数理解析研究所講究録
1190巻 2001年 61-81

組み合わせ構造の研究への表現の利用法

萩田 真理子　慶應義塾大学 理工学部

Mariko Hagita　Department of Mathematics, Keio University

Abstract

群が関わる組み合わせ構造で、その存在性を調べるために群の表現を利用できるものをいくつかあげ、それによって導かれた結果を紹介する。

1 Introduction

1.1 Difference Sets and Symmetric Designs

Let G be a group of order v. A k-subset D in G is called a (v,k,λ)-*difference set* of G if the list of "differences" $\{xy^{-1}(x,y\in D)\}$ contains each nonidentity element of G exactly λ times.

Let $G:=Z/7Z=\{0,1,2,\ldots,6\}$ and $D:=\{1,2,4\}\subset G$. Then the list of nonzero "differences" is

$$2-1=1,\quad 1-2=-1=6,\quad 4-1=3,$$

$$1-4=-3=4,\quad 4-2=2,\quad 2-4=-2=5.$$

Hence D is a $(7,3,1)$-difference set of G.

We call $n:=k-\lambda$ the order of D. Difference sets of order $n=0$ or 1 (i.e. $D=$ empty set, single sets, or their complements in G) are called "trivial" difference sets. Note that for any (v,k,λ)-difference set D of order n, $D'=G\setminus D$ is a $(v,v-k,v-2k+\lambda)$-difference set of the same order n. Therefore we can assume $1<k\leq\frac{k}{2}$. If there exists a (v,k,λ)-difference set D in some group G of order v, then by counting the number of nonidentity elements we have $k(k-1)=\lambda(v-1)$.

The main problem on difference set is which group has a nontrivial difference set. For abelian cases, Jungnickel(1992,[17]) constructed a list of solutions of the problem for all possible parameters with order n of the difference sets up to 30. Many constructions for difference sets and many nonexistence theorems for difference sets are known. However, much work remains to fill the gap between constructions and nonexistence theorems, even for abelian cases.

An *incidence structure* is a triple (P, B, I), where P is a set of points, B is a set of blocks, and I is an incidence relation between P and B. An incidence structure is called a *t-design* if for any set T of t points, there are exactly λ blocks incident to all points in T for some λ. A *symmetric* (v, k, λ)*-design* is a 2-design satisfying $|P| = |B| = v$.

For any (v, k, λ)-difference set D in G, we can define an incidence structure with point set G, block set $\{Dg | g \in G\}$ and inclusion for incidence relation. Then the incidence structure is a symmetric (v, k, λ)-design.

The following theorem is the connection between difference sets and symmetric designs.

Theorem 1 *A (v, k, λ)-difference set in G is equivalent to a symmetric (v, k, λ)-design with a regular automorphism group.*

1.2 Group Rings and Characters

Let G be a multiplicatively written group of order v. In the group ring ZG, a subset S of G is identified with $\sum_{s \in S} s$. Also, for $A = \sum_{g \in G} a_g g$, $\sum_{g \in G} a_g g^t$ is denoted by $A^{(t)}$. So $D = \sum_{d \in D} d$, $D^{(-1)} = \sum_{d \in D} d^{-1}$ and $G = \sum_{g \in G} g$. Then a k-subset D is a (v, k, λ)-difference set of G if and only if

$$DD^{(-1)} = n \cdot 1 + \lambda G$$

in ZG, where 1 is the identity element of G.

We write ξ_t for a primitive complex t-th root of unity and $[k]$ for the set $\{0, 1, \ldots, k-1\}$. The cyclic group of order k is denoted as Z_k, and is often identified with Z/kZ or $[k]$ without explicitly mentioning it.

Let G be an abelian group and G^* be the character group of G. For a subgroup U of G, we denote the set of all $\chi \in G^*$ which are trivial on U by $U^{\perp}$. We write $\exp(G)$ for the exponent

of G.

A prime p is called *self-conjugate* mod e if there exists an i, such that $p^i \equiv -1 \pmod{e'}$ where e' is the p-free part of e. If each prime divisor of n is self-conjugate mod e, then we say n is self-conjugate mod e.

For any prime ideal $\wp$ and any ideal $\Re$ in a ring, we write $\nu_\wp(\Re) = i$ if and only if $\wp^i \supset \Re$ and $\wp^{i+1} \not\supset \Re$.

The following was used by Turyn in [31].

Lemma 2 *Let $\wp$ be a prime ideal of $Z[\xi_e]$ over a prime integer p. If p is self-conjugate mod e, then $\wp = \bar{\wp}$ holds, where $^-$ denotes the complex conjugation.*

We have the following well-known result.

Lemma 3 (Inversion Formula) *Let G be a finite abelian group, and let $A = \sum_{g\in G} a_g g \in ZG$. Then*

$$a_g = \frac{1}{|G|} \sum_{\chi \in G^*} \chi(A)\chi(B).$$

Hence, if $A, B \in ZG$ satisfies $\chi(A) = \chi(B)$ for all characters χ of G, then $A = B$ holds.

Then D is a (v, k, λ)-difference set of abelian group G if and only if

$$DD^{(-1)} = n \cdot 1 + \lambda G$$

in ZG, where 1 is the identity element of G, and this is equivalent to

$$\chi(D)\overline{\chi(D)} = n \quad \text{for all nontrivial characters } \chi \text{ of } G.$$

If we assume that n is a square, and is self-conjugate mod $\exp(G)$, then the condition is equivalent to

$$\frac{1}{\sqrt{n}}\chi(D) = u_\chi \tag{1}$$

for all nontrivial characters χ of G, where u_χ is a root of unity. This follows from Lemma 2 because $\nu_\wp(\chi(D)) = \nu_\wp(\overline{\chi(D)})$ for all prime ideals $\wp$ in $Z[\xi_e]$ over p, where $e = \exp(G)$.

Suppose that the cyclic decomposition of G is $C_1 \times C_2 \times \ldots \times C_t$, where C_i is isomorphic to Z/u_iZ for $i = 1, 2, \ldots, t$. Then the group ring ZG is isomorphic to the ring

$$Z[x_1, x_2, \ldots, x_t]/(x_1^{u_1} - 1, x_2^{u_2} - 1, \ldots, x_t^{u_t} - 1).$$

In this ring, we can express the difference set D as

$$D = D(x_1, x_2, \ldots, x_t) = \sum_{a_i \in [u_i]} d_{a_1 a_2 \ldots a_t} \cdot x_1^{a_1} x_2^{a_2} \ldots x_t^{a_t}$$

with $d_{a_1 \ldots a_t} = 0$ or 1. Here, the condition (1.1) is equivalent to that

$$\frac{1}{\sqrt{n}} D(\zeta_1^{\alpha_1}, \zeta_2^{\alpha_2}, \ldots, \zeta_t^{\alpha_t}) \quad \text{is a root of unity}$$

for all $(\alpha_1, \alpha_2, \ldots, \alpha_t) \in G$ except $(0, 0, \ldots, 0)$, where $\zeta_i = \xi_{u_i}$.

