The field descent method

Bernhard, Schmidt.; Ka, Hin Leung.

2005

Bernhard, S., & Ka, H. L. (2005). The field descent method. Journal of designs codes and cryptography, 36(2), 171-188.

https://hdl.handle.net/10356/91963

https://doi.org/10.1007/s10623-004-1703-7

The field descent method

Ka Hin Leung
Department of Mathematics
National University of Singapore
Kent Ridge, Singapore 119260
Republic of Singapore

Bernhard Schmidt
Institut für Mathematik
Universität Augsburg
86135 Augsburg
Germany

Abstract

We obtain a broadly applicable decomposition of group ring elements into a "subfield part" and a "kernel part". Applications include the verification of Lander's conjecture for all difference sets whose order is a power of a prime > 3 and for all McFarland, Spence and Chen/Davis/Jedwab difference sets. We obtain a new general exponent bound for difference sets. We show that there is no circulant Hadamard matrix of order v with $4 < v < 548,964,900$ and no Barker sequence of length l with $13 < l \leq 10^{22}$.

1 Introduction

The character method for studying combinatorial objects with a suitable group G of symmetries consists of the investigation of certain equations in cyclotomic integers. These equations arise from applying complex representations to group ring equations characterizing the objects in question. The three almost exclusively used methods in this direction are multiplier theorems [4, 5, 9, 20], the self-conjugacy approach [27] and the field descent method [23, 24]. See [21] and [6, Chapter VI] for a comprehensive treatment of these topics. Although these methods yield impressive results for certain *explicit parameter families*, they still are not strong enough for a uniform treatment of larger classes of objects. This is the reason why, for instance, the investigation of difference sets belonging to different kinds of parameter families has split into almost independent branches of research.

The purpose of the present paper is to enhance the field descent method introduced in [23] with new algebraic-combinatorial ideas so that a uniform treatment of a broader spectrum of parameters becomes possible. A crucial step towards our main results will be to show that the field descent implies a *decomposition* of a difference set into two parts: One part corresponding to the subfield given by the field descent and a second part corresponding to the kernel of a map from the integral group ring to a group ring with cyclotomic integers as coefficients. The exact formulation of this decomposition can be found in Theorems 3.1 and 3.4.

In Section 4, we also utilize the decomposition of difference sets to obtain a new general exponent bound which strengthens the results from [23] and [24] considerably. This yields progress towards the longstanding Circulant Hadamard Matrix and Barker Sequence Conjectures. In particular, we are able to extend the range of lengths for which the Barker Sequence Conjecture is verified by a factor of $2.5 \cdot 10^9$.

We believe that the decomposition of difference sets into a "small field part" and a "kernel part" discovered here is a general pattern that still has to be exploited, even beyond the results presented here. In fact, it provides the crucial step in our proof to Lander's conjecture when the order is of the form p^r where p is a prime larger than 3,

[17].

2 Preliminaries

In this section, we list the definitions and basic facts we need in the rest of paper. We first fix some notation. Let R be a ring and let G be a finite group. We will always identify a subset A of G with the element $\sum_{g\in A} g$ of the group ring $R[G]$. For $B = \sum_{g\in G} b_g g \in R[G]$ we write $B^{(-1)} := \sum_{g\in G} b_g g^{-1}$ and $|B| := \sum_{g\in G} b_g$. We call $\{g \in G : b_g \neq 0\}$ the **support** of B. A group homomorphism $G \to H$ is always assumed to be extended to a homomorphism $\mathbb{Z}[G] \to \mathbb{Z}[H]$ by linearity. We will write $o(g)$ for the order of $g \in G$ in G. The exponent of G, i.e. the order of the largest cyclic subgroup of G, will be denoted by $\exp G$.

For an abelian group H we denote the group of complex characters of H by H^*. The character sending all $h \in H$ to 1 is called **trivial**. For a subgroup W of H, we write $W^\perp$ for the subgroup of H^* consisting of all characters which are trivial on W.

The following is a standard result [6, Chapter VI, Lemma 3.5].

Result 2.1 *Let G be a finite abelian group and $D = \sum_{g\in G} d_g g \in \mathbb{C}[G]$. Then*

$$d_g = \frac{1}{|G|} \sum_{\chi\in G^\perp} \chi(Dg^{-1})$$

for all $g \in G$. In particular, two elements of $\mathbb{C}[G]$ are equal if and only if all their character values are equal.

If H is a subgroup of G and $A, B \in \mathbb{Z}[G]$ with $\chi(A) = \chi(B)$ for all $\chi \in G^* \setminus H^\perp$, then $A = B + XH$ for some $X \in \mathbb{Z}[G]$.

We need some notation for cyclotomic fields. By $\mathbb{Q}(\xi_m)$, $\xi_m = e^{2\pi i/m}$, we denote the mth cyclotomic field over $\mathbb{Q}$. By a fundamental result of algebraic number theory [22, p. 269, Theorem. 4B (3)] the ring of algebraic integers of $\mathbb{Q}(\xi_m)$ is $\mathbb{Z}[\xi_m]$. For the basic properties of $\mathbb{Z}[\xi_m]$, see [10, Chapter 12], for instance. For relatively prime integers t and

s, we denote the multiplicative order of t modulo s by $\mathrm{ord}_s(t)$. Finally, φ denotes the Euler totient function.

For a simple proof of the following result, see [6, Chapter VI, Theorem. 15.2].

Result 2.2 *Let p be a rational prime, let P be a prime ideal above p in $\mathbb{Z}[\xi_m]$, and write $m = p^a m'$ with $(m', p) = 1$. The decomposition group of P consists of all $\sigma \in \mathrm{Gal}(\mathbb{Q}(\xi_m)/\mathbb{Q})$ for which there is an integer j such that*

$$\xi_{m'}^{\sigma} = \xi_{m'}^{p^j}. \tag{1}$$

We will need the following basic property of Gauss sums. For a proof, see [18, Theorem. 5.11].

Lemma 2.3 *Let p be an odd prime and let S be a Gauss sum over $\mathbb{Z}_p$, i.e. $S = \sum_{i=1}^{p-1} \eta^i \xi^{t^i}$ where $\eta \neq 1$ is a $(p-1)$th root of unity, ξ is a primitive pth root of unity and t is a primitive root modulo p. Then $|S|^2 = p$.*

Next, we restate a version of a well known result, see [16, Theorem 2.2], that will be used very often.

