JOURNAL OF COMBINATORIAL THEORY, Series A 70, 313–322 (1995)

The Structure of the Abelian Groups Containing McFarland Difference Sets

SIU LUN MA

Department of Mathematics, National University of Singapore, Kent Ridge, Singapore 0511, Republic of Singapore

AND

BERNHARD SCHMIDT

Mathematisches Institut, Universität Augsburg, Universitätsstrasse 2, 86135 Augsburg, Germany

Communicated by William M. Kantor

Received December 7, 1993

A McFarland difference set is a difference set with parameters $(v, k, \lambda) = (q^{d+1}(q^d + q^{d-1} + \cdots + q + 2), q^d(q^d + q^{d-1} + \cdots + q + 1), q^d(q^{d-1} + q^{d-2} + \cdots + q + 1))$, where $q = p^f$ and p is a prime. Examples for such difference sets can be obtained in all groups of G which contain a subgroup $E \cong EA(q^{d+1})$ such that the hyperplanes of E are normal subgroups of G. In this paper we study the structure of the Sylow p-subgroup P of an abelian group G admitting a McFarland difference set. We prove that if P is odd and P is self-conjugate modulo $\exp(G)$, then $P \cong EA(q^{d+1})$. For $p = 2$, we have some strong restrictions on the exponent and the rank of P. In particular, we show that if $f \geqslant 2$ and 2 is self-conjugate modulo $\exp(G)$, then $\exp(P) \leqslant \max\{2^{f-1}, 4\}$. The possibility of applying our method to other difference sets has also been investigated. For example, a similar method is used to study abelian (320, 88, 24)-difference sets.

1. INTRODUCTION

Let G be a multiplicative group of order v and let D be a subset of G with k elements. Then D is called a (v, k, λ)-*difference set* in G if the expressions $d_1 d_2^{-1}$, for $d_1, d_2 \in D$ and $d_1 \neq d_2$, represent every nonidentity element in G exactly λ times. Using the notation of the group ring $\mathbb{Z}[G]$, D is a difference set precisely when it satisfies the equation

$$DD^{(-1)} = \lambda G + n, \tag{1.1}$$

0097-3165/95 $6.00

where $n = k - \lambda$ and $D^{(-1)} = \{g^{-1}: g \in D\}$. For detailed descriptions of difference sets, please consult [3, 8, or 10]. McFarland [12] has given a construction for difference sets having the parameters (v, k, λ, n) equal to

$$(q^{d+1}(q^d + q^{d-1} + \cdots + q + 2), q^d(q^d + q^{d-1} + \cdots + q + 1),$$
$$q^d(q^{d-1} + q^{d-2} + \cdots + q + 1), q^{2d}),$$

where q is any prime power and d is any positive integer. In this paper, a difference set with these parameters is called a *McFarland difference set.*

It is known that McFarland difference sets exist in all groups G which contain a subgroup $E \cong EA(q^{d+1})$ such that the hyperplanes of E are normal subgroups of G. (Actually, the condition on the hyperplanes can be relaxed; see [5, 7].) When $q = 2$, we have $(v, k, \lambda, n) = (2^{2d+2}, 2^{2d+1} - 2^d, 2^{2d} - 2^d, 2^{2d})$ and these difference sets are also known as *Menon difference sets* in 2-groups; see [8]. There are various constructions of these difference sets; see [4, 6, 9, 11]. We summarize the results in the abelian case in the following.

THEOREM 1.1. *Let $q = p^f$, where p is a prime. Let G be an abelian group of order $q^{d+1}(q^d + q^{d-1} + \cdots + q + 2)$ and let P be the Sylow p-subgroup of G. Then a McFarland difference set exists in G if*

(a) *p is odd and $P \cong EA(q^{d+1})$; or*

(b) *$p = 2, f \geqslant 2$, and $P \cong EA(2^{fd+f+1})$ or $\mathbb{Z}_4 \times EA(2^{fd+f-1})$; or*

(c) *$p = 2, f = 1$, and $\exp(P) \leqslant 2^{d+2}$.*

Based on a result of Turyn [13], it is easy to obtain the following necessary conditions on the existence of McFarland difference sets. Let p be a prime and $m = p^t w$, where $(p, w) = 1$ Then p is called *self-conjugate* modulo m if $p^j \equiv -1 \pmod{w}$ for some integer j.

