JOURNAL OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 12, Number 4, Pages 929–952
S 0894-0347(99)00298-2
Article electronically published on May 5, 1999

CYCLOTOMIC INTEGERS AND FINITE GEOMETRY

BERNHARD SCHMIDT

1. Introduction

The most powerful method for the study of finite geometries with regular or quasiregular automorphism groups G is to translate their definition into an equation over the integral group ring $\mathbb{Z}[G]$ and to investigate this equation by applying complex representations of G. For the definitions and the basic facts, see Section 2. If G is abelian, this approach boils down to proving or disproving the existence of elements of $\mathbb{Z}[G]$ with 0-1 coefficients whose character values are cyclotomic integers of certain prescribed absolute values. Up to now there have been two general methods to tackle this problem, namely, Hall's multiplier concept and Turyn's self-conjugacy approach. However, both methods need severe technical assumptions and thus are not applicable to many classes of problems. Despite many efforts over a period of more than 30 years no general method has been found to overcome these difficulties.

In this paper, we present a new approach to the study of combinatorial structures via group ring equations which works without any restrictive assumptions.

In order to understand the method of the present paper it will be instructive to briefly discuss the self-conjugacy concept first. Turyn [51] demonstrated that the character method for the study of group ring equations works very nicely under the so-called self-conjugacy condition. An integer n is called self-conjugate modulo m if all prime ideals above n in the mth cyclotomic field $\mathbb{Q}(\xi_m)$ are invariant under complex conjugation. Under this condition it is possible to find all cyclotomic integers in $\mathbb{Q}(\xi_m)$ of absolute value $n^{t/2}$ for any positive integer t. It is the complete knowledge of the cyclotomic integers of prescribed absolute value which makes the character method work so well under the self-conjugacy condition. Since Turyn's fundamental work [51] there have been dozens of papers extending and refining his approach. However, all these results are restricted to the case of self-conjugacy, and that is a very severe restriction indeed. Namely, the "probability" that n is self-conjugate modulo m decreases exponentially fast in the number of distinct prime divisors of n and m; see Remark 2.2. This means that the self-conjugacy method fails in almost all cases. One may ask if it is possible to extend Turyn's method in order to get rid of the self-conjugacy assumption. It turns out that in general this is impossible – at least with present day methods. The required complete knowledge of the cyclotomic integers of prescribed absolute value would yield an

Received by the editors March 2, 1998 and, in revised form, May 8, 1998.
1991 *Mathematics Subject Classification.* Primary 05B10; Secondary 05B20.
Key words and phrases. Finite geometries with Singer groups, cyclotomic fields, absolute value problem, Ryser's conjecture, circulant Hadamard matrices, quasiregular projective planes, planar functions, group invariant weighing matrices.

almost complete determination of the class group of the underlying cyclotomic field modulo the class group of its maximal real subfield [48, Prop. 3.1]. However, this is a problem of algebraic number theory far beyond the scope of our present knowledge.

Thus there is an urgent need for more general results on cyclotomic integers of prescribed absolute value. However, I am not aware of any substantial progress in this direction since Turyn's work in 1965. In this paper, we will present a new approach to the absolute value problem. We will show that up to multiplication with a root of unity a cyclotomic integer of prescribed absolute value n often already can be found in a small subfield of the original cyclotomic field K. This will be achieved by exploiting the decomposition groups of the prime ideals above n in K.

The reduction to subfields will enable us to obtain a general bound on the absolute value of cyclotomic integers with strong implications on virtually all problems accessible to the character method. In particular, we will obtain strong asymptotic exponent bounds for groups containing difference sets without any restrictive assumptions. In many cases, previously literally nothing had been known on the existence of these difference sets. Our results are a major step towards two longstanding open problems in difference sets, namely Ryser's conjecture and the circulant Hadamard matrix conjecture; see Section 6.

Furthermore, we will derive a general exponent bound on groups containing relative difference sets. As a consequence, we obtain strong necessary conditions for the existence of quasiregular projective planes which, in particular, lead to an asymptotic exponent bound for abelian groups admitting planar functions. Finally, we will utilize our methods for the study of group invariant weighing matrices.

It is interesting to compare our method with the multiplier approach to the study of difference sets which was introduced by Hall [22]. Since Hall's fundamental work in 1947 multipliers have played a dominant role in the investigation of difference sets. The reader is referred to [3, 4, 5, 28, 32, 36, 43] for many applications and variants of Hall's multiplier theorem.

The existence of a multiplier of a difference set D essentially is equivalent to the property that all character values of a suitable translate of D lie in a certain proper subfield of the underlying cyclotomic field. This holds – contrary to the approach of the present paper – not only up to multiplication with a root of unity. Tiny as it may appear at first sight this difference is actually dramatic. It turns out that the existence of multipliers can only be guaranteed under much more restrictive assumptions than we will need to obtain our exponent bounds: In order to prove the existence of a nontrivial multiplier of a (v, k, λ, n)-difference set in an abelian group one usually at least needs the existence of a divisor of n relatively prime to v which is greater than λ; see [3, 5, 32, 43]. This is the reason why, for instance, the multiplier method does not apply to any of the parameter series of known difference sets with $\gcd(v, n) > 1$. Our approach is more general and enables us to prove exponent bounds even in cases which previously had been completely intractable; see Section 6.

2. Preliminaries

In this section, we list the definitions and basic facts we need in the rest of paper. We first fix some notation. We will always identify a subset A of a group G with the element $\sum_{g\in A} g$ of the integral group ring $\mathbb{Z}[G]$. For $B = \sum_{g\in G} b_g g \in \mathbb{Z}[G]$ we

write $B^{(-1)} := \sum_{g\in G} b_g g^{-1}$. A group homomorphism $G \to H$ is always assumed to be extended to a homomorphism $\mathbb{Z}[G] \to \mathbb{Z}[H]$ by linearity.

For an abelian group H we denote its character group by H^*, and for a subgroup W of H, we write $W^\perp$ for the subgroup of all characters which are trivial on W.

We will also 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 [45, p. 269, Thm. 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 [25, chapter 12], for instance. For $\sigma \in \mathrm{Gal}(\mathbb{Q}(\xi_m)/\mathbb{Q})$, we write $\mathrm{Fix}(\sigma)$ for the subfield of $\mathbb{Q}(\xi_m)$ fixed by $\langle\sigma\rangle$. For relatively prime integers t and s, we denote the multiplicative order of t modulo s by $o_s(t)$. Finally, φ denotes the Euler φ-function.