Lemma 2.4 *Let $G = \langle a \rangle \times H$ be an abelian group where $o(a) = u$ and let $\rho : \mathbb{Z}[G] \to \mathbb{Z}[\xi_u][H]$ be the homomorphism defined by $\rho(a) = \xi_u$ and $\rho|_H = \mathrm{id}$. Then*

$$\ker \rho = \{\sum_{i=1}^{r} \langle a^{u/p_i} \rangle x_i : x_i \in \mathbb{Z}[G]\}$$

where $p_1, ..., p_r$ are the prime divisors of u.

The following "multiplier lemma" is from [1, Lemma 1].

Result 2.5 *Let $G = \langle a \rangle \times H$ be an abelian group where $o(a) = u$. Write $v = \exp G$. Let $D \in \mathbb{Z}[G]$ and $n, t \in \mathbb{N}$ such that*

(i) $(|H|, n) = 1$,

(ii) $|\chi(D)|^2 = n$ *for all characters* χ *of* G *with* $\chi(a) = \xi_u$,

(iii) the Galois automorphism σ *of* $\mathbb{Q}(\xi_v)$ *defined by* $\xi_v^\sigma = \xi_v^t$ *fixes all prime ideal divisors of* n. *Then*

$$D^{(t)} = (-1)^\ell bD + \sum_{i=1}^{r} \langle a^{u/p_i} \rangle x_i$$

where $\ell \in \{0, 1\}, b \in G$, $x_1, ..., x_r \in \mathbb{Z}[G]$ *and* $p_1, ..., p_r$ *are all the prime divisors of* u. *Furthermore, if* u *is even,* ℓ *can be set as* 0.

The following definition will be needed for our field descent arguments.

Definition 2.6 *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* $q^{\mathrm{ord}_{m_q}(q)} \not\equiv 1 \pmod{p_i^{b_i+1}}$.

The next results are well known and they can be proved by using standard arguments concerning the structure of the multiplicative groups modulo p^a, see [11, pp. 274-276], for instance.

Lemma 2.7 *Let* p *be a prime, and let* b *be a positive integer.*

(a) Assume $(p, b) \neq (2, 1)$. *If* s *is an integer satisfying* $s \equiv 1 \pmod{p^b}$ *and* $s \not\equiv 1 \pmod{p^{b+1}}$ *then* $\mathrm{ord}_{p^c}(s) = p^{c-b}$ *for all* $c \geq b$.

(b) Let s *and* t *be integers such that* $\mathrm{ord}_{p^b}(s) = \mathrm{ord}_{p^b}(t)$ *is a power of* p. *Furthermore, assume* $s \equiv t \equiv 1 \pmod 4$ *if* $p = 2$. *Then* s *and* t *generate the same subgroup of the multiplicative group* $\mathbb{Z}_{p^b}^*$.

Now we come to the definitions and basic properties of the combinatorial structures we will study. A $(\mathbf{v}, \mathbf{k}, \lambda, \mathbf{n})$**-difference set** in a finite group G of order v is a k-subset D of G such that every element $g \neq 1$ of G has exactly λ representations $g = d_1 d_2^{-1}$ with $d_1, d_2 \in D$. The positive integer $n := k - \lambda$ is called the **order** of the difference set.

A difference set in a group G is equivalent to a symmetric design $\mathcal{D}$ admitting G as a regular automorphism group [6, Chapter VI, Theorem. 1.6]. Sometimes G is called a **Singer group** of $\mathcal{D}$. For detailed treatments of difference sets, see [5, 13, 14, 15, 21]. In the group ring language, difference sets can be characterized as follows [6, Chapter VI, Lemma 3.2].

Lemma 2.8 *Let D be a k-subset of a group G of order v. Then D is a (v, k, λ, n) difference set in G if and only if*

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

in $\mathbb{Z}[G]$.

We will need the following consequence of a well-known result on symmetric designs [6, Chapter II, Cor. 3.9].

Result 2.9 *If a (v, k, λ, n)-difference set exists and v is even, then n is a square.*

The following lemma essentially contained in [27] and has turned out to be a *conditio sine qua non* for the study of difference sets in abelian groups. See [6, Chapter VI, Lemma 3.12] for a proof.

Lemma 2.10 *Let D be a k-subset of an abelian group G. Then D is a (v, k, λ, n)-difference set in G if and only if $|\chi(D)|^2 = n$ for every nontrivial character χ of G.*

A **circulant Hadamard matrix of order v** is a matrix of the form

$$H = \begin{pmatrix} a_1 & a_2 & \cdots & a_v \\ a_v & a_1 & \cdots & a_{v-1} \\ \cdots & \cdots & \cdots & \cdots \\ a_2 & a_3 & \cdots & a_1 \end{pmatrix}$$

with $a_i = \pm 1$ and $HH^t = vI$ where I is the identity matrix. It is conjectured that no circulant Hadamard matrix of order $v > 4$ exists. A sequence $(a_i)_{i=1}^v$, $a_i = \pm 1$, is called a **Barker sequence of length v** if $|\sum_{i=1}^{v-j} a_i a_{i+j}| \leq 1$ for $j = 1, ..., v-1$. The Barker Sequence Conjecture asserts that there are no Barker sequences of length $v > 13$. Storer and Turyn [26] proved the Barker Sequence Conjecture for all odd v. The following is well known, see [6, Chapter VI, §14] and [7, 8].

Result 2.11 *(a) If a Barker sequence of length $l > 13$ exists, then l has no prime divisor $\equiv 3 \pmod 4$ and there is a circulant Hadamard matrix of order v.*

(b) If a circulant Hadamard matrix of order v exists, then $v = 4u^2$ for some odd u and there is a $(4u^2, 2u^2 - u, u^2 - u, u^2)$ difference set in the cyclic group of order v.

3 Decomposition of group ring elements

In this section, we show that group ring elements whose character values have a prescribed absolute value can be decomposed into a "subfield part" and a "kernel part". The applications of this method will be given in the remaining sections.

We begin with a basic decomposition which works in a very general setting. After this we prove a stronger result which needs some additional assumptions.

