Difference Sets Corresponding to a Class of Symmetric Designs

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

Bernhard Schmidt
Mathematisches Institut
Universität Augsburg
Universitätsstraße 15
86135 Augsburg
Germany

April 10, 1996

Dedicated to Professor Dr. Hanfried Lenz

Abstract

We study difference sets with parameters $(v,k,\lambda) = (p^s(r^{2m}-1)/(r-1), p^{s-1}r^{2m-1}, p^{s-2}(r-1)r^{2m-2})$, where $r=(p^s-1)/(p-1)$ and p is a prime. Examples for such difference sets are known from a construction of McFarland which works for $m=1$ and all p, s. We will prove a structural theorem on difference sets with the above parameters; it will include the result, that under the self-conjugacy assumption McFarland's construction yields all difference sets in the underlying groups. We also show that no abelian $(160,54,18)$-difference set exists. Finally, we give a new nonexistence prove of $(189,48,12)$-difference sets in $\mathbf{Z}_3 \times \mathbf{Z}_9 \times \mathbf{Z}_7$.

1 Introduction

A (v,k,λ)-difference set in a finite group 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. Such a (v,k,λ)-difference set in G is equivalent to a symmetric (v,k,λ)-design admitting G as a regular automorphism group [see Lander (1983)]. We will study difference sets with parameters

$$\begin{array}{rcl} v & = & p^s(r^{2m}-1)/(r-1), \\ k & = & p^{s-1}r^{2m-1}, \\ \lambda & = & p^{s-2}(r-1)r^{2m-2}, \\ n & = & p^{2s-2}r^{2m-2}, \end{array} \tag{1}$$

where p is a prime, $r=(p^s-1)/(p-1)$, $s \geq 2$ and $m \geq 1$. Wallis (1971) was the first who constructed symmetric designs with parameters (1), and McFarland (1973) gave a contruction of difference sets with these parameters. Both constructions only work for $m=1$, but also include symmetric designs respectively difference sets with parameters different from (1). The parameter series covered by the constructions of Wallis and McFarland is

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

where $q = p^f$ is any prime power. For $f = 1$ this series coincides with series (1), where we have to choose $m = 1$.
Finally, by generalizing a result of Spence (1993), Jungnickel and Pott (1995) constructed symmetric designs with parameters (1) for all $m > 1$ and all $s \geq 2$, such that r is a prime power.
In this paper, we first study difference sets with parameters (1) in general. Section 2 will provide the necessary theoretical background. In Section 3 we will give a theorem on the structure of such difference sets including a proof of the uniqueness of McFarlands construction under the self-conjugacy condition. In Section 4 the special case $p = s = m = 2$, i.e. the case of $(160, 54, 18)$-difference sets, will be studied in detail. We will show that no abelian difference sets with these parameters exist; this fills two open entries in Kopilovich's table of noncyclic abelian difference sets with $k \leq 100$ [Kopilovich (1989)]. Section 5 contains a new proof for the nonexistence of a $(189, 48, 12)$-difference set in $\mathbf{Z}_3 \times \mathbf{Z}_9 \times \mathbf{Z}_7$; this case does not belong to the parameter series (1), but can be handled by similar methods. The only proof available up to now [Arasu, McDonough, Seghal (1993)] required complicated calculations in cyclotomic fields, which will be avoided by our approach.

2 Preliminary Results

In this section we state some technical results, which are very useful for the study of difference sets and will be needed in the later sections.
Throughout the paper, we will use following notation. Let G be a finite group. We identify a subset A of G with the element $\sum_{g \in A} g$ of the group ring $\mathbf{Z}G$. For $B = \sum_{g \in G} b_g g \in \mathbf{Z}G$ we write $|B| := \sum_{g \in G} b_g$ and $B^{(-1)} := \sum_{g \in G} b_g g^{-1}$. Let U be a normal subgroup of G; the natural epimorphism $G \to G/U$ is always assumed to be extended to $\mathbf{Z}G$ by linearity and is denoted by ρ_U. Furthermore, we write $G_U := G/U$ and $g_U := \rho_U(g)$ for $g \in G$. If D is a subset of G with $\rho_U(D) = \sum_{g \in G_U} d_g g$, then the numbers $d_g = |D \cap Ug|$ are called coefficients of $\rho_U(D)$ or intersection numbers of D with respect to U.
In the case of a double projection, i.e. if we have two subgroups $U_1 \leq U_2$ of G, we identify (for $B \in \mathbf{Z}G$) $\rho_{U_2}(B)$ with $\rho_{U_2/U_1}(\rho_{U_1}(B))$ in order to avoid a clumsy notation.
A multiset containing exactly λ_i "copies" of the element a_i $(i = 1, 2, ..., t)$ will be denoted by $\{\lambda_1 \cdot a_1, ..., \lambda_t \cdot a_t\}$.

