Journal of Algebraic Combinatorics **7** (1998), 77–89

Difference Sets with $n = 2p^m$

MIKHAIL MUZYCHUK* muzychuk@macs.cs.biu.ac.il
Department of Mathematics and Computer Science, Bar-Ilan University, 52900, Ramat-Gan, Israel

Received October 28, 1994; Revised September 26, 1996

Abstract. Let D be a (v, k, λ) difference set over an abelian group G with even $n = k - \lambda$. Assume that $t \in \mathbf{N}$ satisfies the congruences $t \equiv q_i^{f_i} \pmod{\exp(G)}$ for each prime divisor q_i of $n/2$ and some integer f_i. In [4] it was shown that t is a multiplier of D provided that $n > \lambda$, $(n/2, \lambda) = 1$ and $(n/2, v) = 1$. In this paper we show that the condition $n > \lambda$ may be removed. As a corollary we obtain that in the case of $n = 2p^a$ when p is a prime, p should be a multiplier of D. This answers an open question mentioned in [2].

Keywords: difference set, abelian group

1. Introduction

Let G be a finite abelian group with unit 1, where the group operation is written multiplicatively. We use $\exp(G)$ to denote an exponent of G and $\mathbf{Z}G$ for a group algebra of G over integers.

For an arbitrary $X = \sum_{g\in G} x_g g \in \mathbf{Z}G$ and $m \in \mathbf{Z}$, we set $X^{(m)} = \sum_{g\in G} x_g g^m$. If $(m, |G|) = 1$, then the mapping $X \to X^{(m)}$ is an automorphism of the group algebra $\mathbf{Z}G$. An integer m is called *a* (*numerical*) *multiplier* of X if $X^{(m)} = Xg$ for a suitable $g \in G$.

If T is a subset of G, then we use the same letter for the element $\sum_{t\in T} t \in \mathbf{Z}G$. In what follows we use a notation $|X|$, $X \in \mathbf{Z}G$ for a sum of all coefficients of X. The mapping $X \to |X|$ is a homomorphism of $\mathbf{Z}$-algebras. It satisfies the equality $XG = |X|G$.

A subset T of G is called *a* (v, k, λ)-*difference set* if it satisfies the equality

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

where $n = k - \lambda$, $k = |T|$, $v = |G|$.

In 1967 Mann and Zaremba proved the following (Theorem 4 in [4]).

Theorem 1.1 *Let G be an abelian group and D be a difference set over G with parameters (v, k, λ). Assume that $n = 2m$, $(m, |G|) = 1$, $(m, \lambda) = 1$, $n > \lambda$ and for some $t \in \mathbf{N}$, $t \equiv q_i^{f_i} \pmod{\exp(G)}$ for every prime divisor q_i of m and some integer f_i. Then t is a multiplier.*

In this paper we prove

Theorem 1.2 *Theorem* 1.1 *remains true if we remove the condition $n > \lambda$.*

*Supported by the Research Grant # 3889 of the Ministry of Science of Israel.

As a consequence we obtain the following

Corollary 1.1 *Let D a (v, k, λ)-difference set and $n = 2p^m$ for some odd prime p, $(p, |G|) = 1$. Then p is a multiplier of D.*

This claim answers an open question from [2].

In [5] the following situation was studied. Let D be an abelian difference set over a group G. Assume that $n = k - \lambda = 3m$ where $(m, |G|) = 1$ and there exists an integer t satisfying $t \equiv q_i^{f_i} (\mathrm{mod}\ \exp(G))$ for each prime divisor q_i of m. In the case of $(|G|, 3 \cdot 13) = 1$ Qiu Weisheng proved in [5] that t is a multiplier of D provided that one of six conditions of Theorem 5 of [5] holds. Here we strengthen his result and prove the following claim.

Theorem 1.3 *Let D be a (v, k, λ)-difference set over an abelian group G. Assume that $n = k - \lambda = 3m$ with $(m, |G|) = 1$ and t be an integer satisfying the congruence $t \equiv q_i^{f_i} (\mathrm{mod}\ \exp(G))$ for each prime divisor q_i of n and a suitable exponent f_i. If t is not a multiplier of D, then m is a square and exactly one of the following conditions is satisfied.*

(i) $11 \parallel |G|$ *and for each prime divisor p of $|G|$ $\mathrm{ord}_p(t)$ is even if $p = 11$ and odd otherwise*; *t^2 is a multiplier of D*;

(ii) $13 \parallel |G|$ *and for each prime divisor p of $|G|$ $\mathrm{ord}_p(t)$ is even if $p = 13$ and odd otherwise*; *t^4 is a multiplier of D.*

2. Basic facts

In what follows G^* will stand for a group of permutations acting on G which consists of all mappings $g \to g^m$, $(m, |G|) = 1$. It is a well-known fact that $G^* \cong \mathbf{Z}^*_{\exp(G)}$ and two numbers $m_1, m_2 \in G^*$ induce the same permutation if and only if $m_1 \equiv m_2 (\mathrm{mod}\ \exp(G))$.

