Bijections between Group Rings Preserving Character Sums

Mariko Hagita
Department of Mathematics, Keio University
Yokohama 223-8522
Japan
email: hagita@comb.math.keio.ac.jp

Bernhard Schmidt
Universität Augsburg
Universitätsstraße 14
86135 Augsburg
Germany
email: schmidt@math.uni-augsburg.de

Abstract

Generalizing an idea in [13], we exhibit some, in general nonhomomorphic, bijections between finite groups which preserve the absolute value of character sums. As a consequence, the existence of a single difference set, relative difference set, building set etc. in certain groups implies the existence such objects in many other groups.

1 Introduction

The main aim of this paper 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 $\alpha : G \to H$ preserving certain combinatorial properties of group ring elements like being a difference set. More precisely, considering the example of difference sets, we require that $\alpha(D)$ is a difference set in H for every difference set D in G. We do *not* require the converse, i.e., we do not require $\alpha^{-1}(E)$ do be a difference set in G for difference sets E in H.
The main motivation for the study of switching groups is to gain more insight into the existence of the combinatorial objects in question. One of the most striking

phenomena in the theory of difference sets is that (v, k, λ)-difference sets with $\gcd(v, k-\lambda) > 1$ "prefer to live" in groups of low exponent and high rank. For instance, Turyn, Davis and Kraemer [26, 9, 18] proved that an abelian 2-group G of order 2^{2d} has a difference set if and only if $\exp G \leq 2^{d+1}$. As a consequence of our main theorem, we can show, for example, that the existence of a difference set in $\mathbb{Z}_{2^{d+1}} \times \mathbb{Z}_2^{d-1}$ implies the existence of a difference set in $P \times \mathbb{Z}_2^{d-1}$ for any abelian 2-group P of order 2^{d+1}. Though, in view of the Turyn/Davis/Kraemer result, our result does not yield new groups containing difference sets, it sheds some light on the low exponent – high rank phenomenon.
Under which conditions can a switching of groups possibly work? First of all, there are already some bijections between nonisomorphic groups preserving difference sets known in the literature. For example, Dillon (cf. [4], [19]) found such bijections between generalized dihedral groups and corresponding abelian groups. Moreover, Bruck [5] constructed nonabelian projective planes by finding bijections between cyclic groups and certain nonabelian groups preserving the difference set property. These two constructions only work for very special types of groups. The aim of this paper is to find bijections preserving difference sets in a more general setting. Though we will succeed under some conditions, our results do not imply the existence of difference sets in any groups which previously had not been known to contain difference sets. However, our result *can* be applied to several families of difference sets, only the groups with difference sets we obtain are already covered by previously known constructions. Nevertheless, we believe that our result is still helpful for the understanding of difference sets.
When we try to find general difference set preserving bijections, we have to be aware of the following facts.

1. Difference sets with Singer parameters (see [4, 19, 25], cf. Section 6) 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. In fact, it is conjectured that no noncyclic abelian difference sets with Singer parameters exist, cf. [4, VI.§17]. So, bijections $G \to H$ where H has lower exponent (and higher rank) than G cannot work in general.

2. As mentioned above, Turyn, Davis and Kraemer [26, 9, 18] proved that an abelian 2-group G of order 2^{2d} has a difference set if and only if $\exp G \leq 2^{d+1}$. This shows that bijections $G \to H$ where G and H are abelian groups with $\exp H > \exp G$ cannot be difference set preserving in general.

3. Arasu, Davis, Jedwab, and Sehgal [1, 2] proved that a Hadamard difference set in $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{3^a} \times K$ with K abelian, $|K| = 3^a$, exists if and only if K is cyclic. Thus bijections $G \to H$ with $\exp H = \exp G$, rank $H >$ rank G also cannot work in general.

However, we still will be able to exhibit quite general difference set preserving

bijections by using appropriate lexicographic orderings together with some non-homomorphic permutations. The facts 1.-3. above show that some assumptions will be necessary to make bijections difference set preserving. This will reflect in two assumptions of our main Theorem 4.6. The first assumption puts some restrictions on the group structure; the second assumption is a *subfield condition* which requires that all character values of a group ring element essentially (i.e., up to multiplication with roots of unity) lie in a certain cyclotomic field. The subfield condition is closely related to recent results of Schmidt [22, 23, 24], in particular, to the so-called "field descent", see Result 3.3. It is interesting to note that the subfield condition is satisfied for *all known* difference sets with $\gcd(v, k-\lambda) > 1$ since all their character values essentially lie in $\mathbb{Q}$, see [4, VI.§9]. The bad news is that we do not know of any difference sets in *cyclic groups* for which the subfield condition is satisfied.