Lemma 4 *If an abelian group G has a difference set whose order n is self-conjugate mod $exp(G)$, then n is a square.*

Proof. Let p be a prime divisor of n. If there is a prime $q \neq p$, $q|v$, then from Lemma 2, for any character χ of order q of G,

$$\nu_\wp(n) = 2\nu_\wp(\chi(D))$$

for any prime ideal $\wp$ over p in $Z[\xi_q]$. But since p is unramified in $Z[\xi_q]$,

$$\nu_\wp(n) = \nu_p(n).$$

Thus, $\nu_p(n)$ is even.

If there is no prime q which satisfies $q|v$, $q \neq p$, then v is a prime power p^a. Let $\nu_p(n) = b$. Since $v > n$, we have $a > b$. Then, since $p^a | \lambda v = k^2 - n$ and $a > b$, we have $b = \nu_p(k^2) = 2\nu_p(k)$. So b is an even integer.

Since n is positive, n is a square. □

For nonabelian groups, we can use irreducible matrix representations instead of characters. The following result sometimes helps us to extend some theorems on abelian groups to that of nonabelian groups.

Theorem 5 (Brauer, see [8](41.1)) *Let e be the exponent of G, and let Q denote the rational number field. Then $Q(1^{\frac{1}{e}})$ is a splitting field for G.*

1.3 Famous Constructions, Nonexistence Theorems and Conjectures

For any prime power q and any integer $d > 1$, there exists a cyclic (v, k, λ)-difference set D with parameters

$$v = \frac{q^{d+1}-1}{q-1}, \quad k = \frac{q^d-1}{q-1} \text{ and } \lambda = \frac{q^{d-1}-1}{q-1}.$$

This is equivalent to the symmetric design of points and hyperplains in the projective d-space $PG(d, q)$ over $GF(q)$.

Let $q = 4n-1$ be a prime power. Then the set D of nonzero squares in F_q is a $(4n-1, 2n-1, n-1)$-difference set in the additive group of F_q.

[Generalized McFarland's Difference Sets by Dillon] Let G be a group of order $q^{d+1}(q^d + \ldots + q^2 + q + 2)$ which contains elementary abelian normal subgroup E of order q^{d+1}. For $r = q^d + \ldots + q^2 + q$, let $H_0, \ldots, H_r$ be the hyperplanes of E (i.e., the subgroups of order q^d), and let $g_0, \ldots, g_{r+1}$ be a system of coset representatives of E in G. Then the subset

$$D = g_0 H_0 + \ldots + g_r H_r$$

of G is a difference set with parameters

$$v = q^{d+1}(q^d + \ldots + q^2 + q + 2),\ k = q^d(q^d + \ldots + q + 1),\ \lambda = q^d(q^{d-1} + \ldots + q + 1).$$

Following two nonexistence theorems are due to Turyn (see Turyn [31], Lander [22]).

Theorem 6 *Let D be an abelian (v, k, λ)-difference set in G, and let p be a prime with $p|v$, $p|n$ and self-conjugate mod $exp(G)$. Then the p-Sylow subgroup of G is not cyclic.*

Theorem 7 *Let D be an abelian (v, k, λ)-difference set in G, let H be a subgroup of G of order s and index u. Assume the existence of a positive integer m with $m^2|n$, $(m, u) \neq 1$ which is self-conjugate mod $exp(G/H)$. If the p-Sylow subgroup of G/H is cyclic for every prime p with $p|m, p|u$, then*

$$m \leq 2^{r-1}s, \text{ where } r \text{ is the number of distinct primes dividing } (m, u).$$

By the way, from these nonexistence theorems and known difference sets, Ryser and Lander suggested the following conjectures.

[Ryser's Conjecture] There is no cyclic (v, k, λ)-difference set with $(v, n) \neq 1$.

[Lander's Conjecture] Assume that there exists an abelian (v, k, λ)-difference set in G. If p is a prime with $p|v$, $p|n$, then p-Sylow subgroup of G is not cyclic.

In particular, these conjectures contain the following famous conjecture.

[Circulant Hadamard Conjecture] There exists no circulant Hadamard matrix of order $m > 4$. This is equivalent to that there is no cyclic $(4u^2, 2u^2 - u, u^2 - u)$-difference set with $u > 1$.

2 Foldings of Difference Sets

Let G, G' be finite groups of the form $G = Z_{p^m} \times H$, $G' = U \times H$ where p is a prime, H is an abelian group with $p^2 \exp H$, and U is any abelian group of order p^m. We exhibit a family of bijections $G \to G'$ which – extended to bijections $ZG \to ZG'$ of the integral group rings – under some conditions preserve the character values of group ring elements up to roots of unity. We get similar results for related combinatorial structures like relative difference sets, building sets and group invariant weighing matrices. The results can be generalized to cases where H is nonabelian.

The content of this chapter has appeared in [16].

2.1 Introduction

The main aim of this chapter is the study of the *problem of switching groups* for various types of difference sets and related structures. That is, for groups G, H of the same order, we ask whether we can find bijections between G and H preserving certain combinatorial properties of group ring elements like being a difference set. The main motivation is to gain more insight into the existence of these combinatorial objects. If we can find bijections which work for many H, then the construction of a single difference set, for instance, solves the existence problem for difference sets in many groups simultaneously.

There are some known bijections between nonisomorphic groups preserving difference sets.

[Dillon, see [4]] Let D be a $(n^2+n+1, n+1, 1)$-difference set in $G = Z_v$ with $v = n^2+n+1$, $n \equiv 1 \bmod 3$. (It always exists when v is a prime power.) Then we can write $G = Z_3 \times Z_w =< a > \times < b >$ for $w = v/3$ since $3||v$. Let

$$H :=< x, b | x^3 = b^w = 1, x^{-1}bx = b^n >,$$

$$f : G \to H \text{ with } f(a^i b^j) = x^i b^j \text{ for all } i, j.$$

Then $f(D)$ is a $(n^2+n+1, n+1, 1)$-difference set in H.

