数理解析研究所講究録
1109 巻 1999 年 201-211

Folding maps in group rings

Mariko Hagita
Department of Mathematics, Keio University

Bernhard Schmidt
California Institute of Technology

Abstract

Let G, H be finite groups of the form $G = C \times H$, $G' = U \times H$ where C is a a cyclic p-group, U is any abelian group with $|U| = |C|$, and H is any finite abelian group. Using a lexicographic ordering of U, we define a bijection $f : ZG \to ZG'$ which we call a folding. We show that $X \in ZG$ and $f(X) \in ZG'$ up to roots of unity have the same character values provided that $p^2 \not| \exp H$ and the character values of X up to roots of unity lie in $Q(\xi_p, \xi_{\exp H})$. The main consequence is that folding preserves combinatorial properties like being a difference set, relative difference set, building set, or a group invariant weighing matrix. The results can be generalized to cases where H is nonabelian.

1 Introduction

In this paper, we study the *problem of switching groups* for various types of difference sets and related structures. That is, for nonisomorphic groups G, H of the same order, we ask whether we can find bijections between G and H preserving certain combinatorial properties 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 preserving difference sets. For example, Dillon ([17], [3]) found such a bijection from generalized dihedral groups to abelian groups and Bruck ([4]) constructs nonabelian projective planes by finding bijections from cyclic groups to nonabelian groups preserving the difference set property. However, these two constructions only work for very special types of groups. The aim of this paper is to find bijections preserving difference sets for more general groups. But when we try to find such bijections for general groups, we meet with some at first sight discouraging facts:

1) Difference sets with Singer parameters ([20], [17], [3]) exist in cyclic groups, but in many cases it can be shown that they don 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/Kraemer ([21], [8], [16]) proved that an abelian 2-group G of order 2^{2d} has a difference set if and only if $expG \leq 2^{d+1}$. So bijections from G to H where H has higher

exponent, also cannot work in general.
3) Arasu/Davis/Jedwab/Sehgal ([1], [2]) 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 $expH = expG$, $rankH > rankG$ also cannot work in general.

However, we still will be able to exhibit quite general difference set preserving bijections by using an appropriate lexicographic ordering. Let us recall some basics on difference sets in order to explain the main results of this paper.

A k-subset D of an abelian group G of order v is called a (v, k, λ)*-difference set* of G if the list of $xy^{-1}(x, y \in D)$ contains each nonidentity element of G exactly λ times. We call $n := k - \lambda$ the *order* of D.

In the group ring ZG, a subset S of G is identified with $\sum_{s \in S} s$. Also, $\sum_{s \in S} s^t$ is denoted by $S^{(t)}$. 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 in G if and only if

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

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

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

where $\bar{a}$ is the complex conjugate of a.

Let $G = C \times K$, $H = U \times K$ be finite groups where C is a a cyclic p-group, U is any abelian group with $|U| = |C|$, and H is any finite abelian group such that $p^2 \not| w := \exp H$. Using a lexicographic ordering of U, we define a bijection $f : ZG \rightarrow ZH$ 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 like (1). Finally, we note that the "small field condition", i.e., $\chi(D)u_\chi \in Q[\xi_p, \xi_w]$, is often satisfied automatically by a theorem of [19] which we will state in Section 3,5 .

2 Preliminaries

We write ξ_t for a primitive complex t-th root of unity, $[k]$ for the set $\{0, 1, \ldots, k-1\}$, and G^* for the character group of an abelian group G. 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 $m > 1$ 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 $f^{-1}(b_1,\dots,b_s) = \sum_{i=1}^{s} b_i p^{\sum_{j=i+1}^{s} r_j}$.

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 all our results on folding maps. For the background on representation theory, see [7].