For two natural numbers n, λ we denote $D(n, \lambda) = \{X \in \mathbf{Z}G \mid XX^{(-1)} = n + \lambda G\}$. Clearly, $X \in D(n, \lambda)$ implies $|X|^2 = n + \lambda|G|$.

If $X = \sum_{g \in G} x_g g \in \mathbf{Z}G$ and $Y = \sum_{g \in G} y_g g \in \mathbf{Z}G$, then we write $X \equiv Y (\mathrm{mod}\ m)$, $m \in \mathbf{Z}$ if $x_g \equiv y_g (\mathrm{mod}\ m)$ holds for all $g \in G$.

First we list a few elementary properties of elements from $D(n, \lambda)$. We omit proofs, since they are straightforward.

Proposition 2.1 *An integer t is a multiplier of $X \in D(n, \lambda)$ if and only if $X^{(t)} X^{(-1)} - \lambda G = ng$, $g \in G$.*

Proposition 2.2 *For any $X, Y \in D(n, \lambda)$, $|x|\,|y| > 0$ it holds that $XY - \lambda G \in D(n^2, 0)$.*

The set $D(n^2, 0)$ contains elements of the form $\pm ng$, $g \in G$. Following [5] we call these elements *trivial*.

Proposition 2.3 *Let $X = \sum_{g \in G} x_g g \in D(n^2, 0)$. If all x_g are non-negative, then $X = ng$, $g \in G$ (i.e., X is trivial).*

Proof: The equation $XX^{(-1)} = n^2$ implies $\sum_{g\in G} x_g^2 = n^2$ and $\sum_{g\in G} x_g = n$.

If X is non-trivial, then there are at least two $g \neq h \in G$ with non-zero x_g and x_h. Since all x_f are non-negative, $gh^{-1} \neq 1$ appears in the product $XX^{(-1)}$ with positive coefficient, a contradiction. $\square$

Proposition 2.4 *Let $X = \sum_{g\in G} x_g g \in D(n^2, 0)$. If $X \equiv 0(\mathrm{mod}\ n)$, then $X = \pm ng, g \in G$ (i.e., X is trivial).*

Proof: By assumption $X = nY, Y \in \mathbf{Z}G$, implying $YY^{(-1)} = 1$. Let $y_g, g \in G$ be the coefficients of Y. Then $\sum_{g\in G} y_g^2 = 1$. Now the claim is evident. $\square$

Next claim plays the central role in this chapter. In fact, it is the straight consequence of Lemma 7.5 from [3]. Nevertheless, we prefer to give here an independent original proof.

Lemma 2.5 *Let $X \in D(n, \lambda)$ for some $n, \lambda \in \mathbf{Z}$. Let $p \mid n$ be a prime divisor relatively prime to $|G|$. Then for any $j \in \mathbf{Z}$, $X^{(p^j)}X^{(-1)} - \lambda G \equiv 0(\mathrm{mod}\ p^a)$, where $p^a \parallel n$.*

Proof: It is sufficient to prove the claim only for non-negative j.

Define b to be the maximal natural number satisfying the property

$$\forall j \in \mathbf{Z}^+, X^{(p^j)}X^{(-1)} - \lambda G \equiv 0(\mathrm{mod}\ p^b).$$

It is clear that our claim is equivalent to the inequality $b \geq a$.[1]

By the definition of b there exists $j \in \mathbf{Z}^+$ such that

$$\begin{aligned} X^{(p^j)}X^{(-1)} - \lambda G &\equiv 0(\mathrm{mod}\ p^b), \\ X^{(p^j)}X^{(-1)} - \lambda G &\not\equiv 0(\mathrm{mod}\ p^{b+1}). \end{aligned}$$

In other words, $X^{(p^j)}X^{(-1)} - \lambda G = p^b Y$, where $Y \in \mathbf{Z}G$ satisfies $Y \not\equiv 0(\mathrm{mod}\ p)$. The direct computations give us

$$\begin{aligned} Y^{(p^j)}Y &= \frac{1}{p^{2b}}\left(X^{(p^j)}X^{(-1)} - \lambda G\right)^{(p^j)}\left(X^{(p^j)}X^{(-1)} - \lambda G\right) \\ &= \frac{1}{p^{2b}}\left(X^{(p^{2j})}X^{(-p^j)} - \lambda G\right)\left(X^{(p^j)}X^{(-1)} - \lambda G\right) \\ &= \frac{n}{p^b}\ \frac{X^{(p^{2j})}X^{(-1)} - \lambda G}{p^b}. \end{aligned}$$

By the definition of b,

$$\frac{X^{(p^{2j})}X^{(-1)} - \lambda G}{p^b} \in \mathbf{Z}G.$$

Thus we have $Y^{(p^j)}Y = \frac{n}{p^b}Z$, $Z \in \mathbf{Z}G$. If $b < a$, then $Y^{p^j+1} \equiv Y^{(p^j)}Y \equiv 0 (\mathrm{mod}\ p)$, i.e., Y is nilpotent in the group algebra $\mathbf{F}_pG$. But this algebra is semisimple, therefore $Y \equiv 0 (\mathrm{mod}\ p)$, a contradiction. □

As a corollary we obtain the following statement whose parts (i) and (ii) are equivalent to Lemma 2 of [5].