All our results rely on the following complete description of the decomposition groups of prime ideals of cyclotomic fields. This result has been used in many papers and books, however, none that I am aware of contains an appropriate reference. For the convenience of the reader, we shall include a short proof. We recall that the decomposition group of a prime ideal P of $\mathbb{Z}[\xi_m]$ is the set of all $\sigma \in \mathrm{Gal}(\mathbb{Q}(\xi_m)/\mathbb{Q})$ with $P^\sigma = P$.

Theorem 2.1. *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*

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

Proof. The ideal $(1 - \xi_{p^a})$ of $\mathbb{Z}[\xi_m]$ is divisible by P since $(p) = (1 - \xi_{p^a})^{(p-1)p^{a-1}}$ if $a > 0$; see [34, (8.24)]. Hence $(\xi_{p^a}^i)^\tau \equiv 1 \pmod P$ for all $i \in \mathbb{Z}$, and all $\tau \in \mathrm{Gal}(\mathbb{Q}(\xi_m)/\mathbb{Q})$. Let A be any element of $\mathbb{Z}[\xi_m]$, and write $A = \sum_{i=0}^{p^a-1} \xi_{p^a}^i f_i(\xi_{m'})$ with $f_i \in \mathbb{Z}[x]$. If $\sigma \in \mathrm{Gal}(\mathbb{Q}(\xi_m)/\mathbb{Q})$ satisfies (1), then

$$\begin{aligned} A^\sigma &= \sum_{i=0}^{p^a-1} (\xi_{p^a}^i)^\sigma f_i(\xi_{m'}^{p^j}) \equiv \sum_{i=0}^{p^a-1} f_i(\xi_{m'}^{p^j}) \\ &\equiv \Big(\sum_{i=0}^{p^a-1} f_i(\xi_{m'})\Big)^{p^j} \equiv \Big(\sum_{i=0}^{p^a-1} \xi_{p^a}^i f_i(\xi_{m'})\Big)^{p^j} \equiv A^{p^j} \pmod P. \end{aligned}$$

Now, $A \in P$ implies $A^{p^j} \in P$ and thus $A^\sigma \in P$. Hence $P^\sigma \subset P$, implying $P^\sigma = P$ since P^σ is a prime ideal and thus maximal [25, p. 177, Cor. 2]. Thus σ fixes P if it satisfies (1). Note that the number of $\sigma \in \mathrm{Gal}(\mathbb{Q}(\xi_m)/\mathbb{Q})$ satisfying (1) is $\varphi(p^a)o_{m'}(p)$. By the orbit formula, there cannot be any further Galois automorphism of $\mathbb{Q}(\xi_m)$ fixing P since $\mathrm{Gal}(\mathbb{Q}(\xi_m)/\mathbb{Q})$ acts transitively on the set of prime ideals dividing p [25, Prop. 12.3.3] and since there are exactly $\varphi(m')/o_{m'}(p)$ of these ideals [34, Thm. 8.8]. □

Remark 2.2. By Theorem 2.1 a prime ideal P above p in $\mathbb{Q}(\xi_m)$ is invariant under complex conjugation if and only if there is an integer j with $p^j \equiv -1 \mod m'$. In this case p is called self-conjugate modulo m; see [29, 43, 51]. A composite integer n is called self-conjugate modulo m if every prime divisor of n has this property. One can see that a prime p can only be self-conjugate modulo m if the exact power of 2 dividing $o_q(p)$ is the same for all prime divisors $q \neq p$ of m. Thus, loosely speaking, the probability that n is self-conjugate modulo m decreases exponentially fast in

the number of distinct prime divisors of n and in the number of distinct prime divisors of m.

Corollary 2.3 (Turyn [51]). *Assume that $A \in \mathbb{Z}[\xi_m]$ satisfies*

$$A\overline{A} \equiv 0 \mod t^{2b}$$

where b, t are positive integers, and t is self-conjugate modulo m. Then

$$A \equiv 0 \mod t^b.$$

Proof. By Theorem 2.1 the prime ideals above t in $\mathbb{Z}[\xi_m]$ are invariant under complex conjugation. □

We will need the following result of Kronecker. See [6, Section 2.3, Thm. 2] for a proof.

Result 2.4. *An algebraic integer all of whose conjugates have absolute value 1 is a root of unity.*

Note that Result 2.4 implies that any cyclotomic integer of absolute value 1 must be a root of unity since the Galois group of a cyclotomic field is abelian.

Now we are going to prove an ugly as well as necessary lemma on the behavior of the coefficients of cyclotomic integers in basis representations. It generalizes a result of [51].

Lemma 2.5. *Let $m = \prod_{i=1}^{t} p_i^{a_i}$ be the prime power decomposition of a positive integer m, and let k be any divisor of m, say $k = \prod_{i=1}^{s} p_i^{b_i}$ with $s \le t$ and $1 \le b_i \le a_i$ for $i = 1, ..., s$. Then*

$$\begin{aligned} B_{m,k} : \quad = \quad & \{\prod_{i=1}^{s} \xi_{p_i^{a_i}}^{r_i} \prod_{i=s+1}^{t} \xi_{p_i}^{k_i} \xi_{p_i^{a_i}}^{l_i} : 0 \le r_i \le p_i^{a_i - b_i} - 1, \\ & 0 \le k_i \le p_i - 2,\ 0 \le l_i \le p_i^{a_i - 1} - 1\} \end{aligned}$$

is an integral basis of $\mathbb{Q}(\xi_m)$ over $\mathbb{Q}(\xi_k)$. Furthermore, the following hold.

a) Assume that an element X of $\mathbb{Z}[\xi_m]$ has the form

$$X = \sum_{j=0}^{m-1} b_j \xi_m^j \tag{2}$$

where $b_0, ..., b_{m-1}$ are integers with $0 \le b_j \le C$ for some constant C. Then

$$X = \sum_{x \in B_{m,k}} x \sum_{j=0}^{k-1} c_{xj} \xi_k^j \tag{3}$$

where the c_{xj}'s are integers with $|c_{xj}| \le 2^{t-s-1}C$ if $t > s$ and $0 \le c_{xj} \le C$ if $t = s$.

b) If the assumption on the coefficients is replaced by $|b_j| \le C$, then (3) holds with $|c_{xj}| \le 2^{t-s}C$ in any case.