2 Background

In this section, we recall some well known facts on the combinatorial objects we will study. Let G be a finite group of order mn, and let N be a subgroup of G of order n. A subset R of G is called an $(\mathbf{m}, \mathbf{n}, \mathbf{k}, \lambda)$ **difference set in G relative to N** if every $g \in G \setminus N$ has exactly λ representations $g = r_1 r_2^{-1}$ with $r_1, r_2 \in R$, and no nonidentity element of N has such a representation. The subgroup N is called the **forbidden subgroup**.
In the case $n = 1$, i.e., when the forbidden subgroup is trivial, we write v instead of m and speak of a $(\mathbf{v}, \mathbf{k}, \lambda)$ **difference set** in G. The nonnegative integer $n = k - \lambda$, which should not be confused with the n of a relative difference set, is called the **order** of the difference set. If $n \in \{0, 1\}$, the difference set is called **trivial**. By a "difference set" we will always mean a nontrivial difference set. Sometimes it is useful to attach n to the parameters of a difference set. Thus we also speak of $(\mathbf{v}, \mathbf{k}, \lambda, \mathbf{n})$ **difference sets**.
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 [11] for a survey and [6, 7, 12, 20] 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 $k \in G$. We will identify a G-invariant weighing matrix H with the element $\sum_{g \in G} h_{1,g} g$ of $\mathbb{Z}[G]$.

A standard method for the study of difference sets and similar objects is the use of complex characters. We summarize the necessary facts here, see [4, Chapter XI] for proofs. Let G be a finite abelian group. A complex character of G is a homomorphism $\chi : G \to \mathbb{C}^*$. The character χ_0 defined by $\chi_0(g) = 1$ for all $g \in G$ is called the **trivial** character. For a subgroup N of G, we denote the

group of all characters of G which are trivial on N by $N^\perp$. The set of characters of G forms a group G^* isomorphic to G where the group operation is defined by $\chi_1\chi_2(g) = \chi_1(g)\chi_2(g)$. If χ is a character of G of order e, then $\chi(g)$ is a complex eth root of unity for all $g \in G$. Any character of G can be extended to the group ring $\mathbb{Z}[G]$ by linearity. A subset D of G will be identified with $\sum_{d\in D} d \in \mathbb{Z}[G]$. For $X = \sum_{g\in G} a_g g \in \mathbb{Z}[G]$ we write $X^{(-1)} := \sum_{g\in G} a_g g^{-1}$. Throughout this paper, use the notation $\xi_t = e^{2\pi i/t}$.
The following well known characterizations of (relative) difference sets and group invariant weighing matrices in terms of characters is basic. See [4, Chapter VI] and [22], for proofs.

Lemma 2.1 *A k-subset R of an abelian group G of order mn is an (m, n, k, λ)-difference set in G relative to a subgroup N of order n if and only if*

$$\chi(R)\overline{\chi(R)} = \begin{cases} k & \text{if } \chi \in G^* \setminus N^\perp \\ k - \lambda n & \text{if } \chi \in N^\perp \end{cases} \tag{1}$$

for every nontrivial character χ of G.

Lemma 2.2 *A k-subset D of an abelian group of order v is a (v, k, λ, n) difference set in G if and only if*

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

for every nontrivial character χ of G.

Lemma 2.3 *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 $\mathbb{Z}[G]$.

By the results above, (relative) difference sets and group invariant weighing matrices can be viewed as group ring elements whose character sums have a prescribed absolute value. This shows that it is interesting to look for bijections between group rings which preserve the absolute value of character values of group ring elements. This is the theme of the present paper.

3 Number theoretic tools

Our results will rely on a certain "subfield condition" involving cyclotomic fields over $\mathbb{Q}$. We recall the necessary number theoretic facts here. As before, we use the notation $\xi_t := e^{2\pi i/t}$. We say that $X \in \mathbb{Q}(\xi_t)$ **essentially lies** in $\mathbb{Q}(\xi_{t'})$ for some $t'|t$ if $X\xi_t^j \in \mathbb{Q}(\xi_{t'})$ for some j.