We also use a bijection from generalized quaternion groups to abelian groups in the previous chapter.

However, these two constructions only work for very special types of groups. The aim of this chapter is to find bijections preserving difference sets for more general groups.

But when we try to find such bijections for general groups, we have some troubles:

1) Difference sets with Singer parameters (see [29, 4]) exist in cyclic groups, but in many cases it can be shown that they do not exist in any other abelian groups of the same order. So, bijections from G to H where H has lower exponent (and higher rank) than G cannot work in general.

2) Turyn, Davis and Kraemer [31, 9, 21] proved that an abelian 2-group G of order 2^{2d} has a difference set if and only if $\exp G \leq 2^{d+1}$. So bijections from G to H where H has higher exponent, also cannot work in general.

3) Arasu, Davis, Jedwab, and Sehgal [2, 3] proved that an Hadamard difference set in $Z_2 \times Z_2 \times Z_{3^a} \times K$ with K abelian, $|K| = 3^a$, exists if and only if K is cyclic. So bijections from G to H with $\exp H = \exp G$, rank $H >$ rank G also cannot work in general.

However, we can still exhibit that quite general difference sets are preserved by some bijections given by using appropriate lexicographic orderings together with some nonhomomorphic permutations.

Let $G = C \times K$, $H = U \times K$ be finite groups where C is a cyclic p-group, U is any abelian group with $|U| = |C|$, and K is any finite abelian group such that $p^2 \nmid w := \exp H$. Using a lexicographic ordering of U, we define a bijection $f : ZG \to ZH$ which we call a *folding*. We

will show that for any difference set D in G such that $\chi(D)u_\chi \in Q[\xi_p, \xi_w]$ for every character χ of G and for some root of unity u_χ, the folding $f(D)$ of D is also a difference set in H. We get similar results for several other combinatorial structures which can be described by group ring equations. It is interesting to note that the "small field condition", i.e., $\chi(D)u_\chi \in Q[\xi_p, \xi_w]$, is often satisfied automatically by a consequence of [28, Thm. 3.5] which we will state as Theorem 11 .

2.2 Preliminaries

Let $m > 1$ be an integer, and let p be a prime. For any partition $(r_1, r_2, \ldots, r_s)$ of m, we define the lexicographic order on $[p^{r_1}] \times [p^{r_2}] \ldots \times [p^{r_s}]$ by

$$(b_1, b_2, \ldots, b_s) > (b'_1, b'_2, \ldots, b'_s) \Longleftrightarrow b_t > b'_t \text{ for } t = \min\{i | b_i \neq b'_i\}.$$

Using this ordering of U, we can define a bijective map naturally:

$$f : K := Z/p^m Z \longrightarrow K' := Z/p^{r_1} Z \times Z/p^{r_2} Z \times \ldots \times Z/p^{r_s} Z$$

sending the element i of $K = [p^m]$ to the i-th element of $K' = [p^{r_1}] \times [p^{r_2}] \ldots \times [p^{r_s}]$. We call f the *folding map* from K to K'.

We extend f to a bijection between $G = K \times H$ and $G' = K' \times H$ for any group H by setting $f((x, y)) = (f(x), y)$. This map is also denoted by f and called the folding map from G to G'. For $T = \sum_{g \in K} H_g g \in ZG$ with $H_g \in ZH$, we define the folding $f(T) \in ZG'$ by

$$f(T) := \sum_{k \in K'} H_{f^{-1}(k)} k.$$

We say $f(T)$ is the *folding* of T. Note that $f^{-1}(b_1, \ldots, b_s) = \sum_{i=1}^{s} b_i p^{\sum_{j=i+1}^{s} r_j}$.

Write $K = Z/p^m Z = \langle g \rangle$, $K' = Z/p^{r_1} Z \times \ldots \times Z/p^{r_s} Z = \langle g_1 \rangle \times \ldots \times \langle g_s \rangle$, $\eta = \xi_{p^m}$, $\eta_i = \xi_{p^{r_i}}$. The following correspondence between the absolutely irreducible representations of G and G' is essential in all our results on folding maps. For the background on representation theory, see [8].

Let $G = K \times H$ and $G' = K' \times H$ as above where H is any finite group. For $\psi \in K'^*$ with $\psi(g_1, \ldots, g_s) = \eta_1^{a_1} \eta_2^{a_2} \ldots \eta_s^{a_s}$, $0 \leq a_i < p^{r_i}$, we define the *character* $\omega_\psi \in K^*$ *corresponding to* ψ by $\omega_\psi(g) = \eta^t$ where $t = a_1 + a_2 p^{r_1} + a_3 p^{r_1 + r_2} + \ldots + a_s p^{r_1 + \ldots + r_{s-1}}$.

By Brauer's theorem [8, Thm. 41.1], $F := Q(\xi_{\exp G})$ is a splitting field for G as well as G'. Moreover, any irreducible FG' representation τ can be written as $\tau = \psi \otimes \varphi$ for a character ψ of K' and an irreducible FH representation φ. Then $\chi_\tau := \omega_\psi \otimes \varphi$ will be called the *FG representation corresponding to τ*. Note that τ and χ_τ are actually characters if H is abelian, so we speak of the *character χ_τ corresponding to τ* in this case.

2.3 The Folding Theorem

In this section, we prove that folding maps preserve the character values of certain group ring elements up to roots of unity. As a consequence, we will be able to show that some combinatorial properties of group ring elements like being a difference set, relative difference set, building set, or group weighing matrix are preserved under folding. We shall introduce these applications in Section 2.4.

Theorem 8 *Let $G = Z_{p^m} \times H$ where H is an abelian group and p^2 does not divide $\exp H$, $m \geq 2$. Let K be an abelian group of order p^m, and let $f : G \to G' = K \times H$ be the folding map. Let $T \in ZG$. Let $\tau \in G'^*$, and let $\chi_\tau \in G^*$ be the corresponding character of τ.*

If $\chi_\tau u \in Q[\xi_{\exp H}, \xi_p]$ for some root of unity u, then

$$\tau(f(T)) = \chi_\tau(T)u', \tag{2}$$

for some root of unity u'.

