A sharp exponent bound for McFarland difference sets with $p = 2$

Siu Lun Ma
Department of Mathematics
National University of Sinagpore
Kent Ridge
Singapore 119260
Republic of Singapore

Bernhard Schmidt
Mathematisches Institut
Universität Augsburg
Universitätsstrasse 15
86135 Augsburg
Germany

Abstract

We show that under the self-conjugacy condition a McFarland difference set with $p = 2$ and $f \geq 2$ in an abelian group G can only exist, if the exponent of the Sylow 2-subgroup does not exceed 4. The method also works for odd p (where the exponent bound is p and is necessary and sufficient), so that we obtain a unified proof of the exponent bounds for McFarland difference sets. We also correct a mistake in the proof of an exponent bound for $(320, 88, 24)$-difference sets in a previous paper.

1 Introduction

A (v,k,λ)-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 integer $n := k - \lambda$ is called the order of the difference set. If we use the notation of the group ring $\mathbf{Z}G$ and identify a subet A of G with the element $\sum_{g\in A} g$ of $\mathbf{Z}G$, a k-subset D of G is a (v,k,λ)-difference set in G if and only if

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

where $D^{(-1)} := \sum_{g\in D} g^{-1}$. For $A = \sum_{g\in G} a_g g \in \mathbf{Z}G$, we will write $|A| := \sum_{g\in G} a_g$.

A McFarland difference set is a difference set with parameters

$$\begin{aligned} v &= q^{d+1}[1 + (q^{d+1}-1)/(q-1)], \\ k &= q^d(q^{d+1}-1)/(q-1), \\ \lambda &= q^d(q^d-1)/(q-1), \\ n &= q^{2d}, \end{aligned}$$

where $q = p^f$ is a prime power. McFarland (1973) constructed such difference sets in all abelian groups G of order $v = q^{d+1}[1 + (q^{d+1}-1)/(q-1)]$ which contain a subgroup isomorphic to the elementary abelian group $EA(q^{d+1})$ of order q^{d+1}. For odd p this means that the Sylow p-subgroup P of G has to be elementary abelian, and for $p = 2$ this means $P \cong EA(2^{f(d+1)+1})$ or $P \cong EA(2^{f(d+1)-1}) \times \mathbf{Z}_4$. In the previous paper Ma, Schmidt (1995) we showed that for odd p under the self-conjugacy assumption actually no other abelian groups can contain McFarland difference sets. For $p = 2$ we only obtained a weaker result.

In this paper, we will show that under the self-conjugacy assumption a McFarland difference set with $p = 2$ and $f \geq 2$ in an abelian group G can only exist if the exponent of the Sylow 2-subgroup P of G does not exceed 4. This exponent bound is best possible, since, as mentioned above, examples of McFarland difference sets with $exp(P) = 4$ are known. Furthermore, a recent construction of Davis, Jedwab (1996) shows that the exponent bound 4 is sufficient in the case $f = 2$.

As our method also works for odd p, we are able to give a unified proof of the exponent bounds for McFarland difference sets.

In the last section, we correct the proof of an exponent bound for $(320, 88, 24)$-difference sets in our previous paper Ma, Schmidt (1995).

2 A Lemma

In this section, we prove a lemma, which is crucial for all results on McFarland difference sets obtained in this paper. The lemma can also be used to study other difference sets. For example, in a subsequent paper we will show that a relative $(p^{2a+1}, p^b, p^{2a+1}, p^{2a-b+1})$-difference set (where p is an odd prime) in an abelian group G can only exist if $exp(G) \le p^{a+1}$.

