# Further Results On The Multiplier Conjecture For The Case $n = 2n_1$ (I)*

Qiu Weisheng
Institute of Mathematics
Peking University
Beijing 100871
People's Republic of China

ABSTRACT. In this paper we obtain further results on the Multiplier Conjecture for the case $n = 2n_1$ using our method.

**First Multiplier Theorem.** *Let $D$ be an abelian $(v, k, \lambda)$-difference set, and let $p$ be a prime dividing $n = k - \lambda$ but not $v$. If $p > \lambda$, then $p$ is a numerical multiplier of $D$.*

**Multiplier Conjecture.** *The First Multiplier Theorem holds without the assumption that $p > \lambda$.*

**Second Multiplier Theorem.** *Let $D$ be a $(v, k, \lambda)$-difference set in an abelian group $G$, and let $v_0$ be the exponent of $G$. Let $n_1$ be a divisor of $n$ such that $(n_1, v) = 1$, and $n_1 > \lambda$. Suppose that $t$ is an integer such that for every prime divisor $p$ of $n_1$, there exists a nonnegative integer $j$ with $t \equiv p^j (\mod v_0)$. Then $t$ is a numerical multiplier of $D$.*

Virtually all further multiplier theorems have arisen in an attempt to weaken the condition $p > \lambda$ or $n_1 > \lambda$.

In 1992 We [11] presented a method of studying the Multiplier Conjecture, where one of the main theorems is the following:

**Theorem 1.** *Let $D$ be a $(v, k, \lambda)$-difference set in an abelian group $G$, and let $v_0$ be the exponent of $G$. Set $n = k - \lambda$. Let $n = dn_1 (n_1 > 1)$ and $(n_1, v) = 1$. Suppose that $t$ is an integer such that for every prime divisor $p$ of $n_1$, there exists a nonnegative integer $j$ such that $p^j \equiv t (\mod v_0)$.*

*The project supported by National Natural Science Foundation of China.

*Then $t$ is a numerical multipler of $D$ if and only if no nontrivial solution $\xi$ of the CH-equations of $d$ for $G$ satisfies*

$$D^{(t)}D^{(-1)} = n_1\xi + \lambda G. \tag{1}$$

The CH-equations of $d$ for $G$ are

$$\sum_{g\in G} c_g = d, \tag{2}$$

$$\xi\xi^{(-1)} = d^2 \cdot 1, \tag{3}$$

where $\xi = \sum_{g\in G} c_g g \in ZG$. Obviously $\xi = dg$ ( $\forall g \in G$ ) are solutions, they are called trivial. The other solutions are called nontrivial.

The equation (1) is well-known. However, our method not only finds the conditions such that the equations (2) and (3) have *only trivial* solutions, but also further finds *nontrivial* solutions, and studies the conditions under which *no nontrivial solutions satisfies the equation* (1). Hence we are abel to weaken some assumptions under which $t$ is a numerical multiplier.

In this paper we prove the following theorem 2:

**Theorem 2.** *Let $n = 2n_1$. If $7^2|v$, then the Second Multiplier Theorem holds without the assumption $n_1 > \lambda$.*

**Proof:** The case $2|n_1$ is trivial (replace $n_1$ by $n$). Now assume that $n_1$ is odd, thus $v$ must be odd.

We [11] have found only possible nontrivial solutions of CH-equations of 2 for $G$ which have the form:

$$\xi = g_r(-1 + g_u + g_u^2 + g_u^4),$$

where $g_u$ is any element of order 7, and $g_r$ is any element in $G$.

Now assume that $7^2|v$. We denote the order of 2 modulo $7^e$ by $Ord_{7^e}(2)$ . It is easy to see that $Ord_{7^e}(2) = 3 \cdot 7^{e-1}$, and $\frac{\phi(7^e)}{Ord_{7^e}(2)} = 2$, where $e \geq 1$.