Proof. Using the identities $\xi_{p_i}^{p_i - 1} = -1 - \xi_{p_i} - \cdots - \xi_{p_i}^{p_i - 2}$ for $i = s+1, ..., t$, we see that the linear combinations of elements of $B_{m,k}$ with coefficients from $\mathbb{Z}[\xi_k]$ cover $\mathbb{Z}[\xi_m]$. This shows that $B_{m,k}$ is an integral basis of $\mathbb{Q}(\xi_m)$ over $\mathbb{Q}(\xi_k)$ since $|B_{m,k}| = \varphi(m)/\varphi(k) = \dim(\mathbb{Q}(\xi_m) : \mathbb{Q}(\xi_k))$.

For any j with $0 \le j \le m-1$ we may write

$$\xi_m^j = \xi_k^{u_j} \prod_{i=1}^{s} \xi_{p_i^{a_i}}^{r_{ij}} \prod_{i=s+1}^{t} \xi_{p_i}^{k_{ij}} \xi_{p_i^{a_i}}^{l_{ij}} \tag{4}$$

with $0 \le u_j \le k-1$, $0 \le r_{ij} \le p_i^{a_i-b_i}-1$, $0 \le k_{ij} \le p_i - 1$, $0 \le l_{ij} \le p_i^{a_i-1}-1$.

In order to transform X from form (2) into form (3) we have to get rid of all terms $b_j \xi_m^j$ in (2) for which ξ_m^j contains a factor $\xi_{p_i}^{p_i-1}$ in the second product of representation (4). We do this subsequently for $i = s+1, ..., t$ using the identities $\xi_{p_i}^{p_i-1} = -1 - \xi_{p_i} - \cdots - \xi_{p_i}^{p_i-2}$. This takes $t-s$ steps, and in each step the range of coefficients at most doubles. □

In Section 6 we will need an estimate for the number $\delta(x)$ of distinct prime divisors of a positive integer x. We do not give the best possible bound here. Instead we use a version which easily follows from results of analytic number theory [24, 46] and suffices for the purposes of this paper.

Lemma 2.6. *We have*

$$\delta(x) < \frac{\log x}{\log 2 \log\log x}$$

for every integer $x \ge 3$.

Proof. Let $\pi(y)$ denote the number of primes $\le y$, and write $\vartheta(y) := \sum_{p \le y} \log p$ where the sum ranges over all primes $\le y$. By Corollary 2 and Theorem 10 of [46], we have $\pi(y) < 5y/(4 \log y)$ for all $y \ge 114$ and $\vartheta(y) > 0.89y$ for all $y \ge 227$. Write $\alpha := 0.89$. Let x be an integer with $\log x \ge 227\alpha$. Then $\delta(x) < \pi(\alpha^{-1} \log x)$ since $\prod_{p \le \alpha^{-1} \log x} p = \exp(\vartheta(\alpha^{-1} \log x)) > \exp(\alpha\alpha^{-1} \log x) = x$. Using the estimate for $\pi(y)$ from above we get

$$\begin{aligned} \delta(x) &< 5\alpha^{-1} \log x / (4 \log(\alpha^{-1} \log x)) \\ &< (5\alpha^{-1}/4) \frac{\log x}{\log\log x} \\ &< \frac{\log x}{\log 2 \log\log x}, \end{aligned}$$

proving the assertion for all $x \ge \exp 227\alpha$.

Let b_i denote the product of the first i primes. We have $b_{49} > \exp 227\alpha$. Furthermore, $\delta(x) = \delta(b_{\delta(x)})$ and $x \ge b_{\delta(x)}$ for all integers $x \ge 2$. Since $\log x/(\log 2 \log\log x) > 3$ for all $x \ge 3$ and since $\log x / \log\log x$ is an increasing function for $x \ge 16$, it now suffices to verify the assertion for $x = b_4, b_5, ..., b_{48}$. This can be done with a computer or with patience. □

Corollary 2.7. *For any* $\varepsilon \in \mathbb{R}^+$ *we have*

$$2^{\delta(x)} < x^{\varepsilon}$$

for all integers $x \ge \exp\exp 1/\varepsilon$.

The next result from [2] on the structure of group ring elements whose character values are divisible by a fixed prime power will be needed in Section 7 for the study of quasiregular projective planes.

Lemma 2.8. *Let p be a prime, and let G be an abelian group with a cyclic Sylow p-subgroup of order p^s. If $Y \in \mathbb{Z}[G]$ satisfies*

$$\chi(Y) \equiv 0 \pmod{p^a}$$

for all characters χ of G, then there are $X_0, X_1, ..., X_r \in \mathbb{Z}[G]$ with

$$Y = p^a X_0 + p^{a-1} P_1 X_1 + \cdots + p^{a-r} P_r X_r$$

where $r = \min\{a, s\}$ and P_i, $i = 1, ..., r$, is the subgroup of order p^i of G (viewed as an element of $\mathbb{Z}[G]$).

Now we come to the definitions and basic properties of the combinatorial structures we will study. A (v, k, λ, 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 [5, VI, Thm. 1.6]. Sometimes G is called a Singer group of $\mathcal{D}$. For detailed treatments of difference sets; see [4, 28, 29, 31, 43]. The following lemma is essentially contained in [51] and has turned out to be a *conditio sine qua non* for the study of difference sets.

Lemma 2.9. *Let D be a (v, k, λ, n)-difference set in a group G, let U be a normal subgroup of G such that G/U is abelian, and let $\rho : G \to G/U$ be the canonical epimorphism. Then*

$$\rho(D)\rho(D)^{(-1)} = n + \lambda |U| (G/U)$$

in $\mathbb{Z}[G/U]$ and hence

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

for every nontrivial character χ of G/U.

Proof. The first part follows from $DD^{(-1)} = n + \lambda G$ which is just a translation of the definition of a difference set into $\mathbb{Z}[G]$. To get the second part from the first, we only have to note that $\chi(G/U) = 0$ by the orthogonality relations for characters of abelian groups; see [35, Lemma 7.2], for instance. □

We will need the following consequence of [51, Thm. 6] in Section 6. This result is known as Turyn's exponent bound.