Let G be a finite abelian group, and let P be be the Sylow p-subgroup of G. For any $a \in P$ and any subgroup $A = \langle b_1 \rangle \times \cdots \langle b_r \rangle$ of P such that $A \cap \langle a \rangle = \{1\}$ and $o(a) \ge exp(A)$, define

$$\mathcal{S}(a, A) = \{U < P |\; U = \langle a_1 b_1 \rangle \times \cdots \langle a_r b_r \rangle,\; a_i \in \langle a \rangle,\; o(a_i) \le o(b_i)\}.$$

Let $D = \sum_{g \in G} a_g g$ be an element of $\mathbf{Z}G$. For $U \le G$ and $h \in G$, we define $D(Uh) = \sum_{g \in Uh} a_g$. Now we are ready to state the lemma.

Lemma 2.1 *Let $D = \sum_{g \in G} a_g g$ be an element of $\mathbf{Z}G$ with $a_g \ge 0$ for all g. Let $a \in P$, and let $A = \langle b \rangle \times W$ be a subgroup of P such that $A \cap \langle a \rangle = \{1\}$, $o(a) = p^t \ge exp(A)$ and $o(b) \ge p$. Assume that there exists a positive integer δ such that for any $U \in \mathcal{S}(a, A)$ and $g \in G$ either*
(1a) $D(Ug) - D(Uga^{p^{t-1}}) \ge \delta$ and
(1b) $D(Uga^{ip^{t-1}}) < \delta/p$ for $i = 1, ..., p-1$ or
(2) $D(Ug) < \delta/p$,
and that there is at least one coset Ug satisfying (1). Let $B =< b^p > \times W$. Then for any $U' \in S(a, B)$ and $g \in G$, the coset $U'g$ satisfies either (1) or (2); and there is at least one coset $U'g$ satisfying (1).

Proof
We write $U' =< a_1 b^p > \times V$ with $a_1 \in < a >$, $o(a_1) \le o(b^p)$ and $V \in S(a, W)$. Let $a'_1 \in < a >$, $a'^p_1 = a_1$. Define

$$U_i =< a'_1 a^{ip^{t-1}} b > \times V$$

for $i = 0, ..., p-1$. Note $U' < U_i$ and $U_i \in S(a, A)$. Let $g \in G$. If some $U_i g$ satisfies (2) then obviously U' also satisfies (2). Suppose that all $U_i g$ satisfy (1). We have $U_i = U' \sum_{j=0}^{p-1} a'^j_1 a^{ijp^{t-1}}$. Hence

$$\sum_{j=0}^{p-1} [D(U' a'^j_1 a^{ijp^{t-1}} g) - D(U' a'^j_1 a^{(ij+1)p^{t-1}} g)] \ge \delta$$

for $i = 0, ..., p-1$. Thus

$$\sum_{i=0}^{p-1}\sum_{j=0}^{p-1}[D(U'a_1'^j a^{ijp^{t-1}}g) - D(U'a_1'^j a^{(ij+1)p^{t-1}}g)] \geq p\delta.$$

If $j \neq 0$, then $\{a^{ijp^{t-1}} : i = 0, ..., p-1\} = \{a^{(ij+1)p^{t-1}} : i = 0, ..., p-1\}$. Hence

$$D(U'g) - D(U'ga^{p^{t-1}}) \geq \delta,$$

i.e. the coset $U'g$ satisfies (1a). It is clear that $U'g$ also satisfies (1b).
It remains to show that at least one coset $U'g$ satisfies (1). It is given that there is a coset U_0g satisfying (1). Hence $D(< a^{p^{t-1}} > \times < a_1'b > \times Vg) \geq \delta$. As

$$< a^{p^{t-1}} > \times < a_1'b > \times Vg = \bigcup_{j=0}^{p-1} U_i a^{jp^{t-1}} g$$