Lemma 2.6 *Let $X \in D(n, \lambda)$ and let $m \mid n$ be a divisor of n relatively prime to $|G|$. Assume also that there exists an integer t satisfying the following condition*:

For every prime p dividing m there exists an integer j such that $p^j \equiv t (\mathrm{mod}\ \exp(G))$.

Then there exists $Y_t \in \mathbf{Z}G$ such that

(i) $X^{(t)}X^{(-1)} - \lambda G = mY_t$;

(ii) $Y_tY_t^{(-1)} = (\frac{n}{m})^2$;

(iii) $XY_t = (n/m)X^{(t)}$.

Proof: (i)–(ii) Let $p \mid m$ be a prime. By assumption $X^{(t)} = X^{(p^j)}$. Now Lemma 2.5 gives us $X^{(p^j)}X^{(-1)} - \lambda G \equiv 0 (\mathrm{mod}\ p^b)$, $p^b \parallel n$. Thus $X^{(t)}X^{(-1)} - \lambda G \equiv 0 (\mathrm{mod}\ p^b)$ for every prime p dividing m. This implies $X^{(t)}X^{(-1)} - \lambda G = mY_t$ for some $Y_t \in \mathbf{Z}G$. By Proposition 2.2 we have $(mY_t)(mY_t)^{(-1)} = n^2$, whence $Y_tY_t^{(-1)} = (n/m)^2$.

To get (iii) it is sufficient to multiply both sides of the identity $X^{(t)}X^{(-1)} - \lambda G = mY_t$ by X and to collect the terms. □

Using this lemma and Proposition 2.3 one can easily prove the well-known *Second Multiplier Theorem*.

Second Multiplier Theorem *Keep the assumptions of the previous claim. If, in addition, $m > \lambda$, then t is a multiplier of X.*

Proof: Consider the equality $X^{(t)}X^{(-1)} - \lambda G = mY_t$, $Y_t \in \mathbf{Z}G$, which holds due to (i) of Lemma 2.6. We claim that $m > \lambda$ implies that all coefficients of Y_t are non-negative. Indeed, if it is not the case, then the minimal coefficient in the right side of the equality is less or equal to $-m$. On the other hand the minimal coefficient in the left part is greater or equal to $-\lambda > -m$. Contradiction.

Since coefficients of Y_t are non-negative, part (ii) of Lemma 2.6 together with Proposition 2.3 yield $Y_t = (n/m)g$, $g \in G$, whence $X^{(t)}X^{(-1)} - \lambda G = ng$. By Proposition 2.1, t is a multiplier of X. □

Lemma 2.7 *Let $X \in D(n, \lambda)$, $(n, |G|) = 1$. Assume that $X = X^{(-1)}g$, $g \in G$. Then n is a square.*

Proof: This is a direct consequence of Theorem 7.2 from [3]. □

3. Multipliers

Lemma 3.1 *Let $X \in \mathbf{Z}G$ be an element satisfying the equation $X^k = n^k h$ for some $k \in \mathbf{N}, h \in G$. Then $(n, |G|) = 1$ implies $X = \pm ng$ for some $g \in G$.*

Proof: Denote by d the greatest common divisor of the coefficients of X. We can write that $X = dY, Y \in \mathbf{Z}G$. It is clear that the greatest common divisor of the coefficients of Y is equal to one and $Y^k = m^k h, m = n/d$. Our proof will be finished if we show that $Y = \pm g, g \in G$. If $m \neq 1$, then a prime $p \mid m$ gives us the congruence $Y^k \equiv 0 (\mathrm{mod}\ p)$. But $(p, |G|) = 1$, whence $Y \equiv 0 (\mathrm{mod}\ p)$. Hence p divides the greatest common divisor of the coefficients of Y, a contradiction. Hence $m = \pm 1$ and $Y^k = \pm h$. This implies that $Y \in \mathbf{Z}G$ is a unit of $\mathbf{Z}G$. Hence, (see Corollary 37.6 [1]) $Y = \pm g, g \in G$. □

Corollary 3.2 *Let $X \in \mathbf{Z}G$ be an element invertible in $\mathbf{Q}G$. Assume that for some $t \in G^*$ there exists $Y \in \mathbf{Z}G$ such that $XY = |Y|X^{(t)}, (|Y|, |G|) = 1$. If t is a multiplier of Y, then t is also a multiplier of X.*

Proof: Since t is a multiplier of Y, $Y^{(t)} = hY, h \in G$. Let l be a natural number such that t^l is a multiplier of X, i.e., $X^{(t^l)} = Xg, g \in G$. One can write the sequence of equalities:

$$\begin{aligned} |Y|X^{(t)} &= h_1 YX \\ |Y|X^{(t^2)} &= h_2 YX^{(t)} \\ \cdot &= \cdot \\ \cdot &= \cdot \\ \cdot &= \cdot \\ |Y|X^{(t^l)} &= h_l YX^{(t^{l-1})}, \end{aligned}$$

where $h_1 = 1, h_2 = h, \ldots, h_l$ are elements of G. Since $X^{(t^l)} = Xg, g \in G$, we have

$$|Y|^l X^{(t)} X^{(t^2)} \ldots X^{(t^{l-1})} X = (h_1 h_2 \ldots h_l g^{-1}) Y^l X X^{(t)} X^{(t^2)} \ldots X^{(t^{l-1})}.$$