Result 3.1 *Let $m = p^a m'$ where p is a prime, $a \geq 2$ and $\gcd(m', p) = 1$. Then $1, \xi_{p^a}, ..., \xi_{p^a}^{p^{a-1}-1}$ are independent over $\mathbb{Q}(\xi_{pm'})$.*

Proof This follows from the well known fact $[\mathbb{Q}(\xi_m) : \mathbb{Q}(\xi_{pm'})] = \varphi(m)/\varphi(pm') = p^{a-1}$, see [8] or [14], for instance. □

Definition 3.2 *Let m, n be positive integers, and let $m = \prod_{i=1}^{t} p_i^{c_i}$ be the prime power decomposition of m. For each prime divisor q of n let*

$$m_q := \begin{cases} \prod_{p_i \neq q} p_i & \text{if } m \text{ is odd or } q = 2, \\ 4 \prod_{p_i \neq 2,q} p_i & \text{otherwise.} \end{cases}$$

Let $\mathcal{D}(n)$ be the set of prime divisors of n. We define $F(m, n) = \prod_{i=1}^{t} p_i^{b_i}$ to be the minimum multiple of $\prod_{i=1}^{t} p_i$ such that for every pair (i, q), $i \in \{1, ..., t\}$, $q \in \mathcal{D}(n)$, at least one of the following conditions is satisfied.
(a) $q = p_i$ and $(p_i, b_i) \neq (2, 1)$,
(b) $b_i = c_i$,
(c) $q \neq p_i$ and $q^{\mathrm{ord}_{m_q}(q)} \not\equiv 1 \pmod{p_i^{b_i+1}}$.

Result 3.3 (Field descent [22]) *Assume $X\overline{X} = n$ for $X \in \mathbb{Z}[\xi_m]$ where n and m are positive integers. Then X essentially lies in $\mathbb{Q}(\xi_{F(m,n)})$.*

4 The folding theorem

In this section, we prove our main result. We need some preparations. We denote the cyclic group of order t by $\mathbb{Z}_t$ and often identify $\mathbb{Z}_t$ with $[t] := \{0, ..., t-1\}$. So, if z is a fixed generator of $\mathbb{Z}_t$, we identify z^i with i. We use z^i in the multiplicative and i in the additive notation. Let $P = \mathbb{Z}_{p^{t_1}} \times \cdots \times \mathbb{Z}_{p^{t_s}}$ be an abelian p-group. We define a lexicographic order on P by

$$(a_1, ..., a_s) > (b_1, ..., b_s) \Leftrightarrow a_i > b_i \text{ for } i = \min\{j : a_j \neq b_j\}.$$

Let $m := \sum t_i$. The **folding** $f : \mathbb{Z}_{p^m} \to P$ is defined by $f(i)$ being the ith element of P in the lexicographic order. Note

$$f^{-1}(a_1, ..., a_s) = a_1 p^{t_2+\cdots+t_s} + a_2 p^{t_3+\cdots+t_s} + \cdots + a_s. \tag{2}$$

Let $G = \mathbb{Z}_{p^m} \times T$, $m \geq 2$, be an abelian group where p^2 does not divide $\exp T$, and let P be an abelian group of order p^m. The **p-folding** $f : G \to P \times T$ is defined by $f(a, w) = f(a)w$ for $a \in P$ and $w \in T$. We extend p-foldings to group rings by linearity. If G has not the form $\mathbb{Z}_{p^m} \times T$, $m \geq 2$, $p^2 \not| \exp T$, we say that **no p-folding of G exists**. Note that a p-folding of an abelian group G exists if and only if G^p has a nontrivial cyclic Sylow p-subgroup.

Let α_i be a generator of $\mathbb{Z}_{t_i}$, $i = 1, ..., s$. We call a subgroup U of $P = \mathbb{Z}_{t_1} \times \cdots \times \mathbb{Z}_{t_s}$ **left full** if it has the form

$$U = \langle \alpha_1, ..., \alpha_{r-1}, \alpha_r^l \rangle$$

for some l and some $r \in \{1, ..., s\}$.
Being bijections between nonisomorphic groups, foldings are non-homomorphic, of course. However, one of the main facts which makes foldings work is that they are *partially* homomorphic. The following lemma makes this precise.

