Nonexistence of Some (945, 177, 33)-difference Sets *

Tao Feng
School of Mathematical Sciences, Peking University, Beijing 100871,China

Abstract

In this note, we show that there is no (945, 177, 33)-difference set in any group G of order 945 with a normal subgroup K such that $G/K \cong C_{27} \times C_5$, and hence no cyclic difference set with such parameters exists. This fills one entry of Baumert and Gordon's table with 'No'.

keywords: difference set, cyclic difference set, inversion formula

1 Introduction

Let G be a multiplicative group of order v. A (v, k, λ)-difference set D in G is a subset of cardinality k such that every non-identity element of G can be written exactly λ ways as $d_1 d_2^{-1}$, where $d_1, d_2 \in D$. In the group ring language, we have $DD^{(-1)} = n + \lambda G$, where $n = k - \lambda$, $D = \sum_{d \in D} d \in \mathbb{Z}[G]$, $D^{(-1)} = \sum_{d \in D} d^{-1} \in \mathbb{Z}[G]$. We say that D is abelian, nonabelian or cyclic if G has the corresponding property. We refer the reader to [2] for details.

For a finite abelian group G, we denote by $\hat{G}$ the character group of G. We also denote by $\exp(G)$ the least common multiple of the orders of elements in G. For $\chi \in \hat{G}$ and $\sigma \in \mathrm{Gal}(\mathbb{Q}(\xi_{exp(G)})/\mathbb{Q})$, we have $\chi^\sigma \in \hat{G}$ where $\chi^\sigma(g) = \sigma(\chi(g))$ for each $g \in G$. It is well known that character theory is a sufficient tool for the study of abelian difference sets. The inversion formula is a standard result concerning abelian characters and is stated below:

Inversion formula. Let G be an abelian group of order v. If $A = \sum_{g \in G} a_g g \in \mathbb{Z}[G]$, then $a_g = \frac{1}{v} \sum_\chi \chi(Ag^{-1})$, $g \in G$, where the summation is taken over all characters of G.

Our main result is the following theorem.

*Supported by National Natural Science Foundation of China(10331030).

Theorem 1. *There is no* $(945, 177, 33)$*-difference set in any group* G *of order* 945 *with a normal subgroup* K *such that* $G/K \cong C_{27} \times C_5$.

As a corollary, we have

Corollary 2. *There is no cyclic* $(945, 177, 33)$*-difference set.*

In the second section, we will give the preliminaries needed for our proof. We give the proof of our main result in the last section.

2 Preliminaries

For a positive integer m, ξ_m is a primitive m-th root of unity in the complex number field, and $\mathbb{Z}_m^*$ is the unit group in $\mathbb{Z}_m$. The algebraic integer ring of the cyclotomic field $\mathbb{Q}(\xi_m)$ is $\mathbb{Z}[\xi_m]$, see [6]. We say $X \in \mathbb{Q}(\xi_m)$ essentially lies in $\mathbb{Q}(\xi_t)$ for some $t|m$ if $X\xi_m^j \in \mathbb{Q}(\xi_t)$ for some j. We have the following deep result due to Schmidt.

Result 3. *[5, Theorem 2.2.8] Assume* $X\bar{X} = n$ *for* $X \in \mathbb{Z}[\xi_m]$, *where* n *and* m *are positive integers. Then* $X\xi_m^j \in \mathbb{Z}[\xi_{F(m,n)}]$ *for some* j, *where* $F(m,n)$ *is a positive integer determined by* m, n.

Usually, $F(m,n)$ is much smaller than n, so X essentially lies in a smaller cyclotomic field. We do not include a definition for $F(m,n)$ here, since we do not have to invoke this deep result in our special case. The interested reader can find it in [5, Definition 2.2.5].

We define the function $\delta^{(m)} : \mathbb{Z} \mapsto \{0,1\}$, $\delta^{(m)}(t) = 1$ if $t \equiv 0 \mod m$, and $\delta^{(m)}(t) = 0$ otherwise. We need the following result from [3].