THEOREM 1.2. [9, Theorem 4.33]. *Use the notation of Theorem* 1.1. *Suppose that p is self-conjugate modulo* $\exp(G)$. *If G contains a McFarland difference set, then*

(a) *p is odd and* $\exp(P) \leqslant p^f$; *or*

(b) *$p = 2, f \geqslant 2$, and* $\exp(P) \leqslant 2^{f+1}$; *or*

(c) *$p = 2, f = 1$, and* $\exp(P) \leqslant 2^{d+2}$.

Note that Theorems 1.1 and 1.2 give necessary and sufficient conditions for the existence of McFarland difference sets when $p = 2$ and $f = 1$, i.e., case (c). (For this case, it is obvious that 2 is self-conjugate modulo $\exp(G)$.) Thus it is natural to ask whether we can narrow the gaps between

the two theorems in the remaining cases. Recently, Arasu, Davis, Jedwab, and Ma [1] have improved the bound in cases (a) and (b) of Theorem 1.2 to p^{f-1} and 2^f, respectively, when $d=1$ and $f \geqslant 2$. In this paper, we shall show that if p is odd and p is self-conjugate modulo $\exp(G)$, then $P \cong EA(q^{d+1})$; i.e., in this case, Theorem 1.1(a) is necessary and sufficient. For $p=2$ and $f \geqslant 2$, an upper bound better than Theorem 1.2(b) will be obtained. Furthermore, we shall provide necessary conditions on the rank of the Sylow 2-subgroup and the size of d if the exponent of G falls between our upper bound and the lower bound given by Theorem 1.1. Also, our technique will be shown to be applicable to other difference sets as well. In Section 2, some useful lemmas will be given. The cases when p is odd and $p=2$ will be studied separately in Sections 3 and 4.

2. Preliminaries

In this section, we shall state some lemmas which will be used in the later sections. Throughout this paper, all the groups considered are abelian and we assume that all group homomorphisms are extended to the group rings in the natural way. Also, we adopt the following notation: for $y = \sum_{g \in G} a_g g \in \mathbb{Z}[G]$, where G is a group and $a_g \in \mathbb{Z}$, let $y^{(-1)} = \sum_{g \in G} a_g g^{-1}$ and $|y| = \sum_{g \in G} a_g$.

The following is a well-known result for the study of difference sets.

Lemma 2.1. *Let G be an abelian group and let $y \in \mathbb{Z}[G]$, satisfying $yy^{(-1)} = \lambda G + n$. Then for every character χ of G:*

$$\chi(y)\overline{\chi(y)} = \begin{cases} |y|^2 & \text{if } \chi \text{ is principal on } G \\ n & \text{if } \chi \text{ is nonprincipal on } G. \end{cases}$$

In order to make use of Lemma 2.1, we need some lemmas linking up the results on algebraic numbers with the results on group rings.

Lemma 2.2. (Turyn [13]). *Let p be a prime and let $c \in \mathbb{Z}[\zeta]$, where ζ is an mth root of unity. If p is self-conjugate modulo m and $c\bar{c} \equiv 0 \pmod{p^{2a}}$, then $c \equiv 0 \pmod{p^a}$.*

The following is one of the variations of Ma's lemma.

Lemma 2.3. (Arasu, Davis, Jedwab, and Ma [1]). *Let p be a prime and let G be an abelian group with a cyclic Sylow p-subgroup of order p^s. If*

$y \in \mathbb{Z}[G]$ satisfies $\chi(y) \equiv 0 \pmod{p^a}$ for every character χ of G, then there exist $x_0, x_1, \ldots, x_r \in \mathbb{Z}[G]$, where $r = \min\{a, b\}$, so that

$$y = p^a x_0 + p^{a-1} P_1 x_1 + \cdots + p^{a-r} P_r x_r,$$

where the P_i are the unique subgroups of order p^i in G. Furthermore, if the coefficients of y are nonnegative, then $x_1, x_2, \ldots, x_r$ can be chosen to have coefficients $0, 1, \ldots, p-1$ only while x_0 can be chosen to have nonnegative coefficients.