Result 2.10. *Assume the existence of a (v, k, λ, n)-difference set in an abelian group G. Let p be a prime divisor of v, and denote the Sylow p-subgroup of G by S_p. Let U be any subgroup of G with $U \cap S_p = \{1\}$, and assume that p^{2a} divides n for some $a \geq 1$. If p is self-conjugate modulo $\exp(G/U)$, then*

$$\exp(S_p) \leq \frac{|U|}{p^a} |S_p|.$$

Let G be a group of order nm, and let N be a subgroup of G of order n. A subset R of G is called an (m, n, k, λ)-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. We have the following analogue to Lemma 2.9.

Lemma 2.11. *A k-subset R of a group G of order mn is a relative (m,n,k,λ)-difference set in G relative to a subgroup N of order n if and only if*

$$RR^{(-1)} = k + \lambda(G - N)$$

in $\mathbb{Z}[G]$. Let U be a normal subgroup of G, and let $\rho : G \to G/U$ be the canonical epimorphism. Then $\rho(N) = |N \cap U| N_U$ in $\mathbb{Z}[G/U]$ where $N_U = \{Uh : h \in N\}$, and hence

$$\rho(R)\rho(R)^{(-1)} = k + \lambda|U|(G/U) - \lambda|N \cap U|N_U$$

in $\mathbb{Z}[G/U]$. Thus, if G/U is abelian,

$$\chi(\rho(R))\overline{\chi(\rho(R))} = \begin{cases} k & \text{if } \chi \in (G/U)^* \setminus N_U^{\perp}, \\ k - \lambda n & \text{if } \chi \in N_U^{\perp} \end{cases}$$

for every nontrivial character χ of G/U.

Let H and N be groups of order n. A mapping $f : H \to N$ is called a planar function of degree n if $h \mapsto f(gh)f(h)^{-1}$ is a bijection between H and N for every $g \in H \setminus \{1\}$. The standard example for a planar function is the mapping $f : (\mathbb{F}_q, +) \to (\mathbb{F}_q, +), x \mapsto x^2$ where $(\mathbb{F}_q, +)$ is the additive group of the finite field with q elements and q is odd. Here $x^2 := x \cdot x$ where "$\cdot$" is the multiplication in $\mathbb{F}_q$. It is straightforward to check the following.

Lemma 2.12. *A mapping $f : H \to N$ is a planar function if and only if $R := \{(h, f(h)) : h \in H\}$ is an $(n,n,n,1)$-difference set in $H \times N$ relative to N.*

In Section 7 we will prove an asymptotic exponent bound on abelian groups admitting planar functions.

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 [20] for a survey, [15, 40, 41, 49] for some older results and [11, 10, 21, 30, 32, 42] for 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 identify a G-invariant weighing matrix H with the element $\sum_{g \in G} h_{1,g} g$ of $\mathbb{Z}[G]$ and get the following useful result.

Lemma 2.13. *Assume that a weighing matrix $H = W(m,n)$ is G-invariant. Let U be a subgroup of G such that G/U is abelian. Let $\rho : G \to G/U$ denote the canonical epimorphism. Then*

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

for all nontrivial characters χ of G/U when H is viewed as an element of $\mathbb{Z}[G]$.

Proof. The equation $HH^t = nI$ is equivalent to

$$\sum_{g \in G} h_{i,g} h_{j,g} = \sum_{g \in G} h_{1,i^{-1}g} h_{1,j^{-1}g} = \delta_{ij} n$$

for all $i, j \in G$ where δ_{ij} is the Kronecker symbol.

Thus $HH^{(-1)} = \sum_{g,k \in G} h_{1,g} h_{1,k} g k^{-1} = \sum_{l \in G} \left(\sum_{g \in G} h_{1,g} h_{1,l^{-1}g} \right) l = n$ in $\mathbb{Z}[G]$, and the assertion follows by applying $\chi \circ \rho$ to this equation. □

Let s_1 be the number of times the entry 1 occurs in each row of a G-invariant weighing matrix $H = W(m,n)$, and let s be the sum of the entries of the first row (and thus of any row) of H. Then $nG = HH^{(-1)}G = H(H^{(-1)}G) = H(sG) = s^2G$ in $\mathbb{Z}[G]$ and thus $n = s^2$ and $s = s_1 - (s^2 - s_1)$, i.e. $s_1 = s(s+1)/2$. So we have the following.

Lemma 2.14. *If a G-invariant weighing matrix $H = W(m,n)$ exists, then $n = s^2$ for some integer s, and the number of entries 1 in each row of H is $s(s+1)/2$.*

Note that we may assume that s is positive by replacing H by $-H$ if necessary.

3. Character values in small subfields

All that can be said *a priori* about the character sums $\chi(X)$ corresponding to combinatorial structures such as difference sets, planar functions or group invariant weighing matrices is that $\chi(X)$ is an algebraic integer of a prescribed absolute value in the eth cyclotomic fields $\mathbb{Q}(\xi_e)$ over the rationals where e is the order of χ.

The basic fact behind almost all our results is that in most cases one can say much more, namely that $\chi(D)$ times a root of unity lies in a small subfield of $\mathbb{Q}(\xi_e)$. The exact formulation of this basic result will be given in Theorem 3.5.

It will turn out that the integer $F(m,n)$ defined below describes a subring $\mathbb{Z}[\xi_{F(m,n)}]$ of $\mathbb{Z}[\xi_m]$ that already contains all solutions $X \in \mathbb{Z}[\xi_m]$ of $X\overline{X} = n$ up to multiplication with a root of unity.

The prime 2 will need special attention in our considerations as the multiplicative group modulo 2^a is noncyclic for $a \geq 3$.

Definition 3.1. 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

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

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 $q^{o_{m_q}(q)} \not\equiv 1 \pmod{p_i^{b_i+1}}$.