Theorem 3.1 *Let $G = \langle a \rangle \times H$ be an abelian group where $w := \exp H$ and $u := o(a)$ are coprime. Let n be a positive integer coprime to w. Let D be an element of $\mathbb{Z}[G]$ such that $|\chi(D)| = n$ for all characters χ of G with $\chi(a) = \xi_u$. Let $F_u := \gcd(u, F(uw, n))$ and let A be the subgroup of order F_u in $\langle a \rangle$. Then there is $D_A \in \mathbb{Z}[A \times H]$ such that*

$$D = gD_A + \sum_{i=1}^{r} \langle a^{u/p_i} \rangle x_i \tag{2}$$

for some $g \in G$ and $x_1, ..., x_r \in \mathbb{Z}[G]$ where $p_1, ..., p_r$ are the prime divisors of u.

Remark 3.2 The decomposition (2) is useful because D_A lies in $\mathbb{Z}[A \times H]$ and $A \times H$ often is much smaller than the whole group G. The size of the subgroup A is determined by

the parameter $F(uw, n)$ which comes from a field descent. This is why we call term gD_A the "subfield part". The second term in (2) stems from the kernel of a homomorphism from $\mathbb{Z}[G]$ to a group ring with cyclotomic integers as coefficients and is thus called the "kernel part" of D. Also, we want to note that similar decompositions in some particular situations, e.g. n is a prime power, have also been studied before, see [1, 2, 19].

Proof of Theorem 3.1 Write $u = \prod_{i=1}^{r} p_i^{c_i}$ and $F_u = \prod_{i=1}^{r} p_i^{b_i}$. Choose an integer t with $\mathrm{ord}_{p_i^{c_i}}(t) = p_i^{c_i - b_i}$ for $i = 1, ..., r$ and $t \equiv 1 \bmod w$. By Lemma 2.7 we may choose t such that $p_i^{b_i}$ is the exact power of p_i dividing $t - 1$ for all i. Let σ be the Galois automorphism of $\mathbb{Q}(\xi_{uw})$ defined by $\xi_{uw}^{\sigma} = \xi_{uw}^{t}$.

Claim: σ fixes all prime ideal divisors of n in $\mathbb{Q}(\xi_{uw})$.

Proof of the claim: Write $uw = \prod_{i=1}^{s} p_i^{c_i}$ where $s \geq r$ and the p_i are the distinct prime divisors of uw. Let q be an arbitrary prime divisor of n. Let

$$u_q := \prod_{i=1, p_i \neq q}^{s} p_i^{c_i}, \qquad m_q := \begin{cases} \prod_{p_i \neq q} p_i & \text{if uw is odd or } q = 2, \\ 4 \prod_{p_i \neq 2, q} p_i & \text{otherwise,} \end{cases}, \quad Q := q^{\mathrm{ord}_{m_q}(q)}.$$

Recall that $(n, w) = 1$ and thus $(q, w) = 1$ by assumption. We will show that there is an integer j with $q^j \equiv t \bmod u_q$ (together with Result 2.2 this implies the claim since q is arbitrary). Note that $Q \equiv 1 \pmod{p_i}$ for all i with $p_i \neq q$ by definition of m_q and Q. Furthermore, we have $Q \equiv 1 \pmod 4$ if $q \neq 2$ and uw is even. By conditions (b) and (c) of Definition 2.6 and Lemma 2.7(a), we know that $\mathrm{ord}_{p_i^{c_i}}(Q)$ is a power of p_i which is at least $\mathrm{ord}_{p_i^{c_i}}(t) = p_i^{c_i - b_i}$ for every $i \leq r$ with $p_i \neq q$. Thus, by Lemma 2.7(b), for every $i \leq s$ with $p_i \neq q$, there is an integer $s(i)$ with $Q^{s(i)} \equiv t \bmod p_i^{c_i}$. By the Chinese remainder theorem there is an integer h such that $h \equiv s(i) \bmod p_i^{c_i}$ for all i with $p_i \neq q$. It follows that $Q^h \equiv t \bmod p_i^{c_i}$ for all i with $p_i \neq q$. This implies $Q^h \equiv t \bmod u_q$ and completes the proof of the claim since Q is a power of q.

Note that $(|H|, n) = 1$ since $w = \exp H$ and $(w, n) = 1$ by assumption. Hence condition (i) of Result 2.5 is satisfied. Condition (ii) holds by assumption. Finally, the claim ensures condition (iii). Hence we can apply Result 2.5 and get

$$D^{(t)} = (-1)^{\ell} bD + \sum_{i=1}^{r} \langle a^{u/p_i} \rangle x_i \tag{3}$$

where $\ell \in \{0,1\}, b \in G$, $x_1, ..., x_r \in \mathbb{Z}[G]$ and ℓ can be set to be 0 if u is even. Let $\rho : \mathbb{Z}[G] \to \mathbb{Z}[\xi_u][H]$ be the homomorphism defined by $\rho(a) = \xi_u$ and $\rho|_H = \mathrm{id}$. Note that $\rho(\langle a^{u/p_i} \rangle) = 0$ for all i. Let σ be the automorphism defined before the claim. We now interpret σ as an automorphism of $\mathbb{Z}[\xi_u][H]$ by setting $(\sum_{h \in H} a_h h)^{\sigma} = \sum_{h \in H} a_h^{\sigma} h$ for all $a_h \in \mathbb{Z}[\xi_u]$. Let $E := \rho(D)$. Since $\xi_u^{\sigma} = \xi_u^t$ and $h^t = h$ for all $h \in H$, we have $E^{\sigma} = E^{(t)}$. Thus (3) implies

$$E^{\sigma} = (-1)^{\ell} c \xi_u^j E \tag{4}$$

for some integer j and $c \in H$. Let $y := \mathrm{ord}_{uw}(t)$. By the definition of t, we have $y = \prod_{i=1}^{r} p_i^{c_i - b_i}$. Thus $(y, w) = 1$ since $(u, w) = 1$. Using (4) repeatedly, we get