Since X is invertible in $\mathbf{Q}G$, we obtain $h|Y|^l = Y^l, h \in G$. By the previous statement $Y = \pm|Y|g, g \in G$. Taking into account that $|g| = 1$, we get $Y = |Y|g$. After substitution of $Y = |Y|g$ into the equality $|Y|X^{(t)} = YX$ and cancelling of $|Y|$ we get $X^{(t)} = gX$. □

In what follows, by $M_H(X)$ where $X \in \mathbf{Z}G$ and $H \leq G^*$ we denote a subgroup of H consisting of all multipliers of X, i.e.,

$$M_H(X) = \left\{ t \in H \mid X^{(t)} = g_t X, g_t \in G \right\}.$$

Theorem 3.1 *Let $X \in D(n, \lambda), (n, |G|) = 1$. Take any $t \in G^*$ and denote $Y_t = X^{(t)} X^{(-1)} - \lambda G$. Then*

$$M_{\langle t \rangle}(X) = M_{\langle t \rangle}(Y_t).$$

Proof: By definition of Y_t $M_{\langle t\rangle}(X) \subset M_{\langle t\rangle}(Y_t)$. To prove the inverse inclusion we multiply both sides of the equality $Y_t = X^{(t)}X^{(-1)} - \lambda G$ by X. After simple transformations we obtain

$$|Y_t|X^{(t)} = Y_t X. \tag{2}$$

The group $M_{\langle t\rangle}(Y_t)$ is cyclic, hence it has a generator, say t^l for some l (i.e., $Y_t^{(t^l)} = gY_t$). To finish the proof we have to show that t^l is a multiplier of X. Applying t to (2) $l-1$ times we obtain

$$\begin{aligned} |Y_t|X^{(t)} &= Y_t X \\ |Y_t|X^{(t^2)} &= Y_t^{(t)}X^{(t)} \\ &\vdots \\ |Y_t|X^{(t^l)} &= Y_t^{(t^{l-1})}X^{(t^{l-1})} \end{aligned}$$

By multiplication of all these equalities we obtain

$$|Y_t|^l X^{(t^l)}\big(X^{(t^{l-1})}\dots X^{(t)}\big) = Y_t\dots Y_t^{(t^{l-1})}X\big(X^{(t)}\dots X^{(t^{l-1})}\big).$$

Since $(n,|G|)=1$, $n+\lambda|G|\neq 0$ which implies that X is invertible in $\mathbf{Q}G$. Hence one can cancel the common factors in the both sides of the latter equality. This gives

$$|Y_t|^l X^{(t^l)} = \big(Y_t\dots Y_t^{(t^{l-1})}\big)X. \tag{3}$$

We claim that t (and, therefore, t^l) is a multiplier of the element $Y_t\dots Y_t^{(t^{l-1})}$. Indeed,

$$\big(Y_t\dots Y_t^{(t^{l-1})}\big)^{(t)} = Y_t^{(t)}\dots Y_t^{(t^l)} = Y_t^{(t)}\dots Y_t^{(t^{l-1})}Y_t g = g\big(Y_t\dots Y_t^{(t^{l-1})}\big).$$

Since $|Y_t\cdot\ldots\cdot Y_t^{(t^{l-1})}| = |Y_t|^l = n^l$ is relatively prime to $|G|$, the equality (3) shows that X and t^l satisfy the condition of Corollary 3.2. Hence t^l is a multiplier of X. □

To formulate next results we need an additional notation. For any element $X = \sum_{g\in G} x_g g \in \mathbf{Z}G$ by $[X]$, we denote a subgroup generated by a set $\{gh^{-1} \mid x_g \neq 0 \text{ and } x_h \neq 0\}$.

Lemma 3.3 *Let $X \in D(n,\lambda)$, $(n,|G|)=1$. Define $Y_t = X^{(t)}X^{(-1)} - \lambda G$, $t \in G^*$. Assume that n is a non-square. Then the permutation $\bar g \to \bar g^t$, $\bar g \in G/[Y_t]$ is of odd order.*

Proof: Since n is a non-square, $|G|$ is odd. Denote the natural projection $G \to G/[Y_t]$ by f. Consider $f(X)$. It is clear that $f(X)$ satisfies the equation $f(X)f(X)^{(-1)} = n + \bar\lambda\,\bar G$ (here $\bar G = G/[Y_t]$, $\bar\lambda = \lambda|[Y_t]|$). One can easily find that $f(Y_t) = |Y_t|\bar g$, for a suitable $\bar g \in \bar G$. Applying f to both sides of the identity $|Y_t|X^{(t)} = Y_t X$ we obtain $f(X)^{(t)} = \bar g f(X)$, i.e., t is a multiplier of $f(X)$.