Finally, we prove a lemma on intersections of subgroups. It is basically a generalization of the argument of the two-subgroup intersection used in [1].

LEMMA 2.4. *Let p be a prime, let G be an abelian group, and let P be the Sylow p-subgroup of G. Let $p^c = |P|/\exp(P)$ and $\mathfrak{P} = \{U < P: |U| = p^c$ and P/U is cyclic$\}$. Also, for each $U \in \mathfrak{P}$, let $U' = \{g \in P: g^{p^s} \in U\}$, where $p^s \leqslant \exp(P)$. Suppose that there exists a subset D of G such that for each $U \in \mathfrak{P}$ and $g \in G$, either*

(1) *$|D \cap Uh| \geqslant \delta$ and $|D \cap (U' \backslash U)h| \leqslant \varepsilon$ for some $h \in U'g$ or*

(2) *$|D \cap U'g| \leqslant \varepsilon'$*

where $\delta, \varepsilon, \varepsilon', \delta > \varepsilon'$, are fixed numbers which do not depend on U and there is at least one coset $U'g$ satisfying (1). *Furthermore, let $t = \operatorname{rank}(P)$ and write $P = \langle g_0 \rangle \times \langle g_1 \rangle \times \cdots \times \langle g_{t-1} \rangle$, where $o(g_0) = \exp(P)$ and $o(g_i) = p^{a_i} \leqslant \exp(P)$ for $i = 1, 2, \ldots, t-1$. Also, let $b_i = \min\{s, a_i\}$. Then*

$$\delta - m\varepsilon \leqslant p^{c - \sum_{i=1}^{m} b_i}$$

for $m = 1, 2, \ldots, t-1$.

Proof. Let $U_0 = \langle g_1 \rangle \langle g_2 \rangle \times \cdots \times \langle g_{t-1} \rangle$ and for $i = 1, 2, \ldots, t-1$, $U_i = \langle g_1 \rangle \times \cdots \times \langle g_{i-1} \rangle \times \langle g_i g^{p^{s-bi}} \rangle \times \langle g_{i+1} \rangle \times \cdots \times \langle g_{t-1} \rangle$, where $g \in \langle g_0 \rangle$ is an element of order p^s. Note that $U_i' = U_0'$, $U_1 \in \mathfrak{P}$, and $|\bigcap_{i=0}^{m} U_i| = p^{c - \sum_{i=1}^{m} b_i}$. Choose $h_0 \in G$ such that $|D \cap U_0 h_0| \geqslant \delta$ and $|D \cap (U_0' \backslash U_0)h_0| \leqslant \varepsilon$. Since $|D \cap U_i' h_0| = |D \cap U_0' h_0| \geqslant \delta > \varepsilon'$, there exists $h_i \in U_0' h_0$ such that $|D \cap U_i h_i| \geqslant \delta$ and $|D \cap (U_i' \backslash U_i)h_i| \leqslant \varepsilon$ for $i = 1, 2, \ldots, t-1$. Now consider

$$T_m = U_0 h_0 \Big\backslash \left(\bigcup_{i=1}^{m} (U_i' \backslash U_i) h_i \right) = \bigcap_{i=0}^{m} U_i h_i.$$

Obviously, $|T_m| \leqslant p^{c - \sum_{i=1}^{m} b_i}$. On the other hand, we have

$$|T_m| \geqslant |D \cap T_m| \geqslant \delta - m\varepsilon$$

from the hypothesis of the lemma. Hence $\delta - m\varepsilon \leqslant p^{c - \sum_{i=1}^{m} b_i}$. ∎

3. When p Is Odd

In this section, we shall prove that Theorem 1.1(a) is necessary and sufficient when p is self-conjugate modulo $\exp(G)$.