$$E = E^{(\sigma^y)} = (-1)^{\ell y} c^y \xi_u^{j(t^y - 1)/(t-1)} E$$

and thus $E(1 - (-1)^{\ell y} c^y \xi_u^{j((t^y-1)/(t-1))}) = 0$ in $\mathbb{Z}[\xi_u][H]$. Since $|\tau(E)| = n$ for all characters τ of H by assumption, we have $\tau(1 - (-1)^{\ell y} c^y \xi_u^{j((t^y-1)/(t-1))}) = 0$ for all characters τ of H. Thus

$$(-1)^{\ell y} c^y \xi_u^{j((t^y-1)/(t-1)} = 1 \tag{5}$$

in $\mathbb{Z}[\xi_u][H]$ by Result 2.1. Since $c^w = 1$ and $(y, w) = 1$, we get $c = 1$ from (5). Next, we claim that $\ell = 0$. In that respect, we only need to consider the case u is odd. But then y is odd and the order of ξ_u is odd. Hence, it follows easily from (5) that $\ell = 0$. Thus, we obtain

$$E^{\sigma} = \xi_u^j E \tag{6}$$

and $\xi_u^{j((t^y-1)/(t-1)} = 1$ and thus

$$j \frac{t^y - 1}{t - 1} \equiv 0 \bmod u. \tag{7}$$

Recall that the exact power of p_i dividing $t - 1$ is $p_i^{b_i}$ for $i = 1, ..., r$. Note that $b_i \geq 1$ for all i by Definition 2.6. Hence, by Lemma 2.7 a, the exact power of p_i dividing $t^y - 1$

is $p_i^{b_i+c_i-b_i} = p_i^{c_i}$. Thus, the exact power of p_i dividing $(t^y-1)/(t-1)$ is $p_i^{c_i-b_i}$. By (7) we have $j(t^y-1)/(t-1) \equiv 0 \bmod p_i^{c_i}$. This implies

$$j \equiv 0 \bmod p_i^{b_i}. \tag{8}$$

Since $p_i^{b_i+1}$ does not divide $t-1$ for all i, there is a solution d of the simultaneous congruences

$$(t-1)d + j \equiv 0 \bmod p_i^{c_i}, \quad i = 1, ..., r,$$

by the Chinese remainder theorem. Thus $(t-1)d + j \equiv 0 \bmod u$. Hence, using (6), we get

$$(E\xi_u^d)^\sigma = E\xi_u^{j+dt} = E\xi_u^d. \tag{9}$$

Now write $E\xi_u^d = \sum_{h\in H} E_h h$ with $E_h \in \mathbb{Z}[\xi_u]$. Then (9) implies $E_h^\sigma = E_h$ for all $h \in H$ and thus $E_h \in \mathbb{Z}[\xi_{F_u}]$ since $\mathbb{Q}(\xi_{F_u})$ is the fixed field of $\langle \sigma|_{\mathbb{Q}(\xi_u)}\rangle$. Recall that A is the subgroup of $\langle a\rangle$ of order F_u. Since $E_h \in \mathbb{Z}[\xi_{F_u}]$ for all h, there is $D_A \in \mathbb{Z}[A\times H]$ with $\rho(D_A) = E\xi_u^d$. Hence $\rho(D) = E = \rho(a^{-d}D_A)$. Now Result 2.4 implies

$$D = a^{-d}D_A + \sum_{i=1}^{r} \langle a^{u/p_i}\rangle x_i \tag{10}$$

for some $x_1, ..., x_r \in \mathbb{Z}[G]$. □

Remark 3.3 It is possible to require the supports of $\sum_{i=1}^r \langle a^{u/p_i}\rangle x_i$ to be in $g(G\backslash A\times H)$. As such, the supports of gD_A and $\sum_{i=1}^r \langle a^{u/p_i}\rangle x_i$ will be disjoint. To do so, we note that $p_1p_2\cdots p_r$ is a divisor of F_u. Therefore, $\langle a^{u/p_i}\rangle \subset A\times H$. Clearly, x_i can be rewritten as $x_i' + x_i''$ such that the support of x_i' is in $g(A\times H)$ and the support of x_i'' is in $G\backslash g(A\times H)$. Replacing gD_A by $gD_A + \sum_{i=1}^r \langle a^{u/p_i}\rangle x_i'$ and x_i by x_i'' if necessary, it is clear then the support of $\sum_{i=1}^r \langle a^{u/p_i}\rangle x_i$ is in $G\backslash g(A\times H)$.

In the next result we obtain a more precise description of D_A in Theorem 3.1 under some additional assumptions. Loosely speaking, the underlying method is to factor out a group ring element looking like a Gauss sum from D_A so that we go down to an even smaller subfield than that in Theorem 3.1.

Theorem 3.4 *Let $G = \langle a \rangle \times H$ be an abelian group where $w := \exp H$ and $u := o(a)$ are coprime. Let n be a positive integer coprime to w. Let D be an element of $\mathbb{Z}[G]$ such that $|\chi(D)| = n$ for all characters χ of G with $\chi(a) = \xi_u$. Let p be an odd prime divisor of u. For each prime divisor q of n let $m(q)$ be the largest divisor of uw coprime to pq. Assume that*

(i) p^2 does not divide $F(uw, n)$,

(ii) $\mathrm{ord}_p(q) = p - 1$ for all prime divisors $q \neq p$ of n,

(iii) $\gcd(\mathrm{ord}_{m(q)}(q), p - 1) = 1$ for all prime divisors $q \neq p$ of n.

Let $F_u := \gcd(u, F(uw, n))$ and let B be the subgroup of $\langle a \rangle$ of order F_u/p. Then there are $g, h \in G$ with $o(g)|(p-1)$, $\ell \in \{0, 1\}$, $x_1, ..., x_r \in \mathbb{Z}[G]$ and $D_B \in \mathbb{Z}[B \times H]$ such that

$$D = hD_B \sum_{i=1}^{p-1} ((-1)^\ell g)^i a_p^{t^i} + \sum_{i=1}^{r} \langle a^{u/p_i} \rangle x_i. \tag{11}$$

Here $p_1, ..., p_r$ are all the prime divisors of u, t is a primitive root modulo p and a_p is an element of order p of G.