Let

$$G = < g_{l_1} > \times < g_{l_2} > \times \cdots \times < g_{l_s} >, \tag{4}$$

where the order of $g_{l_i}$ is $p_i^{\alpha_i}$, $1 \leq i \leq s$, and $p_1 = 7$, and $g_u = {g_{l_1}}^{7^{\alpha_1 - 1}}$. Let $\omega_i$ be a primitive $p_i^{\alpha_i}$-th root of unity, $1 \leq i \leq s$. Let $g_i \longmapsto \chi_i$ ($0 \leq i \leq v-1$ ) be an isomorphism of $G$ onto its complex character group $\hat{G}$, where $\chi_0$ is the principal character of $G$.

Since $7^2|v$, there are only two possible cases: $\alpha_1 \geq 2$, or $\alpha_1 = 1$ and $p_2 = 7$.

**Case 1.** $\alpha_1 \geq 2$. We have $\chi_{l_1}(g_u) = {\omega_1}^{7^{\alpha_1 - 1}}$, and $\chi_u(g_u) = 1$.

Set $\varepsilon = \omega_1^{7^{\alpha_1-1}}$, and $\zeta = \omega_1$. Let $B$ denote the ring of algebraic integers in $Q(\zeta)$.

We have $(\chi_u(\xi)) = (2)$. It is not difficult to show that $(\chi_{l_1}(\xi)) \neq (2)$.

Since the ideal (2) is unramified in $Q(\zeta)$ and $\frac{\phi(7^{\alpha_1})}{Ord_{7^{\alpha_1}}(2)} = 2$, we have $(2) = E_1E_2$, where the $E_i's$ are distinct prime ideals of $B$.

It is not difficult to show that for $\chi_i \in <\chi_{l_1}>$ and $i \neq 0$ we have

$$(\chi_i(D^{(t)}))(\chi_i(D^{(-1)})) = \sigma_t(E_{i_1})E_{i_2}(n_1), \tag{5}$$

where $\{E_{i_1}, E_{i_2}\} = \{E_1, E_2\}$.

Since $Gal(Q(\zeta)/Q)$ transitively acts on $\Omega = \{E_1, E_2\}$, thus there is a homomorphism of $Gal(Q(\zeta)/Q)$ into the symmetric group $S_2$. We denote the homomorphic image of $\sigma_t$ by $\tilde{\sigma_t}$. Then there are only two possible cases: $\tilde{\sigma_t} = 1$, or $\tilde{\sigma_t} = (12)$.

Suppose that $\tilde{\sigma_t} = 1$. If $\xi$ satisfies the equation (1), then we have

$$(\chi_{l_1}(D^{(t)}))(\chi_{l_1}(D^{(-1)})) = (n_1)(\chi_{l_1}(\xi)) \neq (n_1)(2).$$

This contradicts the equation (5).

Suppose that $\tilde{\sigma_t} = (12)$. If $\xi$ satisfies the equation (1), then we have

$$(\chi_u(D^{(t)}))(\chi_u(D^{(-1)})) = (n_1)(\chi_u(\xi)) = (n_1)(2).$$

This contradicts the equation (5).

Hence in case 1 $\xi$ does not satisfy (1).

**Case 2.** $\alpha_1 = 1$ and $p_2 = 7$.

Set $g_{l_2}' = g_{l_2}^{7^{\alpha_2-1}}$. We have $\chi_u(g_u) = \omega_1$, and $\chi_{l_2'}(g_u) = 1$.

It is similar to the case 1 that $\xi$ does not satisfy (1).

By theorem 1 $t$ is a numerical multiplier of $D$. □

**Remark.**

(1) Theorem 2 improves Newman, and McFarland's results which required $(v, 7) = 1$; Theorem 2 also improves Turyn's result which required that $t$ is a quadratic residue modulo 7 for $7|v$.

(2) Suppose that there exists an abelian $(v, k, \lambda)$-difference set with $n = 2n_1$ and $n_1$ is odd and $(n_1, v) = 1$, then we have the following results:

(i) let $p$ be any prime divisor of $v$. Then $Ord_p(2)$ must be odd. It follows that $p \equiv 1( \mod 8)$ or $p \equiv -1( \mod 8)$. If $p \equiv 1( \mod 8)$, then $Ord_p(2)|\frac{p-1}{2^e}$, where $2^e||p-1$.