Remark 3.2. For the sake of clarity, we also provide an explicit formula for the numbers b_i. First note that, for fixed i, the set of positive integers x satisfying

$$q^{o_{m_q}(q)} \not\equiv 1 \pmod{p_i^{x+1}}$$

for all $q \in \mathcal{D}(n) \setminus \{p_i\}$ is a ray $[e_i, \infty)$ with $e_i \geq 1$. We have

$$b_i = \begin{cases} 2 & \text{if } p_i = 2,\ c_i \geq 2 \text{ and } e_i = 1, \\ \min(c_i, e_i) & \text{otherwise.} \end{cases}$$

The reason why $b_i = 2$ if $p_i = 2$, $e_i = 1$ and $c_i \geq 2$ is the following. Note that n must be a power of 2 if $p_i = 2$ and $e_i = 1$ (if n has an odd prime divisor q, then $q^{o_{m_q}(q)} \equiv 1 \pmod 4$ by the definition of m_q since m is even if $p_i = 2$). If $p_i = 2$ and n is a power of 2, then (a) or (b) must hold for $p_i = q = 2$, and the condition $(p_i, b_i) \neq (2,1)$ in (a) makes sure that $b_i = 2$ if $c_i \geq 2$. Also note that we have $b_i \geq 2$ if $p_i = 2$ and $m \not\equiv 2 \pmod 4$.

It is worth noting the following important property of $F(m,n)$.

Proposition 3.3. *Let P be a finite set of primes, and let Q be the set of all positive integers which are products of powers of primes in P. Then there is a computable constant $C(P)$ such that*

$$F(m,n) \leq C(P)$$

for all $m,n \in Q$.

We will need a well-known elementary lemma on multiplicative orders for which, however, I do not know a reference. The proof only requires standard arguments concerning the structure of the multiplicative groups modulo p^a (see [26, pp. 274-276], for instance) and will be skipped.

Lemma 3.4. *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 $o_{p^c}(s) = p^{c-b}$ for all $c \geq b$.

b) Let s and t be integers such that $o_{p^b}(s) = o_{p^b}(t)$ 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 $\mathbb{Z}^*_{p^b}$.

Note that the assumption $(p,b) \neq (2,1)$ in Lemma 3.4 a) is necessary since, for instance, $o_8(3) = 2 \neq 2^{3-1}$. The assumption $s \equiv t \equiv 1 \pmod 4$ in part b) also is essential. For instance, $o_8(3) = o_8(5) = 2$, but 3 and 5 generate different subgroups of $\mathbb{Z}^*_8$. Now we are ready to prove the main result of this section.

Theorem 3.5. *Assume $X\overline{X} = n$ for $X \in \mathbb{Z}[\xi_m]$ where n and m are positive integers. Then*

$$X\xi_m^j \in \mathbb{Z}[\xi_{F(m,n)}]$$

for some j.

Proof. Since $\mathbb{Z}[\xi_m] = \mathbb{Z}[\xi_{m/2}]$ for $m \equiv 2 \pmod 4$, we may assume $m \not\equiv 2 \pmod 4$. Write $m = \prod_{i=1}^t {p_i}^{c_i}$ and $F(m,n) = \prod_{i=1}^t {p_i}^{b_i}$ as in Definition 3.1. Recall that $b_i \geq 1$ for all i since the squarefree part of m divides $F(m,n)$. Furthermore, $b_i \geq 2$ if $p_i = 2$; see Remark 3.2. For each $i = 1,...,t$, let s_i be an integer satisfying $s_i \equiv 1 \pmod{p_i^{b_i}}$, $s_i \not\equiv 1 \pmod{p_i^{b_i+1}}$ and $s_i \equiv 1 \pmod{\prod_{j\neq i} p_j^{c_j}}$. Then $o_{p_i^{c_i}}(s_i) = p_i^{c_i-b_i}$ by Lemma 3.4 a). We define $\sigma_i \in \mathrm{Gal}(\mathbb{Q}(\xi_m)/\mathbb{Q})$ by $\sigma_i(\xi_m) = \xi_m^{s_i}$. Then $\xi_{p_i^{b_i}}^{\sigma_i} = \xi_{p_i^{b_i}}^{s_i} = \xi_{p_i^{b_i}}$ since $s_i \equiv 1 \pmod{p_i^{b_i}}$. Thus $\mathrm{Fix}(\sigma_i) = \mathbb{Q}(\xi_{F_i})$ where $F_i = m/p_i^{c_i-b_i}$ since σ_i fixes all elements of $\mathbb{Q}(\xi_{F_i})$ and $\mathbb{Q}(\xi_{F_i})$ has the dimension it is supposed to have by the Galois correspondence [26, p. 239].

Claim 1: For every $i = 1,...,t$ and every prime divisor q of n, the automorphism σ_i fixes all prime ideals dividing q in $\mathbb{Z}[\xi_m]$.

We fix a prime divisor q of n and an $i \in \{1,...,t\}$. By Theorem 2.1, Claim 1 is proven if we can find an integer l_i such that $\sigma_i(\xi_{M_q}) = \xi_{M_q}^{s_i} = \xi_{M_q}^{q^{l_i}}$ where $M_q = \prod_{p_j \neq q} p_j^{c_j}$. If $p_i = q$, then we can take $l_i = 0$ since $s_i \equiv 1 \pmod{\prod_{j\neq i} p_j^{c_j}}$. Thus we may assume $p_i \neq q$. Write $Q := q^{o_{m_q}(q)}$. Note that $o_{p_j^{c_j}}(Q)$ is a power of p_j for any $p_j \neq q$ since $Q \equiv 1 \pmod{p_j}$ by the definition of m_q. We first show that $o_{p_i^{c_i}}(Q)$ is divisible by $p_i^{c_i-b_i}$. This is trivial if $c_i = b_i$. Otherwise condition (c) of Definition 3.1 is satisfied and thus $Q \not\equiv 1 \pmod{p_i^{b_i+1}}$. Then Lemma 3.4 a) shows

that $o_{p_i^{c_i}}(Q)$ indeed is divisible by $p_i^{c_i-b_i}$. Note that we need $b_i \geq 1$ for all i and $b_i \geq 2$ for $p_i = 2$ here in order to apply Lemma 3.4 a).