Proof Let A be the subgroup of $\langle a \rangle$ of order F_u. By Theorem 3.1 we have

$$D = fD_A + \sum_{i=1}^{r} \langle a^{u/p_i} \rangle x_i \tag{12}$$

for some $f \in G$ and $D_A \in \mathbb{Z}[A \times H]$. Note that p^2 does not divide $|A \times H|$ since it does not divide F_u. Thus we can write $A \times H = \langle y \rangle \times H'$ where y is an element of order p of G and p does not divide $v := |H'|$. Let t be a primitive root modulo p with $t \equiv 1 \bmod v$. Let σ be the automorphism of $\mathbb{Q}(\xi_{pv})$ defined by $\xi_{pv}^\sigma = \xi_{pv}^t$.

Claim: σ fixes all prime ideal divisors of n.

Proof of the claim: Let q be an arbitrary prime divisor of n. By Result 2.2 we have to show that there is $j \in \mathbb{Z}$ with

$$t \equiv q^j \bmod v(q)$$

where $v(q)$ is the largest divisor of pv coprime to q. If $q = p$ then $v(q) = v$ and we can take $j = 0$ since $t \equiv 1 \bmod v$. Thus assume $q \neq p$. Recall that $m(q)$ is the largest divisor

of uw coprime to pq. Thus we can write $v(q) = pz$ where z is a divisor of $m(q)$. By assumption (iii) there is an l such that $(l, p-1) = 1$ and $q^l \equiv 1 \bmod z$. By assumption (ii) the order of q and thus of q^l modulo p is $p-1$. Thus there is $k \in \mathbb{Z}$ with $q^{lk} \equiv t \bmod p$. Since we also have $q^{lk} \equiv 1 \equiv t \bmod z$ it follows that $t \equiv q^{lk} \bmod v(q)$ and this concludes the proof of the claim.

Recall that $D_A \in \mathbb{Z}[A \times H]$, $|A|$ is a divisor of $u = o(a)$ and $|H|$ is coprime to n and u. Note that $a^{u/|A|}$ is a generator of A and that $|\chi(D_A)| = n$ for all characters χ of $A \times H$ that sends $a^{u/|A|}$ to be primitive $|A|$-th root of unity. Let $\rho : \mathbb{Z}[A \times H] \to \mathbb{Z}[\xi_{|A|}][H]$ be the homomorphism defined by $\rho(\alpha) = \xi_{|A|}$ and $\rho|_H = \mathrm{id}$. Write $E := \rho(D_A)$. Result 2.5 implies

$$E^{(t)} = \pm \eta h E \tag{13}$$

with $h \in H$ and η an $|A|$-th root of unity. Write $\eta = \eta_p \gamma$ where the order of γ is coprime to p and η_p is a p-th root of unity. Let x be an integer satisfying $x(t-1) \equiv -1 \bmod p$. Then $1 + tx \equiv x \bmod p$ and thus $(E\eta_p^x)^{(t)} = \pm \eta_p^x \gamma h E$ by (13). Replacing the original D by a translate if necessary we thus may assume

$$E^{(t)} = \pm \gamma h E. \tag{14}$$

Using (14) repeatedly gives

$$E = E^{(t^{p-1})} = \gamma^{p-1} r^{p-1} E. \tag{15}$$

Applying the characters of H to (15) and using Result 2.1 we see that $(\gamma h)^{p-1} = 1$ in $\mathbb{Z}[\xi_{|A|}][H]$. This implies that the order of h is a divisor of $p-1$ and $\gamma^{gcd(p-1,|A|)} = 1$. Write $\mu := \pm \gamma h$. Then

$$E^{(t)} = \mu E \tag{16}$$

by (14). Write

$$E = \sum_{i=1}^{p-1} \xi_p^i E_i \tag{17}$$

with $E_i \in \mathbb{Z}[\xi_{|A|/p}][H]$. Since $t \equiv 1 \pmod{v}$, we have $E_i^{(t)} = E_i$ for all i. Using (16) we get

$$E^{(t)} = \sum_{i=1}^{p-1} \xi_p^{ti} E_i = \mu E = \sum_{i=1}^{p-1} \xi_p^i (\mu E_i) = \sum_{i=1}^{p-1} \xi_p^{ti} (\mu E_{ti}).$$

Since $\mu E_i \in \mathbb{Z}[\xi_{|B|}][H]$ (note that $|B| = |A|/p$) for all i and $\xi_p, ..., \xi_p^{p-1}$ are independent over $\mathbb{Z}[\xi_{|B|}][H]$, this implies $E_i = \mu E_{ti}$ for $i = 1, ..., p-1$ and thus $E_{t^j} = \mu^{-j} E_1$ for $j = 1, ..., p-1$. Using (17) we get

$$E = \sum_{j=1}^{p-1} \xi_p^{t^j} E_{t^j} = E_1 \sum_{j=1}^{p-1} \mu^{-j} \xi_p^{t^j}. \tag{18}$$

where $E_1 \in \mathbb{Z}[\xi_{|B|}][H]$. Now choose $D_B \in \mathbb{Z}[B \times H]$, $g' \in B$ such that $\rho(D_B) = E_1$, $\rho(g') = \gamma^{-1}$. (Note that g' exists as $\gamma^{gcd(p-1,|B|)} = 1$.) Hence, there exists $\ell \in \{0, 1\}$ such that $\rho((-1)^\ell g' h^{-1}) = \mu^{-1}$. (Here, we take $\ell = 1$ only when $\mu = -\gamma h$ and $|B|$ is odd.)

Let $g = g'h$ and $a_p \in G$ with $o(a_p) = p$ and $\rho(a_p) = \xi_p$. Then

$$\rho(D_B \sum_{i=1}^{p-1} ((-1)^\ell g)^i a_p^{t^i}) = E_1 \sum_{i=1}^{p-1} \mu^{-i} \xi_p^{t^i} = E = \rho(D_A).$$

Thus Lemma 2.4 and (12) imply

$$D = f D_B \sum_{i=1}^{p-1} ((-1)^\ell g)^i a_p^{t^i} + \sum_{i=1}^{r} \langle a^{u/p_i} \rangle y_i \tag{19}$$

for some $y_1, ..., y_r \in \mathbb{Z}[G]$ and thus the validity of (11). □

Remark 3.5

1. Even though the conditions in Theorem 3.4 seem to be quite restrictive, one easily checks that it is applicable in case n is a p-power. In that case, we obtain a result by Jia [12, Lemma 3.1 (i)]. Indeed, Jia's result was also implicitly shown in [3].

