambda$,*
2) $\gcd(m, u) \neq 1$,
3) *$m$ is self-conjugate modulo* $\exp G/H$,
4) *for every prime $p$ dividing $m$ and $u$, the Sylow $p$-subgroup of $G/H$ is cyclic.*

*Then $m \leq 2^{r-1}|H|$, where $r$ is the number of distinct prime divisors of* $\gcd(m, u)$.

**Corollary 2.2.** *Let $D$ be a difference set with the parameters* (1.2) *in an abelian group $G$, where $q \geq 3$ is a power of a prime $p$ that is self-conjugate modulo* $\exp G$. *Let $P$ be the Sylow $p$-subgroup of $G$. Then* $\exp P \leq 2q$ *if $p = 2$ and* $\exp P \leq q$ *if $p$ is an odd prime.*

*Proof.* Let $\exp P = p^e$. Then $P$ can be written as the internal direct product $P = H \times K$, where $K$ is a cyclic group of order $p^e$. Hence $P/H$ is a cyclic group of order $p^e$. Let $m = q^d = p^{fd}$. Then, by the Theorem, $p^{fd} \leq |H|$. If $p = 2$, then $|H| = 2^{f(d+1)+1-e}$, so $2^e \leq 2q$. If $p$ is an odd prime, then $|H| = p^{f(d+1)-e}$, so $p^e \leq q$. □

Note that if $q = 2$ in Corollary 2.2, then the parameters (1.2) become $(v, k, \lambda, n) = (2^{2d+2}, 2^{2d+1} - 2^d, 2^{2d} - 2^d, 2^{2d})$. Repeating the argument in the proof of Corollary 2.2 for these parameters yields $\exp G \leq 2^{d+2}$ — a result obtained by Turyn [**14**, Corollary 2, p. 333]. Davis [**5**] and Kraemer[**9**] have shown that this necessary condition (known as Turyn's exponent bound) is also sufficient — see also the survey articles by Davis and Jedwab [**6**] and Jungnickel [**8**, pp. 284–285].

The following lemma, which we state without proof, appears in Chan, Ma, and Siu [**4**, Theorem 2.2], but the basic idea of the proof goes back to Turyn [**14**, Lemma 3, p. 326].

**Lemma 2.3.** *Let $G$ be an abelian group whose order is divisible by a prime $p$ that is self-conjugate modulo* $\exp G$. *Let $\chi$ be a character of $G$ and let $a$ be a positive integer. If $A \in Z[G]$ satisfies $\chi(AA^{(-1)}) \equiv 0 \pmod{p^{2a}}$, then $\chi(A) \equiv 0 \pmod{p^a}$.*

The next lemma, which we also state without proof, is due to Ma [**11**, Lemma 3.4].

**Lemma 2.4.** *Let $G$ be an abelian group with a nontrivial cyclic Sylow $p$-subgroup and let $P_1$ be the unique subgroup of order $p$. If $A \in Z[G]$ satisfies $\chi(A) \equiv 0 \pmod{p^a}$ for some positive integer $a$ and all nonprincipal characters $\chi$ of $G$, then $A = p^a E + P_1 F$ for some $E, F \in Z[G]$.*

**Lemma 2.5.** *If the group ring element $A$ in Lemma* 2.4 *has nonnegative integer coefficients, then the group ring elements $E$ and $F$ can be chosen to have nonnegative integer coefficients.*

*Proof.* Let $\{g_1, g_2, \ldots\}$ be a set of coset representatives of $P_1$ in $G$. Then we can write $A = \sum_i A_i g_i$ with each $A_i$ in $Z[P_1]$. If $x$ is a generator of $P_1$, then the Lemma implies that each $A_i$ is of the form

$$A_i = \sum_{j=1}^{p} a_{ij} x^j = p^a \sum_{j=1}^{p} b_{ij} x^j + c_i P_1,$$

where the $a_{ij}$'s, $b_{ij}$'s, and $c_i$'s are integers. The following argument applies for each index $i$. Let $k$ be an index for which $a_{ik} = \min\{a_{i1}, a_{i2}, \ldots, a_{ip}\}$. The hypothesis that $A$ has nonnegative coefficients implies that $a_{ik} \geq 0$ and $a_{ij} - a_{ik} \geq 0$ for all $j$. Furthermore,

$$a_{ij} - a_{ik} = (p^a b_{ij} + c_i) - (p^a b_{ik} + c_i) \equiv 0 \pmod{p^a}$$

for all $j$. Hence

$$A_i = \sum_{j=1}^{p} (a_{ij} - a_{ik}) x^j + a_{ik} P_1$$

yields a representation for $A = \sum_i A_i g_i = p^a E + F P_1$ for which $E$ and $F$ have nonnegative integer coefficients. □

**Lemma 2.6.** *Let $D$ be a difference set with the parameters* (1.2) *in an abelian group $G$, where $q = p^f \geq 3$ for some prime $p$ that is self-conjugate modulo* $\exp G$. *Let $P$ be the Sylow $p$-subgroup of $G$ and suppose that* $\exp P = 2q$ *if $p = 2$ and* $\exp P = q$ *if $p$ is an odd prime. If $U$ is any subgroup of $P$ such that $P/U$ is a cyclic group of order* $\exp P$, *then $|U| = q^d$ where $d$ is as defined in* (1.2). *Moreover, some coset of $U$ is a subset of $D$.*