$(i = 0, ..., p-1)$, there must be $j_i \in \{0, ..., p-1\}$ such that the coset $U_iga^{j_ip^{t-1}}$ satisfies (1) $(i = 0, ..., p-1)$. Since $U_0ga^{j_0p^{t-1}} \cap U_1ga^{j_1p^{t-1}} \neq \emptyset$, we can assume $j_0 = j_1 = 0$. As $U' = U_0 \setminus \bigcup_{j=1}^{p-1} U_1a^{jp^{t-1}}$ and $D(U_1ga^{jp^{t-1}}) < \delta/p$ for $j = 1, ..., p-1$, it follows that $D(U'g) > \delta/p$. Thus $U'g$ must be contained in $U_iga^{j_ip^{t-1}}$ for all i, i.e. $j_i = 0$ for all i. By the same argument as above, it follows that the coset $U'g$ satisfies (1a) and (1b). □

Corollary 2.2 *In the situation of the Lemma 2.1 we have*

$$\delta \leq \max\{a_g : g \in G\}.$$

Proof
Apply Lemma 2.1 repeatedly until $A = \{1\}$. □

3 The exponent bounds

Before we can state our main result, we need the following definition.

Definition 3.1 *A prime p is called self-conjugate modulo a positive integer m if there exists a positive integer j with*

$$p^j \equiv -1 \ mod \ m',$$

where $m = p^a m'$ *with* $(m', p) = 1$.

Theorem 3.2 *Assume that there exists a McFarland difference set D in an abelian group G of order $q^{d+1}[1+(q^{d+1}-1)/(q-1)]$, where $q=p^f$ is a prime power, and p is self-conjugate modulo $exp(G)$. Let P be the Sylow p-subgroup of G. Then the following holds.*
(a) If p is odd then P is elementary abelian.
(b) If $p=2$ and $f \geq 2$ then $exp(P) \leq 4$.

Proof
Let a be an element of P order $p^e := exp(P)$ and write $P = \langle a \rangle \times A$ for a suitable $A < P$.
(a) Asssume that p is odd and $e \geq 2$. By the equation (3.3) of the proof of Theorem 3.1 of Ma, Schmidt (1995), the assumptions of Lemma 2.1 are satisfied with $\delta = q^d > 1$ yielding a contradiction to Corollary 2.2.
(b) Asssume that $p=2$ and $e \geq 3$. By the equations (4.3) and (4.4) of the proof of Theorem 4.1 of Ma, Schmidt (1995), the assumptions of Lemma 2.1 are satisfied with $\delta = q^d > 1$ again yielding a contradiction to Corollary 2.2.
□

Remark
(a) From the construction of McFarland (1973) we know that the condition in Theorem 3.2 (a) is also sufficient.
(b) Davis, Jedwab (1996) showed that condition in Theorem 3.2 (b) is sufficient for $f=2$. It is an open question if this remains true for $f>2$.

4 (320,88,24)-difference sets

As has been pointed out to us by J.A.Davis and J. Jedwab, we missed a case while trying to prove an exponent bound for (320,88,24)-difference sets in the previous paper Ma, Schmidt (1995). In the following, we give a correct proof a generalization of which can be found in Schmidt (submitted).

Theorem 4.1 *No (320,88,24)-difference sets exists in any abelian group of exponent exceeding 20.*

Proof
Let G be an abelian group of order 320, and let D be a $(320,88,24)$-difference set in G. By Theorem 4.33 of Lander (1983) we have $exp(G) \leq 40$. Assume $exp(G) = 40$ and write $G = G_5 \times G_8 \times H$ with $G_5 \cong \mathbf{Z}_5$, $G_8 \cong \mathbf{Z}_8$ and