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

By Brauer's theorem [7, Thm. 41.1], $F := Q(\xi_{\exp G})$ is a splitting field for $G$ as well as G'. Moreover, any irreducible FG' representation $\tau$ can be written as $\tau = \psi \otimes \varphi$ for a character $\psi$ of K' and an irreducible $FH$ representation $\varphi$. Then $\chi_\tau := \omega_\psi \otimes \varphi$ will be called the *FG representation corresponding to* $\tau$. Note that $\tau$ and χ_τ are actually characters if $H$ is abelian, so we speak of the *character* χ_τ *corresponding to* $\tau$ in this case.

3 The Folding Theorem

In this section, we prove the main result of this paper which improves and generalizes a result of [12]. Our result will show that some combinatorial properties like being a difference set, relative difference set, building set, or group weighing matrix are preserved by folding maps. We shall introduce these applications in section 4.

Theorem 2 *Let $G = Z_{p^m} \times H$ where $H$ is an abelian group and p^2 does not divide $exp(H)$, $m \ge 2$. 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 $\tau$.*

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 proof 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 corresponding character of $\tau$.

Since $\rho \in H^*$, and $p^2 \not| exp(H)$, 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

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

Hence Theorem 2 follows from the next lemma.

Lemma 3 *Let $p^2 \not| w$. For non-negative 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 $0 \leq e < r_j$.

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 roots of unity u' for any $\beta_1, \ldots, \beta_s \in Z$.

Proof. 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 an 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.

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

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 $p^{r_j-e-1} \cdot p^{m-r_1-\ldots-r_j} := p^{m-i-1}$.

So if we fix $b'_j, b_{j+1},\ldots,b_s$, then the coefficient of $\eta_j^{p^e a\cdot b'_j} \eta_{j+1}^{\beta_{j+1}\cdot b_{j+1}} \ldots \eta_s^{\beta_s\cdot b_s}$ is

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

If we put

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

then 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 all over $[p^{r_1+\cdots+r_{j-1}}]$ 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

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

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 values of $[p^{m-i-1}]$.

So the coefficients correspond to the coefficients of $d(p^i a)$. Then except only one case, for any $(s-j+1)$-tuple $(b_j,\ldots,b_s)$, the coefficients are 0, and the non-zero cace 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 2 and will be omitted.

Theorem 4 *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 $f : G \rightarrow G' = K \times H$ be the folding map. Let $F := Q(\xi_{\exp G})$, let $\tau$ be an irreducible FG' matrix representation, and let χ_τ be the corresponding $FG$ representation, see Definition 1. 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'.

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 [19, Theorem 3.5] we see that the "small field assumption" is satisfied *automatically* in many cases.

Theorem 5 ([19]) *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.*

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

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

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

for some $j$. In particular, (5) <u>always</u> holds if $n$ is a power of $p$.

4 Applications

4.1 Difference sets

Theorem 6 *Let $G = Z_{p^m} \times H$ be an abelian group of order $v$ such that $p^2 \not| w := \exp H$. Suppose there is a $(v,k,\lambda)$-difference set $D$ in $G$ such that for any $\chi$ of $G$, $\chi(D)u_\chi \in Q[\xi_p, \xi_w]$ for a 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 $(v,k,\lambda)$-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 2. 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 7 By applying Theorem 6 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, wee believe that Theorem 6 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 6 certainly is of interest for the study of putative new families of difference sets and Lander's conjecture, see Corollary 9.

Combining Theorem 6 with Theorem 5 we get the following result.

Cororally 8 *Let $G = Z_{p^m} \times H$ be an abelian group of order v such that $p^2 \not| \exp H$, $p \neq 2$. Suppose there is a (v, k, λ, n)-difference set in G and that the assumption $A(\exp G, n, p)$ from Theorem 5 holds. Then there is a (v, k, λ)-difference set in $U \times H$ for any abelian group U of order p^m.*

An important unsolved conjecture of Lander [17] 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 8 is of particular interest. Note that in this situation, folding works without any assumptions besides the existence of a difference set.