We begin with a fundamental lemma which is a direct consequence of the definition of a difference set.

Lemma 2.1 *Let D be a (v, k, λ)-difference set in a group G, and let U be a normal subgroup of G, such that G_U is abelian. Then*

$$\rho_U(D)\rho_U(D)^{(-1)} = n + |U|\lambda G_U,$$

and hence

$$\chi(\rho_U(D))\overline{\chi(\rho_U(D))} = n$$

for every nontrivial character χ of G_U.

Definition 2.2 *A prime p is called self-conjugate modulo a positive integer m, if there is a positive integer j with*

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

where $m = p^a m'$ with $(m', p) = 1$. An integer t is called self-conjugate modulo m if every prime divisor of t is self-conjugate modulo m.

Lemma 2.3 (Turyn (1965)) *Let ξ be a complex m-th root of unity, and let t be an integer, which is self-conjugate modulo m. If $A \in \mathbf{Z}[\xi]$ and*

$$A\overline{A} \equiv 0 \bmod t^{2a}$$

for a positive integer a, then

$$A \equiv 0 \bmod t^a.$$

The next lemma is a direct consequence of the inversion formula [see for instance Curtis, Reiner (1962)].

Lemma 2.4 *Let G be a finite abelian group, and let t be a postive integer relatively prime to $|G|$. If $B \in \mathbf{Z}G$ with*

$$\chi(B) \equiv 0 \bmod t$$

for all characters of G, then

$$B \equiv 0 \bmod t.$$

The next result will be an essential tool in this paper.

Lemma 2.5 (Ma (1985)) *Let p be a prime, and let G be a finite abelian group with cyclic Sylow p-subgroup. If $Y \in \mathbf{Z}G$ satisfies the condition*

$$\chi(Y) \equiv 0 \ mod \ p^a$$

for all nontrivial characters χ of G, then there are $X_1, X_2 \in \mathbf{Z}G$ with

$$Y = p^a X_1 + P X_2,$$

where P is the unique subgroup of order p of G.
Furthermore, the coefficients of X_1 and X_2 can be chosen to be nonnegative if Y has nonnegative coefficients.

We will also need a lemma on sums of squares.

Lemma 2.6 *Let $a_1, a_2, ..., a_n, m \in \mathbf{N}_0$ with $\sum_{i=1}^n a_i = m$. Then*

$$\sum_{i=1}^n a_i^2 = min\{\sum_{i=1}^n b_i^2 : b_i \in \mathbf{N}_0, \sum_{i=1}^n b_i = m\}$$

if and only if $|a_i - a_j| \leq 1$ for all $i, j \leq n$.

Proof
If $a_i - a_j \geq 2$, then we can replace a_i by $a_i - 1$ and a_j by $a_j + 1$, and $\sum a_i^2$ decreases. The lemma follows by induction. □

Example 2.7 Let G be a group of order 20, and let $w = \sum_{g \in G} a_g g$ be an element of $\mathbf{Z}G$ with $a_g \geq 0$ for all $g \in G$ and $\sum a_g = 27$, which satisfies

$$ww^{(-1)} = 9 + 36G.$$

Then $\sum a_g^2 =$ coefficient of 1 in $ww^{(-1)} = 45$. If we had $a_g = 4$ for any g, then Lemma 2.6 would imply

$$\sum a_g^2 \geq 4^2 + 4 \cdot 2^2 + 15 \cdot 1^2 = 47,$$

a contradiction. Hence $a_g \leq 3$ for all g. Using similar arguments, it is easy to show that $\{a_g : g \in G\}$ must be one of the multisets $\{9 \cdot 2, 9 \cdot 1, 2 \cdot 0\}$, $\{1 \cdot 3, 6 \cdot 2, 12 \cdot 1, 2 \cdot 0\}$, $\{2 \cdot 3, 3 \cdot 2, 15 \cdot 1\}$.

The following result is a special case of Lemma 3.2 from Ma, Schmidt (1995).

Lemma 2.8 *Let p be a prime, and let $G = E \times H$ be an abelian group with $E \cong (\mathbf{Z}_p)^s$ and $(p, |H|) = 1$. Let $\mathcal{R}$ be the set of subgroups of order p^{s-1} of E. If D is a subset of G with*

$$\chi(D) \equiv 0 \ mod \ p^{s-1}$$

for all nontrivial characters χ of G, then D can be written as

$$D = \sum_{U \in \mathcal{R}} UX_U + EY,$$

with $X_U, Y \subset G$.

3 Some general Results

In Result 3.1 we recall the construction of McFarland (1973), which shows that there are difference sets with parameters (1) for all p and s if $m = 1$. For $m > 1$, no example of a difference set with parameters (1) is known. As there are examples of symmetric designs with these parameters [see section 1], it is interesting to ask if the corresponding difference sets exist, i.e. if there are symmetric designs belonging to this parameter series admitting a regular automorphism group.
In the Results 3.1-3.3 we summarize what is already known about difference sets with parameters (1). Our Theorem 3.4 gives some more structural information and shows that in the case of self-conjugacy the contruction in Result 3.1 yields **all** difference sets in the underlying group.
The following is a special case of McFarlands contruction [McFarland (1973)].