$|H| = 8$. It is shown in Arasu, Sehgal (1995) that H cannot be cyclic. Thus we may assume $\mathrm{rank}(H) \geq 2$.
Let U be any complement of $G_5 \times G_8$ in G and let $\rho : G \to G/U$ be the canonical epimorphism. By the self-conjugacy argument (see Turyn (1965)) and Ma's Lemma (see Ma (1985)) we get

$$\rho(D) = 8X + PY, \tag{1}$$

where P is the subgroup of order 2 in G/U and X, Y are elements of $\mathbf{Z}[G/U]$ with nonnegative coefficients. Since $\rho(D)$ cannot have coefficients greater than $|U| = 8$, we conclude that X and PY cannot overlap.
Applying a character of order 8 to the equation

$$\rho(D)\rho(D)^{(-1)} = 64(1 + 3G/U) \tag{2}$$

we infer $|X| \geq 1$. Furthermore, writing $\rho(D) = \sum_{g \in G/U} a_g g$, (2) implies

$$\sum a_g^2 = 256. \tag{3}$$

Define $b_g = a_g - 2$. Then a calculation using $|G_U| = 40$, $\sum a_g = 88$ and (3) gives

$$\sum b_g^2 = 64. \tag{4}$$

If $|X| \geq 2$ then $\sum b_g^2 \geq 72$ which is impossible. Thus $|X| = 1$. Let z be the element of order 2 of G_8. Since X and PY do not overlap, we conclude that $(*)$ for every complement U of $G_5 \times G_8$ in G there is a coset L_U of $U\langle z \rangle$ such that one coset of U in L_U is completely contained in D and the other has empty intersection with D.
Write $H = < g_1, g_2 > \times K$, where possibly $|K| = 1$. Let $U_{ij} = < g_1 z^i, g_2 z^j > \times K$, $i, j = 0, 1$. By $(*)$, obviously $L_{U_{ij}} \neq L_{U_{i'j'}}$ for $(i,j) \neq (i',j')$. Let $\tau : G \to G/H$ be the canonical epimorphism. The cosets $L_{U_{ij}}$, $(i,j) \neq (0,0)$, lead to 6 coefficients 4 in $\tau(D)$ since every $L_{U_{ij}}$, $(i,j) \neq (0,0)$, is the union of two cosets of H which both intersect each of the two cosets of U_{ij} in $L_{U_{ij}}$ in exactly 4 elements.
Now, we will derive a contradiction to (4) for $U = H$. We know from above that $\tau(D)$ has one coefficient 8 and at least 6 coefficients 4. Let $\{a_g : g \in T\}$ be the remaining coefficients of $\tau(D)$. Since

$$\begin{aligned} \sum_{g \in T} b_g &= 88 - (8 + 4 \cdot 6) - 2(40 - 7) \\ &= -10, \end{aligned}$$

we infer $\sum_{g\in T} b_g^2 \geq 10$. Thus

$$\begin{aligned} \sum b_g^2 &\geq (8-2)^2 + 6(4-2)^2 + 10 \\ &= 70 \end{aligned}$$

contradicting (4). □

Remark
It is shown in Davis, Jedwab (1996) that $(320, 88, 22)$-difference sets exist in all abelian groups of exponent less than 40, except possibly $(\mathbf{Z}_4)^3 \times \mathbf{Z}_5$.

5 References

1. K.T. Arasu, S.K. Sehgal (1995): Difference sets in abelian groups of p-rank two. Designs, Codes and Cryptography 5, 5-12.

2. J.A. Davis, J. Jedwab: A unifying construction of difference sets. Technical Report HPL-96-31, Hewlett-Packard Labs., Bristol (1996).

3. E.S. Lander (1983): Symmetric Designs: An Algebraic Approach. Cambridge University Press, Cambridge.

4. S.L. Ma (1985). Polynomial addition sets. Ph.D. thesis. University of Hong Kong.

5. S.L. Ma, B. Schmidt (1995): The Structure of Abelian Groups Containing McFarland Difference Sets. J. Comb. Theory A 70, 313-322.

6. R.L. McFarland (1973): A family of difference sets in noncyclic groups. J. Comb. Theory A 15, 1-10.

7. B. Schmidt (submitted): Nonexistence Results on Chen and Davis-Jedwab Difference Sets.

8. R.J. Turyn (1965): Character sums and difference sets. Pacific J. Math. 15 (1965), 319-346.