Proof. Write $K = Z_{p^{r_1}} \times \ldots \times Z_{p^{r_s}} = < g_1 > \times \ldots \times < g_s >$, let $f : G \to G' = K \times H$ be the folding map and let $\eta = \xi_{p^m}, \eta_i = \xi_{p^{r_s}}$. Let $T \in ZG$. All we have to prove is that for any $\tau \in K^*$, $\rho \in H^*$, if $\chi_\tau \otimes \rho(T)u \in Q[\xi_{\exp H}, \xi_p]$ for some root of unity u, then

$$\tau \otimes \rho(f(T)) = \chi_\tau \otimes \rho(T)u' \tag{3}$$

for some root of unity u' where $\chi_\tau \in Z_{p^m}^*$ is the character corresponding to τ. Since $\rho \in H^*$, and $p^2 \nmid \exp H$, for $\chi_\tau(g) = \eta^\beta$, we can write

$$\chi_\tau \otimes \rho(T) = \sum_{b \in [p^m]} d_b \cdot \eta^{\beta b}$$

with some $d_b \in Q[\xi_p, \xi_w]$, and for $\tau(g_1, \ldots, g_s) = \eta_1^{\beta_1} \ldots \eta_s^{\beta_s}$, we can write

$$\tau \otimes \rho(f(T)) \sum_{(b_1,\ldots,b_s)\in[p^{r_1}]\times\ldots\times[p^{r_s}]} d_{f^{-1}(b_1,\ldots,b_s)} \cdot \eta_1^{\beta_1 b_1} \eta_2^{\beta_2 b_2} \ldots \eta_s^{\beta_s \cdot b_s}.$$

Hence Theorem 8 follows from the next lemma.

Lemma 9 *Let $p^2 \nmid w$. For nonnegative integers β, β_i, let*

$$d(\beta) := \sum_{b\in[p^m]} d_b \cdot \eta^{\beta b},$$

$$d'(\beta_1, \ldots, \beta_s) := \sum_{(b_1,\ldots,b_s)\in[p^{r_1}]\times\ldots\times[p^{r_s}]} d_{f^{-1}(b_1,\ldots,b_s)} \cdot \eta_1^{\beta_1 b_1} \eta_2^{\beta_2 b_2} \ldots \eta_s^{\beta_s \cdot b_s},$$

where all $d_b \in Q[\xi_p, \xi_w]$. Suppose

$$d(p^i a)u \in Q[\xi_p, \xi_w]$$

for some root of unity u where $(p, a) = 1$. Then, for any $\beta_{j+1}, \ldots, \beta_s \in Z$, there is a root of unity $u' = u'(\beta_{j+1}, \ldots, \beta_s)$ such that

$$d'(0, \ldots, 0, p^e a, \beta_{j+1}, \ldots, \beta_s) = d(p^i a)u'$$

where $i = r_1 + r_2 + \ldots + r_{j-1} + e$ with $0 \le e < r_j$.

Proof. Note that $d'(0, \ldots, 0, p^e a, \beta_{j+1}, \ldots, \beta_s) = d'(0, \ldots, 0, p^e a + p^{r_j} t, \beta_{j+1}, \ldots, \beta_s)$ for any t since $\eta_j^{p^{r_j}} = 1$, i.e., $d'(\beta_1, \ldots, \beta_s) = d(f^{-1}(\beta_1, \ldots, \beta_s))u'$ for some root of unity u' for any $\beta_1, \ldots, \beta_s \in Z$. Let $\omega = \xi_p = \eta^{p^{m-1}} = \eta_i^{p^{m_i-1}}$. Now

$$d(p^i a)u = \sum_{b\in[p^{m-i-1}]} \sum_{t\in[p^{i+1}]} d_{b+tp^{m-i-1}} \cdot \omega^{at} \eta^{p^i a \cdot b} u \in Q[\omega, \xi_w].$$

But $\eta^{p^i a}, (\eta^{p^i a})^2, \ldots, (\eta^{p^i a})^{p^{m-i-1}-1}$ are independent over $Q[\omega, \xi_w]$. So, since $d_b \in Q[\omega, \xi_w]$, there is a unique $b = b_0$ such that

$$\sum_{t\in[p^{i+1}]} d_{b_0+tp^{m-i-1}} \cdot \omega^{at} u \in Q[\omega, \xi_w],$$

and all the other sums are 0. Define

$$\begin{aligned} d' &:= d'(0, \ldots, 0, p^e a, \beta_{j+1}, \ldots, \beta_s) \\ &= \sum_{(b_1,\ldots,b_s)\in[p^{r_1}]\times\ldots\times[p^{r_s}]} d_{f^{-1}(b_1,\ldots,b_s)} \cdot \eta_j^{p^e a \cdot b_j} \eta_{j+1}^{\beta_{j+1} \cdot b_{j+1}} \ldots \eta_s^{\beta_s \cdot b_s} \end{aligned}$$

and let

$$L := f^{-1}(0,\ldots,0,b_{j+1},\ldots,b_s) + b_1 \cdot p^{m-r_1} + \ldots + b_j \cdot p^{m-r_1-\ldots-r_j}.$$

Then we have

$$d' = \sum_{b'_j \in [p^{r_j-e-1}]} \sum_{b_1,\ldots,b_{j-1},b_{j+1},\ldots,b_s} \sum_{t\in[p^{e+1}]} d_{L+t\cdot p^{m-i-1}} \cdot \omega^{at} \eta_j^{p^e a\cdot b'_j} \eta_{j+1}^{\beta_{j+1}\cdot b_{j+1}} \ldots \eta_s^{\beta_s\cdot b_s},$$

because $(\eta_j^{p^e a})^{p^{r_j-e-1}} = \omega^a$ and $p^{r_j-e-1} \cdot p^{m-r_1-\ldots-r_j} = p^{m-i-1}$. Thus, if we fix $b'_j, b_{j+1}, \ldots, b_s$, the coefficient of $\eta_j^{p^e a\cdot b'_j} \eta_{j+1}^{\beta_{j+1}\cdot b_{j+1}} \ldots \eta_s^{\beta_s\cdot b_s}$ in d' is

$$\sum_{b_1,\ldots,b_{j-1}} \sum_{t\in[p^{e+1}]} d_{L+t\cdot p^{m-i-1}} \cdot \omega^{at}.$$