Result 3.1 *Let p be a prime, and let G be a group of order*

$$v = p^s(\frac{p^s - 1}{p - 1} + 1)$$

with an elementary abelian Sylow p-subgroup E. Let $H_1, ..., H_r$ ($r = \frac{p^s-1}{p-1}$) be the subgroups of order p^{s-1} of E, and let $g_1, ..., g_r$ be representatives of distinct cosets of E in G. Then

$$D = \sum_{i=1}^{r} H_i g_i$$

is a difference set in G with parameters (1) (where $m = 1$).

The next result follows from the so-called Mann-Test [see Jungnickel (1992)]. For the convenience of the reader, we include a proof.

Theorem 3.2 *Let D be a difference set with parameters (1) in a group G, and assume $m > 1$. If there exists a normal subgroup U of G, such that G_U is abelian, and if there exists a divisor t of r, which is self-conjugate modulo $exp(G_U)$, then*

$$|U| \geq 1 + (t-1)\frac{p^s - 1}{p^{s-1} - 1}.$$

Proof
By Lemmas 2.1, 2.3 and 2.4 we can write

$$\rho_U(D) = tw$$

for some $w \in \mathbf{Z}G_U$, and we have

$$ww^{(-1)} = \frac{n}{t^2} + \frac{\lambda}{t^2}|U|G_U.$$

Comparing the coefficient of 1 in this equation yields

$$\frac{k}{t} \leq \frac{n}{t^2} + \frac{\lambda}{t^2}|U|,$$

hence

$$\begin{aligned} |U| &\geq \frac{1}{\lambda}(kt - n) \\ &= 1 + (t-1)\frac{k}{\lambda} \\ &= 1 + (t-1)\frac{p^s - 1}{p^{s-1} - 1}. \end{aligned}$$

□

The next result is a consequence of Theorem 4.33 of Lander (1983).

Result 3.3 *Assume that there exists a difference set with parameters (1) in an abelian group G. Let U be a subgroup of G, such that the Sylow p-subgroup of G_U is cyclic and p is self-conjugate modulo exp(G_U). Then*

$$|U| \geq p^{s-1}.$$

Now we prove a new result dealing with the case of equality in Result 3.3.

Theorem 3.4 *Let D be a difference set with parameters (1) in an abelian group G, where $(p, 2m) = 1$ and p is self-conjugate modulo exp(G).*
Then the Sylow p-subgroup E of G is elementary abelian, and we have

$$D = \sum_{i=1}^{r} H_i X_i,$$

where $H_1, ..., H_r$ are the subgroups of order p^{s-1} of E, and $X_1, ..., X_r$ are subsets of G with $|X_1| = \cdots = |X_r| = r^{2m-2}$, such that no two elements of $X_1 \cup \cdots \cup X_r$ are in the same coset of E.
Furthermore, $\rho_E(D) \equiv 0 \ mod\ p^{s-1}$, and $\rho_E(D)/p^{s-1}$ is the complement of a difference set in G_E with parameters

$$(v, k, \lambda) = (\frac{r^{2m}-1}{r-1}, \frac{r^{2m-1}-1}{r-1}, \frac{r^{2m-2}-1}{r-1}).$$

Remark
a) A classical construction of Singer (1938) shows that difference sets with parameters

$$(v, k, \lambda) = (\frac{r^{2m}-1}{r-1}, \frac{r^{2m-1}-1}{r-1}, \frac{r^{2m-2}-1}{r-1})$$

exist if r is prime power. It is widely conjectured that this condition is also necessary [see Jungnickel (1992)].
b) The assumptions of Theorem 3.4 are always satisfied for $m = 1$ and $p = 3$, since $3^s \equiv -1 \bmod (3^s - 1)/(3 - 1) + 1$.

Proof of Theorem 3.4
First of all, we observe that p^s is the exact divisor of v, since

$$\frac{r^{2m}-1}{r-1} = \frac{(p^s-1)^{2m} - (p-1)^{2m}}{p(p^{s-1}-1)(p-1)^{2m-1}}$$

and

$$(p^s-1)^{2m}-(p-1)^{2m} \equiv 2mp \bmod p^2.$$

From Result 3.3 we see that E is elementary abelian. By Lemmas 2.1 and 2.3 we have

$$\chi(D) \equiv 0 \bmod p^{s-1}$$

for every nontrivial character χ of G. Thus we can apply Lemma 2.8 and get

$$D = \sum_{i=1}^{r} H_i X_i + EY$$

with $X_i, Y \subset G$, where $H_1, ..., H_r$ are the subgroups of order p^{s-1} of E. Let $\{h_1, ..., h_p\}$ be a complete system of coset representatives of H_1 in E. Replacing X_1 by $X_1 + Y\sum_{i=1}^{p} h_i$ we can assume $Y = 0$, i.e.