*Proof.* The order of any subgroup $U$ for which $P/U$ is a cyclic group of order $\exp P$ is $|P|/\exp P$. If $p = 2$, then $|P| = 2q^{d+1}$ and $\exp P = 2q$, so $|U| = q^d$. If $p$ is an odd prime, then $|P| = q^{d+1}$ and $\exp P = q$, so again $|U| = q^d$. Let $D_U$ be the contraction of $D$ with respect to $U$. The remarks in the Introduction together with Lemmas 2.3 and 2.4 imply that $D_U$ can be written in the form $D_U = q^d E + P_1 F$, where $P_1$ is the unique subgroup of order $p$ in $G/U$ and $E, F \in Z[G/U]$. We assert that $E \neq 0$. Assume, to the contrary, that $E = 0$. Then $D_U = P_1 F$, so $D_U D_U^{(-1)} = P_1^2 F F^{(-1)} = p P_1 F F^{(-1)}$. Hence the multiset $D_U D_U^{(-1)}$ is a sum of cosets of $P_1$. Since $D_U D_U^{(-1)} = n + \lambda |U| G/U$, this is impossible for $n \neq 0$. Therefore $E \neq 0$, as asserted. Hence $D_U$ must have at least one coefficient equal to $q^d$. Since $D$ has coefficients 0, 1 and $D_U$ is the contraction of $D$ by a subgroup $U$ of order $q^d$, we conclude that some coset of $U$ must be a subset of $D$. □

We now show that the exponent bounds given in Corollary 2.2 can be improved for difference sets with parameters (1.1) if $q$ is a prime power but not a prime. The argument is similar to that used by Arasu, Davis and Jedwab **[1]** to establish an exponent bound for Hadamard difference sets.

**Theorem 2.7.** *Let $G$ be an abelian group of order $q^2(q+2)$, where $q = p^f$ for some integer $f > 1$ and some prime $p$ that is self-conjugate modulo* $\exp G$. *Let $P$ be the Sylow $p$-subgroup of $G$. Then a necessary condition for $G$ to contain a $(q^3+2q^2, q^2+q, q)$-difference set is that* $\exp P < 2q$ *if $p = 2$ and* $\exp P < q$ *if $p$ is an odd prime.*

*Proof.* Suppose that there exists a difference set $D$ with the specified parameters in $G$. Then, by Corollary 2.2, $\exp P \leq 2q$ if $p = 2$ and $\exp P \leq q$ if $p$ is an odd prime. We prove the Theorem by showing that the assumption $\exp P = 2q$ or $q$, according as the prime $p$ is even or odd, leads to a contradiction. We can write $P$ as the internal direct product $P = \langle x \rangle \times \langle y_1 \rangle \times \langle y_2 \rangle \times \cdots \times \langle y_r \rangle$, where $\langle x \rangle$ is a maximal cyclic subgroup of $P$, that is $|\langle x \rangle| = \exp P$; say $|\langle x \rangle| = p^e$. Let $z = x^{p \uparrow (e-1)} y_1$, where $p \uparrow (e-1) = p^{e-1}$. Then $P = \langle x \rangle \times \langle z \rangle \times \langle y_2 \rangle \times \cdots \times \langle y_r \rangle$. Let $U = \langle y_1 \rangle \times \langle y_2 \rangle \times \cdots \times \langle y_r \rangle$ and let $V = \langle z \rangle \times \langle y_2 \rangle \times \cdots \times \langle y_r \rangle$. Then $P/U \cong \langle x \rangle \cong P/V$.. Hence by Lemma 2.6, $D$ contains a coset of $U$ and a coset of $V$, and $|U| = |V| = q$. Let $W = U \cap V$. Then $W = \langle z^p \rangle \times \langle y_2 \rangle \times \cdots \times \langle y_r \rangle$, so $|W| = |V|/p = p^{f-1}$ and $V = W + zW + \cdots + z^{p-1}W$. Furthermore, $z^i W \subseteq z^i U = (x^{p \uparrow (e-1)})^i U$. Since the cosets $\{x^{ip \uparrow (e-1)} U : i = 0, 1, \ldots, p-1\}$ are distinct, the elements of $V$, and hence the elements of any coset of $V$, are distributed over $p$ of the cosets of U with exactly $p^{f-1}$ elements in each of these $p$ cosets. Let $D_U$ be the contraction of $D$ with respect to $U$, and let $t_1, \ldots, t_{v/q}$ be the resulting intersection numbers. Since $D$ contains a coset of

$V$, the above argument shows that at least $p$ of the $t_i$'s satisfy $t_i \geq p^{f-1}$. Since $D$ contains a coset of $U$, at least one $t_i$ is equal to $|U| = q$; say $t_j = q$. The intersection number equations $\sum t_i = k = q^2 + q$ and $\sum t_i{}^2 = k - \lambda + \lambda|U| = 2q^2$ then yield

$$\sum_{i \neq j} t_i = q^2 = \sum_{i \neq j} t_i{}^2.$$

Since the $t_i$'s are nonnegative integers, we conclude that all $t_i$'s, except $t_j$, are 0 or 1. Since $f > 1$, this contradicts the statement above that at least $p$ of the $t_i$'s satisfy $t_i \geq p^{f-1}$. □

Suppose $q = 25$ in Theorem 2.7. Then the group $G$ has order $v = q^2(q+2) = 5^4 \cdot 3^3 = 16875$. Since $5^9 \equiv -1 \pmod{27}$, 5 is self-conjugate modulo 3, 9, and 27. Thus the Theorem and McFarland's construction **[12]** imply that there exists an abelian $(16875, 650, 25)$-difference set if and only if the Sylow 5-subgroup of the group of the difference set is elementary abelian.