2. If $\gcd(p-1, |G|) = 1$, then the g found in Theorem 3.4 is actually the identity of G. If we further assume n is a p-power, we obtain [19, Theorem 2.7] and [1, Lemma 2].

The next result is proved in [17, Lemma 3.2]. For completeness, we include a proof here.

Lemma 3.6 *Let D_B be the one found in Theorem 3.4. Suppose $r = 1$ and all coefficients in D lie in the interval $[0, C]$. Then all coefficients in D_B lie in the interval $[-C, C]$. In particular, if D is a subset of G, then all nonzero coefficients of D_B are ± 1 and all nonzero coefficient of x_1 in 1.*

Proof Note that $r = 1$ implies $p = p_1$. Thus, we may assume $a_p = a^{u/p_1}$. Write $\Gamma := D_B \sum_{i=1}^{p-1}((-1)^\ell g)^i a_p^{t^i}$ and $\Omega := h^{-1}\langle a^{u/p_1}\rangle x_1$.

First, we show all nonzero coefficients in Ω are between 0 and C. For any f in the support of Ω, we let α_f be its coefficient in Ω. Note that the coefficient remains unchanged if f is replaced by any element in $f\langle a^{u/p}\rangle$. Therefore, to find α_f, we may assume $\circ(f)$ is not divisible by p. On the other hand, the order of every element in the support of Γ is divisible by p. Hence, f is not in the support of Γ. Therefore, α_f is the coefficinet of f in D as well. Thus, α_f lies in the interval $[0, C]$.

Next, we consider those f in the support of $D_B \in \mathbb{Z}[B \times H]$ and let α be the coefficient of f in Γ. We claim that the coefficient of fga_p^t in Γ is $(-1)^\ell\alpha$. It suffice to show that if f' is also in the support of D_B with $f \neq f'$, then the supports of $f\sum_{i=1}^{p-1}((-1)^\ell g)^i a_p^{t^i}$ and $f'\sum_{i=1}^{p-1}((-1)^\ell g)^i a_p^{t^i}$ are disjoint. Observe that if they are not disjoint, then we have $fg^i a_p^{t^i} = f'g^j a_p^{t^j}$ for some $1 \leq i, j \leq p-1$. Since p does not divide the $|B| \cdot |H|$, we deduce that $a_p^{t^i} = a_p^{t^j}$. As t is primitive root moduluo p, we conclude $i = j$. Therefore, $f = f'$.

If f does not lie in the support of Ω, then clearly $(-1)^\ell\alpha \in [0, C]$. Thus, $\alpha \in [-C, C]$. Suppose now f lies in the support of Ω. Then as we have seen from the above argument that α_f, the coefficient of f in Ω, lies in $[0, C]$. Since $\alpha + \alpha_f \in [0, C]$, we conclude that $\alpha \in [-C, C]$.

Finally, if every nonzero coefficient of D is 1, then $C = 1$. Since all coefficients lie in $\mathbb{Z}$, we conclude that every nonzero coefficient of x and D' is ± 1. $\square$

4 Applications

In this section, we give some applications of our main results. We shall continue with the notations and assumptions used in Theorem 3.4.

Theorem 4.1 *Let D be a (v, k, λ, n) difference set in an abelian group $G = \mathcal{P} \times H$ where $\mathcal{P} = \langle a \rangle$ is a cyclic p-subgroup with p odd and $gcd(p, |H|) = 1$. Write $w = \exp H$. For each prime divisor q of n let $m(q)$ be the largest divisor of $|\mathcal{P}|w$ coprime to pq. Assume that*

(i) p^2 does not divide $F(|\mathcal{P}|w, n)$,

(ii) $\mathrm{ord}_p(q) = p - 1$ for all prime divisors $q \neq p$ of n,

(iii) $\gcd(\mathrm{ord}_{m(q)}(q), p - 1) = 1$ for all prime divisors $q \neq p$ of n.

Then there are $g, h \in G$, $Y \subset G$ and $A, B \subset H$ such that A, B are disjoint, $o(g)|(p-1)$ and

$$D = h(A - B) \sum_{i=1}^{p-1} g^i a_p^{t^i} + PY \tag{20}$$

where P is the subgroup of G of order p and a_p is a generator of P.

Furthermore, if either $\gcd(p - 1, |H|) = 1$ or p does not divide n, then g in (20) is 1 and D can be written as

$$D = h(B - A) + PY. \tag{21}$$

Proof By Lemma 2.10 and Theorem 3.4 we have

$$D = hD_B \sum_{i=1}^{p-1} ((-1)^\ell g)^i a_p^{t^i} + PY \tag{22}$$

with $g, h \in G$, $Y \in \mathbb{Z}[G]$, $D_B \in \mathbb{Z}[H]$, and $o(g)|(p-1)$. Observe that $D_B \neq 0$. Otherwise, $\chi(D) = 0$ for every character χ nonprincipal on P and thus D is not a difference set. As shown in Lemma 3.6, every nonzero coefficient of D_B is ± 1 and every nonzero coefficient of Y is 1. In particular, D_B can be written as $A - B$ where A, B are disjoint subsets

in H. Since $D_B \neq 0$, at least one of the A, B is nonempty. Moreover, as we have seen before, the supports of $hA\sum_{i=1}^{p-1}(-g)^i a_p^{t^i}$ and $hB\sum_{i=1}^{p-1}(-g)^i a_p^{t^i}$ are disjoint.

We claim that $\ell = 0$. Otherwise, we then have

$$D = h(A-B)\sum_{i=1}^{p-1}(-g)^i a_p^{t^i} + PY. \tag{23}$$

Take an element $f \in A$.(The case when $f \in B$ can be treated similarly). Write $X := h(A-B)\sum_{i=1}^{p-1}(-g)^i a_p^{t^i}$. Observe that the coefficient of $hfa_p^{t^{p-1}}$ in X is also 1. If $o(g)$ is odd, then the coefficient of $hfg^\alpha a_p^{t^{o(y)}} = hfa_p^{t^\alpha}$ in X is -1. Since all nonzero coefficients in $D = X + PY$ is 1, it follows that the coefficient of $hfa_p^{t^{o(y)}}$ in PY must be 1. Thus, the coefficient of hf in PY must also be 1. As a result, the coefficient of hf in $D = X + PY$ is then 2. But this is impossible. Thus the order of $o(g)$ must be even.