Lemma 4.1 *Let p be a prime, and let z be a generator of $\mathbb{Z}_{p^m}$. Let $f : \mathbb{Z}_{p^m} \to P$ be a folding. Let U be a left full subgroup of P, and let W be the subgroup of $\mathbb{Z}_{p^m}$ of order $|U|$. Then*

$$f(z^i w) = f(z^i) f(w)$$

for $0 \leq i < p^m/|U|$ and all $w \in W$.

Proof Write $U = \langle \alpha_1, ..., \alpha_{r-1}, \alpha_r^{p^v} \rangle$ with $0 \leq v < t_r$. Note $|U| = |W| = p^{t_1 + \cdots + t_r - v}$. Let $w \in W$. Write $w = a_1 p^{t_2 + \cdots + t_s} + a_2 p^{t_3 + \cdots + t_s} + \cdots + a_s$ with $0 \leq a_k < p^{t_k}$. Since $w \equiv 0 \pmod{p^m/|W|}$, we have $a_{r+1} = ... = a_s = 0$ and $a_r = j p^v$ for some $j < p^{t_r - v}$. Write $i = b_1 p^{t_2 + \cdots + t_s} + b_2 p^{t_3 + \cdots + t_s} + \cdots + b_s$ with $0 \leq b_k < p^{t_k}$. Then $b_1 = ... = b_{r-1} = 0$ and $b_r < p^v$ since $i < p^m/|U|$. Note $a_r + b_r < p^{t_r}$. Using (2), we get

$$\begin{aligned} f(z^i w) &= f(a_1 p^{t_2 + \cdots + t_s} + a_2 p^{t_3 + \cdots + t_s} + \cdots + a_{r-1} p^{t_r + \cdots + t_s} \\ &\quad + (b_r + a_r) p^{t_{r+1} + \cdots + t_s} + b_{r+1} p^{t_{r+2} + \cdots t_s} + \cdots + b_s) \\ &= (a_1, ..., a_{r-1}, a_r + b_r, b_{r+1}, ..., b_s) \\ &= (0, ..., 0, b_r, b_{r+1}, ..., b_s) + (a_1, ..., a_{r-1}, a_r, 0, ..., 0) \\ &= f(z^i) f(w) \end{aligned}$$

concluding the proof. □

For $X = \sum_{g \in G} x_g g \in \mathbb{Z}[G]$ and $S \subset G$, we write $X \cap S := \sum_{s \in S} x_s s$. Furthermore, we write $X \subset S$ if the support of X is contained in S.

Lemma 4.2 *Let $G = \mathbb{Z}_{p^m} \times T$ be an abelian group where $\exp T$ is not divisible by p^2. Let τ be a character of G whose order is p^l, $1 \leq l \leq m$, when restricted to $\mathbb{Z}_{p^m}$. Let W be the subgroup of $\mathbb{Z}_{p^m}$ of order p^{m-l+1}, and write $W = \bigcup_{i=0}^{p-1} W^p w^i$ where $w \in W \setminus W^p$. Let $D = \sum_{g \in G} d_g g \in \mathbb{Z}[G]$. If $\chi(D) \in \mathbb{Q}(\xi_p, \xi_{\exp T})$, then*

$$\chi(D \cap W) = \chi(D)$$

and

$$\chi(D \cap Wh) = 0$$

for $Wh \neq W$.

Proof Let z be a generator of $\mathbb{Z}_{p^m}$. Write $D = \sum_{i=0}^{p^{l-1}-1} D_i z^i$ with $D_i \in \mathbb{Z}[W \times T]$. Note $\chi(D_i) \in \mathbb{Q}(\xi_p, \xi_{\exp T})$ for all i. By Result 3.1, $\chi(1), \chi(z), ..., \chi(z^{p^{l-1}-1})$ are independent over $\mathbb{Q}(\xi_p, \xi_{\exp T})$. Thus $\chi(D_i) = 0$ for $i > 0$ and $\chi(D) = \chi(D_0)$ implying the assertion. □

Lemma 4.3 *Let $f : \mathbb{Z}_{p^m} \times T \to P \times T$ be a p-folding. Let χ be a character of $\mathbb{Z}_{p^m} \times T$ which is nontrivial on P, and let U be the maximal left full subgroup of P contained in* $\ker\chi$. *Let W be the subgroup of $\mathbb{Z}_{p^m}$ of order $p|U|$. Then there is a character τ of $\mathbb{Z}_{p^m} \times T$ such that*

$$\tau(x) = \chi(f(x))$$

for all $x \in W \times T$ and τ has order $p^m/|U|$ when restricted to $\mathbb{Z}_{p^m}$.