Result 4. *[3, Lemma 2.1] Let* $w_1, w_2 \in \mathbb{Z}[\xi_m]$ *such that* $w_1 \in w_2\mathbb{Z}[\xi_m]$ *and* $|w_1| = |w_2|$, *then* $w_1 = \pm w_2 \xi_m^c$ *for some integer* c.

Proposition 5. *For a positive integer* r *and a prime* p, *define* $C_{p^r}(u) = \sum_{i\in \mathbb{Z}_{p^r}^*} \xi_{p^r}^{ui}$, *then* $C_{p^r}(u) = \begin{cases} p^{r-1}(p\delta^{(p)}(u') - 1) & \text{if } u = p^{r-1}u', u' \in \mathbb{Z}_p, \\ 0 & \text{otherwise.} \end{cases}$.

Proof. We have that $\prod_{i\in\mathbb{Z}_{p^r}^*}(x - \xi_{p^r}^i) = \frac{x^{p^r}-1}{x^{p^{r-1}}-1}$. By counting the coefficient of $x^{p^{r-1}(p-1)-1}$ on both sides, we have $C_{p^r}(1) = 0$ if $r > 1$ and $C_p(1) = -1$. Now the result follows from an inductive process and the fact that $\mathbb{Z}_{p^r}^*$ is a multiplicative group. □

Lemma 6. *Suppose* $G = \langle\alpha\rangle \times \langle\beta\rangle$, $o(\alpha) = p^a$, $o(\beta) = q$, *and* p, q *are distinct primes,* $p \geq a \geq 3$. $D \in \mathbb{Z}[G]$ *and for any character* $\tau \in \hat{G}$, $\tau(D)$ *essentially lies in* $\mathbb{Q}(\xi_{pq})$. *Further suppose* $q \nmid |\tau(D)|^2$ *for* $\tau \in \hat{G}$ *and* $o(\tau) = p^i, i \geq 2$. *If we write* $D = \sum_{i=0}^{p-1} D_i\alpha^i$ *with* $D_i \in \mathbb{Z}[\langle\alpha^p\rangle \times \langle\beta\rangle]$, *then we have* $D_t = \langle\alpha^p\rangle \times L_0$ *with* $L_0 \in \mathbb{Z}[\langle\beta\rangle]$ *for some* t.

Proof. We denote by $\chi_{u,j}$ the character of G which maps α, β to $\xi_{p^a}^u$ and ξ_q^j respectively. Fix some i, $0 \le i \le a-2$. Since $\chi_{p^i,j}(D_k) \in \mathbb{Z}[\xi_{p^{a-i-1}q}]$, and $1, \xi_{p^{a-i}}, \cdots, \xi_{p^{a-i}}^{p-1}$ are linear independent over $\mathbb{Z}[\xi_{p^{a-i-1}q}]$, which is clear from the fact that $[\mathbb{Q}(\xi_{p^{a-i}q}) : \mathbb{Q}(\xi_{p^{a-i-1}q})] = p$, we must have some $t(i,j) \in \{0, 1, \cdots, p-1\}$ such that $\chi_{p^i,j}(D) = \chi_{p^i,j}(D_{t(i,j)})\xi_{p^{a-i}}^{t(i,j)}$, and $\chi_{p^i,j}(D_k) = 0$ when $k \ne t(i,j)$.

We have $t(i,j) = t(i,1)$ for $j \in \mathbb{Z}_q^*$, since $\chi_{p^i,j} = \chi_{p^i,1}^{\sigma}$ for some $\sigma \in \mathrm{Gal}(\mathbb{Q}(\xi_{p^{a-i}q})/\mathbb{Q}(\xi_{p^{a-i}}))$. We show that $t(i,1) = t(i,0)$. Since $(1-\xi_q) | (\chi_{p^i,1}(D_j) - \chi_{p^i,0}(D_j))$ in $\mathbb{Z}[\xi_{p^{a-i}q}]$, we have $(1-\xi_q)|\chi_{p^i,0}(D_j)$ for $j \ne t(i,1)$. It follows that $q|\chi_{p^i,0}(D_j)$ in $\mathbb{Z}[\xi_{p^{a-i}}]$ for $j \ne t(i,1)$. Because $q \nmid |\chi_{p^i,0}(D)|^2$, we must have $\chi_{p^i,0}(D_j) = 0$ for $j \ne t(i,1)$, and hence $t(i,1) = t(i,0)$. Write $t(i) := t(i,0)$.