Suppose $q = 2^f$ in Theorem 2.7 for some integer $f > 1$. Then the group $G$ has order $v = q^2(q+2) = 2^{2f+1}(2^{f-1}+1)$. Since 2 is self-conjugate modulo $2^{f-1}+1$, we have:

**Corollary 2.8.** *A necessary condition for the existence of an abelian $(2^{2f}(2^f+2), 2^f(2^f+1), 2^f)$-difference set for any integer $f > 1$ is that the exponent of the Sylow 2-subgroup of the group of the difference set be at most $2^f$.*

A recent listing by Jungnickel **[8**, pp. 311–317**]** of the $(v, k, \lambda, n)$-parameters with $n \leq 30$ for which abelian difference sets might exist leaves undecided only the parameters $(96, 20, 4, 16)$ in the following three groups:

$$Z_4 \times Z_8 \times Z_3, \quad Z_2^2 \times Z_8 \times Z_3, \quad Z_2 \times Z_4^2 \times Z_3.$$

Corollary 2.8 rules out the first two of these groups. However, Arasu and Sehgal **[2]** have also shown, using different techniques, that there cannot exist a difference set in the first group. Arasu and Sehgal **[3]** have recently found a difference set in the third group. Combined with the constructions of McFarland **[12]** and Dillon **[7]**, this shows that an abelian $(96, 20, 4)$-difference set exists if and only if the Sylow 2-subgroup of the group of the difference set has exponent at most 4. Thus for $f = 2$, the necessary condition of Corollary 2.8 is also sufficient. It would be of interest to know if this were true for larger values of $f$.

## 3. Generalization

The techniques used in the previous section can be extended to difference sets with other parameter values. Suppose the $v, k, \lambda, n$ parameters are related by $n = p^f\lambda$, where $p$ is a prime and $f$ is a positive integer. Since $n = k - \lambda$, $k = (p^f + 1)\lambda$. The basic parameter relationship $k(k-1) = \lambda(v-1)$ then yields $v = (p^f+1)^2\lambda - p^f$. Suppose, moreover, that $p^f$ divides $v$. Then $p^f$ divides $\lambda$, so $\lambda = p^f\alpha$ for some integer $\alpha$.

Hence

$$(v, k, \lambda, n) = (p^f[(p^f+1)^2\alpha - 1], p^f(p^f+1)\alpha, p^f\alpha, p^{2f}\alpha). \tag{3.1}$$

Setting $\alpha = 1$ and $q = p^f$ yields the parameters (1.1) that were considered in the previous section.

We begin by generalizing a lemma of Ma **[11]** which we have stated as Lemma 2.4.

**Lemma 3.1.** *Let $p$ be a prime and let $G$ be a finite abelian group with a cyclic Sylow $p$-subgroup of order $p^e$ with $e = 0$ permitted. Let $P_i$ be the cyclic subgroup of order $p^i$ for $i = 0, 1, \ldots, e$. Suppose $A$ is an element of the group ring $Z[G]$ that satisfies $\chi(A) \equiv 0 \pmod{p^f}$ for some positive integer $f$ and all nonprincipal characters $\chi$ of $G$. Moreover, if $e < f$ assume that $\chi_0(A) \equiv 0 \pmod{p^f}$ for the principal character $\chi_0$. Then $A$ can be expressed in the form*

$$A = \sum_{i=0}^{m} p^{f-i} P_i E_i,$$

*where $m = \min\{e, f\}$ and the $E_i$ are elements of $Z[G]$. Furthermore, if the coefficients of $A$ are nonnegative, then the $E_i$ can be chosen to have nonnegative integer coefficients.*

*Proof.* We first assume that $e \geq 1$ (hence $m \geq 1$), and prove by induction on $m$ that $A$ can be expressed in the from

$$A = \sum_{i=0}^{m-1} p^{f-i} P_i E_i + P_m F_m, \tag{3.2}$$

where $E_0, \ldots, E_{m-1}, F_m$ are elements of $Z[G]$. We then note that if $A$ has nonnegative coefficients, then $E_0, \ldots, E_{m-1}, F_m$ can be chosen to have nonnegative integer coefficients. If $e = 0$, we set $A = F_0$. To complete the proof we show that if $0 \leq e < f$ (hence $f - m \geq 1$), then $F_m$ can be chosen so that its coefficients are divisible by $p^{f-m}$ while retaining, if hypothesized, nonnegative coefficients.