Since the orders of Q modulo $p_j^{c_j}$, $j = 1, ..., t$, $p_j \neq q$, are relatively prime, there is an integer k_i such that $o_{p_i^{c_i}}(Q^{k_i}) = o_{p_i^{c_i}}(Q)$ and $Q^{k_i} \equiv 1 \pmod{p_j^{c_j}}$ for all $j \neq i$ with $p_j \neq q$. As $o_{p_i^{c_i}}(Q^{k_i}) = o_{p_i^{c_i}}(Q)$ is divisible by $p_i^{c_i-b_i}$ and as $o_{p_i^{c_i}}(s_i) = p^{c_i-b_i}$, there is an integer r_i with $Q^{k_i r_i} \equiv s_i \pmod{p_i^{c_i}}$ by Lemma 3.4 b). Note that we need $Q \equiv 1 \pmod 4$ here if $p_i = 2$ in order to apply Lemma 3.4 b). However, $Q \equiv 1 \pmod 4$ follows from the definition of m_q in this case. We conclude that $Q^{k_i r_i} \equiv s_i \pmod{M_q}$ since $Q^{k_i r_i} \equiv s_i \pmod{p_i^{c_i}}$ and $Q^{k_i r_i} \equiv 1 \equiv s_i \pmod{p_j^{c_j}}$ for all $j \neq i$ with $p_j \neq q$. Thus we can take $l_i = o_{m_q}(q) k_i r_i$. This proves Claim 1.

Claim 2: For every $i = 1, ..., t$ there is an integer j_i with $X\zeta_i^{j_i} \in \mathbb{Z}[\xi_{F_i}]$ where $\zeta_i := \xi_{p_i^{a_i}}$.

Since Claim 2 is vacuous if $c_i = b_i$, we may assume $c_i > b_i$ for the proof. From the assumption $X\overline{X} = n$ and Claim 1 we know that X and X^{σ_i} generate the same ideals in $\mathbb{Z}[\xi_m]$. Hence $X^{\sigma_i} = X\varepsilon$ for some unit ε in $\mathbb{Z}[\xi_m]$. Since σ_i commutes with complex conjugation, we have $|X^{\sigma_i}|^2 = (X\overline{X})^{\sigma_i} = n^{\sigma_i} = n = |X|^2$ and thus $|\varepsilon| = 1$. Hence Result 2.4 shows that ε is a root of unity in $\mathbb{Z}[\xi_m]$. All roots of unity in $\mathbb{Q}(\xi_m)$ have the form $\pm\xi_m^j$ for some j (if there was a further root of unity in $\mathbb{Q}(\xi_m)$, then $\mathbb{Q}(\xi_m) \supset \mathbb{Q}(\xi_t)$ for some multiple $t > m$ of m where $t > 2m$ if m is odd, contradicting $\dim(\mathbb{Q}(\xi_r) : \mathbb{Q}) = \varphi(r)$ for all $r \in \mathbb{Z}^+$ [25, Section 13.2, Cor. 1 to Thm. 1]). Thus we may write $\varepsilon = \delta \prod_{j=1}^t \zeta_j^{e_j}$ with $\delta = \pm 1$ and $\delta = 1$ if m is even. Writing $y_i := o(\sigma_i) = p_i^{c_i-b_i}$ and applying σ_i repeatedly $y_i - 1$ times to the equation $X^{\sigma_i} = X\varepsilon$ yields

$$\delta^{y_i} \zeta_i^{e_i \frac{s_i^{y_i}-1}{s_i-1}} \prod_{j \neq i} \zeta_j^{y_i e_j} = 1.$$

This implies $\delta = 1$, $\zeta_j^{e_j} = 1$ for $j \neq i$ and $\zeta_i^{e_i \frac{s_i^{y_i}-1}{s_i-1}} = 1$ since the orders of the ζ_k, $k = 1, ..., t$, are relatively prime and $\delta = 1$ if m is even. Thus $\varepsilon = \zeta_i^{e_i}$. By definition, $p_i^{b_i}$ is the exact power of p_i dividing $s_i - 1$. Since $o_{p_i^{c_i}}(s_i) = p^{c_i-b_i} = y_i$ and $o_{p_i^{c_i+1}}(s_i) = p^{c_i-b_i+1}$ by Lemma 3.4 a), the exact power of p_i dividing $s_i^{y_i} - 1$ is p^{c_i}. Thus $\zeta_i^{e_i \frac{s_i^{y_i}-1}{s_i-1}} = 1$ implies $e_i \equiv 0 \pmod{p_i^{b_i}}$. Hence there is a solution j_i of the congruence $(s_i - 1)j_i + e_i \equiv 0 \pmod{p_i^{c_i}}$. This implies $(X\zeta_i^{j_i})^{\sigma_i} = X\varepsilon\zeta_i^{j_i s_i} = X\zeta_i^{j_i s_i + e_i} = X\zeta_i^{j_i}$. Hence $X\zeta_i^{j_i} \in \mathrm{Fix}(\sigma_i) = \mathbb{Q}(\xi_{F_i})$ proving Claim 2.

Finally, let $\xi := \prod_{i=1}^t \zeta_i^{j_i}$. Then $X\xi = (X\zeta_i^{j_i}) \prod_{k \neq i} \zeta_k^{j_k} \in \mathbb{Z}[\xi_{F_i}]$ for every i because $X\zeta_i^{j_i} \in \mathbb{Z}[\xi_{F_i}]$ by Claim 2 and $\prod_{k \neq i} \zeta_k^{j_k} \in \mathbb{Z}[\xi_{F_i}]$ by the definition of F_i. Hence $X\xi \in \bigcap_{i=1}^t \mathbb{Z}[\xi_{F_i}] = \mathbb{Z}[\xi_{F(m,n)}]$. □

Remark 3.6. Note that the best we can hope for in Theorem 3.5 is $F(m, n) = m_0$ where $m_0 = \prod_{i=1}^t p_i$. The worst that can happen is $F(m, n) = m$. As the integers b_i from the definition of $F(m, n)$ have to satisfy quite a lot of conditions of the form

$$q^{o_{m_q}(q)} \not\equiv 1 \pmod{p_i^{b_i+1}}$$

it may seem that $F(m, n)$ is usually much bigger than m_0. In order to understand the significance of Theorem 3.5 it is important to note that exactly the opposite is the case. Therefore, we consider the following heuristic argument. We assume

$n \leq m$ and $m_0 \approx \sqrt{m}$ which is the case for many applications we have in mind ("$\approx$" is not used in a strict sense here). Our claim is that $F(m,n) \approx m_0$ in almost all cases.