Proof Since $f|_T$ is the identity, it suffices to consider the case $T = \{1\}$. Write $U = \langle \alpha_1, ..., \alpha_{r-1}, \alpha_r^{p^v} \rangle$ with $0 \le v < t_r$. Note $|U| = p^{t_1+\cdots+t_r-v}$. By the definition of U, we have $\chi(\alpha_1) = \cdots = \chi(\alpha_{r-1}) = 1$ and $\chi(\alpha_r) = \xi_{p^v}^i$ for some i relatively prime to p. Define a character of τ of $\mathbb{Z}_{p^m} = [p^m]$ by $\tau(x) = \xi_{p^m/|U|}^{ix}$ for all $x \in [p^m]$. Now, fix any $x \in W$. Note $x \equiv 0 \pmod{p^{m-1}/|U|}$ and $p^{m-1}/|U| = p^{v-1+t_{r+1}+\cdots+t_s}$. Write

$$x = a_1 p^{t_2+\cdots+t_s} + a_2 p^{t_3+\cdots+t_s} + \cdots + a_s$$

with $0 \le a_k < p^{t_k}$. Then $a_{r+1} = \cdots = a_s = 0$ and $a_r \equiv 0 \pmod{p^{v-1}}$ since $x \equiv 0 \pmod{p^{v-1+t_{r+1}+\cdots+t_s}}$. Write $a_r = jp^{v-1}$. By (2), we have $f(x) = \alpha_1^{a_1} \cdots \alpha_{r-1}^{a_{r-1}} \alpha_r^{jp^{v-1}}$. We get

$$\begin{aligned}
\tau(x) &= \xi_{p^m/|U|}^{i(a_1 p^{t_2+\cdots+t_s}+\cdots+a_{r-1}p^{t_r+\cdots+t_s}+jp^{v-1+t_{r+1}+\cdots+t_s})} \\
&= \xi_p^{ij} \\
&= \xi_{p^v}^{ijp^{v-1}} \\
&= \chi(\alpha_1^{a_1} \cdots \alpha_{r-1}^{a_{r-1}} \alpha_r^{jp^{v-1}}) \\
&= \chi(f(x))
\end{aligned}$$

concluding the proof. □

Definition 4.4
Let G be an abelian group. We say that $D \in \mathbb{Z}[G]$ is **p-foldable** *if, for every p-folding $f : G \to H$ and every nontrivial character χ of H, there is a root of unity η and a nontrivial character τ of G such that*

$$\chi(f(D)) = \eta\tau(D). \tag{3}$$

The motivation for the definition of foldable group ring elements is given by the following.

Theorem 4.5 *Let G be an abelian group and let $f : G \to H$ be a p-folding. Let $D \in \mathbb{Z}[G]$ be p-foldable.*
a) If D is a difference set in G, then $f(D)$ is a difference set in H.
b) If D is a difference set in G relative to a subgroup N, then $f(D)$ is a relative difference set in H relative to $f(N)$.
c) If D is a G-invariant weighing matrix, then $f(D)$ is a H-invariant weighing matrix.

Proof This is straightforward checking using Lemmas 2.1, 2.2 and 2.3. □

We remark that results similar to Theorem 4.5 can also be proved for divisible difference sets (cf. [21]) and building sets (cf. [9]). Now we prove our main result.