Let $e \geq 1$. Then the hypothesis of the Lemma and Lemma 2.4 imply that $A = p^f P_0 E_0 + P_1 F_1$ for some $E_0$, $F_1$ in Z[G]—which proves (3.2) when $m = 1$. If $A$ has nonnegative integer coefficients, then Lemma 2.5 implies that $E_0$ and $F_1$ can be chosen to have nonnegative coefficients. Now suppose that $m > 1$ and inductively assume that $A$ can be expressed in the form

$$A = \sum_{i=0}^{t-1} p^{f-i} P_i E_i + P_t F_t \tag{3.3}$$

for some integer $t$ with $1 \leq t < m$, where $E_0, \ldots, E_{t-1}, F_t$ belong to Z[G]. Furthermore, assume that if $A$ has nonnegative integer coefficients, then so do $E_0, \ldots, E_{t-1}, F_t$.

Let $H$ be a group isomorphic to $G/P_t$ and let $\rho\colon G \to H$ be a group epimorphism with kernel $P_t$. Let $\rho^*\colon Z[G] \to Z[H]$ be the natural group ring epimorphism induced by $\rho$. For any character $\psi$ of $H$ there corresponds a character $\psi_G$ of $G$ such that $\psi_G$ has the same value on all elements in any coset of $P_t$ in $G$ (i.e., $P_t$ is in the kernel of

$\psi_G$) and $\psi_G(g) = \psi(\rho(g))$ for all $g$ in $G$. Hence

$$\psi_G(B) = \psi(\rho^* B)$$

for all $B$ in $Z[G]$. By hypothesis $P_e$ is cyclic, so $P_0 \subset P_1 \subset \cdots \subset P_e$. Hence $\psi_G(P_i) = p^i$ for $i = 0, \ldots, t$. Applying $\psi_G$ to (3.3) thus yields

$$\begin{aligned}\psi_G(A) &= p^f \sum_{i=0}^{t-1} \psi_G(E_i) + p^t \psi_G(F_t) \\ &= p^f \sum_{i=0}^{t-1} \psi_G(E_i) + p^t \psi(\rho^* F_t).\end{aligned} \tag{3.4}$$

By hypothesis $\chi(A) \equiv 0 \pmod{p^f}$ for all nonprincipal characters $\chi$ of $G$, so (3.4) implies that $\chi(\rho^* F_t) \equiv 0 \pmod{p^{f-t}}$ for all nonprincipal characters $\chi$ of $H$. Therefore, by Lemma 2.4, there exists $E'_t$, $F'_{t+1}$ in $Z[H]$ such that

$$\rho^* F_t = p^{f-t} E'_t + P' F'_{t+1}, \tag{3.5}$$

where $P'$ is the subgroup of order $p$ in $H$. Suppose $H = \{h_1, \ldots, h_s\}$ with $P' = \{h_1, \ldots, h_p\}$. Since $H \cong G/P_t$, there is a set $\{g_1, \ldots, g_s\}$ of coset representatives of $P_t$ in $G$ indexed so that $\rho(g_i k) = h_i$ for $i = 1, \ldots, s$ and all $k \in P_t$.

We assert that if $B$ is any element of $Z[G]$, then the coefficients of $P_t B$ are uniquely determined by the coefficients of $\rho^* B$. For if

$$B = \sum_{i=1}^{s} \sum_{k \in P_t} b_{ik} g_i k,$$

then

$$\begin{aligned}\rho^* B &= \sum_{i=1}^{s} \sum_{k \in P_t} b_{ik} \rho(g_i k) \\ &= \sum_{i=1}^{s} \left( \sum_{k \in P_t} b_{ik} \right) h_i\end{aligned}$$

and

$$\begin{aligned}P_t B &= \sum_{i=1}^{s} \sum_{k \in P_t} b_{ik} g_i k P_t \\ &= \sum_{i=1}^{s} \left( \sum_{k \in P_t} b_{ik} \right) g_i P_t.\end{aligned}$$

Thus if $E_t$, $P$, $F_{t+1}$ are any elements of $Z[G]$ that are mapped by $\rho^*$ to $E'_t$, $P'$, $F'_{t+1}$, respectively, then $P_t E_t$ and $P_t P F_{t+1}$ are uniquely determined. In particular, $\rho^* P = P' = h_1 + \cdots + h_p$ implies that

$$P_t P = g_1 P_t + \cdots + g_p P_t = \{g \in G\colon \rho(g) \in P'\}.$$

Hence $P_tP$ contains $p|P_t| = p^{t+1}$ elements and is a subgroup of $G$. Since the Sylow $p$-subgroup of $G$ is cyclic, $G$ contains a unique subgroup of order $p^{t+1}$. Thus $P_tP = P_{t+1}$. Then (3.5) implies that

$$P_tF_t = p^{f-t}P_tE_t + P_{t+1}F_{t+1}.$$

Substitution of this expression for $P_tF_t$ in (3.3) completes the induction proof of (3.2).

Note that, if $F_t$ has nonnegative integer coefficients, then so does $\rho^*F_t$. Then Lemma 2.5 implies that $E_t'$ and $F_{t+1}'$ in (3.5) can be chosen to have nonnegative integer coefficients. And then $E_t$ and $F_{t+1}$ can be chosen to have nonnegative integer coefficients.

If $f \le e$, then $m = f$, so (3.2) expresses $A$ in the form stated in the Lemma; hence the proof is complete in this case. Thus assume $0 \le e < f$. Then $m = e$, so $f - m \ge 1$. Let $F_m$ be defined by (3.2) if $m \ge 1$, and if $m = 0$ let $F_0 = A$. To complete the proof we show that $F_m$ can be chosen so that all its coefficients are divisible by $p^{f-m}$.