To see this we estimate the "probability" that one of the conditions

$$(*) \qquad q^{o_{m_q}(q)} \not\equiv 1 \pmod{p_i^2}$$

is violated for a "large" prime divisor p_i of m. Note that $q^{o_{m_q}(q)} \equiv 1 \pmod{p_i}$ by the definition of m_q. Furthermore, the probability that p_i divides $o_{m_q}(q)$ is very low if p_i is large. So $q^{o_{m_q}(q)}$ should take each of the p_i values $1,\ p_i+1, ...,\ (p_i-1)p_i+1$ modulo p_i^2 roughly with the same probability. In particular, the probability that $(*)$ is violated should be approximately around $1/p_i$.

Except for a set of density zero all positive integers x have approximately $\log\log x$ prime divisors [23, Thm. 436]. Note $\log\log n \leq \log\log m \approx \log\log m_0^2 = \log 2 + \log\log m_0 \approx \log\log m_0$. Thus we usually do not have more than approximately $(\log\log n)(\log\log m_0) \approx (\log\log m_0)^2$ of the conditions $(*)$.

Now fix any large p_i, say $p_i \approx m_0^{1/\log\log m_0}$ or larger. By the argument above, the probability that $(*)$ is violated for p_i and some fixed q should be around $1/p_i \leq 1/m_0^{1/\log\log m_0}$. Hence the probability that <u>any</u> of the $\approx (\log\log m_0)^2$ conditions $(*)$ is violated for any large p_i should be less than $(\log\log m_0)^2/m_0^{1/\log\log m_0} = y^2 \exp(-\frac{1}{y}\exp y)$ where $y := \log\log m_0$. Thus, for large m_0, the condition $(*)$ should hold for <u>all</u> large p_i and all q with very high probability. By Definition 3.1 this amounts to $F(m,n) \approx m_0$.

4. An upper bound for the absolute value of cyclotomic integers

In this section, we will obtain an upper bound on the absolute value of cyclotomic integers which will be basic for our further results. By $\delta(r)$ ($\delta_{odd}(r)$) we denote the number of distinct (odd) prime divisors of r.

Theorem 4.1. *Let $X \in \mathbb{Z}[\xi_m]$ be of the form*

$$(5) \qquad X = \sum_{i=0}^{m-1} a_i \xi_m^i$$

where $a_0, ..., a_{m-1}$ are integers with $0 \leq a_i \leq C$ for some constant C. Furthermore, assume that $X\overline{X}$ is an integer and that $X \in \mathbb{Z}[\xi_f]$ for some divisor f of m. Then

$$X\overline{X} \leq 2^{2\delta(m)-\delta(f)-2} C^2 f$$

if $\delta(f) < \delta(m)$ and

$$X\overline{X} \leq 2^{\delta_{odd}(m)-1} C^2 f$$

if $\delta(f) = \delta(m)$.

If the assumption on the coefficients a_i is replaced by $|a_i| \leq C$, then in any case

$$X\overline{X} \leq 2^{2\delta(m)-\delta(f)} C^2 f.$$

Proof. <u>Case 1:</u> We first consider the case $0 \leq a_i \leq C$ and $\delta(f) < \delta(m)$. By Lemma 2.5 a) we may write (5) in the form

$$(6) \qquad X = \sum_{x \in B_{m,f}} x \sum_{j=0}^{f-1} b_{xj} \xi_f^j$$

with $|b_{xj}| \le 2^{\delta(m)-\delta(f)-1}C$. As $X \in \mathbb{Z}[\xi_f]$, all terms $\sum_{j=0}^{f-1} b_{xj}\xi_f^j$ with $x \ne 1$ vanish. So we get

$$X = \sum_{j=0}^{f-1} b_{1j}\xi_f^j \tag{7}$$

with $|b_{1j}| \le 2^{\delta(m)-\delta(f)-1}C$. Thus

$$X\overline{X} = \sum_{i,j=0}^{f-1} b_{1i}b_{1j}\xi_f^{i-j} \tag{8}$$

$$= \sum_{k=0}^{f-1} c_k\xi_f^k \tag{9}$$

with $|c_k| \le 2^{2\delta(m)-2\delta(f)-2}C^2 f$.

Using part b) of Lemma 2.5 now, we get

$$X\overline{X} = \sum_{x\in B_{f,1}} d_x x \tag{10}$$

with $|d_x| \le 2^{2\delta(m)-\delta(f)-2}C^2 f$.

Recall that $B_{f,1}$ is an integral basis of $\mathbb{Q}(\xi_f)$ over $\mathbb{Q}$. Since we assumed that $X\overline{X}$ is an integer, (10) implies $d_1 = X\overline{X}$ and $d_x = 0$ for $x \ne 1$. Thus $X\overline{X} = d_1 \le 2^{2\delta(m)-\delta(f)-2}C^2 f$, proving the assertion in Case 1.

Case 2: Now we consider the case $0 \le a_i \le C$ and $\delta(f) = \delta(m)$. By Lemma 2.5 a) we have $0 \le b_{xj} \le C$ in (6) and thus $0 \le b_{1j} \le C$ in (7), $0 \le c_k \le C^2 f$ in (9) and $|d_x| \le 2^{\delta(m)-1}C^2 f$ in (10). This proves the assertion in Case 2 if m is odd.

Now assume that m is even. Since we assumed $\delta(f) = \delta(m)$ for Case 2, f is also even, say $f = 2^a r$ with $a \ge 1$ where r is odd. Since $\xi_{2^a}^{2^{a-1}} = -1$ we may write (7) in the form

$$X = \sum_{i=0}^{2^{a-1}-1}\sum_{k=0}^{r-1} b'_{ik}\xi_{2^a}^i\xi_r^k$$

with $|b'_{ik}| \le C$. Then, again using $\xi_{2^a}^{2^{a-1}} = -1$, we get

$$X\overline{X} = \sum_{i,j=0}^{2^{a-1}-1}\sum_{k,l=0}^{r-1} b'_{ik}b'_{jl}\xi_{2^a}^{i-j}\xi_r^{k-l}$$

$$= \sum_{i=0}^{2^{a-1}-1}\xi_{2^a}^i\sum_{j=0}^{r-1} c_{ij}\xi_r^j$$

with $|c_{ij}| \le C^2 2^{a-1}r$. Using Lemma 2.5 b) we get

$$X\overline{X} = \sum_{i=0}^{2^{a-1}-1}\xi_{2^a}^i\sum_{x\in B_{r,1}} d_{ix}x$$

with $|d_{ix}| \le 2^{\delta(r)}C^2 2^{a-1}r$. Since $X\overline{X}$ is an integer and since $\{\xi_{2^a}^i x : 0 \le i \le 2^{a-1}-1,\ x \in B_{r,1}\}$ is independent over $\mathbb{Q}$, we get $X\overline{X} = d_{01} \le 2^{\delta(r)}C^2 2^{a-1}r = 2^{\delta_{odd}(m)-1}C^2 f$, concluding the proof for Case 2.