Because $p \ge a$, we have at least one t between 0 and $p-1$ that is distinct from any $t(i), 0 \le i \le a-2$. Then for any character $\tau \in \hat{G}$, $p^2|o(\tau)$, we have $\tau(D_t) = 0$. It follows that $D_t = \langle\alpha^p\rangle \times L_0$ with $L_0 \in \mathbb{Z}[\langle\beta\rangle]$ by an application of the inversion formula, or use [4, Cor 1.2.5, p.18]. □

Remark: If $D = \sum_{u,v} d_{u,v}\alpha^u\beta^v$, then $D_t = \sum_{u',v} d_{t+pu',v}\alpha^{pu'}\beta^v$. Under the assumption of the above lemma, in order to get the coefficient of D_t using $\chi(D)$, $\chi \in \hat{G}$, we need only to consider the characters of G whose orders divide pq. For example, for a fixed i, $0 \le i \le a-2$, if we have $\chi_{p^i,1}(D) = \xi_{p^{a-i}}^{t(i)} \sum_l a_l \xi_{pq}^l$ and $\chi_{p^i,0}(D) = \xi_{p^{a-i}}^{t(i)} \sum_{l'} b_{l'} \xi_{pq}^{l'}$, $a_l, b_{l'} \in \mathbb{Z}$, then

$$\sum_{m\in\mathbb{Z}_{p^{a-i}}^*} \sum_{n\in\mathbb{Z}_q^*} \chi_{mp^i,n}(D\alpha^{-t-pu'}\beta^{-v}) = \sum_l C_{p^{a-i}}(-t-pu'+t(i)+slp^{a-i-1})H_l(v),$$

$$\sum_{m\in\mathbb{Z}_{p^{a-i}}^*} \chi_{mp^i,0}(D\alpha^{-t-pu'}\beta^{-v}) = \sum_{l'} C_{p^{a-i}}(-t-pu'+t(i)+sl'p^{a-i-1})F_{l'}(v),$$

with $H_l, F_{l'}$ being integer-valued functions of v, and $rp + sq = 1$. Both terms are equal to 0 according to Proposition 5. So we have

$$d_{t+pu',v} = \frac{1}{p^a q} \sum_{\chi\in\hat{G}, o(\chi)|pq} \chi(D\alpha^{-t}\beta^{-v}).$$

From now on, we suppose G is a group of order 945 with a normal subgroup K such that $H := G/K = \langle\alpha\rangle\times\langle\beta\rangle$, $o(\alpha) = 27$, $o(\beta) = 5$, and D is a putative (945, 177, 33)-difference set in G. Let $\rho : G \mapsto H$ be the canonical epimorphism, and write $S := \rho(D) = \sum_{i=0}^{26}\sum_{j=0}^{4} S_{i,j}\alpha^i\beta^j \in \mathbb{Z}[H]$. Here $S_{i,j}$'s are nonnegative integers not exceeding 7.

We denote the character of H which maps α to ξ_{27}^i and β to ξ_5^j by $\chi_{i,j}$, $0 \le i \le 26$, $0 \le j \le 4$. Then $\chi_{li,mj} = \chi_{i,j}^{\sigma_{l,m}}$, where $\sigma_{l,m} \in \mathrm{Gal}(\mathbb{Q}(\xi_{135})/\mathbb{Q})$ such that $\sigma_{l,m}(\xi_{27}) = \xi_{27}^l$, $\sigma_{l,m}(\xi_5) = \xi_5^m$, $l \in \mathbb{Z}_{27}^*, m \in \mathbb{Z}_5^*$.