If $m = e$, then $P_m = P_e$ is the Sylow $p$-subgroup of $G$, so $G$ has a subgroup $H$ such that $G = H \times P_m$. As before, let $\rho: G \to H \cong G/P_m$ be the group epimorphism defined by $\rho(hk) = h$ for $h \in H$ and $k \in P_m$. Thus $\rho^*F_m$ is an element of $Z[H] \subseteq Z[G]$. We can write $F_m$ in the form

$$F_m = \sum_{h\in H}\sum_{k\in P_m} f_{hk}hk$$

for integers $f_{hk}$. Then

$$\begin{aligned}
(\rho^*F_m)\,P_m &= \left(\sum_{h\in H}\sum_{k\in P_m} f_{hk}\rho(hk)\right)P_m \\
&= \sum_{h\in H}\sum_{k\in P_m} f_{hk}hP_m \\
&= \sum_{h\in H}\sum_{k\in P_m} f_{hk}h\,(kP_m) \\
&= \left(\sum_{h\in H}\sum_{k\in P_m} f_{hk}hk\right)P_m \\
&= F_mP_m.
\end{aligned}$$

By hypothesis, $\chi(A) \equiv 0 \pmod{p^f}$ for *all* characters $\chi$ of $G$ since $e < f$. Repeating the argument that led to (3.4) with $t = m$ thus yields $\psi(\rho^*F_m) \equiv 0 \pmod{p^{f-m}}$ for *all* characters $\psi$ of $H$. The well-known inversion formula for the group ring applied to $\rho^*F_m$ yields

$$f_i|H| = \sum_{\psi}\psi(\rho^*F_m)\psi(h_i^{-1}),$$

where $f_i$ is the coefficient of $\rho^*F_m$ on $h_i \in H$ and the summation is over all characters $\psi$ of $H$. Since $p$ does not divide the order of $H$, all coefficients of $\rho^*F_m$ are divisible by $p^{f-m}$. Clearly $\rho^* F_m$ has nonnegative integer coefficients if $F_m$ does. Substitution of $\rho^* F_m$ for $F_m$ completes the proof of Lemma 3.1. □

**Theorem 3.2.** *Let $G$ be a finite group with a normal subgroup $U$ of order $p^f$, where $p$ is a prime and $f$ is any positive integer, such that $G/U$ is abelian with a cyclic Sylow $p$-subgroup. Suppose furthermore that $p$ is self-conjugate modulo* $\exp G/U$. *Let $\phi^*: Z[G] \to Z[G/U]$ be the natural group ring epimorphism induced by the group epimorphism $\phi: G \to G/U$ with kernel $U$. Let $D$ be a difference set with parameters* (3.1) *in $G$. Then $p^f$ divides the order of $G/U$ and $\phi^* D = p^f S + P_f T$, where $P_f$ is the subgroup of order $p^f$ in $G/U$ and $S, T$ are subsets of $G/U$ with cardinalities $|S| = \alpha$, $|T| = p^f \alpha$. Moreover, each coset of $P_f$ in $G/U$ contains at most one element of $S \cup T$. Hence $P_f T$ is a subset of $G/U$ that is disjoint from $S$.*

*Proof.* For all nonprincipal characters $\chi$ of $G/U$,

$$\chi(\phi^* D)\chi^{-1}(\phi^* D) = \chi\left(\phi^*(DD^{(-1)})\right) = n \equiv 0 \pmod{p^{2f}}.$$

Since $p$ is self-conjugate modulo $\exp G/U$, Lemma 2.3 implies $\chi(\phi^* D) \equiv 0 \pmod{p^f}$ for all nonprincipal characters $\chi$. Also, $\chi_0(\phi^* D) = k \equiv 0 \pmod{p^f}$ for the principal character $\chi_0$. Hence Lemma 3.1 implies that $\phi^* D$ can be expressed in the form

$$\phi^* D = \sum_{i=0}^{m} p^{f-i} P_i E_i, \tag{3.6}$$

where the $P_i$'s are the unique subgroups of respective orders $p^i$ in $G/U$, the $E_i$'s are elements of $Z[G/U]$ with nonnegative coefficients, and $m = \min\{e, f\}$, where $p^e$ is the order of the Sylow $p$-subgroup of $G/U$. Let $\rho^*: Z[G/U] \to Z[(G/U)/P_m]$ be the natural group ring epimorphism induced by the group epimorphism $\rho: G/U \to (G/U)/P_m$ with kernel $P_m$. Since $P_0 \subset \cdots \subset P_m$, $\rho^* P_i = p^i$ for $i = 0, \ldots, m$. Hence (3.6) yields

$$\rho^* \phi^* D = p^f B, \tag{3.7}$$

where

$$B = \rho^* E_0 + \cdots + \rho^* E_m. \tag{3.8}$$

Then

$$\begin{aligned}\left(\rho^*\phi^* D\right)\left(\rho^*\phi^* D^{(-1)}\right) &= n + \lambda |U||P_m|(G/U)/P_m \\ &= p^{2f}\alpha + p^{2f+m}\alpha(G/U)/P_m,\end{aligned}$$