Cororally 9 *Let $G = Z_{p^m} \times H$ be a abelian group where $(p, |H|) = 1$, $p \neq 2$. 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)-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 6. 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 10 *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

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

□

Theorem 11 *Let $G = Z_{p^m} \times H$ where p is a prime, and H is a (possibly nonabelian) group with $p^2 \not| \exp H$. 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 [?], 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 4 and Definition 1 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. □

4.2 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

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

Generally the proof for relative difference sets is more difficult than for difference sets because of the special role of N. But in this case, the correspondence for characters guarantees the same property.

Theorem 12 *Let $G = Z_{p^l} \times H$ be an abelian group such that $p^2 \not| w = exp(H)$, $l > 1$. 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 $(r_1, r_2, \dots, r_s)$ of l, the folding $D' = f(D)$ of D is a (m, n, k, λ)-relative difference set in $G' = Z_{p^{r_1}} \times Z_{p^{r_2}} \times \dots \times Z_{p^{r_s}} \times H$.*

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 $G = Z_{p^l} \times H =< g > \times H$, $G' = Z_{p^{r_1}} \times \dots \times Z_{p^{r_s}} \times H =< g_1 > \times \dots \times < g_s > \times H$. 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 2. 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 proofs the claim and the theorem. □

4.3 Building sets

Davis and Jedwab [9] 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 $\{D_1, \dots, D_h\}$ of subsets of G with the following properties.

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

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

Theorem 13 *Let $G = Z_{p^l} \times H$ be an abelian group such that $p^2 \not| w = exp(H)$, $l > 1$. Suppose $\{D_1, \dots, D_h\}$ be a $(a, m, h, \pm)$ 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 $(r_1, r_2, \dots, r_s)$ of l, the folding $\{f(D_1), \dots, f(D_h)\}$ of $\{D_1, \dots, D_h\}$ is also a $(a, m, h, \pm)$ covering EBS in $G' = Z_{p^{r_1}} \times Z_{p^{r_2}} \times \dots \times Z_{p^{r_s}} \times H$.

Proof. 1) $|f(D_1)| = |D_1| = a \pm m$ and $|f(D_i)| = |D_i| = a$ for $i = 2, \dots, h$.
2) For every nonprincipal character τ of G', $\tau(f(D_i)) = \chi_\tau(D_i)$ from Theorem 2. Then 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 $j \neq i$. □

4.4 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 [10] for a survey and [5, 6, 11, 18] for some more recent results. 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 necessary criterion, see [19], for example.

Lemma 14 *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 $\chi$ of where $H$ is viewed as an element of $ZG$.

Theorem 15 *Let $G = Z_{p^l} \times K$ be an abelian group such that $p^2 \not| w = exp(K)$, $l > 1$. Suppose $H$ is a $G$-invariant weighing matrix such that for any $\chi$ 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 $G' = Z_{p^{r_1}} \times Z_{p^{r_2}} \times \ldots \times Z_{p^{r_s}} \times K$.*

The proof is similarly.

References

[1] 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.

[2] 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.

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

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

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

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

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

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

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

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

[11] 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.

[12] Hagita, M.: Foldings of Difference Sets in Abelian Groups. *Graphs and Combinatorics*, to appear.

[13] Jungnickel, D.: Difference sets. In: *Contemporary design theory: A collection of surveys* (Eds. J.H. Dinitz and D.R. Stinson). Wiley, New York (1992), 241-324.

[14] 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.

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

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

[17] Lander, E.S.: *Symmetric designs: an algebraic approach.* London Mathematical Society Lecture Note Series **74**, Cambridge University Press, Cambridge-New York, 1983.

[18] Liebler, R.A. The inversion formula. *J. Comb. Math. Comb. Comp.* **13** (1993), 143-160.

[19] Ohmori, H: Classification of weighing matrices of order 12 and weight 9. *Discrete Math.* **116** (1993), 55-78.

[20] Schmidt, B.: Cyclotomic Integers and Finite Geometry. *J. Amer. Math. Soc.*, to appear.

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

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