Putting

$$N := f^{-1}(0,\ldots,0,b_{j+1},\ldots,b_s) + b_j \cdot p^{m-r_1-r_2-\ldots-r_j},$$

we can write

$$\begin{aligned} L &= N + b_1 \cdot p^{m-r_1} + b_2 \cdot p^{m-r_1-r_2} + \ldots + b_{j-1} \cdot p^{m-r_1-r_2-\ldots-r_{j-1}} \\ &= N + k \cdot p^{e+1} \cdot p^{m-i-1} \end{aligned}$$

for some k. Since $\omega^p = 1$ and k runs through $[p^{r_1+\ldots+r_{j-1}}]$ when $b_1, \ldots, b_{j-1}$ run through all values, the above coefficient $\sum_{b_1,\ldots,b_{j-1}} \sum_{t\in[p^{e+1}]} d_{L+t\cdot p^{m-i-1}} \cdot \omega^{at}$ is

$$\sum_{k\in[p^{r_1+\ldots+r_{j-1}}]} \sum_{t\in[p^{e+1}]} d_{N+(k\cdot p^{e+1}+t)p^{m-i-1}} \cdot \omega^{at}$$

$$\begin{aligned} &= \sum_{t\in[p^{r_1+\ldots+r_{j-1}+e+1}]} d_{N+t\cdot p^{m-i-1}} \cdot \omega^{at} \\ &= \sum_{t\in[p^{i+1}]} d_{N+t\cdot p^{m-i-1}} \cdot \omega^{at}. \end{aligned}$$

If $b_j, \ldots, b_s$ run through all values, $N = f^{-1}(0,\ldots,0,b_{j+1},\ldots,b_s) + b_j \cdot p^{m-r_1-\ldots-r_j}$ runs through all of $[p^{m-i-1}]$. So the coefficients occurring in d' coincide with the coefficients of $d(p^i a)$. Thus, with at most one exception, for each $(s-j+1)$-tuple $(b_j, \ldots, b_s)$, the coefficient occurring in d' is 0, and the only putative nonzero coefficient is

$$\sum_{t\in[p^{i+1}]} d_{b_0+tp^{m-i-1}},$$

i.e., $d' = d(p^i a)u'$ for some root of unity u'. □

For the sake of completeness, we mention that the folding theorem can be generalized to the case where H is nonabelian. The proof of the following theorem is a straightforward adaptation of the proof of Theorem 8 and will be omitted.

Theorem 10 *Let $G = Z_{p^m} \times H$ where H is a (possibly nonabelian) group and p^2 does not divide $\exp H$. Let K be an abelian group of order p^m, and let $f : G \to G' = K \times H$ be the folding map. Let $F := Q(\xi_{\exp G})$, let τ be an irreducible FG' matrix representation, and let χ_τ be the corresponding FG representation. If, for some $T \in ZG$, the matrix $\chi_\tau(T)u$ has entries in $Q[\xi_{\exp H}, \xi_p]$ only for some root of unity u, then*

$$\tau(f(T)) = \chi_\tau(T)u', \tag{4}$$

for some root of unity u'.

In the abelian case, the basic assumption necessary to make folding work is that the character values of the group ring element we want to fold up to a root of unity lie in a rather small field. For the combinatorial applications we have in mind, the character values will be cyclotomic integers of prescribed absolute value. From the following consequence of [28, Theorem 3.5] we see that the "small field assumption" is satisfied *automatically* in many cases.

Theorem 11 ([28]) *Assume $X\overline{X} = n$ for $X \in Z[\xi_m]$ where n and m are positive integers, $m = p^a m'$, $(p, m') = 1$, and p is an odd prime. Let $\mathcal{P}$ be the set of prime divisors of m. For each prime divisor q of n define $m_q := \prod_{r \in \mathcal{P} \setminus \{q\}} r$. Consider the following assumption.*

$$A(m,n,p): \quad q^{\mathrm{ord}_{m_q}(q)} \not\equiv 1 \bmod p^2 \text{ for all prime divisors } q \neq p \text{ of } n.$$

If $A(m,n,p)$ holds, then

$$X\xi_m^j \in Z[\xi_{pm'}] \tag{5}$$

for some j. In particular, (5) always holds if n is a power of p.

2.4 Applications

In this final section, we present some applications of the folding and permutation theorems to difference sets, relative difference sets, building sets, and group invariant weighing matrices. We give the details for the nonabelian case only for difference sets. The other applications of the folding theorem have similar nonabelian generalizations.

Difference Sets

We begin with an application of the folding theorem to difference sets.

Theorem 12 *Let $G = Z_{p^m} \times H$ be an abelian group of order v such that $p^2 w := \exp H$. Suppose there is a (v, k, λ)-difference set D of order n in G such that $\chi(D)u_\chi \in Q[\xi_p, \xi_w]$ for any $\chi \in G^*$ for some root of unity u_χ. Then for any partition $(r_1, r_2, \ldots, r_s)$ of m, the folding $f(D)$ of D is a (v, k, λ)-difference set in $G' = Z_{p^{r_1}} \times Z_{p^{r_2}} \times \ldots \times Z_{p^{r_s}} \times H$.*

Proof. For any character $\tau \neq id$ of G', we have $\tau(f(D)) = \chi_\tau(D)u_\tau$ for some root of unity u_τ by Theorem 8. Then,

$$\tau(f(D))\overline{\tau(f(D))} = \chi_\tau(D)u_\tau\overline{\chi_\tau(D)}\overline{u_\tau} = \chi_\tau(D)\overline{\chi_\tau(D)} = n$$

concluding the proof. □

Remark 13 By applying Theorem 12 to the *known* families of difference sets, we do not obtain the existence of difference sets in any groups which previously had not been known to contain difference sets. However, we believe that Theorem 12 is important for the understanding of the phenomenon that difference sets with $(v, n) > 1$ seem to "prefer" groups of low exponent and high rank. Also, Theorem 12 certainly is of interest for the study of putative new families of difference sets and Lander's conjecture, see Corollary 16.

The following result is useful.

Cororally 14 *Let $G = Z_{p^m} \times H$ be an abelian group with $p^2 \exp H$. Suppose that there is a (v, k, λ)-difference set in G such that n is self-conjugate mod $exp(H)$. Then there is a (v, k, λ)-difference set in $U \times H$ for any abelian group U of order p^m.*

Combining Theorem 12 with Theorem 11 we get the following result.

Cororally 15 *Let $G = Z_{p^m} \times H$ be an abelian group where p is an odd prime and $p^2 \exp H$. Suppose there is a (v, k, λ)-difference set of order n in G and that the assumption $A(\exp G, n, p)$ of Theorem 11 holds. Then there is a (v, k, λ, n)-difference set in $U \times H$ for any abelian group U of order p^m.*

An important unsolved conjecture of Lander [22] asserts that the Sylow p-subgroup of an abelian group containing a (v, k, λ, n)-difference set with $p|(v, n)$ cannot be cyclic. In view of Lander's conjecture, the following special case of Corollary 15 is of particular interest. Note that in this situation, folding works without any assumptions besides the existence of a difference set.