To prove the claim let us assume the contrary, i.e., $t^{2m} \equiv 1(\mathrm{mod}\ \exp(\bar{G}))$ and $t^m \not\equiv 1(\mathrm{mod}\ \exp(G))$. Denote t^m by s. Since $\bar{G}$ is of odd order and $s^2 \equiv 1(\mathrm{mod}\ \exp(\bar{G}))$, the group $\bar{G}$ is a direct product $\bar{G} = \bar{G}_1 \times \bar{G}_{-1}$ where $\bar{G}_a = \{\bar{g} \in \bar{G} \mid \bar{g}^s = \bar{g}^a\}$, $a = \pm 1$. Since $s \not\equiv 1(\mathrm{mod}\ \exp(\bar{G}))$, $\bar{G}_{-1}$ is nontrivial.

Let $h : \bar{G} \to \bar{G}_{-1}$ be a natural projection. Denote $Z = h(f(X))$. It is clear that Z satisfies the equation $ZZ^{(-1)} = n + \mu\bar{G}_{-1}, \mu \in \mathbf{Z}$. Since t is a multiplier of $f(X)$, $Z^{(t)} = Zg, g \in \bar{G}_{-1}$. From here, it follows that $uZ = Z^{(t^m)} = Z^{(s)} = Z^{(-1)}$ for a suitable $u \in \bar{G}_{-1}$. In other words -1 is a multplier of Z. Due to Lemma 2.7 n should be a square, a contradiction. □

Corollary 3.4 *Keep the notations and the assumptions of the previous statement. Suppose, in addition, that $[Y_t]$ is a subgroup of a prime order, say p. If t is of even order modulo p, then $p \parallel |G|$.*

Proof: This is rather simple, so we omit. □

4. Proof of Theorem 1.3

In this section X always denotes a (v, k, λ)-difference set over an abelian group G. As we mentioned before, $X \in D(n, \lambda)$ where $n = k - \lambda$. In what follows we assume that there exists a divisor m of n such that

(i) $(m, |G|) = 1$;
(ii) There exists a number t such that for every prime $p \mid m$, $t \equiv p^j(\mathrm{mod}\ \exp(G))$ for some j.

Due to Lemma 2.6 the conditions above imply $X^{(t)}X^{(-1)} - \lambda G = mY_t$, where $Y_t \in \mathbf{Z}G$ should satisfy the equation

$$Y_tY_t^{(-1)} = \left(\frac{n}{m}\right)^2. \tag{4}$$

In this section we consider the case $n/m \in \{2, 3\}$. It should be mentioned that all results concerning here with the case $n/m = 2$ are known due to [4]. The results about the case $n/m = 3$ strengthen ones obtained in [5]. We devote the next section to the detailed investigation of the case $n/m = 2$.

Lemma 4.1 *Let X be a difference set. Assume that n/m is a prime, say q. Then $(n, |G|) = 1$. If, in addition, t is not a multiplier, then $(m, q) = 1$.*

Proof: Due to the assumption $n = qm$ and $(m, |G|) = 1$. Hence, if $(n, |G|) \neq 1$, then $(n, |G|) = q$. Since X is a difference set, $|X| = n + \lambda$ and $(n + \lambda)^2 = n + \lambda|G|$. Both n and $|G|$ are divisible by q. Therefore $q \mid \lambda$, which in turn, implies $q \mid m$. As $q \mid m$ contradicts the assumption $(m, |G|) = 1$, we must have $(n, |G|) = 1$.

If $q \mid m$, then Lemma 2.6 implies that $X^{(t)}X^{(-1)} - \lambda G \equiv 0 (\mathrm{mod}\, n)$. From Propositions 2.1, 2.2 and 2.4 it follows that t is a multiplier of X, a contradiction. □

Thus we have $(|G|, 2) = 1$ in the case $n/m = 2$, and $(|G|, 3) = 1$ if $n/m = 3$. Moreover, Lemma 4.1 implies that n is not a square if t is not a multiplier. Therefore the order of G is odd for both values of n/m.

In what follows we assume that t is not a multiplier. Under this assumption the element Y_t defined above is a non-trivial solution of (4). All these solutions were found in [5]. They are:

(i)

$$\begin{aligned} Y_t \;=\; g(-2 + y + y^3 + y^4 + y^5 + y^9), \quad g, y \in G, \quad [Y_t] = \langle y \rangle, \\ y^{11} = 1, \quad n/m = 3, \end{aligned}$$

(ii)

$$\begin{aligned} Y_t \;=\; g(-y - y^3 - y^9 + y^7 + y^8 + y^{11} + y^a + y^{3a} + y^{9a}), \quad g, y \in G, \\ a = 2, 4, \quad [Y_t] = \langle y \rangle, \quad y^{13} = 1, \quad n/m = 3, \end{aligned}$$

(iii)

$$Y_t = g(-1 + y + y^2 + y^4), \quad g, y \in G, \quad [Y_t] = \langle y \rangle, \quad y^7 = 1, \quad n/m = 2.$$

First we show that g may be assumed to be equal to 1 in all three cases (i)–(iii). We shall prove it only for the case (iii), since all other cases can be considered analogously.

Proposition 4.2 *There exists a translation hX, $h \in G$ of X such that*

$$(hX)^{(t)}(hX)^{(-1)} - \lambda G = m(-1 + y + y^2 + y^4).$$

Proof: By definition $mg(-1 + y + y^2 + y^4) = mY_t = X^{(t)}X^{(-1)} - \lambda G$. Therefore it is sufficient to show that $g = h^{t-1}$ for a suitable $h \in G$.