Theorem 4.6 (Folding theorem) *Let $G = \mathbb{Z}_{p^m} \times T$ be an abelian group where p^2 does not divide $\exp T$. If the character values of $D \in \mathbb{Z}[G]$ essentially lie in $\mathbb{Q}(\xi_p, \xi_{\exp T})$, then D is p-foldable.*

Proof Let $f : G \to H$ be a p-folding where $H = P \times T$, $|P| = p^m$. Let χ be a nontrivial character of H. We have to find a nontrivial character τ of G satisfying (3). If χ is trivial on P, then the character τ of G which is trivial on $\mathbb{Z}_{p^m}$ and satisfies $\tau|_T = \chi|_T$ does it since $f|_T$ is the identity. If χ is nontrivial on P, we choose U, W and τ as in Lemma 4.3. Let z be a generator of $\mathbb{Z}_{p^m}$ and write

$$D = \sum_{i=0}^{p^m/|W|-1} z^i W_i$$

with $W_i \in \mathbb{Z}[W \times T]$. By Lemma 4.3, we have $\tau(W_i) = \chi(f(W_i))$ for all i. By Lemma 4.2, we have $\tau(z^j W_j) = \tau(D)$ for one j and $\tau(W_i) = 0$ for $j \neq i$. Using Lemma 4.1, we get

$$\begin{aligned}
\chi(f(D)) &= \chi(f(\textstyle\sum z^i W_i)) \\
&= \chi(\textstyle\sum f(z^i W_i)) \\
&= \chi(\textstyle\sum f(z^i) f(W_i)) \\
&= \textstyle\sum \chi(f(z^i))\chi(f(W_i)) \\
&= \textstyle\sum \chi(f(z^i))\tau(W_i) \\
&= \chi(f(z^j))\tau(z^j)^{-1}\tau(D).
\end{aligned}$$

concluding the proof. □

5 Permutations Preserving Character Sums

In this section, we exhibit some nonhomomorphic permutations of the elements of abelian groups which once again preserve the character values of certain group ring elements. As a consequence, the existence of a single difference set in such an abelian group implies the existence of a large number of inequivalent difference sets in the same group under some conditions. Let us begin with the definition of the permutations we want to consider.

Definition 5.1 Let $G = \mathbb{Z}_{p^m} \times T$ be an abelian group where p is a prime and $m \geq 2$. Let U be a subgroup of $\mathbb{Z}_{p^m}$ of order $\geq p^2$. Let $D \in \mathbb{Z}[G]$, and write

$$D = \sum_{i=0}^{p^m/|U|-1} g_i U_i \tag{4}$$

where $U_i \in \mathbb{Z}[U \times T]$ and $\{g_i\}$ is a complete set of coset representatives of $U \times T$ in G. For each i, let σ_i be an automorphism of $U \times T$ such that $\sigma_i|_T$ is the identity and $\sigma_i|_U$ has order p. Then

$$P(D) := \sum_{i=0}^{p^m/|U|-1} g_i U_i^{\sigma_i} \tag{5}$$

is called a **U-permutation** of D.

Theorem 5.2 (Permutation theorem) *Let $G = \mathbb{Z}_{p^m} \times T$ be an abelian group where p is a prime, $m \geq 2$. Assume $p^m \not| \exp T$, say $p^h || \exp T$ with $h < m$. Let U be the subgroup of $\mathbb{Z}_{p^m}$ of order $\max(p^2, p^{h+1})$. Let $D \in \mathbb{Z}[G]$ and assume that all character values of D essentially lie in $K := \mathbb{Q}(\xi_{|U|}, \xi_{\exp T})$. Let $P(D)$ be a U-permutation of D. Then, for every character χ of G, there is a character τ of G and a root of unity η with*

$$\chi(P(D)) = \eta\tau(D). \tag{6}$$

Proof
Case 1: χ has a nontrivial kernel on U. Let σ be an automorphism of U of order p. Note that $(u/u^\sigma)^p = 1$ for all $u \in U$. Thus $\chi(u^\sigma) = \chi(u)$ for all $u \in U$ since $\chi|_U$ has a nontrivial kernel. Thus (6) holds with $\tau = \chi$.
Case 2: χ has a trivial kernel on U. Then, using Result 3.1, we see that $\chi(g_i)$, $i = 0, ..., p^m/|U| - 1$, are independent over K. W.l.o.g, assume $\chi(g_0) \in K$. From (4), we get

$$\chi(D) = \sum_{i=0}^{p^m/|U|-1} \chi(g_i)\chi(U_i).$$

Note that $\chi(U_i) \in K$ for all i. Since, by assumption, $\chi(D)$ essentially lies in K, we may assume $\chi(D) \in K$. Using the independence of the $\chi(g_i)$ over K, we get

