Nonexistence of a $(783, 69, 6)$-difference set

Bernhard Schmidt
Mathematisches Institut
Universität Augsburg
Universitätsstraße 15
86135 Augsburg
Germany

April 27, 2001

Abstract

It is shown that no $(783, 69, 6)$-difference set exists in $\mathbf{Z}_3^3 \times \mathbf{Z}_{29}$. This excludes one of the last four open cases of abelian (v, k, λ)-difference sets with $k \le 100$.

1 Introduction

A (v, k, λ)-difference set in a group G of order v is a k-subset D of G, such that every nonidentity element g of G has exactly λ representations $g = d_1 d_2^{-1}$ with $d_1, d_2 \in D$. We say that D is abelian if G has this property.
The existence theory of abelian difference sets is highly developed, in particular, there are only four open cases of abelian (v, k, λ)-difference sets with $k \le 100$, see Jungnickel, Pott (1996) and Jungnickel, Schmidt (preprint). These cases are (the entries in the following table are (v, k, λ), group).

$$\begin{aligned}
(783, 69, 6), &\quad \mathbf{Z}_3^3 \times \mathbf{Z}_{29};\\
(640, 72, 8), &\quad \mathbf{Z}_2 \times \mathbf{Z}_4^3 \times \mathbf{Z}_5;\\
(640, 72, 8), &\quad \mathbf{Z}_2^3 \times \mathbf{Z}_4^2 \times \mathbf{Z}_5;\\
(320, 88, 24), &\quad \mathbf{Z}_4^3 \times \mathbf{Z}_5.
\end{aligned}$$

In this note, we will show that in the first case no difference set can exist. Throughout, we use the following notation. 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 $B^{(t)} := \sum_{g\in G} b_g g^t$ for $t\in\mathbf{Z}$. By ξ_m we denote a primitive complex mth root of unity. The following is a standard result on character sums of difference sets, see Turyn (1965).

Lemma 1.1 *Let D be a (v,k,λ)-difference set in an abelian group G, and let U be a subgroup of G. Let $\rho: G\to G/U$ denote the canonical epimorphism. Then*

$$\rho(D)\rho(D)^{(-1)} = n + |U|\lambda G/U,$$

and hence

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

for every nontrivial character χ of G/U.

2 The Result

Theorem 2.1 *There is no $(783,69,6)$-difference set in $G=\mathbf{Z}_3^3\times\mathbf{Z}_{29}$.*

Proof
Assume the existence of a $(783,69,6)$-difference set D in G. We will write G multiplicatively. By the multiplier theorem (see Jungnickel (1992), Theorem 2.1) and the result of McFarland and Mann (1965), we can assume $D^{(7)} = \{d^7 : d\in D\} = D$. Let U be the subgroup of G isomorphic to $\mathbf{Z}_3^3$. By Lemma 1.1, we have $\chi(\rho(D))\overline{\chi(\rho(D))} = 63$ for every nontrivial character χ of G/U, where $\rho: G\to G/U$ is the canonical epimorphism. Since $3^{14}\equiv -1 \bmod 29$, we have $\chi(\rho(D))\equiv 0 \bmod 3$ for every character χ of G/U, see Turyn (1965). Since $(|G/U|,3)=1$, we conclude $\rho(D)=3u$ for some $u\in\mathbf{Z}[G/U]$. Write $u=\sum_{g\in G/U} u_g g$ with $u_g\in\mathbf{Z}$. Then $\sum_{g\in G/U} u_g = 23$ and, since $uu^{(-1)} = 7+18G/U$ by Lemma 1.1, $\sum_{g\in G/U} u_g^2 = 25$. Hence, as a multiset,

$$\{u_g : g\in G/U\} = \{1\cdot 2, 21\cdot 1, 7\cdot 0\},$$

where $x\cdot y$ denotes x copies of y. Hence we have

$$D=\sum_{i=1}^{22} X_i h_i,$$

where $h_1, ..., h_{22}$ are distinct elements of the subgroup H of G of order 29 and $X_i \in \mathbf{Z}U$ with $|X_1| = 6$ and $|X_i| = 3$ for $i > 1$. The automorphism group of H generated by $h \to h^7$ has exactly four orbits O_1, O_2, O_3, O_4 of length 7 and one orbit $O_0 = \{1\}$ of length 1 on H. Since $D^{(7)} = D$, it follows that (w.l.o.g.)

$$D = X_1 + \sum_{i=2}^{4} X_i O_i.$$

We claim that each X_i, $i = 2, 3, 4$, is a coset of a subgroup of order 3 of U. Assume the contrary, say $X_2 = a + ab + ac$, where $b \neq 1$ and $c \notin \langle b \rangle$. Let τ be a character of U, which is trivial on $\langle b \rangle$, but not on $\langle c \rangle$. Then $\tau(X_2) = \tau(a)(2 + \tau(c)) \not\equiv 0 \bmod 3$. Let ψ be a charcacter of G of order 29. Then $\tau \otimes \psi(D) = \tau(X_1) + \sum_{i=2}^{4} \tau(X_i)\psi(O_i)$ is not divisible by 3, since $\tau(X_2) \not\equiv 0 \bmod 3$ and $\{1\} \cup \psi(O_2) \cup \psi(O_3) \cup \psi(O_4)$ is linearly independent over $\mathbf{Q}(\xi_3)$. But this contradicts the fact that $\chi(D) \equiv 0 \bmod 3$ for all nontrivial characters of χ of G, which follows from $3^{14} \equiv -1 \bmod 29$, see Turyn (1965). Hence the X_i, $i = 2, 3, 4$, are indeed cosets of subgroups of U of order 3. Thus it is easy to see that we always can find a character χ' of G with $\chi'(X_i) = 0$ for $i = 2, 3, 4$. But this implies $|\chi'(D)| = |\chi'(X_1)| \leq 6$ contradicting $|\chi'(D)| = 3\sqrt{7}$. $\square$

3 References

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

D. Jungnickel, A. Pott: Difference sets: abelian. In: The CRC handbook of combinatorial designs. Eds. C.J. Colbourn, J. Dinitz. CRC Press, Boca Raton (1996), 297-307.

D. Jungnickel, B. Schmidt: Difference Sets: An Update. Preprint.

R.L. McFarland, H.B. Mann: On multipliers of difference sets. Canad. J. Math. 17 (1965), 542-542.

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