$$D = \sum_{i=1}^{r} H_i X_i. \tag{2}$$

In particular,

$$\rho_E(D) \equiv 0 \bmod p^{s-1}.$$

We write $\rho_E(D) = p^{s-1}w$ with $w \in \mathbf{Z}G_E$. Lemma 2.1 gives

$$ww^{(-1)} = r^{2m-2} + (r-1)r^{2m-2}G_E.$$

The argument described in Example 2.7 shows that w has coefficients 0 and 1 only, i.e. w is a difference set in G_E. It also follows that no two elements of $X_1 \cup \cdots \cup X_r$ are in the same coset of E.
It remains to show $|X_i| = r^{2m-2}$ for $i = 1, ..., r$. From (2) we have

$$\rho_{H_i}(D) = p^{s-1}\rho_{H_i}(X_i) + p^{s-2}P\sum_{j\neq i}\rho_{H_i}(X_j),$$

where P is the subgroup of order p of G_{H_i}. Comparing the coefficient of 1 in the equation

$$\rho_{H_i}(D)\rho_{H_i}(D)^{(-1)} = p^{2s-2}r^{2m-2} + p^{2s-3}(r-1)r^{2m-2}G_{H_i}$$

gives

$$p^{2s-2}|X_i| + p^{2s-3}\sum_{i\neq j}|X_j| = p^{2s-3}r^{2m-2}(r+p-1).$$

Together with $\sum_{j=1}^{r}|X_j| = r^{2m-1}$ this yields $|X_i| = r^{2m-2}$. □

Corollary 3.5 *Let D be a difference set with parameters (1) in an abelian group G, where p is odd and self-conjugate modulo exp(G). If $m = 1$, then D is one of the difference sets constructed in Result 3.1.*

Remark
Corollary 3.5 could also be derived using the methods in the paper Ma, Schmidt (1995a).

4 Abelian (160,54,18)-difference sets

The construction of McFarland [see Result 3.1] gives difference sets with parameters (1) for $m = 1$ and all p and s. It is interesting to ask if this construction can be generalized to $m > 1$. Unfortunately, this seems to be impossible. At least such a construction cannot include the whole series (1), since we will show that there is no abelian difference set with these parameters in the case $m = p = s = 2$ (i.e. $(v, k, \lambda) = (160, 54, 18)$). This also fills two missing entries in Kopilovich's table of noncyclic abelian difference sets with $k \leq 100$ [Kopilovich (1989)].
The nonexistence of abelian $(160, 54, 18)$-difference sets in $G \neq \mathbf{Z}_2 \times \mathbf{Z}_{16} \times \mathbf{Z}_5$, $\mathbf{Z}_4 \times \mathbf{Z}_8 \times \mathbf{Z}_5$ is already known and follows from the Results 3.2 and 3.3. The remaining cases need some more involved arguments dealing with the simultaneous solution of equations arising from Lemma 2.1. We think that similar methods can be used to handle other difference sets, especially such with parameters (1).
It should be mentioned that an additional motivation for the study of difference sets in $\mathbf{Z}_2 \times \mathbf{Z}_{16} \times \mathbf{Z}_5$ and $\mathbf{Z}_4 \times \mathbf{Z}_8 \times \mathbf{Z}_5$ comes from the fact that a projection down to $\mathbf{Z}_8 \times \mathbf{Z}_5$ could be a multiple of a complement of a cyclic $(40, 13, 4)$-difference set (which is known to exist, see Remark a) after Theorem 3.4 and put $r = 3$, $m = 2$).
Finally, we want to speculate on a possible connection to the construction of difference sets in nonabelian groups. In our Lemma 4.3, we come very close to contructing a projected difference set in $\mathbf{Z}_2 \times \mathbf{Z}_4 \times \mathbf{Z}_5$. Therefore, there might be a chance to use this information for the contruction of a difference set in a nonabelian group of order 160.

Proposition 4.1 *There is no* $(160, 54, 18)$*-difference set in an abelian group* $G \neq \mathbf{Z}_2 \times \mathbf{Z}_{16} \times \mathbf{Z}_5$, $\mathbf{Z}_4 \times \mathbf{Z}_8 \times \mathbf{Z}_5$.

Proof
For $G = \mathbf{Z}_{32} \times \mathbf{Z}_5$ this follows from Result 3.3 (with $U = 1$). In the remaining cases there is a subgroup U of order 4, such that $exp(G_U) = 10$. Since 3 is self-conjugate modulo 10, the assertion follows from Result 3.2. □

Theorem 4.2 *There are no* $(160, 54, 18)$*-difference sets in* $\mathbf{Z}_2 \times \mathbf{Z}_{16} \times \mathbf{Z}_5$ *and* $\mathbf{Z}_4 \times \mathbf{Z}_8 \times \mathbf{Z}_5$.