$$\chi(U_i) = 0 \text{ for } i > 0. \tag{7}$$

Let σ_j be an automorphism of $U \times T$ as in Definition 5.1. Then $\tau_j := \chi \circ \sigma_j$ is a character of $U \times T$. Using the facts that σ_j has order p and that $|U|$ is larger than the p-part of $\exp T$, it is straightforward to check that there is $\varphi_j \in \mathrm{Gal}(K/\mathbb{Q})$ with $\tau_j = (\chi|_{U\times T})^{\varphi_j}$. Thus, for every $X \in \mathbb{Z}[U \times T]$, we have $\tau_j(X) = 0 \Leftrightarrow \chi(X) = 0$. Extend τ_j to G by $\tau_j = (\chi)^{\varphi_j}$. By what we have seen, (7) implies $\tau_j(U_i) = 0$ for $i > 0$ for all j. Hence

$$\begin{aligned}
\chi(P(D)) &= \sum \chi(g_i)\tau_i(U_i) \\
&= \chi(g_0)\tau_0(U_0) \\
&= \chi(g_0)\tau_0(g_0)^{-1} \sum \tau_0(g_i)\tau_0(U_i) \\
&= \chi(g_0)\tau_0(g_0)^{-1}\tau_0(D)
\end{aligned}$$

concluding the proof. □

6 Applications

In this final section, we present some application of the folding and permutation theorems to difference sets. Similar applications can be given to relative difference sets, divisible difference sets, group invariant weighing matrices, and building sets. The results also can be generalized to groups $\mathbb{Z}_{p^m} \times T$ where T is nonabelian. All these applications of the folding idea are quite straightforward and will be omitted.

Corollary 6.1 *Let D be a difference set of order n in an abelian group $G = \mathbb{Z}_{p^m} \times T$ where $m \geq 2$. Let P be any abelian group of order p^m, and let $f : G \to P \times T$ be a p-folding.*
a) If $p^2 \not| \exp T$ and the character values of D essentially lie in $\mathbb{Q}(\xi_p, \xi_{\exp T})$, then $f(D)$ is a difference sets in $P \times T$.
b) Assume $p^h || \exp T$ with $h < m$ and that the character values of D essentially lie in $\mathbb{Q}(\xi_{|U|}, \xi_{\exp T})$. Let U be the subgroup of $\mathbb{Z}_{p^m}$ of order $\max(p^2, p^{h+1})$. Then every U-permutation of D is also a difference set in G.

Proof Part a follows from Theorems 4.5 and 4.6. Part b follows from Lemma 2.2 and Theorem 5.2. □

Corollary 6.2 *Let $G = \mathbb{Z}_{p^m} \times T$, and let t be the p-free part of $\exp T$. Let F be the function defined in 3.2. The assertions of Theorem 6.1 still hold if the assumptions on the character values are replaced by*

$$F(|G|, n) \text{ divides } pt$$

for part a respectively

$$F(|G|, n) \text{ divides } |U|t$$

for part b.

Proof This follows from Result 3.3 and Corollary 6.1. □

In the situation of the following result, the subfield condition is always satisfied.

Corollary 6.3 *Let $G = \mathbb{Z}_{p^m} \times T$, $m \geq 2$, be an abelian group, and let D be a difference set in G of order $n = p^a$.*
a) Let $f : G \to H$ be a p-folding. Then $f(D)$ is a difference set in H.
b) Let U be the subgroup of $\mathbb{Z}_{p^m}$ of order $\max(p^2, p^{h+1})$ where $p^h || \exp T$, $h < m$. Then every U-permutation of D is also a difference set in G.

Proof This follows from Corollary 6.2 since the p-part of $F(|G|, n)$ is just p in this situation. □

There are four known families of (v, k, λ, n) difference sets with $\gcd(v, n) > 1$: Hadamard, McFarland, Davis/Jedwab, and Chen difference sets, see [4]. It is interesting to note that all these difference sets satisfy the subfield condition in the folding theorem. In fact, all their character values essentially lie in $\mathbb{Q}$, see [4, Chapter XI]. Thus we have the following.

