The Nepali Math. Sc. Report
Vol. 20 No. 1&2, 2002

Multiplier Theorem Revisited

PARTHA PRATIM DEY

Abstract: An abelian (v, k, λ)-difference set in an abelian group G is a set D consisting of k group elements with the property that the list of the "differences" xy^{-1} with $x,y \in D$ contains every non-identity element of G exactly λ times. We investigate these sets from the viewpoint of the group algebra KG. Using the idempotents in KG we give a new proof of the Hall Multiplier Theorem.

Introduction

For every known (v, k, λ)-difference set, a prime p is a multiplier if p divides $n = k-\lambda$ and $(p, v) = 1$. This fact known as multiplier theorem was first proved by Hall in 1951 in his paper on Cyclic Incidence Matrices [1]. In this paper, we use idempotents in KG to provide a new proof of the multiplier theorem. Throughout, G will denote an abelian group of exponent μ and K will be a field containing a primitive μ th root of unity. Notice that this necessarily requires that the characteristic of K does not divide μ.

Preliminary Results

A character of G is a homomorphism ϕ from G to a multiplicative group of K. For example, the trivial character (or principal character), denoted by ϕ_0, is the map such that $\phi_0(g) = 1$, $\forall_g \in G$. It is not difficult to determine all the characters of G. To see this, let us decompose G as a product of cyclic groups,

$$G = G_1 \times \ldots \times G_n$$

where G_i is generated by g_i. A character ϕ must carry each g_i to a $|G_i|$ th root of unity, and conversely ϕ is completely determined by knowing to which root of unity each g_i is carried. Hence there are precisely $|G| = |G_1| \times \ldots \times |G_n|$ characters of G. In fact the characters form a group isomorphic to G under the rule $(\phi\psi)(g) = \phi(g)\psi(g)$.

Lemma (2.1) [2]. Let G be an abelian group and $ch(G)$ be the group of characters of G with values in K.

(i) For $\forall_g \in G$

$$\sum_{g \in ch(G)} \phi(G) = \begin{cases} |G| & \text{if } g \text{ is an identity element} \\ 0 & \text{otherwise} \end{cases}$$

(ii) For $\forall \phi \in ch(G)$,

$$\sum_{g \in G} \phi(G) = \begin{cases} |G| & \text{if } \phi = \phi_0 \\ 0 & \text{otherwise} \end{cases}$$

Proof: (i) Let $S(g)$ denote the sum in question. If g is the identity element then $S(g)$ certainly equals $|G|$. So let g be a non-identity element. Choose a character ψ such that $\psi(g) \neq 1$. Then

$$S(g) \sum_{\phi \in ch(G)} \phi(G) = \sum_{\phi \in ch(G)} (\phi\psi)(g) = \psi(g)\Big(\sum_{\phi \in ch(G)} \phi(G)\Big) = \psi(g)S(g).$$

Hence $S(g) = 0$.

(ii) If ϕ is the principal character ϕ_0, then clearly

$$\sum_{g \in G} \phi(g) = |G|.$$

Let ϕ be nonprincipal and let $S(\phi)$ be the sum in question. Choose $h \in G$ such that $\phi(h) \neq 1$. Then

$$S(\phi) = \sum_{g \in G} \phi(G) = \sum_{g \in G} \phi(gh) = \sum_{g \in G} \phi(g)\,\phi(h) = \phi(h)\Big(\sum_{g \in G} \phi(g)\Big) = \phi(h)S(\phi).$$

Hence $S(\phi) = 0$. *QED.*

Another concept that we will use in our proof of the Multiplier theorem is the group-ring KG which consists of all formal sums

$$\sum_{g \in G} a_g g$$

with $a_g \in K$. Addition is defined in the usual manner. Multiplication is defined by using the distributive law and the group operation of G:

$$\Big(\sum_{g \in G} a_g g\Big)\Big(\sum_{h \in G} b_h h\Big) = \sum_{g \in G} \sum_{h \in G} (a_g h_n)gh.$$