Rewrite the identity $2X^{(t)} = Y_t X$ as

$$2X^{(t)} + gX = (gy)X + (gy^2)X + (gy^4)X$$

and consider this equality as one of multisets. Then products of all elements in both sides should be equal. Therefore, setting $f = \prod_{x \in X} x$, we can write

$$f^{2t} \cdot g^{|X|} \cdot f = (gy)^{|X|} \cdot f \cdot (gy^2)^{|X|} \cdot f \cdot (gy^4)^{|X|} \cdot f.$$

After simple transformations we obtain

$$f^{2t-2} = g^{2|X|}.$$

Since G is of odd order, $g^{|X|} = f^{t-1}$. Raising both sides to a power of $|X|$ yields

$$\left(f^{|X|}\right)^{t-1} = g^{|X|^2} = g^{n+\lambda|G|} = g^n.$$

But $(n, |G|) = 1$, hence g is $(t-1)$th power, as claimed. □

Proposition 4.3 *Assume that t is not a multiplier. Then t restricted on $[Y_t]$ is of even order.*

Proof: The group $[Y_t]$ is of prime order in all three cases (i)–(iii). Denote it by C_p, where $p = |[Y_t]|$. One can easily check that every element of odd order from $\mathbf{Z}_p^*$ is a multiplier of Y_t in all three cases (i)–(iii). Hence, if the order of the restriction of t on C_p is odd then t is a multiplier of Y_t. By Theorem 3.1, t should be a multiplier of X, a contradiction. □

Corollary 4.4 *m is a square.*

Proof: As above denote $[Y_t]$ by C_p, where p is a prime. Let q be a prime divisor of m. By the assumption, $t \equiv q^j (\mathrm{mod}\ \exp(G))$ for some j. Since t restricted on C_p is of even order, there exists i such that $t^i \equiv -1(\mathrm{mod}\ p)$. Thus $q^{ji} \equiv -1(\mathrm{mod}\ p)$. Now Theorem 7.2 of [3] says that the exponent of q in the decomposition of m into the product of prime powers should be even. □

Next result will immediately imply Theorem 1.3.

We remind that $\mathrm{ord}_p(t)$ (see [2]) means the order of t modulo a prime p. A trivial observation shows that $\mathrm{ord}_p(t)$ of a non-square t is always even. The vice versa is not true in general, but if $p \equiv 3(\mathrm{mod}\ 4)$, then t has an even order if and only if it is a non-square.

Theorem 4.1 *As above we assume that t is not a multiplier and $n/m \in \{2, 3\}$. Then*

(i) *If $n/m = 2$, then m is a square, $7 \parallel |G|$, $\mathrm{ord}_p(t)$ is even for $p = 7$ and odd for all other prime divisors of $|G|$, t^2 is a multiplier of X.*

(ii) *If $n/m = 3$, then m is a square and exactly one of two cases holds*
- — $11 \parallel |G|$, $\mathrm{ord}_p(t)$ *is even for $p = 11$ and odd for all other prime divisors of $|G|$, t^2 is a multiplier of X;*
- — $13 \parallel |G|$, $\mathrm{ord}_p(t)$ *is even for $p = 13$ and odd for all other prime divisors of $|G|$, t^4 is a multiplier of X.*

Proof:

(i) **The case of $\boldsymbol{n/m = 2}$.** In this case $Y_t = g(-1 + y + y^2 + y^4), g, y \in G, y^7 = 1$, and $[Y_t] = C_7$. By Proposition 4.3 $\mathrm{ord}_7(t)$ is even. Hence, by Corollary 3.4, $7 \parallel |G|$. Corollary 4.4 says that m is a square. If $p \neq 7$ is a prime divisor of $|G|$, then it follows from Lemma 3.3 that $\mathrm{ord}_p(t)$ is odd. Finally, it is easy to check that any square is a multiplier of Y_t. Therefore $Y_t^{(t^2)} = Y_t$, whence, by Theorem 3.1, t^2 is a multiplier of X.

(ii) **The case of $\boldsymbol{n/m = 3}$.** There are two opportunities for Y_t only:

$$Y_t = g(-2 + y + y^3 + y^4 + y^5 + y^9), \quad g, y \in G, \quad [Y_t] = \langle y \rangle, \quad y^{11} = 1,$$
$$Y_t = g(-y - y^3 - y^9 + y^7 + y^8 + y^{11} + y^a + y^{3a} + y^{9a}),$$
$$g, y \in G, \quad a = 2, 4, \quad [Y_t] = \langle y \rangle, \quad y^{13} = 1.$$

To prove the claim for $n/m = 3$ one should repeat all the arguments we used above in the case $n/m = 2$. □

5. Proof of Theorem 1.2

Here we consider the case $n/m = 2$ in more detail. It should be mentioned that the case $n/m = 3$ may be treated in the same way.