In the ring $\mathbb{Z}[\xi_m]$, $m = 3, 9, 27$ or 5, the principle ideal (2) is prime. In the ring $\mathbb{Z}[\xi_m]$, $m = 15, 45$ or 135, $(2) = (\xi_{15}^4 - \xi_{15}^3 - 1)\overline{(\xi_{15}^4 - \xi_{15}^3 - 1)}$, where the principle ideal $(\xi_{15}^4 - \xi_{15}^3 - 1)$ is prime in the corresponding ring. In the ring $\mathbb{Z}[\xi_{3^r5^s}]$ ($r \geq 0$, $s = 0$ or 1), the principle ideal (3) decomposes as $(3) = P^{\varphi(3^r)}$, where P is a prime ideal fixed by complex conjugation and φ is the Euler's function. We fix the following notations:

$\Delta_0 = 4$; $\Delta_1 = \xi_{15}^7 - \xi_{15}^6 + \xi_{15}^5 + \xi_{15}^4 - \xi_{15}^3 - \xi_{15}$;

$\Delta_2 = \xi_{15}^{11} + 4\xi_{15}^9 - \xi_{15}^8 - \xi_{15}^7 + \xi_{15}^6 - \xi_{15}^5$;

Then $\Delta_1 = -(\xi_{15}^4 - \xi_{15}^3 - 1)^2$, $|\Delta_1| = 2$, and $\Delta_2 = -\Delta_1^2 \cdot \xi_5$, $|\Delta_2| = 4$.

3 Proof of the main result

In this section, we give the proof of Theorem 1. For any non-principle character χ of H, we have $\chi(S)\overline{\chi(S)} = 144$. From the discussions in the last section, we know that $\chi(S)$ essentially lies in $\mathbb{Q}(\xi_{15})$. We note that this fact also follows easily from Result 3. It follows from Lemma 6 and the remark after it that we can find t such that $S_{t+3u',v} = \frac{1}{135}(A_{t+3u',v} + B_{t+3u',v})$, where $A_{u,v} = \sum_{i=0}^{4} \chi_{0,i}(S\alpha^{-u}\beta^{-v})$, $B_{u,v} = \sum_{i=1}^{2}\sum_{j=0}^{4} \chi_{9i,j}(S\alpha^{-u}\beta^{-v})$.

Now we compute these functions separately.

(1) If $\chi = \chi_{0,1}$, we have $\chi_{0,1}(S) \in 12\mathbb{Z}[\xi_5]$, and it follows from Result 4 that $\chi_{0,1}(S) = 12\epsilon_0\xi_5^c$, $\epsilon_0 = \pm 1$. By replacing S with $S\beta^{-c}$, we can assume that $\chi_{0,1}(S) = 12\epsilon_0$. Then we have: $A_{t+3u',v} = 177 + 12\epsilon_0(5\delta^{(5)}(v) - 1)$.

(2) If $\chi = \chi_{9,0}$, we have $\chi_{9,0}(S) \in 12\mathbb{Z}[\xi_3]$, and hence $\chi_{9,0}(S) = 12\epsilon_1\xi_3^c$, $\epsilon_1 = \pm 1$. By replacing S with $S^{(-1)}$ (and replacing t with $-t$ correspondingly) if necessary, we have three possibilities: $\chi_{9,1}(S) \in 3r_i\Delta_i\mathbb{Z}[\xi_{15}]$ with $0 \leq i \leq 2$ and $r_0 = 1$, $r_1 = 2$, $r_2 = -1$. In each case, we have $\chi_{9,1}(S) = 3\epsilon_{11}r_i\Delta_i\xi_3^{i_1}\xi_5^{m_1}$, $\epsilon_{11} = \pm 1$. Since $1 - \xi_5 | \chi_{9,1}(S) - \chi_{9,0}(S)$ in $\mathbb{Z}[\xi_{15}]$, we must have $\epsilon_{11} = \epsilon_1$, and $i_1 \equiv c \mod 3$. Write $\chi_{9,1}(S) = 3\epsilon_1 r(\sum_l \gamma_l\xi_{15}^l)\xi_3^c\xi_5^{m_1}$, with $r = r_i$, $\Delta_i = \sum_l \gamma_l\xi_{15}^l$, and we have:

$B_{t+3u',v} = 12\epsilon_1 C_3(-t+c) + 3\epsilon_1 r\sum_l \gamma_l C_3(-t-l+c)(5\delta^{(5)}(2l+m_1-v)-1)$.