so

$$BB^{(-1)} = \alpha + p^m \alpha (G/U)/P_m. \tag{3.9}$$

Let $(G/U)/P_m = \{g_1, \ldots, g_s\}$, and let

$$B = \sum_{i=1}^{s} b_i g_i.$$

Then (3.1) and (3.7) imply that

$$\sum_{i=1}^{s} b_i = k/p^f = (p^f + 1)\alpha,$$

and (3.9) implies that

$$\sum_{i=1}^{s} b_i^2 = (1 + p^m)\alpha.$$

Since the $b_i$ 's are integers, $\sum_1^s b_i \leq \sum_1^s b_i^2$, so $f \leq m$. But $m = \min\{e, f\}$, so $m = f \leq e$. Since $p^e$ is the order of the Sylow $p$-subgroup of $G/U$, $p^f$ divides $|G/U| = (p^f + 1)^2\alpha - 1$. Therefore

$$\alpha - 1 \equiv 0 \pmod{p^f}. \tag{3.10}$$

Also $m = f$ implies $\sum_1^s b_i = \sum_1^s b_i^2$, so each $b_i$ is 0 or 1. Hence $B = \rho^* E_0 + \cdots + \rho^* E_f$ has coefficients 0 or 1. Since the $E_i$ 's have nonnegative coefficients, each $E_i$ must have coefficients 0 or 1. Hence each $E_i$ can be considered a subset of $G/U$. Moreover, since $P_f = P_m$ is the kernel of $\rho$, no coset of $P_f$ can contain more than one element of $E_0 \cup \cdots \cup E_f$. Hence if $i \neq j$, then the multiset $E_i E_j^{(-1)}$ contains no elements of $P_f$, and hence no element of $P_1 \subseteq P_f$. Therefore, using the expression for $\phi^* D$ in (3.6), we conclude that the elements of $P_1$ that occur in

$$(\phi^* D)(\phi^* D^{(-1)}) = \left(\sum_{i=0}^{f} p^{f-i} P_i E_i\right)\left(\sum_{i=0}^{f} p^{f-i} P_i E_i^{(-1)}\right)$$

all occur in the terms

$$\sum_{i=0}^{f} p^{2(f-i)} P_i^2 E_i E_i^{(-1)} = \sum_{i=0}^{f} p^{2f-i} P_i E_i E_i^{(-1)}$$

Furthermore, $E_i E_i^{(-1)}$ contains the identity of $P_1$ a total of $|E_i|$ times, but no other elements of $P_1$. Since

$$(\phi^* D)(\phi^* D^{(-1)}) = n + \lambda |U| G/U = p^{2f}\alpha + p^{2f}\alpha G/U,$$

a count of the occurrences of the identity element of $G/U$ in $(\phi^* D)(\phi^* D^{(-1)})$ yields

$$\sum_{i=0}^{f} p^{2f-i} |E_i| = 2p^{2f}\alpha,$$

while a count of the occurrences of a nonidentity element of $P_1$ yields

$$\sum_{i=1}^{f} p^{2f-i} |E_i| = p^{2f}\alpha. \tag{3.11}$$

The last two equations yield

$$|E_0| = \alpha.$$

Applying the principal character to (3.6) yields

$$p^f \sum_{i=0}^{f} |E_i| = k = p^f(p^f + 1)\alpha.$$

These last two equations yield

$$p^f \sum_{i=1}^{f} |E_i| = p^{2f}\alpha. \tag{3.12}$$

Subtracting this equation from (3.11) yields

$$\sum_{i=1}^{f-1} \left(p^{2f-i} - p^f\right) |E_i| = 0.$$

Obviously $|E_i| \geq 0$, so $|E_i| = 0$ for $i = 1, \ldots, f-1$. Hence $E_1, \ldots, E_{f-1}$ are empty sets. Then (3.12) yields $|E_f| = p^f\alpha$. Let $S = E_0$ and $T = E_f$. Then $E_0 \cup \cdots \cup E_f = S \cup T$. If $P_f T$ is not a subset, then $xt_1 = yt_2$ for some $x, y \in P_f$ and $t_1, t_2 \in T$. Hence $P_f t_1 = P_f t_2$, so $t_1, t_2 \in P_f t_1$. This contradicts the result proved above that no coset of $P_f$ contains more than one element of $E_0 \cup \cdots \cup E_f = S \cup T$. A similar argument shows that $P_f T$ and $S$ are disjoint. □

We note that in view of Theorem 3.2, the parameters (3.1) yield equality in the inequality occurring in a theorem of Lander [**10**, Theorem 4.32, p. 166, $m = h = p^f$ ].