We devide the proof of Theorem 4.3 into several steps. Our first goal is the following lemma.
Troughout this section, D denotes a $(160, 54, 18)$-difference set in
$G =< g >< h >< k > \cong \mathbf{Z}_2 \times \mathbf{Z}_{16} \times \mathbf{Z}_5$ (**Case 1**)
or
$G =< g >< h >< k > \cong \mathbf{Z}_4 \times \mathbf{Z}_8 \times \mathbf{Z}_5$ (**Case 2**).

Lemma 4.3 *Let* $U =< h^4 >$ *in Case 1 and* $U =< g^2 >< h^4 >$ *in Case 2. Then (replacing* D *by a translate if necessary) we have*

$$\rho_U(D) = (4b + 2bh_U^2) + X(3 + g_U + 2g_U h_U^2) + Y(1 + 2h_U^2)(1 + g_U)$$

with $b \in G_U$, $X, Y \subset G_U$, $|X| = 2$ *and* $|Y| = 6$, *such that* $\{1\} \cup \{b\} \cup X \cup Y$ *is a complete system of coset representatives of* $T :=< g_U >< h_U^2 >$ *in* G_U.

In order to prove Lemma 4.3 we need some preliminary results.

Lemma 4.4 *Let* U_2 *be a subgroup of* G *with* $G_{U_2} \cong \mathbf{Z}_2 \times \mathbf{Z}_5$, *which contains a subgroup* U_1, *such that* $G_{U_1} \cong \mathbf{Z}_4 \times \mathbf{Z}_5$. *Then (up to a translation)*

$$\rho_{U_2}(D) = 6(G_{U_2} - 1)$$

(in either of the Cases 1 and 2).

Proof
By Lemmas 2.1, 2.3 and 2.4 we have

$$\rho_{U_2}(D) \equiv 0 \bmod 3. \tag{3}$$

From Lemmas 2.1, 2.3 and 2.5 we get

$$\rho_{U_1}(D) = 2X + PY,$$

where $X, Y \in \mathbf{Z}G_{U_1}$ and P is the subgroup of order 2 of G_{U_1}. As $\rho_{U_2}(P) = 2$, it follows that

$$\rho_{U_2}(D) \equiv 0 \bmod 2. \tag{4}$$

By (3) and (4) we can write $\rho_{U_2}(D) = 6w$ for some $w \in \mathbf{Z}G_{U_2}$. Lemma 2.1 implies $ww^{(-1)} = 1 + 8G_{U_2}$. The argument described in Example 2.7 shows that w has coefficients $\{9 \cdot 1, 1 \cdot 0\}$, i.e. $w = G_{U_2} - l$ for some $l \in G_{U_2}$. By replacing D by a translate (if necessary) we can assume $l = 1$. □

Lemma 4.5 *Let $U_3 =< h^2 >$ in Case 1 and $U_3 =< g^2 >< h^2 >$ in Case 2. Then (up to a translation)*

$$\rho_{U_3}(D) = 3(G_{U_3} - (1 + g_{U_3}) + a(1 - g_{U_3}))$$

for some $a \in G_{U_3} \setminus \{1, g_{U_3}\}$.

Proof
By Lemmas 2.1, 2.3 and 2.4 we can write $\rho_{U_3}(D) = 3u$ with $u \in \mathbf{Z}G_{U_3}$. Let $u = \sum_{g \in G_{U_3}} a_g g$. Lemma 2.1 gives $uu^{(-1)} = 4 + 16G_{U_3}$. By the argument described in Example 2.7 we see that $\{a_g\} = \{1 \cdot 2, 16 \cdot 1, 3 \cdot 0\}$, i.e.

$$u = G_{U_3} + g_1 - g_2 - g_3 - g_4, \tag{5}$$

where $g_1, ..., g_4$ are different elements of G_{U_3}. Let $U_2 =< g >< h^2 >$ (in Case 1 and 2). Then by (5) and Lemma 4.4

$$\begin{aligned} \rho_{U_2}(u) &= 2G_{U_2} + (g_1)_{U_2} - (g_2)_{U_2} - (g_3)_{U_2} - (g_4)_{U_2} \\ &= 2G_{U_2} - 2. \end{aligned}$$

Hence (w.l.o.g.) $(g_1)_{U_2} = (g_2)_{U_2}$ and $(g_3)_{U_2} = (g_4)_{U_2} = 1$. Together with (5) this proves the assertion. □

Lemma 4.6 *Let* $U_4 =< g >< h^4 >$ *(in Case 1 and 2). Then* $\rho_{U_4}(D)$ *has coefficients* $0, 2, 4$ *only.*