THEOREM 3.1. *Let G be an abelian group of order $q^{d+1}(q^d + q^{d-1} + \cdots + q + 2)$, where $q = p^f$, p is an odd prime, and p is self-conjugate modulo* $\exp(G)$. *Then G contains a McFarland difference set if and only if the Sylow p-subgroup of G is elementary abelian.*

Proof. Let P be the Sylow p-subgroup of G. By Theorem 1.1 (a), we only have to show that P is elementary abelian if G contains a McFarland difference set. Suppose $\exp(P) = p^{f-r}$, where $2 \leqslant f - r \leqslant f$. Assume that there exists a McFarland difference set D in G. Let U be any subgroup of G of order p^{fd+r} such that G/U is cyclic and let $\rho: G \to G/U$ be the canonical epimorphism. Applying ρ to (1.1), we obtain

$$\rho(D)\,\rho(D)^{(-1)} = p^{2fd+r}(p^{f(d-1)} + p^{f(d-2)} + \cdots + p^f + 1)\,G/U + p^{2fd}. \tag{3.1}$$

By Lemmas 2.1, 2.2, and 2.3, we have

$$\rho(D) = p^{fd}x_0 + p^{fd-1}P_1x_1 + \cdots + p^{fd-f+r}P_{f-r}x_{f-r}, \tag{3.2}$$

where P_i and x_i are chosen as described in Lemma 2.3. Note that $\sum |x_i| = k/p^{fd} = p^{fd} + p^{f(d-1)} + \cdots + p^f + 1$ and applying a character of order p^{f-r} to (3.1) yields $|x_0| \geqslant 1$. Let C be the coefficient of 1 in $\rho(D)\,\rho(D)^{(-1)}$. Then by (3.2),

$$\begin{aligned} C &\geqslant p^{2fd} + p^{2(fd-f+r)+(f-r)}(p^{fd} + p^{f(d-1)} + \cdots + p^f) \\ &= p^{2fd} + p^{2fd+r}(p^{f(d-1)} + p^{f(d-2)} + \cdots + p^f + 1), \end{aligned}$$

where equality holds if and only if

$$\rho(D) = p^{fd}h + p^{fd-f+r}P_{f-r}A \tag{3.3}$$

for some $h \in G/U$ and $A \subset G/U$ such that no two elements of $\{h\} \cup A$ are in the same coset of P_{f-r}. However, by (3.1),

$$C = p^{2fd} + p^{2fd+r}(p^{f(d-1)} + p^{f(d-2)} + \cdots + p^f + 1).$$

Hence, $\rho(D)$ has the form described in (3.3). Now, we apply Lemma 2.4 with $s = f - r - 1$, $m = t - 1$, $\delta = p^{fd}$, $\varepsilon = 0$, $\varepsilon' = p^{fd-f+r+s}$. This yields $p^{fd} \leqslant p^{fd+r-\sum_{i=1}^{t-1} b_i}$ using the notation of Lemma 2.4. Hence $\sum b_i \leqslant r$. However, since $s \geqslant a_i - 1$ for all i, we have $\sum b_i \geqslant \sum a_i - (t-1) = fd + r - t + 1$. Thus $r \geqslant fd + r - t + 1$ which implies $t - 1 \geqslant fd$. On the other hand, since $b_i \geqslant 1$ for all i, we have $\sum b_i \geqslant t - 1 \geqslant fd > r$, which is impossible. ∎

With a detailed analysis of our method, it seems that the technique usually works for difference sets for which there exists a prime p such that p^{2u} divides n and k/p^u is relatively small. In the following, we provide one generalization of Theorem 3.1.

THEOREM 3.2. *Let G be an abelian group of order $p^s w$, where $(p, w) = 1$; p is a prime which is self-conjugate modulo* $\exp(G)$. *If there exists a difference set in G with parameters*

$$(v, k, \lambda, n) = (p^s w, p^u(\gamma + \alpha), p^{2u-s}\gamma, p^{2u}\alpha),$$

where u, γ, α are positive integers and $2u \leqslant s$, then

(i) *the Sylow p-subgroup P of G is elementary abelian; and*

(ii) *there exists a difference set in G/P with parameters $(v, k, \lambda, n) = (w, \gamma + \alpha, \gamma, \alpha)$.*