We know that if $n/m = 2$ and t is not a multiplier, then $|G| = 7h$, $(h, 7) = 1$. Hence $G = H \times C_7$ where C_7 is the unique subgroup of order 7. Further, by Theorem 4.1, $m = q^2$ for a suitable $q \in \mathbf{N}$.

Due to Lemma 3.3 the restriction of t on H is of odd order, say $2l + 1$. On the other hand $\mathrm{ord}_7(t)$ is even, hence $t^3 \equiv -1 (\mathrm{mod}\ 7)$. By Proposition 4.2 we may assume that $X^{(t)}X^{(-1)} - \lambda G = m(-1 + y + y^2 + y^4)$, $\langle y\rangle = C_7$. Multiplication of the both sides of this equality by X gives us $2X^{(t)} = (-1 + y + y^2 + y^4)X$. Applying t to the both sides implies

$$\begin{aligned} 2X^{(t^2)} &= X^{(t)}(-1 + y + y^2 + y^4)^{(t)} = X^{(t)}(-1 + y + y^2 + y^4)^{(-1)} \\ &= \frac{1}{2}X(-1 + y + y^2 + y^4)(-1 + y^{-1} + y^{-2} + y^{-4}) = 2X. \end{aligned}$$

Finally, we obtained $X^{(t^2)} = X$.

Let $s = t^{3(2l+1)}$. Then $s \equiv -1(\mathrm{mod}\ 7)$ and $s \equiv 1(\mathrm{mod}\ \exp(H))$. Moreover, $X^{(t^2)} = X$ implies that $2X^{(s)} = 2X^{(t)} = XY_t$, where $Y_t = -1 + y + y^2 + y^4$. Therefore,

$$2X^{(s)} = 2X^{(t)} = XY_t = X(-1 + y + y^2 + y^4).$$

The set X can be written in the form

$$X = \sum_{h\in H} hA_h, \quad A_h \subset C_7. \tag{5}$$

Then $2X^{(t)} = 2X^{(s)} = \sum_{h\in H} 2hA_h^{(-1)}$. Taking into account the Eq. (5) we get $2A_h^{(-1)} = (-1 + y + y^2 + y^4)A_h$ for all $h \in H$.

Lemma 5.1 *Let $B \subset C_7$ satisfy the equation $2B^{(-1)} = (-1 + y + y^2 + y^4)B$. Then $B \in \{\emptyset, y + y^2 + y^4, 1 + y^6 + y^5 + y^3, C_7\}$.*

Proof: Consider the equation

$$2z^{(-1)} = (-1 + y + y^2 + y^4)z, \quad z \in \mathbf{Z}C_7. \tag{6}$$

One can easily verify that (6) is a linear equation for z. At first we consider all solutions of (6) admitting 2 as a multiplier. In this case z is a linear combination $z = z_0 1 + z_1(y + y^2 + y^4) + z_2 C_7$. Substitution of this expression into (6) gives us $2z_0 + 2(z_1(y + y^2 + y^4) + z_2C_7)^{(-1)} = -z_0 + z_0(y + y^2 + y^4) + 2(z_1(y + y^2 + y^4) + z_2C_7)^{(-1)}$. From here it follows that $z_0 = 0$ and $z = z_1(y + y^2 + y^4) + z_2C_7$. In other words z is linear combination of $y + y^2 + y^4$ and $1 + y^6 + y^5 + y^3$.

Now consider the general case, i.e., $B \subset C_7$ is a solution of (6). We assume B to be nonempty. The completion $C_7 - B$ of B is a solution of (6) as well. So we can assume the $|B| \leq 3$. Take an element $B + B^{(2)} + B^{(4)}$. It also satisfies (6) and has 2 as a multiplier. By previous paragraph $B + B^{(2)} + B^{(4)} = z_1(y + y^2 + y^4) + z_2(1 + y^6 + y^5 + y^3)$ for some non-negative integers z_1, z_2. The numbers z_1, z_2 satisfy the equation $3|B| = 3z_1 + 4z_2$. Since $|B| \leq 3$ and z_1, z_2 are non-negative integers, $z_1 = |B|, z_2 = 0$ is the only solution of this equation. This immediately implies the inclusion $B \subset y + y^2 + y^4$. If $B = y + y^2 + y^4$, then there is nothing to prove. Assume $B \neq y + y^2 + y^4$. Since both B and $y + y^2 + y^4$ are solutions, the set $y + y^2 + y^4 - B$ has the same property. Thus we can assume that $|B| = 1$, i.e., $B = y^i$ for some $i = 1, 2, 4$. The direct substitution of y^i instead of B into (6) gives us

$$2y^{-i} = y^i(-1 + y + y^2 + y^4) \Leftrightarrow 2y^{-i} + y^i = y^i(y + y^2 + y^4).$$

But the non-zero coefficients in the right side of the latter equation are ones only. Therefore y^i cannot be a solution of (6) for any i. $\square$

The lemma we have proved above gives only four values for A_h. Let

$$\begin{aligned}
H_0 &= \{h \in H \ \mid A_h = \emptyset\}, \\
H_1 &= \{h \in H \ \mid A_h = y + y^2 + y^4\}, \\
H_2 &= \{h \in H \ \mid A_h = 1 + y^6 + y^5 + y^3\}, \\
H_3 &= \{h \in H \ \mid A_h = C_7\}.
\end{aligned}$$