**Corollary 3.3.** *Suppose that there exists a difference set in the group $G$ as described in Theorem 3.2. Then $p^{-f}(\rho^*\phi^*D) = \rho^*S + \rho^*T$ is a $([(p^f + 1)^2\alpha - 1]/p^f,\ (p^f + 1)\alpha,\ p^f\alpha)$-difference set in $(G/U)/P_f$, where $\rho^*$ is the natural group ring epimorphism induced by the group epimorphism $\rho: G/U \to (G/U)/P_f$.*

*Proof.* The proof follows from equations (3.7)–(3.9) and the fact that all $E_i$ 's are empty sets except for $E_0 = S$ and $E_f = T$. □

**Lemma 3.4.** *Let $G$ be a finite group with subgroups $H$ and $K$ with $H$ a normal subgroup. Let $S$ be a subset of $G$ that can be expressed as a union of some of the cosets of $H$ in $G$ and also as a union of some of the left cosets of $K$ in $G$. Then the cardinality of $S$ is a multiple of $|H| \cdot |K|/|H \cap K|$.*

*Proof.* Let $x \in S$. Since $S$ is a union of cosets of $H$, the unique coset of $H$ that contains $x$, namely $xH$, must be a subset of $S$. Let $h \in H$. Then $xh \in S$. Since $S$ is a union of left cosets of $K$, the unique left coset of $K$ that contains $xh$, namely $xhK$, must be a subset of $S$. Therefore $xHK \subseteq S$. If $xHK \neq S$, choose $y \in S - xHK$. Since $H$ is a normal subgroup, $xHK = xKH$ is a union of cosets of $H$. Clearly $xHK$ is a union of left cosets of $K$. Thus $S - xHK$ is a union of cosets of $H$ and a union of left cosets of $K$. Now repeat the previous argument to show that $yHK \subseteq S - xHK$. If $S \neq xHK \cup yHK$, choose $z \in S - (xHK \cup yHK)$. Repeat until $S$ is expressed as a disjoint union of left cosets of $HK$. For each $h \in H$ there exists $h' \in H$ such that $hK = h'K$ if and only if $h^{-1}h' \in H \cap K$. Hence $|xHK| = |yHK| = \cdots = |HK| = |H| \cdot |K|/|H \cap K|$. □

**Theorem 3.5.** *Suppose that there exists a difference set in the group $G$ as described in Theorem 3.2. If $G$ has two different subgroups that satisfy the stated conditions for the subgroup $U$, then their intersection must be the trivial group.*

*Proof.* Let $U_1 \neq U_2$ be two subgroups of $G$ that have the properties of the subgroup $U$ in the statement of Theorem 3.2. We show that the assumption that there exists a difference set $D$ in $G$ and $|U_1 \cap U_2| > 1$ leads to a contradiction. In the remainder of the proof all statements/equations that contain an index i are to be read twice, once for $i = 1$ and once for $i = 2$. Let $\phi_i^*$ be the natural group ring epimorphism induced by the group epimorphism $\phi_i : G \to G/U_i$. Theorem 3.2 states that

$$\phi_i^* D = p^f S_i + R_i, \tag{3.13}$$

where $S_i$ and $R_i$ are disjoint subsets of $G/U_i$ with $|S_i| = \alpha$. Hence we can write $D$ as the disjoint union $D = S_i'' \cup R_i''$, where $S_i'' = \{d \in D : \phi_i(d) \in S_i\}$ and $R_i'' = \{d \in D : \phi_i(d) \in R_i\}$. The kernel of $\phi_i$ is $U_i$ which has cardinality $p^f$ and $D$ has coefficients 0, 1, so (3.13) implies that $S_i''$ is the union of $\alpha$ cosets of $U_i$ and each coset of $U_i$ intersects $R_i''$ in at most one element. Since $U_1$ and $U_2$ are normal subgroups of $G$, $U_1 \cap U_2$ is a normal subgroup of $G$ and $U_i/(U_1 \cap U_2)$ is a normal subgroup of $G/(U_1 \cap U_2)$. Hence the group epimorphism $\phi_i : G \to G/U_i$ can be factored as the following composition of two group epimorphisms:

$$G \to G/(U_1 \cap U_2) \to G/U_i.$$

There is a corresponding factorization of $\phi_i^*$:

$$Z[G] \to Z[G/(U_1 \cap U_2)] \to Z[G/U_i].$$

Applying this factorization of $\phi_i^*$ to the components $S_i''$ and $R_i''$ of $D$ yields

$$S_i'' \to |U_1 \cap U_2| S_i' \to p^f S_i,$$
$$R_i'' \to R_i' \to R_i,$$

where $S_i'$, $R_i'$ are disjoint subsets of $G/(U_1 \cap U_2)$. Thus the contraction of $D = S_1'' + R_1'' = S_2'' + R_2''$ by $U_1 \cap U_2$ yields

$$|U_1 \cap U_2| S_1' + R_1' = |U_1 \cap U_2| S_2' + R_2'.$$

Since $|U_1 \cap U_2| > 1$ and the sets $S_i'$, $R_i'$ are disjoint, $S_1' = S_2'$. Thus $S_1''$ and $S_2''$ have the same contraction by $U_1 \cap U_2$. Since $S_i''$ is a union of distinct cosets of $U_i$, it is also a union of distinct cosets of $U_1 \cap U_2$. Hence $S_1'' = S_2''$. Therefore $S_1''$ is a union of cosets of $U_1$ and a union of cosets of $U_2$. Hence by Lemma 3.4, $|S_1''| = p^f \alpha$ is a multiple of $|U_1| \cdot |U_2| / |U_1 \cap U_2| = p^{2f} / |U_1 \cap U_2|$. Thus $p$ divides $\alpha$. However, $p$ divides $\alpha - 1$ by (3.10) or Corollary 3.3. This contradiction completes the proof of Theorem 3.5. □

**Theorem 3.6.** *Suppose that there exists a difference set in the group $G$ as described in Theorem 3.2. If $G$ is abelian, then $f = 1$.*