Proof. Assume that there exists a difference set D in G with the given parameters. By $k = \lambda + n$, we obtain $(p^u - p^{2u-s})\gamma = (p^{2u} - p^u)\alpha \geqslant 0$ and, hence, $s \geqslant u$. By [9, Theorem 4.33], $\exp(P) \leqslant p^{s-u}$. Let $\exp(P) = p^{s-u-r}$, where $1 \leqslant s-u-r \leqslant s-u$. Let U be any subgroup of G of order p^{u+r} such that G/U is cyclic. Let $\rho: G \to G/U$ be the canonical epimorphism. By the same argument as before, we obtain $\rho(D) = p^u x_0 + p^{u-1}P_1 x_1 + \cdots + p^{2u-s+r}P_{s-u-r}x_{s-u-r}$, where P_i and x_i are chosen as described in Lemma 2.3. Let $x_0 = \sum_{g \in G/U} a_g g$ and $h \in P_1 \backslash \{1\}$. Then $p^{2u}\sum a_g^2 \geqslant p^{2u}\sum a_g^2 - p^{2u}\sum a_g a_{gh} =$ [the coefficient of 1 in $\rho(D)\,\rho(D)^{(-1)}$] $-$ [the coefficient of h in $\rho(D)\,\rho(D)^{(-1)}$] $= (p^{u+r}\lambda + n) - p^{u+r}\lambda = p^{2u}\alpha$ which implies $\sum a_g^2 \geqslant \alpha$. Hence the coefficient of 1 in $\rho(D)\,\rho(D)^{(-1)}$ is at least $p^{2u}\alpha + p^{3u-s+1}\gamma$. The minimum value is attained if and only if $\rho(D) = p^u A + p^{2u-s+r}P_{s-u-r}B$, where $A, B \subset G/U$, $|A| = \alpha$, $|B| = \gamma$, and no two elements of $A \cup B$ are in the same coset of P_{s-u-r}. In this case, by projecting $A \cup B$ to $(G/U)/P_{s-u-r} (\cong G/P)$, we obtain a $(w, \gamma + \alpha, \gamma)$-difference set. Finally, the theorem follows by the same argument as Theorem 3.1. ∎

Consider difference sets with parameters $(v, k, \lambda, n) = (17091, 1710, 171, 1539)$ and $(23193, 7137, 2196, 4941)$. By Theorem 3.2, both of them do not exist because there are no cyclic difference sets with parameters $(v, k, \lambda, n) = (211, 190, 171, 19)$ and $(859, 793, 732, 61)$; see [2].

4. WHEN $p = 2$

Now, let us study case (b) of Theorem 1.2, i. e., $p = 2$ and $f \geqslant 2$. This case is more complicated than the case of odd p.

THEOREM 4.1 *Let G be an abelian group of order $2^{f(d+1)}(2^{fd}+2^{f(d-1)}+\cdots+2^f+2)$, where $f\geqslant 2$ is self-conjugate modulo $\exp(G)$. Let P be the Sylow 2-subgroup of G with $\exp(P)=2^{f-r+1}\geqslant 8$ and $\operatorname{rank}(P)=t$. Write $P=\langle g_0\rangle\times\langle g_1\rangle\times\cdots\times\langle g_{t-1}\rangle$, where $o(g_0)=\exp(P)$ and $o(g_i)=2^{a_i}\leqslant \exp(P)$ for $i=1,2,\ldots,t-1$, and let $b_i^{(s)}=\min\{s,a_i\}$. If G contains a McFarland difference set, then*

$$2^{f-r+1}-(2^s-1)m\leqslant 2^{f+1-\sum_{i=1}^{m}b_i^{(s)}} \tag{4.1}$$

for $s=1,2,\ldots,f-r-1$ and $m=1,2,\ldots,t-1$.