But then v is even and n is a square by Result 2.9. Let χ be a character of G which is trivial on H and nontrivial on P. Applying χ to (23) and Lemma 2.10, we obtain $|\chi(A-B)|^2 = n/p$ since $|\sum_{i=1}^{p-1}(-1)^i\xi_p^{t^i}|^2 = p$. But $\chi(A-B) = |A| - |B|$ as A, B are subsets of H and χ is trivial on H. Thus n/p is also a square. This is impossible and our claim is proved.

Next, we assume further either $\gcd(p-1, |H|) = 1$ or p does not divide n. Suppose $\gcd(p-1, |H|) = 1$. This forces $g = 1$ and thus $D = h(A-B)\sum_{i=1}^{p-1} g^i a_p^{t^i} + PY = h(A-B)(P-1) + PY = -h(A-B) + P(h(A-B)+Y)$.

Suppose p does not divide n and $o(g) \geq 2$. Let χ be a character of G which is nontrivial on $\langle g\rangle$ and P. By the previous result and Lemma 2.10, we obtain $n = |\chi(D)|^2 = |\chi(A-B)|^2 p$. But this is impossible since p does not divide n. Thus $g = 1$ and the assertion follows in same way as in Case 1. □

Theorem 4.1 is the key to the proof of [17, Corollary 3.3], which is crucial in the proof of Lander's conjecture in case n is a p-power with $p > 3$.

The decomposition theorem obtained in the last section leads to the following general bound on the modulus of character values of group ring elements.

Theorem 4.2 *Let $G = \langle a\rangle \times H$ be an abelian group where $w := \exp H$ and $u := o(a)$ are coprime. Let n be a positive integer coprime to w, and let D be an element of $\mathbb{Z}[G]$*

with coefficients in $[0, C]$ *such that* $|\chi(D)|^2 = n$ *for all characters* χ *of* G *whose order is divisible by* u. *Let* $F_u := \gcd(u, F(uw, n))$ *and* $h := |H|$. *Then*

$$4n \leq \frac{hF_u^2C^2}{\varphi(F_u)}.$$

Proof Let A be the subgroup of $\langle a \rangle$ of order F_u. By Theorem 3.1 there is $D_A \in \mathbb{Z}[A \times H]$ with coefficients in $[0, C]$ such that

$$D = gD_A + \sum_{i=1}^{r} \langle a^{u/p_i} \rangle x_i$$

for some $g \in G$, $x_1, ..., x_r \in \mathbb{Z}[G]$ where $p_1, ..., p_r$ are the prime divisors of u. Furthermore, D_A can be chosen such that gD_A and $\sum_{i=1}^{r} \langle a^{u/p_i} \rangle x_i$ have disjoint supports. Replacing D by a translate if necessary, we can assume $g = 1$. Note that $\chi(\langle a^{u/p_i} \rangle) = 0$ for every character χ of G whose order is divisible by u. Thus $|\chi(D_A)|^2 = |\chi(D)|^2 = n$ for all these characters. Write $D_A = \sum_{u \in U} a_u u$ where $U = A \times H$ and $a_u \in \mathbb{Z}$. Since D_A and $\sum_{i=1}^{r} \langle a^{u/p_i} \rangle x_i$ have disjoint supports, we have $0 \leq a_u \leq C$. Note $|U| = F_u h$. Let $l := \sum_{u \in U} a_u$. The coefficient of 1 in $D_A D_A^{(-1)}$ is $\sum_{u \in U} a_u^2$. Thus $F_u h \sum_{u \in U} a_u^2 = \sum_{\chi \in U^*} |\chi(D_A)|^2$ by Result 2.1. Since there are exactly $\varphi(F_u)h$ characters χ of U whose order is divisible by u and since $|\chi(D_A)|^2 = n$ for these characters, we get

$$F_u h \sum_{u \in U} a_u^2 \geq l^2 + \varphi(F_u) hn. \tag{24}$$

since $\chi_0(D_A) = l$. On the other hand, $\sum_{u \in U} a_u^2 \leq Cl$ since $0 \leq a_u \leq C$. Thus $F_u h \sum_{u \in U} a_u^2 - l^2 \leq F_u hCl - l^2 \leq F_u^2 C^2 h^2/4$. Combining this with (24), we get $F_u^2 C^2 h^2/4 \geq \varphi(F_u) hn$ and thus the assertion. □

Theorem 4.2 implies the following general exponent bound for difference sets. It improves upon [23, Theorem. 5.3] and [24, Theorem. 5.1].

Theorem 4.3 *Let* $G = A \times H$ *be an abelian group where* $(|A|, |H|) = 1$. *If* G *contains a* (v, k, λ, n) *difference set with* $(n, |H|) = 1$, *then*

$$\exp A \leq |A| \sqrt{\frac{|H|F^2}{4n\varphi(F)}} \tag{25}$$

where $F := \gcd(\exp A, F(\exp G, n))$. *In particular, if* A *is cyclic, then*

$$n \leq \frac{|H|F^2}{4\varphi(F)}.$$

Proof Let $t := \exp A$, $a := |A|$ and let U be a subgroup of A of order a/t such that A/U is cyclic. Let $\rho : G \to G/U$ be the canonical epimorphism and $E := \rho(D)$. Then E has coefficients in $[0, a/t]$ and $|\chi(E)|^2 = n$ for all nontrivial characters χ of G/U. Thus Theorem 4.2 implies

$$4n \leq \frac{|H|F^2(a/t)^2}{\varphi(F)}$$

yielding the assertion. □

Remark 4.4 If we choose $H = \{1\}$ in Theorem 4.3, we recover [24, Theorem. 5.1]. However, usually a better choice of H yields considerable improvements on [24, Theorem. 5.1]. In many applications, the best choice of H is a complement of the Sylow p-subgroup of G where p is a suitable prime divisor of n.