Proof
We have $\rho_{U_4}(D) \equiv 0 \bmod 2$ by the same argument as in the proof of Lemma 4.4. Let $\rho_{U_4}(D) = 2z$ with $z = \sum_{g \in G_{U_4}} b_g g$. Lemma 2.1 yields $zz^{(-1)} = 9 + 36G_{U_4}$. From Example 2.7 we know
$\{b_g\} = \{9 \cdot 2, 9 \cdot 1, 2 \cdot 0\}$ or
$\{b_g\} = \{1 \cdot 3, 6 \cdot 2, 12 \cdot 1, 2 \cdot 0\}$ or
$\{b_g\} = \{2 \cdot 3, 3 \cdot 2, 15 \cdot 1\}$.
The last two cases can not occur, as $\rho_{U_2}(z) = 3(G_{U_2} - 1)$ for $U_2 =< g >< h^2 >$ according to Lemma 4.4. This proves the assertion. □

Now we are able to prove the crucial Lemma 4.3.

Proof of Lemma 4.3
Let $\{g_1, ..., g_{10}\}$ be a complete system of coset representatives of T in G_U. We write

$$\rho_U(D) = \sum_{i=1}^{10} A_i g_i,$$

where $A_1, ..., A_{10}$ are elements of $\mathbf{Z}T$ (which we consider to be imbedded in $\mathbf{Z}G_U$) with nonnegative coefficients. We fix an i and write

$$A_i = a_1 + a_2 g_U + a_3 h_U^2 + a_4 g_U h_U^2,$$

where $a_1, ..., a_4$ are nonnegative integers. Lemma 4.6 gives us

$$a_1 + a_2, a_3 + a_4 \in \{0, 2, 4\}. \tag{6}$$

According to Lemma 4.5 there are three possible cases.

Case (i): $\rho_{U_3}(g_i) = 1$ or g_{U_3}. Then $A_i = 0$.
Case (ii): $\rho_{U_3}(g_i) = a$ or ag_{U_3}. By replacing g_i by $g_i g_{U_3}$ (if necessary) we can assume $\rho_{U_3}(g_i) = a$. Then $a_1 + a_3 = 6$ and $a_2 = a_4 = 0$. Hence $\{a_1, a_3\} = \{2, 4\}$ by (6). By replacing g_i by $g_i h_U^2$ (if necessary) we can assume $a_1 = 4$ and $a_3 = 2$.
Case (iii): $\rho_{U_3}(g_i) \notin < g_{U_3} > \cup\, a < g_{U_3} >$. Then

$$a_1 + a_3 = a_2 + a_4 = 3. \tag{7}$$

We need another case distinction.
a) $a_j = 0$ for some $j \in \{1,2,3,4\}$. By replacing g_i by $g_i t$ with a suitable $t \in T$ (if necessary) we can assume $a_3 = 0$. Then (6) and (7) imply $a_1 = 3$, $a_2 = 1$ and $a_4 = 2$.
b) $a_j \geq 1$ for all j. From (7) we infer $\{a_1, a_3\} = \{a_2, a_4\} = \{1,2\}$. Thus (6) implies $a_1 = a_2$ and $a_3 = a_4$. By replacing g_i by $g_i t$ with a suitable $t \in T$ (if necessary) we can assume $a_1 = a_2 = 1$ and $a_2 = a_4 = 2$.

Summarizing the above results, we have $A_i = 0$ for the i with $g_i \in T$, $A_i = 4 + 2h_U^2$ for the i with $\rho_{U_3}(g_i) = a$ and

$$A_i \in \{3 + g_U + 2g_U h_U^2, (1 + 2h_U^2)(1 + g_U)\}$$

otherwise. Hence we can write

$$\rho_U(D) = (4b + 2bh_U^2) + X(3 + g_U + 2g_U h_U^2) + Y(1 + 2h_U^2)(1 + g_U),$$

where $\{1\} \cup \{b\} \cup X \cup Y$ is a complete system of coset representatives of T in G_U.
It remains to show $|X| = 2$ and $|Y| = 6$. As $|D| = 54$, we have

$$6 + 6|X| + 6|Y| = 54.$$

Comparing the coefficient of 1 in the equation

$$\rho_U(D)\rho_U(D)^{(-1)} = 36 + 72G_U$$

gives

$$(16 + 4) + (9 + 1 + 4)|X| + (1 + 4)2|Y| = 108.$$

Together with the above equation this proves the assertion. □

Lemma 4.7 *Let $U_6 =< g^2 >< gh^2 >$. Then (in either of the Cases 1 and 2)*

$$\begin{aligned} \rho_{U_6}(D) &= 4b_1 + 2b_1 g_{U_6} + X_1(5 + g_{U_6}) + 3Y_1(1 + g_{U_6}) \\ &= (2b_1 + 4X_1) + (2b_1 + X_1 + 3Y_1)(1 + g_{U_6}), \end{aligned}$$

where $b_1 \in G_{U_6}$ and $X_1, Y_1 \subset G_{U_6}$, such that $\{1\} \cup \{b_1\} \cup X_1 \cup Y_1$ is a complete system of coset representatives of $< g_{U_6} >$ in G_{U_6}.
Furthermore, $|X_1| = 2$ and $|Y_1| = 6$.