Proof. Let $\exp(P)=2^{f-r+1}$, where $3\leqslant f-r+1\leqslant f+1$. By [1], we can have $f-r+1\leqslant f$ if $d=1$. Assume that there exists a McFarland difference set D in G. Let U be any subgroup of G of order 2^{fd+r} such that G/U is cyclic. Let $\rho: G\to G/U$ be the canonical epimorphism. Using the same argument as Theorem 3.1, we have

$$\rho(D)=2^{fd}x_0+2^{fd-1}P_1x_1+\cdots+2^{fd-f+r-1}P_{f-r+1}x_{f-r+1}x_{f-r+1} \tag{4.2}$$

where P_i and x_i are chosen as described in Lemma 2.3. Here we can regard $x_1, x_2, \ldots, x_{f-r+1}$ as subsets of G and they can be chosen in a way that for each i no two elements of x_i are in the same coset of P_i. Note that $\sum|x_i|=2^{fd}+2^{f(d-1)}+\cdots+2^f+1$ and $|x_0|\geqslant 1$.

Let $\varphi: G/U\to H=(G/U)/P_{f-r}$ be the canonical epimorphism. From (4.2), we obtain $\varphi\circ\rho(D)\equiv 0 \bmod 2^{fd-1}$. Let $u=\varphi\circ\rho(D)/2^{fd-1}=\sum_{g\in H}a_g g$. From (1.1), we have

$$uu^{(-1)}=4(2^{fd}+2^{f(d-1)}+\cdots+2^f)H+4.$$

Thus $\sum a_g=2(2^{fd}+2^{f(d-1)}+\cdots+2^f+1)$ and $\sum a_g^2=4(2^{fd}+2^{f(d-1)}+\cdots+2^f+1)$. Let b_g, $g\in H$, be integers such that $\sum b_g=2(2^{fd}+2^{f(d-1)}+\cdots+2^f+1)=\sum a_g$. Since $|H|=2^{fd}+2^{f(d-1)}+\cdots+2^f+2$, the minimum possible value of $\sum b_g^2$ is $4(2^{fd}+2^{f(d-1)}+\cdots+2^f)+2=\sum a_g^2-2$ which happens when $\{b_g\}=\{2,2,\ldots,2,1,1\}$. Thus we have either $\{a_g\}=\{2,2,\ldots,2,0\}$ or $\{a_g\}=\{3,2,2,\ldots,2,1,1,1\}$.

Case 1. ($\{a_g\}=\{2,2,\ldots,2,0\}$). Since $u=2\varphi(x_0+\cdots+x_{f-r})+P'\varphi(x_{f-r+1})$, where P' is the unique subgroup of order 2 in H and the coefficients of $P'\varphi(x_{f-r+1})$ are 0 and 1, we conclude that $|x_{f-r+1}|=0$. Together with $|x_0|\geqslant 1$, by comparing the coefficient of 1 in the equation $\rho(D)\,\rho(D)^{(-1)}=2^{fd+r}\lambda G/U+n$, we get $|x_0|=1$, $|x_1|=|x_2|=\cdots=|x_{f-r-1}|=0$, and $|x_{f-r}|=2^{fd}+2^{f(d-1)}+\cdots+2^f$. Hence,

$$\rho(D)=2^{fd}h+2^{fd-f+r}P_{f-r}A, \tag{4.3}$$

where $h\in G/U$, $A\subset G/U$, and no two elements in $\{h\}\cup A$ are in the same coset of P_{f-r}.

Case 2. $(\{a_g\} = \{3, 2, 2, ..., 2, 1, 1, 1\})$. Since $u = 2\varphi(x_0 + \cdots + x_{f-r}) + P'\varphi(x_{f-r+1})$ and the coefficients of $P'\varphi(x_{f-r+1})$ are 0 and 1, it is clear that $|x_{f-r+1}| = 2$. Since $a_g = 3$ for one $g \in H$, there is a nonempty intersection between $P'\varphi(x_{f-r+1})$ and exactly one $\varphi(x_j)$ for $0 \leqslant j \leqslant f-r$. Note that $|\varphi(x_j) \cap P'\varphi(x_{f-r+1})| = 1$ and, hence, $|x_j \cap P_{f-r+1}x_{f-r+1}| = 1$. So the coefficient of 1 in

$$(2^{fd-j}p_jx_j)(2^{fd-f+r-1}P_{f-r+1}x_{f-r+1}) = 2^{2fd-f+r-1}P_{f-r+1}x_jx_{f-r+1}$$

is equal to $2^{2fd-f+r-1}$. By comparing the coefficient of 1 in $\rho(D)\,\rho(D)^{(-1)} = 2^{fd+r}\lambda G/U + n$, we get

$$2^{fd}|x_0| + 2^{2fd-1}|x_1| + \cdots + 2^{2fd-f+r}|x_{f-r}| + 2^{2fd-f+r-1}\cdot 2 + 2^{2fd-f+r-1}\cdot 2 = 2^{fd+r}\lambda + n.$$