(ii) If $7||v$, and v has a prime divisor $p \equiv 1( \mod 8)$ or $p \equiv -1( \mod 8)$ ( $p \neq 7$ ) such that $Ord_p(t)$ is even, then $\xi$ does not satisfy (1). Thus $t$ is a numerical multiplier of $D$.

If $t$ is a quadratic nonresidue modulo 7, then under the assumptions of (ii) no difference set exists by theorem 3 of [7].

**Application.**

Using theorem 2 we can show that there is no (1519, 507, 169)-difference set $D$. Since the Sylow 7-subgroup and Sylow 31-subgroup of a group of order 1519 must be normal subgroups, thus a group $G$ of order 1519 must be abelian. Here $n = 2n_1$ and $n_1 = 13^2$. By theorem 2, 13 is a numerical multiplier of $D$ since $7^2|v$. Since $Ord_{7^2\cdot 31}(13) = 210$ and $Ord_{7\cdot 31}(13) = 30$, by Corollary 7.4 of [3] we get that there is no (1519, 507, 169)-difference set in $G = Z_{7^2} \times Z_{31}$ or $G = Z_7 \times Z_7 \times Z_{31}$.

Using Second Multiplier Theorem one can not rule out the existence of above difference set since from it we only know that 8 is a multiplier of $D$, however, $Ord_{7^2\cdot 31}(8) = 35$, and $Ord_{7\cdot 31}(8) = 5$, these are odd.

Using Turyn' result one can not rule out the existence of above difference set since 13 is a quadratic nonresidue modulo 7.

Using Mann test or Lander's theorem 4.4 one can not rule out the existence of above difference set since $Ord_7(2) = 3$ and $Ord_{31}(2) = 5$ and $13^2||n$.

Using Lander's theorem 4.5 one also can rule out the existence of above difference set since $13^{105} \equiv -1(\mod 7^2 \cdot 31)$ and $13^{15} \equiv -1(\mod 7 \cdot 31)$ but $13|n$.

**Acknowledgment**

The author is thankful to the referee for comments and suggestions.

## References

[1] K.T. Arasu, Recent results on difference sets, In D.Ray-Chaudhuri (ed.), "Coding Theory and Design Theory Part II", Springer, New York, 1990, 1–23.

[2] M. Hall.Jr, Cyclic projective planes, *Duke Math. J.*, 14(1947), 1079–1090.

[3] D. Jungnickel, Difference sets, "Contemporary Design Theory: A Collection of Surveys", J.H. Dinitz and D.R. Stinson (Editors), Wiley-Interscience, New York, 1992.

[4] E.S. Lander, "Symmetric Designs: An algebraic approach", Cambridge University Press , Cambridge, 1983.

[5] R.L. Long, "Algebraic Number Theory", Dekker, New York, 1977.

[6] H.B. Mann, "Addition Theorems", Wiley, New York, 1965.

[7] H.B. Mann and S.K. Zaremba, On multipliers of difference sets, *Illinois J. Math.*, **13**(1969), 378–382.

[8] R.L. McFarland, On multipliers of abelian difference sets, Ph.D. Dissertation, Ohio State University, 1970.

[9] P.K. Menon, Difference sets in abelian groups, *Proc. Amer. Math. Soc.*, **11**(1960), 368–376.

[10] M. Newman, Multipliers of difference sets, *Canad. J. Math.*, **15**(1963), 121–124.

[11] Qiu Weisheng, A Character approach to the multiplier conjecture and a new result on it, Submitted.

[12] Qiu Weisheng, A method of studying the multiplier conjecture and some partial solutions for it, *Ars Comb.*, to appear.

[13] Qiu Weisheng, Further results on the multiplier conjecture for $n = 2n_1$ and $n = 3n_1$, Submitted.

[14] R.J.Turyn, The Multiplier theorm for difference sets, *Canad. J. Math.*, **16**(1964), 386–388.