Cororally 16 *Let $G = Z_{p^m} \times H$ be an abelian group where p is an odd prime and $(p, |H|) = 1$. If there is a (v, k, λ, n)-difference set in G and n is a power of p, then there is a (v, k, λ, n)-difference set in $U \times H$ for any abelian group U of order p^m.*

Now we are going to describe the nonabelian version of Theorem 12. We encounter slight technical difficulties here, since, for an arbitrary nonlinear matrix representation ρ of a group G and $D \in ZG$, the matrix $\rho(D^{(-1)})$ is slightly more difficult to obtain from $\rho(D)$ than in the linear case where just $\rho(D^{(-1)}) = \overline{\rho(D)}$. However, the following lemma is enough to escape all trouble.

Lemma 17 *Let H be a finite group, let F be a subfield of the complex numbers, and let ρ be an FH matrix representation. Then*

$$\rho(h^{-1}) = E^{-1}\, \overline{\rho(h)}^t E \tag{6}$$

for all $h \in H$ where $E = \sum_{g \in H} \overline{\rho(g)}^t \rho(g)$.

Proof. Note that E is nonsingular since it is a positive hermitian matrix. Thus (6) follows from

$$\overline{\rho(h)}^t E \rho(h) = \sum_{g \in H} \overline{\rho(gh)}^t \rho(gh) = E. \square$$

Theorem 18 *Let $G = Z_{p^m} \times H$ where p is a prime, and H is a (possibly nonabelian) group with $p^2 \exp H$. Let $F := Q(\xi_{\exp H})$, and let T be any complete set of nonequivalent irreducible FH matrix representations. Let D be a (v, k, λ, n)-difference set in G. Suppose that, for any $\omega \in Z_{p^m}^*$ and $\varphi \in T$, there is a root of unity $u(\omega, \varphi)$ such that all entries of the matrix $u(\omega, \varphi)[\omega \otimes \varphi(D)]$ lie in $Q(\xi_p, \xi_{\exp H})$. Then, for any partition $(r_1, r_2, \ldots, r_s)$ of m, the folding $f(D)$ is a (v, k, λ, n)-difference set in $G' = K \times H$ where $K = Z_{p^{r_1}} \times Z_{p^{r_2}} \times \ldots \times Z_{p^{r_s}}$.*

Proof. By a standard result on difference sets (see [25], for instance), it suffices to show

$$\tau(f(D))\tau(f(D)^{(-1)}) = nI$$

for every nontrivial irreducible FG' representation τ. Here I is an identity matrix of the appropriate size. Note that any such representation τ is equivalent to a representation of the form $\psi \otimes \varphi$ where $\psi \in K^*$ and $\varphi \in T$. Now, by Theorem 10, we have

$$\psi \otimes \varphi(f(D)) = u\ \omega_\psi \otimes \varphi(D) \tag{7}$$

for some root of unity u. Since D is a (v, k, λ, n)-difference set in G, we know that

$$[\omega_\psi \otimes \varphi(D)][\omega_\psi \otimes \varphi(D^{(-1)})] = nI. \tag{8}$$

From (6) we get

$$\begin{aligned} \psi \otimes \varphi(X^{(-1)}) &= \sum_{x \in X} \psi(x^{-1})\varphi(x^{-1}) \\ &= \sum_{x \in X} \overline{\psi(x)}\ E^{-1}\overline{\varphi(x)}^t\ E \\ &= E^{-1}\ [\overline{\psi \otimes \varphi(X)}^t]\ E \end{aligned}$$

for any $X \subset G'$ and similarly

$$\omega_\psi \otimes \varphi(Y^{(-1)}) = E^{-1}\ [\overline{\omega_\psi \otimes \varphi(Y)}^t]\ E$$

for any $Y \subset G$. Thus, using (7), (8) and $u\overline{u} = 1$,

$$\begin{aligned} [\psi \otimes \varphi(f(D))][\psi \otimes \varphi(f(D)^{(-1)})] &= [\psi \otimes \varphi(f(D))]\ E^{-1}\ [\overline{\psi \otimes \varphi(f(D))}]^t\ E \\ &= [u\ \omega_\psi \otimes \varphi(D)]E^{-1}\ [\overline{u\ \omega_\psi \otimes \varphi(D)}]^t\ E \\ &= [\omega_\psi \otimes \varphi(D)][\omega_\psi \otimes \varphi(D^{(-1)})] \\ &= nI \end{aligned}$$

concluding the proof. □

Remark 19 *The small field conditions or the assumption that n is self-conjugate mod exp(G) in the theorems cannot be dropped. In fact, there is a* $(40, 13, 4)$*-difference set in the cyclic group of order* 40 *(see [17] Example 1,1 PG(3,3)), while there is no* $(40, 13, 4)$*-difference set in either* $Z_4 \times Z_2 \times Z_5$ *or* $Z_2 \times Z_2 \times Z_2 \times Z_5$ *(see [17] Example 7,2). Note that* 3 *is not self-conjugate mod* 40.

Remark 20 *In general, the designs generated by a difference set and by the folded difference set are not isomorphic.*

For example, let $G = Z_4 \times Z_3 \times Z_3 =< a > \times < b > \times < c >$ *and* $G' = Z_2 \times Z_2 \times Z_3 \times Z_3$. *Then*

$$D = \{a, a^2, a^3, c, ac, bc, a^2bc, b^2c, a^3b^2c, c^2, ac^2, bc^2, a^3bc^2, b^2c^2, a^2b^2c^2\}$$

is a $(36, 15, 6)$*-difference set of* G *and the designs generated by* D *and its folding to* G' *are not isomorphic.*

On the other hand, let $G = Z_8 \times Z_2 =< a > \times < b >$ *and* $D = \{1, a, a^2, a^5, b, ba^6\}$. *Then* D *is a* $(16, 6, 2)$*-difference set in* G, *and the designs generated by* D *and its foldings to* $Z_4 \times Z_2 \times Z_2$ *and to* $Z_2 \times Z_2 \times Z_2 \times Z_2$ *are all isomorphic.*

Relative Difference Sets

Let G be a group of order mn with a normal subgroup N of order n. A k-subset D of G is called an (m, n, k, λ)*-relative difference set relative to* N if the list of quotients xy^{-1}, $x, y \in D$, contains each element of $G \setminus N$ exactly λ times and contains no nonidentity element of N. In terms of the group ring, a k-subset D of G is a (m, n, k, λ)-difference set in G if and only if

$$DD^{(-1)} = k \cdot 1 + \lambda(G \setminus N)$$

in ZG where 1 is the identity element of G. This is equivalent to

$$\chi(D)\overline{\chi(D)} = \begin{cases} k + \lambda(mn - n) & \text{for } \chi = \chi_0 \\ k - \lambda n & \text{for } \chi|_N = id, \chi \neq \chi_0 \\ k & \text{for } \chi|_N \neq id \end{cases}$$

The proof for the folding of relative difference sets is slightly more difficult than for difference sets because of the special role of the forbidden subgroup N. But in this case, the explicit correspondence of characters gets us out of trouble.