With $\sum |x_i| = 2^{fd} + 2^{f(d-1)} + \cdots + 2^f + 1$ and $|x_0| \geqslant 1$, we obtain $|x_0| = 1$, $|x_1| = |x_2| = \cdots = |x_{f-r-1}| = 0$, and $|x_{f-r}| = 2^{fd} + 2^{f(d-1)} + \cdots + 2^f - 2$. Thus

$$\rho(D) = 2^{fd}h + 2^{fd-f+r}P_{f-r}A + 2^{fd-f+r-1}P_{f-r+1}B, \tag{4.4}$$

where $h \in G/U$, $A, B \subset G/U$, and no two elements in $\{h\} \cup A$ are in the same coset of P_{f-r}.

By (4.3) and (4.4), we apply Lemma 2.4 with $\delta = 2^{fd}$, $\varepsilon = (2^s - 1)2^{fd-f+r+1}$, and $\varepsilon' = 3 \cdot 2^{fd-f+r+s-1}$ for $s = 1, 2, ..., f-r-1$. Then the theorem follows. ∎

Theorem 4.1 gives us the following corollary.

COROLLARY 4.2. *Let G be an abelian group of order $2^{f(d+1)}(2^{fd} + 2^{f(d-1)} + \cdots + 2^f + 2)$, where $f \geqslant 2$ and 2 is self-conjugate modulo* $\exp(G)$. *If G contains a McFarland difference set, then*

(i) $\exp(P) \leqslant \max\{2^{f-1}, 4\}$; *and*

(ii) *if* $\exp(P) = 2^{f-r+1}$, *where* $\log_2(r+1) < f - r \leqslant f - 2$, *then* $\operatorname{rank}(P) \leqslant r + 1$ *and* $d \leqslant r(f-r)/f$.

Proof. Let $\exp(P) = 2^{f-r+1}$, where $3 \leqslant f - r + 1 \leqslant f + 1$, and $\operatorname{rank}(P) = t$. Assume $f - r > \log_2(r+1)$. Then $2^{f-r+1} - r > 2^{f-r}$. If $t \geqslant r + 2$, we obtain a contradiction by applying Theorem 4.1 with $s = 1$, $m = r + 1$, and $\sum b_i = r + 1$. So we have $t \leqslant r + 1$. By $(2^{f-r+1})^{r+1} \geqslant (\exp(P))^{\operatorname{rank}(P)} \geqslant 2^{fd+f+1}$, we get $d \leqslant r(f-r)/f$ and (ii) follows. Finally, for (i), if $r \leqslant 1$ and $f \geqslant 3$, then $d = 0$, which is impossible. ∎

More restrictions will be obtained if we consider other values of s and m in (4.1). Furthermore, with a slightly improved version of Lemma 2.4, we can even get some inequalities better than (4.1) and, hence, obtain some better bounds. However, it is too tedious to list them here.

COROLLARY 4.3. *Let G be an abelian group of order $2^{f(d+1)}(2^{fd}+2^{f(d-1)}+\cdots+2^f+2)$, where $2\geqslant f\geqslant 3$ and 2 is self-conjugate modulo* $\exp(G)$. *If G contains a McFarland difference set, then the exponent of the Sylow 2-subgroup of G cannot exceed* 4.

For $f=4$, if 2 is self-conjugate modulo $\exp(G)$, $\exp(P)\geqslant 8$ and G contains a McFarland difference set, then by Corollary 4.2, we have $d=1$ and G can only be either $(\mathbb{Z}_8)^3\times(\mathbb{Z}_3)^2$ or $(\mathbb{Z}_8)^3\times\mathbb{Z}_8$. The existence in these two cases is unknown.