Proof
The assertion follows directly from Lemma 4.3 via projection. □

Proof of Theorem 4.2
We will conclude the proof by showing that the $\rho_{U_6}(D)$ described in Lemma 4.7 can not satisfy the equation

$$\rho_{U_6}(D)\rho_{U_6}(D)^{(-1)} = 36 + 144G_{U_6}, \tag{8}$$

which is necessary for D to be a $(160, 54, 18)$-difference set in G.
We write $X_1 = \{c, d\}$. From Lemma 4.7 and (8) we infer

$$(2b_1 + 4c + 4d)(2b_1^{-1} + 4c^{-1} + 4d^{-1}) \equiv 36 \bmod (1 + g_{U_6})$$

(this has to be interpreted as a congruence in $\mathbf{Z}G_{U_6}$). It follows that

$$(b_1c^{-1} + b_1^{-1}c) + (b_1d^{-1} + b_1^{-1}d) + 2(cd^{-1} + c^{-1}d) \equiv 0 \bmod (1 + g_{U_6}).$$

Let $e = b_1^{-1}c$ and $f = b_1^{-1}d$. Then

$$(e + e^{-1}) + (f + f^{-1}) + 2(ef^{-1} + e^{-1}f) \equiv 0 \bmod (1 + g_{U_6}). \tag{9}$$

Since no two elements of $\{b_1, c, d\}$ are in the same coset of $< g_{U_6} >$, the same is true for $\{1, e, f\}$. As $G_{U_6} =< h_{U_6} >< k_{U_6} >$ with $o(h_{U_6}) = 4$, $o(k_{U_6}) = 5$ and $h_{U_6}^2 = g_{U_6}$, we have $\{e, f\} \not\subset < h_{U_6} >$. Therefore, we can assume $5|o(e)$.
Since e appears on the left hand side of (9), eg_{U_6} must also appear on the left hand side of (9). But this is not possible:

1) $eg_{U_6} = e^{-1}$ would imply $e^2 = g_{U_6}$, contradicting $5|o(e)$.
2) $eg_{U_6} = f$ is not possible because e and f are in distinct cosets of $< g_{U_6} >$.
3) Assume $eg_{U_6} = f^{-1}$. Then (9) becomes

$$(e + e^{-1}) + (e^{-1}g_{U_6} + eg_{U_6}) + 2(e^2g_{U_6} + e^{-2}g_{U_6}) \equiv 0 \bmod (1 + g_{U_6}).$$

Hence $e^2 + e^{-2} \equiv 0 \bmod (1 + g_{U_6})$, which implies $e^4 = g_{U_6}$, contradicting $5|o(e)$.
4) $eg_{U_6} = ef^{-1}$ is not possible since $f \notin < g_{U_6} >$.
5) Assume $eg_{U_6} = e^{-1}f$, i.e. $f = e^2g_{U_6}$. Then (9) becomes

$$(e + e^{-1}) + (e^2g_{U_6} + e^{-2}g_{U_6}) + 2(e^{-1}g_{U_6} + eg_{U_6}) \equiv 0 \bmod (1 + g_{U_6}).$$

Hence $e^2 + e^{-2} + e^{-1} + e \equiv 0 \bmod (1 + g_{U_6})$. Thus $eg_{U_6} \in \{e^2, e^{-2}, e^{-1}\}$, contradicting $5|o(e)$ and concluding the proof. □

5 Nonexistence of a (189,48,12)-difference set

Using arguments similar to those in Section 4, we give a new proof for the nonexistence of a (189,48,12)-difference set in $\mathbf{Z}_3 \times \mathbf{Z}_9 \times \mathbf{Z}_7$. This was an open entry in Lander's table [Lander (1983)] for a long time. The only proof available up to now [Arasu, McDonough, Seghal (1993)] is much more involved and uses complicated calculations in cyclotomic fields.
Concerning other abelian $(189, 48, 12)$-difference sets, it is known that the underlying group cannot be cyclic [see Lander (1983)]. Up to our knowledge, it is still unknown if such a difference set exists in $(\mathbf{Z}_3)^3 \times \mathbf{Z}_7$.

Theorem 5.1 *There is no* $(189, 48, 12)$*-difference set in* $\mathbf{Z}_3 \times \mathbf{Z}_9 \times \mathbf{Z}_7$.