Clearly KG is a ring with identity and is commutative as G is abelian. The characters of G can easily be extended to be maps from the group-ring KG onto K and it is convenient to do so. If ϕ is a character of G, simply let

$$\phi\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G} a_g \phi(g)$$

We should also note that any subset A of G can be identified with an element in KG by setting

$$A = \sum_{g\in A} g.$$

Under this definition, a (v, k, λ)-difference set D may be written as

$$D = \sum_{d\in D} d.$$

Also if $A, B \subseteq G$ and ϕ is a character of G, then $\phi(AB) = \phi(A)\phi(B)$. For any integer t and subset A of G we define:

$$A^t = \sum_{g\in G} g^t.$$

Lemma (2.2) [2]. Let D be a (v, k, λ)-difference set in an abelian group G. Then

$$DD^{-1} = (k-\lambda)\, e + \lambda G = ne + \lambda G.$$

where $k-\lambda = n$ and e is the identity element of G.

Proof: Note that

$$DD^{-t} = \sum_{x\in y} xy^{-1} + \sum_{x\neq y} xy^{-1}$$

where $x, y \in D$. Since $|D| = k$, we have

$$\sum_{x=y} xy^{-1} = ke$$

and the definition of difference set yields

$$\sum_{x\neq y} xy^{-1} = \lambda(G - e).$$

Hence

$$DD^{-1} = ke + \lambda(G - e) = (k-\lambda)\, e + \lambda G = ne + \lambda G. QED.$$

Lemma (2.3) [2]. Let D be a (v, k, λ)-difference set in an abelian group G and let ϕ be a nonprincipal character of G. Then

$$\phi(D)\phi(D^{-1}) = n.$$

Proof: We apply ϕ to both sides of $DD^{-1} = ne + \lambda G$. Then

$$\phi(D)\phi(D^{-1}) = n\phi(e) + \lambda\, \phi(G) = n$$

as $\phi(G) = 0$ by lemma (2.1). *QED.*

Lemma (2.4) [2]. Let G be an abelian group of exponent μ and let K be a field containing a μ th root of unity. Given ϕ, a character of G, we define e_ϕ as follows :

$$e_\phi = \frac{1}{|G|}\sum_{g\in G}\phi(g^{-1})g$$

Then (i) If e is the identity of G, we have

$$\sum_{\phi\in ch(G)} e_\phi = e$$

(ii) Moreover for any A,

$$A = \sum_{g\in G} e_g g$$

in KG, we obtain

$$A = \sum_{\phi\in ch(G)} \phi(A)e_\phi$$

Proof. (i) Note that

$$\sum_{\phi\in ch(G)} e_\phi$$

$$= \sum_{\phi\in ch(G)} \left(\frac{1}{|G|}\sum_{g=G}\phi(g^{-1}g)\right)$$

$$= \frac{1}{|G|}\sum_{\phi\in ch(G)}\left(\sum_{g=G}\phi(g^{-1})g\right)$$

$$= \frac{1}{|G|}\sum_{g\in G} g\left(\sum_{\phi\in ch(G)}\phi(g^{-1}g)\right)$$

$$= \frac{1}{|G|}e\sum_{\phi\in ch(G)}\phi(e^{-1})$$

$$= \frac{1}{|G|}e|G|$$

$$= e$$

Note that for $g \neq e$.

$$\sum_{\phi\in ch(G)}\phi(g^{-1}) = 0$$

by lemma (2.1).