Theorem 21 *Let $G = Z_{p^l} \times H$ be an abelian group such that $p^2 w = \exp H$, $l > 1$. Suppose D is a (m, n, k, λ)-relative difference set in G such that for any χ of G, $\chi(D)u_\chi \in Z[\xi_p, \xi_w]$ for a root of unity u_χ. Then for any partition $(r_1, r_2, \ldots, r_s)$ of l, the folding $D' = f(D)$ of D is a (m, n, k, λ)-relative difference set in $G' = Z_{p^{r_1}} \times Z_{p^{r_2}} \times \ldots \times Z_{p^{r_s}} \times H$.*

Proof. Since $DD^{(-1)} = k + \lambda(G \setminus N)$ for some $N \leq G$ of order n, we have $\chi_0(D)\overline{\chi_0(D)} = k + \lambda(mn - n)$, $\chi(D)\overline{\chi(D)} = k - \lambda n$ for $\chi|_N = id, \chi \neq \chi_0$ and $\chi(D)\overline{\chi(D)} = k$ for $\chi|_N \neq id$. Let $G = Z_{p^l} \times H = \langle g \rangle \times H$, $G' = Z_{p^{r_1}} \times \ldots \times Z_{p^{r_s}} \times H = \langle g_1 \rangle \times \ldots \times \langle g_s \rangle \times H$. Let $\eta = \xi_{p^l}$, $\eta_i = \xi_{p^{r_i}}$. We have $\tau(D')\overline{\tau(D')} = \chi_\tau(D)\overline{\chi_\tau(D)}$ by Theorem 8. And we see that for any $\alpha \in Z_{p^l}$,

(1) if $\chi(\alpha) = 1$ then $\tau_\chi(f(\alpha)) = 1$,

(2) if $\chi(\alpha) = \xi_p$ then $\tau_\chi(f(\alpha)) = \xi_p$.

Thus, for any $x \in G$, if $\chi(x) = 1$, then $\tau_\chi(f(x)) = 1$ since $\chi(h), \tau(h) \in Z[\xi_p, \xi_{\exp H}]$ for any χ of G, τ of G', $h \in H$. Let $N' = f(N)$. Then N' is a subgroup in G' of order n, and we see that $\chi_\tau|_N = id$ if and only if $\tau|_{N'} = id$ for any τ of G'.

Claim: $D'D'^{(-1)} = k + \lambda(G' \setminus N')$.

Proof of the claim:

Case 1: $\tau = \tau_0 = id$. Then $\tau_0(D')\overline{\tau_0(D')} = k + \lambda(mn - n)$.

Case 2: $\tau|_{N'} = id, \tau \neq \tau_0$. Then, since $\chi_\tau|_N = id, \chi_\tau \neq \chi_0$, we have $\tau(D')\overline{\tau(D')} = k - \lambda n$.

Case 3: $\tau|_{N'} \neq id$. Then, since $\chi_\tau|_N \neq id$, we have $\tau(D')\overline{\tau(D')} = k$.

This proves the claim and hence the theorem. □

Building Sets

Davis and Jedwab [10] introduced building sets and covering extended building sets (CEBSs) as a powerful tool for the construction of difference sets. In this section, we apply the folding method to CEBSs. Similar results also can be obtained for all other types of building sets.

An $(a, m, h, \pm)$-*covering extended building set* (CEBS) in an abelian group G is a family $\{D_1, \ldots, D_h\}$ of subsets of G with the following properties.

1) $|D_1| = a \pm m$ and $|D_i| = a$ for $i = 2, \ldots, h$.

2) For every nonprincipal character χ of G there is exactly one i with $|\chi(D_i)| = m$ and $\chi(D_j) = 0$ if $j \neq i$.

As was shown in [10], a CEBS in G can be used to construct difference sets in many abelian groups which contain G as a subgroup.

Theorem 22 *Let $G = Z_{p^l} \times H$ be an abelian group such that $p^2 \nmid w = \exp H$, $l > 1$. Suppose $\{D_1, \ldots, D_h\}$ is an $(a, m, h, \pm)$ covering EBS in G such that for any χ of G, $\chi(D)u_\chi \in Z[\xi_p, \xi_w]$ for a root of unity u_χ.*

Then for any partition $(r_1, r_2, \ldots, r_s)$ of l, the folding $\{f(D_1), \ldots, f(D_h)\}$ of $\{D_1, \ldots, D_h\}$ is also an $(a, m, h, \pm)$ covering EBS in $G' = Z_{p^{r_1}} \times Z_{p^{r_2}} \times \ldots \times Z_{p^{r_s}} \times H$.

Proof. 1) Since f is a bijection, we have $|f(D_1)| = |D_1| = a \pm m$ and $|f(D_i)| = |D_i| = a$ for $i = 2, \ldots, h$.

2) For every nonprincipal character τ of G', we have $\tau(f(D_i)) = \chi_\tau(D_i)$ from Theorem 8. Thus we see that there is exactly one i with $|\tau(f(D_i))| = |\chi_\tau(D_i)| = m$ and $|\tau(f(D_j))| = |\chi_\tau(D_j)| = 0$ if $j \neq i$. □

Group Invariant Weighing Matrices

A *weighing matrix* $W(m, n)$ is an $m \times m$ matrix H with entries $-1, 0, 1$ such that $HH^t = nI$ where I is the identity matrix. The integer n is called the *weight* of H. Weighing matrices have been studied intensively, see [14] for a survey and [6, 7, 15] for some more recent results. The proofs of the following results on weighing matrices are similar to those of the previous sections and will be omitted. Let G be a group of order m. We say that a matrix $H = (h_{f,g})_{f,g \in G}$ is *G-invariant* if $h_{fk,gk} = h_{f,g}$ for all $k \in G$. If we identify a G-invariant weighing matrix H with the element $\sum_{g \in G} h_{1,g} g$ of ZG we get the following useful criterion, see [28], for example.