Proof of Theorem 1. We show that there is always some v such that $S_{t,v}$ is not an integer, contradicting that $S_{t,v}$'s are nonnegative integers, and Theorem 1 follows. Write $L_v = A_{t,v} + B_{t,v}$. There are three cases.

Case 1. $\chi_{9,1}(S) = 12\epsilon_1\xi_3^c\xi_5^{m_1}$. In this case, $L_v = 60\epsilon_1(3\delta^{(3)}(c-t) - 1)\delta^{(5)}(m_1 - v) + 12\epsilon_0(5\delta^{(5)}(v) - 1) + 177$. Let v be an element such that $v \neq 0, m_1 \mod 5$, then $L_v = 177 - 12\epsilon_0$ which is never divisible by 135.

Case 2. $\chi_{9,1}(S) = 6\epsilon_1\Delta_1\xi_3^c\xi_5^{m_1}$. Write $\Delta_1 = \sum_l \gamma_l\xi_{15}^l$, with (l, γ_l) being the pairs

$$(7,1), (6,-1), (5,1), (4,1), (3,-1), (1,-1).$$

We have $\sum_l \gamma_l C_3(-t-l+c) = 3 - 9\delta^{(3)}(c-t)$ by a simple calculation. Let $v = 0$, then $L_0 = 177 + 48\epsilon_0 + 6\epsilon_1(-5 + 15\delta^{(3)}(c-t) + 5x)$, where $x = \sum_l \gamma_l(3\delta^{(3)}(-t-l+c) - 1)\delta^{(5)}(2l + m_1)$. When $t - c \equiv 0 \mod 3$, $L_0 = 177 + 48\epsilon_0 + 6\epsilon_1(10 + 5x)$, and x takes on two values: -1, -2. When $t - c \not\equiv 0 \mod 3$, $L_0 = 177 + 48\epsilon_0 + 6\epsilon_1(-5 + 5x)$, and x takes on three values: ±1, -2. In neither case L_0 is divisible by 135.

Case 3. $\chi_{9,1}(S) = -3\epsilon_1\Delta_2\xi_3^c\xi_5^{m_1}$. Write $\Delta_2 = \sum_l \gamma_l \xi_{15}^l$, with (l, γ_l) being the pairs

$$(11,1),(9,4),(8,-1),(7,-1),(6,1),(5,-1).$$

We have $\sum_l \gamma_l C_3(-t-l+c) = -6 + 18\delta^{(3)}(c-t)$. Take any v such that $v \not\equiv 0, m_1 + 3 \mod 5$, then $L_v = 177 - 12\epsilon_0 + 3\epsilon_1(-10 + 30\delta^{(3)}(c-t) - 5y)$, where $y = \sum_l \gamma_l(3\delta^{(3)}(-t-l+c) - 1)\delta^{(5)}(2l + m_1 - v)$. When $t - c \equiv 0 \mod 3$, $L_v = 177 - 12\epsilon_0 + 3\epsilon_1(20 - 5y)$, and y takes on two values: 1, 8. When $t - c \not\equiv 0 \mod 3$, $L_v = 177 - 12\epsilon_0 + 3\epsilon_1(-10 - 5y)$, and y takes on two values: 1, -2. In neither cases L_v is divisible by 135.

Acknowledgement. The author would like to thank his supervisor Professor Qiu Weisheng for his continuous support and encouragement. He also thanks the referee for pointing out the reference [5].

References

[1] L.D.Baumert, D.M.Gordon, On the existence of cyclic difference sets with small parameters, available at http://www.ccrwest.org/diffsets.html.

[2] T. Beth, D. Jungnickel, H. Lenz, Design Theory, Cambridge, 1986.

[3] S.L.Ma, Planar functions, relative difference sets and character theory, J. Algebra 185 (1996), 342-356.

[4] A.Pott, Finite geometry and character theory, LNM 1601, Berlin, Springer-Verlag, 1995.

[5] B. Schmidt, Characters and cyclotomic fields in finite geometry, LNM 1797, Springer-Verlag, 2002.

[6] L.C.Washington, Introduction to cyclotomic fields, GTM 83, New York, Springer-Verlag, 1982.