Corollary 6.4 *Let D be any of the presently known (v, k, λ, n) difference sets with $\gcd(v, n) > 1$ in an abelian group. Then D is p-foldable for every prime divisor p of v.*

Unfortunately, we cannot derive any *new groups* containing difference sets by Corollary 6.4. The existence results we get are already covered by known constructions. However, we think that our results are still of interest since they shed some light on the phenomenon that (v, k, λ, n) difference sets with $\gcd(v, n) > 1$ "prefer to live" in groups of low exponent and high rank. We illustrate this by an example. From the constructions of Davis [9] and Kraemer [18], it is known that every abelian group of order 2^{2d+2} and exponent at most 2^{d+2} contains a difference set. In particular, $\mathbb{Z}_{2^{d+2}} \times \mathbb{Z}_2^d$ has a difference set.

Example 6.5 Let D be a difference set in $G = \mathbb{Z}_{2^{d+2}} \times \mathbb{Z}_2^d$. Let P be any abelian group of order 2^{d+2}, and let $f : G \to P \times \mathbb{Z}_2^d$ be a folding. Then $f(D)$ is a difference set in $P \times \mathbb{Z}_2^d$.

Similar examples can be given for the other families of difference sets with $\gcd(v, n) > 1$ and for many known families of relative difference sets, group invariant weighing matrices, and building sets.

We conclude this paper with some interesting negative remarks. If a difference set in a *cyclic group* satisfied the subfield condition for all prime divisors of the group order, then the folding theorem would show that there are difference sets in *all* abelian groups of the same order. Thus it is interesting to check if any of the known difference sets in cyclic groups is foldable. The only candidates are difference sets with Singer parameters; for all other difference sets in cyclic groups, the group order is squarefree and thus foldings are impossible. So let us consider Singer parameters. Let q be a prime power, and let $d \geq 2$ be an integer. There is a difference set D with parameters

$$(v, k, \lambda, n) = \left(\frac{q^{d+1}-1}{q-1}, \frac{q^d-1}{q-1}, \frac{q^{d-1}-1}{q-1}, q^{d-1} \right) \tag{8}$$

in $\mathbb{Z}_v$ found by Singer [25] which is called a **Singer difference set**, see [4, Chapter XI]. It is conjectured that there are no difference sets with parameters (8) in any *noncyclic* abelian groups. If any Singer difference set was foldable, then, by Theorem 4.5, we would obtain a counterexample to this conjecture. However, it seems that no difference set with Singer parameters is foldable. For small examples, this can be checked using tables of difference sets, cf. [4]. Another fact which indicates that Singer difference sets probably are not foldable is that it can be seen that $F(v, n) = v$ for all Singer parameters (8). Thus Corollary 6.3 does not apply.

Acknowledgement

We would like to thank the referees for their appropriate and helpful criticism of an earlier exposition of this paper.

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] L.D. Baumert: *Cyclic Difference Sets.* Lecture Note 182, Springer, Berlin/Heidelberg/New York 1971.

[4] Beth, T., Jungnickel, D., Lenz, H.: *Design theory* (2nd edition). Cambridge University Press, Cambridge 1999.

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

[12] 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.

[13] Hagita, M.: Foldings of Difference Sets in Abelian Groups. *Graphs and Combinatorics* **15**(1999), 187-193.

[14] N. Jacobson: *Basic Algebra I, II* (2nd edition). W. H. Freeman and Company, New York 1985.

[15] 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.

[16] Jungnickel, D., Schmidt, B.: Difference sets: An update. In: *Geometry, combinatorial designs and related structures.* Eds. J.W.P. Hirschfeld et. al., Cambridge University Press, Cambridge 1997, 89-112.

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

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

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

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

[21] A. Pott: *Finite Geometry and Character Theory.* Springer Lecture Notes 1601, Springer, Berlin/Heidelberg/New York 1995.

[22] B. Schmidt: Cyclotomic Integers and Finite Geometry. *J. Am. Math. Soc.* **12** (1999), 929-952.

[23] B. Schmidt: Towards Ryser's conjecture. *Proceedings 3ecm 2000*, to appear.

[24] B. Schmidt: *Characters and cyclotomic fields in finite geometry.* Habilitationsschrift, Universität Augsburg 2000.

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

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