Lemma 23 *Let G be an abelian group of order m, and let H be a G-invariant $m \times m$ matrix with entries $-1, 0, 1$. Then H is a weighing matrix $W(m, n)$ if and only if*

$$\chi(H)\overline{\chi(H)} = n$$

for all characters χ of G where H is viewed as an element of ZG.

Theorem 24 *Let $G = Z_{p^l} \times K$ be an abelian group such that $p^2 w = \exp K$, $l > 1$. Suppose H is a G-invariant weighing matrix such that for any χ of G, $\chi(H)u_\chi \in Z[\xi_p, \xi_w]$ for a root of unity u_χ. Then for any partition $(r_1, r_2, \ldots, r_s)$ of l, the folding $H' = f(H)$ of H is a G'-invariant weighing matrix where $G' = Z_{p^{r_1}} \times Z_{p^{r_2}} \times \ldots \times Z_{p^{r_s}} \times K$.*

参考文献

[1] Arasu,K.T., Davis,J.A., Jedwab,J., Ma,S.L., and McFarland,R.L.: Exponent bounds for a family of abelian difference sets, *in* "Groups, Difference Sets, and the Monster" Edited by K.T.Arasu, J.F.Dillon, K.Harada, S.K.Sehgal, R.L.Solomon, DeGruyter Verlag, Berlin, New York, (1996),129-143.

[2] Arasu, K. T., Davis, J. A., Jedwab, J., Sehgal, S. K.: New constructions of Menon difference sets. *J. Comb. Theory A* **64** (1993), 329-336.

[3] Arasu, K. T., Davis, J. A., Jedwab, J.: A nonexistence result for abelian Menon difference sets using perfect binary arrays. *Combinatorica* **15** (1995), 311-317.

[4] Beth, T., Jungnickel, D., Lenz, H.: *Design theory* (2nd edition). Cambridge University Press (in press).

[5] Bruck, R.H.: Difference sets in a finite group. *Trans. Amer. Math. Soc.* **78** (1955), 464-481.

[6] Craigen, R.: The structure of weighing matrices having large weights. *Designs, Codes and Cryptography* **5** (1995), 199-216.

[7] Craigen, R., Kharaghani, H.: Hadamard matrices from weighing matrices via signed groups. *Designs, Codes and Cryptography* **12** (1997), 49-58.

[8] Curtis, C.W., Reiner, I.: *Representation theory of finite groups and associative algebras.* Wiley Classics Library. Wiley, New York, 1988.

[9] Davis,J.A: Difference sets in abelian 2-groups. *J. Comb. Theory A* **57** (1991), 262-286.

[10] Davis, J.A., Jedwab, J.: A unifying construction of difference sets. *J. Combin. Theory A* **80** (1997), 13-78.

[11] Dillon,J.F.: Variations on a scheme of McFarland for noncyclic difference sets, *J.Combin.Theory ser.A* **40**(1985), 9-21.

[12] Enomoto,H., Hagita,M., Matsumoto,M.: A note on difference sets, *J.Combin.Theory ser.A* **84**(1998), 133-144.

[13] Fan,C.T., Siu,M.K., Ma,S.L.: Difference sets in dihedral groups and interlocking difference sets, *Ars.Combin.* **20A**(1985), 99-107.

[14] Geramita, A.V., Seberry, J.: Orthogonal designs III. Weighing matrices. *Utilitas Math.* **6** (1974), 209-236.

[15] Gysin, M., Seberry, J: On the weighing matrices of order $4n$ and weight $4n-2$ and $2n-1$. *Australas. J. Combin.* **12** (1995), 157-174.

[16] Hagita,M.: Foldings of difference sets in abelian groups. *Graphs and Combinatorics* **15**(1999), 187-193.

[17] Jungnickel,D.: Difference sets, *in* " Contemporary Design Theory: A Collection of Surveys, " Edited by Jeffrey H.Dinitz and Douglas R.Stinson, (1992),241-324.

[18] Jungnickel, D., Schmidt, B.: Difference sets: An update. In: *Geometry, combinatorial designs and related structures* (Eds. J.W.P. Hirschfeld, S.S. Magliveras and M.J. de Resmini). Cambridge University Press, 1997, 89-112.

[19] Jungnickel, J., Schmidt, B.: Difference Sets: A Second Update. *Rend. Circ. Palermo Serie II, Suppl.* **53** (1998), 89-118.

[20] Kibler, R.E.: A summary of noncyclic difference sets, $k < 20$, *J.Combin.Theory ser.A* **25**(1978), 62-67.

[21] Kraemer, R.G.: Proof of a conjecture on Hadamard 2-groups. *J. Comb. Theory A* **63** (1993), 1-10.

[22] Lander,E.S.: "Symmetric Designs: An Algebraic Approach," London Math. Soc. Lecture Note Series 74, Cambridge Univ. Press, Cambridge,1983.

[23] Lang,S.: " Algebraic Number Theory," Addison-Wesley Series in Mathematics, 1970.

[24] Leung,K.H., Ma,S.L., Wong,V.L.: Difference sets in dihedral groups, *Designs, Codes and Cryptography* **1**(1991), 333-338.

[25] Liebler,R.: On difference sets in certain 2-groups, *in* "Coding Theory, Design Theory, Group Theory," Proceedings of the Marshall Hall Conference, ed. by D.Jungnickel, Jphn Wiley and Sons, 1993.

[26] Ma,S.L.: Polynomial addition sets and polynomial digraphs, *Linear Algebra and its Applications* **69**(1985),213-230.

[27] McFarland,R.L.: A family of difference sets in noncyclic groups. *J.Combin.Theory* A **15**(1973),1-10.

[28] Schmidt, B.: Cyclotomic integers and finite geometry. *J. Amer. Math. Soc.*, to appear.

[29] Singer, J.: A theorem in finite projective geometry and some applications to number theory. *Trans. Amer. Math. Soc.* **43**(1938), 377-385.

[30] Smith,K.W.: Nonabelian Hadamard difference sets. *J.Combin.Theory ser.A* **70**(1995), 144-156.

[31] Turyn,R.J.: Character sums and difference sets, *Pacific J.Math.* **15**(1965),319-346.