Hadamard difference sets are known to exist for every u of the form $u = 2^a 3^b r^2$ where $a, b \geq 0$ and r is any positive integer, see [6, Chapter 6]. Here we will consider arbitrary positive integers u.

Corollary 4.5 *If there is a Hadamard difference set in a cyclic group of order* $4u^2$, *then* $u\varphi(u) \leq F(u^2, u)$. *Moroever, there is no circulant Hadamard matrix of order of order* v *with* $4 < v < 548,964,900$.

Proof

Assume the existence of a Hadamard difference set in $\mathbb{Z}_{4u^2}$. Then u is odd by 2.11. Applying Corollary 4.3 with $|A| = u^2$ and $|H| = 4$, we get $u^2 \leq F^2/\varphi(F)$ where $F = \gcd(u^2, F(4u^2, u))$. Note that the change from $m = u^2$ to $m = 4u^2$ in Definition 2.6 can increase any $\mathrm{ord}_{m_q}(q)$ only by a factor of 2. Since u is odd, this shows $F(4u^2, u) =$

$4F(u^2,u)$ and thus $F = F(u^2,u)$. Now part a follows since $F(u^2,u)/\varphi(F(u^2,u)) = u/\varphi(u)$.

Assume the contrary. By [24, Cor. 6.4] we have $v = 4u^2$ and $u = 165$. By result 2.11 there is a Hadamard difference set in the cyclic group of order v. Hence Corollary 4.5 a implies $u\varphi(u) \leq F(u^2,u)$. But for $u = 165$ we have $F(u^2,u) = u^2/3$ and $u\varphi(u) = u^2(2\cdot 4\cdot 10)/(3\cdot 5\cdot 11) = (16/33)u^2$. Thus $16/3 \leq 31/3$, a contradiction $\Box$.

Finally, we apply Corollary 4.5 to the Barker Sequence Conjecture. In [23, Theorem. 6.4] it has been shown that there is no Barker sequence of length l with $13 < l \leq 4\cdot 10^{12}$. The following result extends this bound considerably.

Corollary 4.6 *There is no Barker sequence of length l with*

$$13 < l \leq 10^{22}.$$

Proof Assume the existence of a Barker sequence of length $l > 13$. By the results of [7, 8, 26, 27] we know that $l = 4u^2$ for some odd u which has no prime divisor $\equiv 3 \pmod 4$ and that there is a Hadamard difference set in the cyclic group of order l. Corollary 4.5 a gives

$$u\varphi(u) \leq F(u^2,u). \tag{26}$$

Now a computer search over all $u \leq 5\cdot 10^{10}$ all of whose prime divisors are $\equiv 1 \pmod 4$ shows that there is no such u satisfying (26). This search was done with the help of a C++ program using the C++ class library NTL [25]. $\Box$

References

[1] K.T. Arasu, S.L. Ma: Abelian difference sets without self-conjugacy. *Des. Codes Cryptogr.* **15** (1998), 223-230.

[2] K.T. Arasu, S.L. Ma: A nonexistence result on difference sets, partial difference sets and divisible difference sets. *J. Stat. Planning and Inference* **95** (2001), 67-73.

[3] K.T. Arasu, S.L. Ma: Some new results on circulant weighing matrices. *J. Alg. Combin.* **14** (2001), 91-101.

[4] K.T. Arasu, Q. Xiang: Multiplier Theorems. *J. Comb. Des.* **3** (1995), 257-267.

[5] L.D. Baumert: *Cyclic Difference Sets.* Springer Lecture Notes **182**, Springer 1971.

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

[7] S. Eliahou, M. Kervaire: Barker sequences and difference sets. *L'Enseignement Math.* **38** (1992), 345-382.

[8] S. Eliahou, M. Kervaire, B. Saffari: A new restriction on the length of Golay complementary sequences. *J. Comb. Theory Ser. A* **55** (1990), 49-59.

[9] M. Hall: Cyclic projective planes. *Duke Math. J.* **14** (1947), 1079-1090.

[10] K. Ireland, M. Rosen: *A Classical Introduction to Modern Number Theory.* Graduate Texts in Math. **84**, Springer 1990.

[11] N. Jacobson: *Basic Algebra I.* Second edition. W. H. Freeman and Company 1985.

[12] Z. Jia: New necessary conditions for the existence of difference sets without self-conjugacy. *J. Comb. Theory Ser. A* **98** (2002), 312-327.

[13] D. Jungnickel: Difference Sets. *Contemporary Design Theory: A Collection of Surveys, eds. J.H. Dinitz, D.R. Stinson.* Wiley 1992, 241-324.

[14] D. Jungnickel, B. Schmidt: Difference Sets: An Update. *Geometry, Combinatorial Designs and Related Structures. Proc. First Pythagorean Conference, eds. J.W.P. Hirschfeld et al.* Cambridge University Press 1997, 89-112.

[15] E.S. Lander: *Symmetric Designs: An Algebraic Approach.* London Math. Soc. Lect. Notes **75**, Cambridge University Press 1983.

[16] T.Y. Lam, K.H. Leung: On Vanishing Sums of Roots of Unity. *J. Algebra* **224** (2000), 91-109.

[17] K.H. Leung, S.L. Ma, B. Schmidt, *Lander's conjecture*, submitted

[18] R. Lidl, H. Niederreiter: *Introduction to finite fields and their applications.* Cambridge University Press 1994.

[19] S.L. Ma: Planar Functions, Relative Difference Sets and Character Theory. *J. Algebra* **185** (1996), 342-356.

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

[21] A. Pott: *Finite geometry and character theory.* Springer Lecture Notes **1601**, Springer 1995.

[22] P. Ribenboim: *Algebraic Numbers.* Wiley 1972.

[23] B. Schmidt: Cyclotomic integers and finite geometry. *J. Am. Math. Soc.* **12** (1999), 929-952.

[24] B. Schmidt: Towards Ryser's conjecture. *Proc. European Congress of Mathematics, Barcelona, 2000.* Progress in Mathematics **201**, Birkhäuser 2001, 533-541.

[25] V. Shoup: *NTL: A Library for doing Number Theory.* `http://www.shoup.net/ntl/`

[26] J. Storer, R. Turyn: On binary sequences. *Proc. Amer. Math. Soc.* **12** (1961), 394-399.

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