*Proof.* Assume that $G$ is abelian and $f > 1$. We prove the Theorem by showing that then there cannot exist a difference set in $G$. Let $P$ be the Sylow $p$-subgroup of $G$

and let $\exp P = p^e$. Suppose that $P$ is isomorphic to $Z_{p^e}$ or $Z_{p^e} \times Z_p$. In both cases there is a subgroup $H$ of order $p$ such that $P/H$ is cyclic. Theorem 3.2 implies that $|P| \geq p^{2f}$, so $p$ divides the index of $H$ in $P$. Thus an application of Theorem 2.1 with $H$ as above and $m = p^f$ yields $p^f = m \leq |H| = p$. Hence $f = 1$, contrary to the above assumption. Therefore, we can write

$$P = \langle x \rangle \times \langle y \rangle \times K, \tag{3.14}$$

where $|\langle x \rangle| = p^e$ and $|\langle y \rangle| \geq p^2$ or $|\langle y \rangle| = p$ and $|K| > 1$. Thus we also have

$$P = \langle x \rangle \times \langle x^{p \uparrow (e-1)} y \rangle \times K. \tag{3.15}$$

For any subgroup $U$ satisfying the hypotheses of Theorem 3.2, the order of the Sylow $p$-subgroup of $G/U$ is at most $\exp P = p^e$; say the order is $p^{e-a}$. Let

$$U_1 = \langle x^{p \uparrow (e-a)} \rangle \times \langle y \rangle \times K,$$
$$U_2 = \langle x^{p \uparrow (e-1)} \rangle \times \langle x^{p \uparrow (e-a)} y \rangle \times K.$$

Then (3.14) and (3.15) imply that $P/U_1$ and $P/U_2$ are both cyclic groups of order $p^{(e-a)}$; hence $U_1$ and $U_2$ satisfy the conditions of Theorem 3.2 for the normal subgroup $U$. Theorem 3.2 then implies that $e - a \geq f$. Hence $e \geq f > 1$, so $U_1$ and $U_2$ are different subgroups. If $|\langle y \rangle| \geq p^2$, then

$$\left(x^{p \uparrow (e-1)} y\right)^p = x^{p \uparrow e} y^p = y^p$$

is a nonidentity element in $U_1 \cap U_2$. If $|\langle y \rangle| = p$, then $|K| > 1$, so again $U_1$ and $U_2$ have a nontrivial intersection. Thus Theorem 3.5 implies that there does not exist a difference set with the specified parameters in $G$. □

## References


[1] K.T. Arasu, J.A. Davis, and J. Jedwab, A nonexistence result for abelian Menon difference sets using perfect binary arrays, Combinatorica, to appear.

[2] K. T. Arasu and S. Sehgal, Difference sets in abelian groups of $p$-rank two, Des. Codes Cryptogr. 5 (1995), 5–12.

[3] K. T. Arasu and S. Sehgal, Some new difference sets, J. Combin. Theory Ser. A 69 (1995), 170–172.

[4] W.-K. Chan, S.-L. Ma, and M.-K. Siu, Non-existence of certain perfect arrays, Discrete Math. 125 (1994), 107–113.

[5] J.A. Davis, Difference sets in abelian 2-groups, J. Combin. Theory Ser. A 57 (1991), 262–286.

[6] J.A. Davis and J. Jedwab, A survey of Hadamard difference sets, in: Groups, Difference Sets, and the Monster, Ohio State Univ. Math. Res. Inst. Publ. 4, pp. 145–156, Berlin-New York 1996.

[7] J.F. Dillon, Variations on a scheme of McFarland for noncyclic difference sets, J. Combin. Theory Ser. A 40 (1985), 9–21.

[8] D. Jungnickel, Difference sets, Chapter 7 in: J.H. Dinitz and D.R. Stinson (eds.), Contemporary Design Theory: A Collection of Surveys, pp. 241–324, Wiley, New York 1992.

[9] R.G. Kraemer, Proof of a conjecture on Hadamard 2-groups, J. Combin. Theory Ser. A 63 (1993), 1–10.

[10] E.S. Lander, Symmetric Designs: An Algebraic Approach, Cambridge Univ. Press, Cambridge 1983.

[11] S.L. Ma, Polynomial addition sets and polynomial digraphs, Linear Algebra Appl. 69 (1985), 213–230.

[12] R.L. McFarland, A family of difference sets in noncyclic groups, J. Combin. Theory Ser. A 15 (1973), 1–10.

[13] K. Takeuchi, On the construction of a series of BIB designs, Rep. Statist. Appl. Res. Un. Japan. Sci. Engrs. 10 (1963), 48.

[14] R.J. Turyn, Character sums and difference sets, Pacific J. Math. 15 (1965), 319–346.

K. T. Arasu
Department of Mathematics and Statistics,
Wright State University
Dayton, Ohio 45435, USA

James A. Davis
Department of Mathematics,
University of Richmond
Richmond, Virginia 23173, USA

Jonathan Jedwab
Hewlett-Packard Laboratories,
Filton Road, Stoke Gifford
Bristol BS12 6QZ, U.K.

Siu Lun Ma
Department of Mathematics
National University of Singapore
Singapore, 0511

Robert L. McFarland
Department of Mathematics and Statistics
University of Minnesota-Duluth
Duluth, Minnesota 55812, USA