Proof
Assume that there exists such a difference set D. Let U be a subgroup of G of order 3, such that G_U is cyclic. From Lemmas 2.1, 2.3 and 2.5 we get

$$\rho_U(D) = 3X + PY, \tag{10}$$

where $X, Y \in \mathbf{Z}G_U$ (with nonegative coefficients), and P is the subgroup of order 3 of G_U. Let W be the subgroup of order 9 of G containing U. By (10) we can write $\rho_W(D) = 3u$, where $u \in \mathbf{Z}G_W$ has nonnegative coefficients. Lemma 2.1 gives $uu^{(-1)} = 4+12G_W$; the argument described in Example 2.7 shows that u has coefficients 0 and 1 only. Hence no two elements of $X \cup Y$ are in the same coset of P. Comparing the coefficient of 1 in the equation

$$\rho_U(D)\rho_U(D)^{(-1)} = 36 + 36G_U \tag{11}$$

yields $9|X| + 3|Y| = 72$. Together with $3(|X| + |Y|) = k = 48$ this implies $|X| = 4$ and $|Y| = 12$. By (10) and (11) we can write

$$XX^{(-1)} = 4 + PZ \tag{12}$$

for some $Z \in \mathbf{Z}G_U$. W.l.o.g. we can assume $Z = \sum_{i=1}^{21} a_i g_i$, where $a_i \in \mathbf{Z}$ and $\{g_1, ..., g_{21}\}$ is a complete system of coset representatives of P in G_U. Since X has nonnegative coefficients only, the a_i's also must be nonnegative.
W.l.o.g. we can assume $1 \in X$; as no two elements of X are in the same coset of P, we can also assume $X = g_1 + g_2 + g_3 + g_4$, $g_1 = 1$, and we have $a_1 = 0$.

From (12) it follows that $a_2, a_3, a_4 > 0$, since the coefficients of g_2, g_3, g_4 in $XX^{(-1)}$ are positive. Thus we can write

$$XX^{(-1)} = 4 + P(A-1) + Ph \tag{13}$$

for some $h \in G_U \setminus P$. However, $(XX^{(-1)})^{(-1)} = XX^{(-1)}$ implies

$$PA^{(-1)} + Ph^{-1} = PA + Ph. \tag{14}$$

Hence there must be $i, j \in \{2, 3, 4\}$ with $Pg_i = Pg_j^{-1}$. We observe that $i = j$ is impossible, as $g_i \notin P$ and G_U has odd order. Hence we can assume $Pg_2 = Pg_3^{-1}$. For the same reason as above, $Ph = Ph^{-1}$ is impossible. Hence $Ph^{-1} \subset PA$ by (14), which implies $Ph^{-1} = Pg_4$. Now (13) becomes

$$XX^{(-1)} = 4 + P(g_2 + g_2^{-1} + g_4 + g_4^{-1}). \tag{15}$$

Recall that W is the subgroup of order 9 of G containing U, and let $a := \rho_W(g_2)$ and $b := \rho_W(g_4)$. Then (15) implies

$$(a + a^{-1})(b + b^{-1}) + (a^2 + a^{-2}) = (a + a^{-1}) + 2(b + b^{-1}). \tag{16}$$

Since the coefficient of b in $(a + a^{-1})(b + b^{-1})$ is at most 1, we must have $b \in \{a^2, a^{-2}\}$, say $b = a^2$. Then (16) becomes $a^3 + a^{-3} = a^2 + a^{-2}$, which is impossible, because the order of a can only be $3, 7$ or 21. □

Acknowledgement
We want to thank the referees for some useful suggestions concerning the exposition.

6 References

K.T.Arasu, T.P McDonough, S.K. Seghal (1993): Sums of Roots of Unity. In: Group Theory (eds. S.K. Seghal, R.L. Solomon). World Scientific, Singapore, 6-20.

C.W. Curtis, I. Reiner (1962): Representation Theory of Finite Groups and Associative Algebras, Wiley, New York, London.

D. Jungnickel (1992): Difference Sets. Contemporary Design Theory. A collection of surveys (eds.J.H Dinitz, D.R. Stinson). Wiley, New York, 241-324.

D. Jungnickel, A. Pott (1995): A new class of symmetric (v, k, λ)-designs. Designs, Codes and Cryptography, 4, 319-325 (1994).

L.E. Kopilovich (1989): Difference sets in noncyclic abelian groups. Kibernetika, no. 2, 20-23.

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

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

S.L. Ma, B. Schmidt (1995): On (p^a, p, p^a, p^{a-1})-Relative Difference Sets. Designs, Codes and Cryptography, 6, 57-71

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

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

J. Singer (1939): A theorem in finite projective geometry and some applications to number theory. Trans. Amer. Math. Soc. 43 (1938): 377-385.

E. Spence (1993): A new family of symmetric 2-(v, k, λ)-designs. Europ. J. Comb. 14, 131-136.

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

W.D. Wallis (1971): Construction of strongly regular graphs using affine designs. Bull. Austr. Math, Soc. 4, 41-49 (II.8,Th.2).