Similar to Section 3, the proof of Theorem 4.1 can certainly be generalized to tackle other difference sets. Instead of proving a general theorem analogous to Theorem 4.1, we prove the nonexistence of some particular difference sets.

THEOREM 4.4. *No* (320, 88, 24)*-difference set exists in any abelian group of exponent at least* 40.

Proof. By [9, Theorem 4.33], no (320, 88, 24)-difference set exists in any abelian group of exponent at least 80. Assume there exists such a difference set D in an abelian group G with exponent 40. Let U be any subgroup of G of order 8 such that G/U is cyclic and let $\rho\colon G\to G/U$ be the canonical epimorphism. By the same argument as before, we have

$$\rho(D)=8x_0+4P_1x_1+2P_2x_2+P_3x_3, \tag{4.5}$$

where P_i and x_i are chosen as described in Lemma 2.3.

Let $\varphi\colon G/U\to H=(G/U)/P_2$ be the canonical epimorphism. As in the proof of Theorem 4.1, with $u=\varphi\circ\rho(D)/4=\sum_{g\in H}a_gg$, we have $\{a_g\}=\{4,2,2,\ldots,2\}$ or $\{a_g\}=\{3,3,3,2,2,\ldots,2,1\}$.

Case 1. ($\{a_g\}=\{4,2,2,\ldots,2\}$): For this case, we have $|x_0|=1$, $|x_1|=0$, $|x_2|=10$, and $|x_3|=0$. But then the element of x_0 must be in the same coset of P_2 as some element of x_2 which is not possible as the coefficients of $\rho(D)$ cannot exceed 8.

Case 2. $\{a_g\}=\{3,3,3,2,2,\ldots,2,1\}$: Using the same argument as Case 2 of the proof of Theorem 4.1, we obtain $|x_g|=1$, $|x_1|=0$, $|x_2|=8$, and $|x_3|=2$ and, hence, (4.5) becomes

$$\rho(D)=8h+2P_2A+P_3B, \tag{4.6}$$

where $h \in G/U$, $A, B \subset G/U$, and no two elements in $\{h\} \cup A$ are in the same coset of P_2. Now, we choose another subgroup U_1 of G of order 8 such that G/U_1 is cyclic and $|U \cap U_1| = 4$. By the argument above, there is a coset $U_1 g$ which is completely contained in D. However, since $U_1 g$ can be written as a union of two cosets of $U \cap U_1$, we must have at least two coefficients $\geqslant 4$ in $\rho(D)$. This contradicts (4.6). ∎

REFERENCES

1. K. T. ARASU, J. A. DAVIS, J. JEDWAB, AND S. L. MA, A nonexistence result for abelian McFarland difference sets, preprint.
2. L. D. BAUMERT, "Cyclik Difference Sets," Springer-Verlag, New York, 1971.
3. T. BETH, D. JUNGNICKELS, AND H. LENZ, "Design Theory," Cambridge Univ. Press, Cambridge, 1986.
4. J. A. DAVIS, Difference sets in non-abelian 2-groups, *in* "Coding Theory and Design Theory, Part II" (D. Ray-Chaudhuri, Ed.), pp. 65–69, Springer-Verlag, New York, 1990.
5. J. A. DAVIS, A result on Dillon's conjecture in difference sets, *J. Combin. Theory Ser. A* **57** (1991), 238–242.
6. J. A. DAVIS, Difference sets in 2-groups, *J. Combin. Theory Ser. A* **57** (1991), 262–286.
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, *in* "Contemporary Design Theory" (J. H. Dinitz and D. R. Stinson, Eds.), 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. K. H. LEUNG AND S. L. MA, Construction of partial difference sets and relative difference sets on p-groups, *Bull. London Math. Soc.* **22** (1990), 533-539.
12. R. L. MCFARLAND, A family of difference sets in non-cyclic groups, *J. Combin. Theory Ser. A* **15** (1973), 1–10.
13. R. J. TURYN, Character sums and difference sets, *Pacific J. Math.* **15** (1965), 319–346.