Then $H = H_0 \cup H_1 \cup H_2 \cup H_3$ is a partition of H and $X = H_1(y + y^2 + y^4) + H_2(1 + y^6 + y^5 + y^3) + H_3C_7$. Denote $|H_i| = h_i$. Clearly $2q^2 + \lambda = 3h_1 + 4h_2 + 7h_3$ (we remind that $m = 2q^2$). Let χ be an irreducible character of H and ρ be a non-principal one of C_7. Then $\rho \otimes \chi$ is a irreducible character of $G = C_7 \times H$. Since G is abelian, $\rho \otimes \chi$ is also a one-dimensional representation of $\mathbf{Z}G$. Hence a value $z = (\rho \otimes \chi)(X)$ is equal to $\chi(H_1)\rho(y + y^2 + y^4) + \chi(H_2)\rho(1 + y^6 + y^5 + y^3) + \chi(H_3)\rho(C_7)$. Since $\rho(C_7) = 0$, then $\rho(1 + y^6 + y^5 + y^3) = -\rho(y + y^2 + y^4)$ and $z = \rho(y + y^2 + y^4)(\chi(H_1) - \chi(H_2))$. Since X satisfies the equation $XX^{(-1)} = 2q^2 + \lambda G$, we can write

$$\bar{z}z = \rho(y + y^2 + y^4)\overline{\rho(y + y^2 + y^4)}(\chi(H_1 - H_2))(\overline{\chi(H_1 - H_2)}) = 2q^2$$

Taking into account that $\rho(y + y^2 + y^4)\overline{\rho(y + y^2 + y^4)} = 2$ we obtain

$$\chi(H_1 - H_2)\overline{\chi(H_1 - H_2)} = q^2$$

for all irreducible characters of the group H. Therefore $(H_1 - H_2)(H_1 - H_2)^{(-1)} = q^2$. This equation implies two ones: $(h_1 - h_2)^2 = q^2, h_1 + h_2 = q^2$.

Thus we have the following equation for h_1, h_2, h_3

$$\begin{cases} h_1 - h_2 = \pm q \\ h_1 + h_2 = q^2 \\ 3h_1 + 4h_2 + 7h_3 = \lambda + 2q^2 \end{cases}$$

This system has the following solutions:

$$h_1 = \frac{q^2 \pm q}{2}, \quad h_2 = \frac{q^2 \mp q}{2}, \quad 7h_3 = \lambda + \frac{-3q^2 \pm q}{2}.$$

The last expression gives us the inequality $\lambda \geq (3q^2 - q)/2$. Applying this inequality to the complement difference set $G \setminus X$ we obtain:

$$\frac{2q^2(2q^2-1)}{\lambda} \geq \frac{3q^2 - q}{2}.$$

Thus we have the following scope for λ:

$$\frac{3q^2 - q}{2} \leq \lambda \leq \frac{4q(2q^2-1)}{3q-1}. \tag{7}$$

Proof of Theorem 1.2: Assume the contrary, i.e., t is not a multiplier. Then λ satisfies (7).

Since $(q^2, \lambda) = 1$ and $\lambda \mid 2q^2(2q^2-1)$, the number $l = (4q^2-2)/\lambda$ is an integer. From the inequality (7) it follows that

$$3 > 2\frac{4q^2 - 2}{3q^2 - q} \geq l \geq \frac{3q-1}{2q} > 1$$

and we have the only solution $l = 2$, i.e., $\lambda = 2q^2 - 1$. But in this case $n > \lambda$, and by Theorem 4 of [4] t is a multiplier of X, a contradiction. □

As a consequence we are able to give a proof of Corollary 1.1.

Proof of Corollary 1.1: Suppose the contrary, i.e., p is not a multiplier of D. Then, by Theorem 1.2, λ should be divisible by p. Applying of the same claim to the complement difference set yields $p \mid n(n-1)/\lambda$. But this is impossible, because the order $|G| = \lambda + n(n-1)/\lambda + 4p^{2b}$ of the group G is divisible by p in this case[2]. □

Acknowledgments

The author is very grateful to the anonymous referee who read the paper carefully and proposed very helpful suggestions.

Notes

1. In fact this inequality implies $b = a$, because of $XX^{(-1)} - \lambda G = n$ and $p^a \parallel n$.
2. Here b is defined by the equality $n = 2p^{2b}$.

References

1. C.W. Curtis and I. Reiner, *Representation Theory of Finite Groups and Associative Algebras*, John Wiley & Sons, New York, London, 1962.
2. D. Jungnickel, "Difference Sets," in *Contemporary Design Theory: A Collection of Surveys*, J.H. Dinitz and D.R. Stinson (Eds.), John Wiley & Sons, pp. 241–324, 1992.
3. H.B. Mann, *Addition Theorems*, Wiley, New York, 1965.
4. H.B. Mann and S.K. Zaremba, "On multipliers of difference sets," *Illinois J. Math.* **13** (1969), 378–382.
5. Qiu Weisheng, "On character approach to multiplier conjecture and a new result on it," 1993, submitted.