(ii) Let $h \in G$. Then

$$he_\phi$$

$$= h\left(\frac{1}{|G|}\sum_{g\in G}\phi(g^{-1})g\right)$$

$$= \frac{1}{|G|}\sum_{g\in G}\phi(g^{-1})hg$$

$$= \frac{1}{|G|}\sum_{g\in G}\phi(g^{-1})\phi(h^{-1})\ \phi(h)hg$$

$$= \frac{1}{|G|}\phi(h)\sum_{g\in G}\phi(g^{-1})\phi(h^{-1})hg$$

$$= \frac{1}{|G|}\phi(h)\sum_{g\in G}\phi(g^{-1}h^{-1})hg$$

$$= \frac{1}{|G|}\phi(h)\sum_{g\in G}\phi(hg)^{-1})hg$$

$$= \phi(h)\left(\frac{1}{|G|}\sum_{g\in G}\phi(hg)^{-1})hg\right)$$

$$= \phi(h)e_\phi$$

Then

$$Ae_\phi$$

$$= \left(\sum_{g\in G} a_g g\right)e_\phi$$

$$= \sum_{g\in G} a_g g\, e_\phi$$

$$= \sum_{g\in G} a_g \phi(g)\, e_\phi$$

$$= \left(\sum_{g\in G} a_g \phi(g)\right)e_\phi$$

$$= \phi(A)e_\phi$$

Hence

$$A$$

$$= Ae$$

$$= A\left(\sum_{\phi\in ch(G)} e_\phi\right)$$

$$= \sum_{\phi \in ch(G)} Ae_\phi$$

$$= \sum_{\phi \in ch(G)} \phi(A) e_\phi \ .QED.$$

3. The Multiplier Theorem

Finally we are ready to prove the Multiplier Theorem by Hall.

Theorem 3.1. (*Multiplier Theorem*). *Let D be an abelian* (v, k, λ)-difference set of *an abelian group G. Suppose that p is a prime such that* $(p,v) = 1$, $p > \lambda$, $p|n = k-\lambda$. *Then p is a multiplier of D.*

Proof. Let K be a field of characteristic p such that K contains a primitive μ^{th} root of unity, where μ is the exponent of G. Then $D^p = D^{(p)}$ in $Z_p G$, which implies $\phi(D)^p = \phi(D)^p = \phi(D^{(p)})$ for any character ϕ of G. We now compute $D^{(p)} Dg^{(-1)}$.

$$D^{(p)} Dg^{(-1)}.$$

$$= \sum_{\phi \in ch(G)} \phi(D^{(p)}) Dg^{(-1)} e_\phi$$

$$= \sum_{\phi \in ch(G)} \phi(D^{(p)}) \phi(Dg^{(-1)}) e_\phi$$

$$= \sum_{\phi \in ch(G)} \phi(D^{(p)}) \phi(D) \phi(g^{(-1)}) e_\phi$$

$$= \sum_{\phi \in ch(G)} \phi(D)^{p-1} \phi(D) \phi(D^{(-1)}) \phi(g^{-1}) e_\phi .$$

If ϕ is nonprincipal, then $\phi(D)\phi(D^{(-1)}) = n = 0$ by Lemma (2.3) and the fact that p divides n. Hence

$$D^{(p)} \ Dg^{(-1)}$$

$$= \phi_0(D)^{p-1} \phi_0(D) \phi_0(D^{(-1)}) \phi_0(g^{(-1)}) e_{\phi 0}$$

$$= k^{p+1} \frac{1}{|G|} \sum_{g \in G} g$$

$$= \frac{k^{p+1}}{v} \sum_{g \in G} g$$

Because $|D^{(p)} \cap Dg|$ is the coefficient of e in $D^{(p)}\, Dg^{(-1)}$, we have $|D^{(p)} \cap Dg| = \frac{k^{p+1}}{v}$. Further $k(k-1) = \lambda(v-1)$ implies $k^2 - n = \lambda v$. If p divides k, then p divides λv and since $p > \lambda$, p divides v, a contradiction. Hence p does not divide k. Finally $k(k-1) = \lambda(v-1)$ implies $k = v\ (modp)$. Thus

$$\frac{k^{p+1}}{v} = \frac{\lambda^{p+1}}{\lambda} = \lambda^p = \lambda (modp)$$

Hence $|D^{(p)} \cap Dg| = \lambda + tp$. As $p > \lambda$, the integer t has to be nonnegative which shows $|D^{(p)} \cap Dg| \geq \lambda$. As $D^{(p)}$ intersects every block Dg in at least λ points, $D^{(p)}$ is a block of the development of D. Thus p is a multiplier. *QED.*

REFERENCE

[1] Hall, M. and Ryser, H.J. (1951). *Cyclic Incidence Matrices*, Canadian J. Math., 3, 495–502.

[2] Lander, E.S. (1983). *Symmetric Designs: An Algebraic Approach*, London,-New York-New Rochelle-Melbourne-Sydney: Cambridge Press.

PARTHA PRATIM DEY
Department of Computer Science
North South University
Dhaka, Bangladesh