Case 3: Now assume $|a_i| \leq C$. Then we have $|b_{xj}| \leq 2^{\delta(m)-\delta(f)}C$ in (7) by Lemma 2.5 b) and thus $|c_k| \leq 2^{2\delta(m)-2\delta(f)}C^2 f$ in (9) and $|d_x| \leq 2^{2\delta(m)-\delta(f)}C^2 f$ in (10), concluding the proof. □

Combining Theorem 3.5 and Theorem 4.1 we obtain the following.

Theorem 4.2. *Let $X \in \mathbb{Z}[\xi_m]$ be of the form*

$$X = \sum_{i=0}^{m-1} a_i \xi_m^i \tag{11}$$

where $a_0, ..., a_{m-1}$ are integers with $0 \leq a_i \leq C$ for some constant C. Furthermore, assume that $X\overline{X} = n$ is an integer. Then

$$n \leq 2^{s-1}C^2 F(m,n)$$

where s is the number of distinct odd prime divisors of m.

If the assumption on the coefficients a_i is replaced by $|a_i| \leq C$, then

$$n \leq 2^t C^2 F(m,n)$$

where t is the number of distinct prime divisors of m.

5. A general exponent bound for difference sets

In this section, we derive a strong exponent bound for abelian groups containing difference sets. Our result does not rely on any restrictive assumption such as self-conjugacy and therefore is more general than all previously known nonexistence results on difference sets.

For a (v,k,λ,n)-difference set D in an abelian group G define

$$f(D) := \min\{t : \ \chi(D)\xi_v^{j(\chi)} \in \mathbb{Z}[\xi_t] \text{ for some } j(\chi) \text{ for all } \chi \in G^*\}.$$

In other words, $f(D)$ is the smallest positive integer such that up to multiplication with a root of unity all character values of D lie in the $f(D)$th cyclotomic field. The results of this section will show that the parameter $f(D)$ is of fundamental importance for the study of difference sets. It is a striking fact that $f(D) = 1$ for all known difference sets with $\gcd(v,n) > 1$ in abelian groups. However, I am not aware of any previous general results on $f(D)$ besides the self-conjugacy condition which guarantees $f(D) = 1$, but does not apply in most cases.

We first state the most general version of our exponent bound. The main aim of this section being the study of difference sets in abelian groups, we also obtain a very strong nonexistence result on difference sets in nonabelian groups as a by-product.

Theorem 5.1. *Let G be a (possibly nonabelian) group with a normal subgroup U such that G/U is cyclic of order e. Let $\rho : G \to G/U$ denote the canonical epimorphism. Assume that G contains a (v,k,λ,n)-difference set and that*

$$\chi(\rho(D))\xi_e^j \in \mathbb{Z}[\xi_f]$$

for some character χ of G/U of order e, some integer j and some divisor f of e. Then

$$e \leq \left(\frac{2^{2\delta(e)-\delta(f)-2+\varepsilon} f}{n}\right)^{\frac{1}{2}} v$$

where $\varepsilon = 0$ if e is even or $\delta(f) < \delta(e)$ and $\varepsilon = 1$ otherwise.

Proof. By replacing D by a translate if necessary, we may assume $\chi(\rho(D)) \in \mathbb{Z}[\xi_f]$. Since D is a subset of G, we have $\rho(D) = \sum_{g \in G/U} d_g g$ for some integers d_g with $0 \le d_g \le |U|$. As the kernel of χ on G/U has order $v/(|U|e)$, we can write

$$\chi(\rho(D)) = \sum_{i=0}^{e-1} a_i \xi_e^i \tag{12}$$

with $0 \le a_i \le v/e$. Combining Lemma 2.9 and Theorem 4.1 gives

$$n = \chi(\rho(D))\overline{\chi(\rho(D))} \le 2^{2\delta(e)-\delta(f)-2}\frac{v^2}{e^2}f$$

for $\delta(f) < \delta(e)$ and

$$n \le 2^{\delta_{odd}(e)-1}\frac{v^2}{e^2}f$$

for $\delta(f) = \delta(e)$. To complete the proof, we only have to note $\delta_{odd}(e) = \delta(e) - 1$ if e is even and $\delta_{odd}(e) = \delta(e)$ if e is odd. □

Combining Theorem 4.1 and Theorem 5.1 we arrive at the main result of this section.

Theorem 5.2. *Assume the existence of a (v, k, λ, n)-difference set D in a group G. If U is a normal subgroup of G such that G/U is cyclic of order e, then*

$$e \le \left(\frac{2^{s-1}F(e,n)}{n}\right)^{\frac{1}{2}} v$$

where s is the number of distinct odd prime divisors of e.

Proof. By Lemma 2.9 and Theorem 3.5 the assumptions of Theorem 5.1 are satisfied for $f = F(e, n)$. This proves Theorem 5.2 since $\delta(F(e, n)) = \delta(e)$ by Definition 3.1 and $\delta(e) - 2 + \varepsilon = s - 1$ if $\delta(e) = \delta(f)$. □

It is worth stating the abelian case separately.

Theorem 5.3. *Assume the existence of a (v, k, λ, n)-difference set in an abelian group G. Then*

$$\exp(G) \le \left(\frac{2^{s-1}F(v,n)}{n}\right)^{\frac{1}{2}} v$$

where s is the number of distinct odd prime divisors of v.

Remark 5.4. In order to understand the strength of Theorem 5.3 we once more resort to an intuitive argument. For many parameters of putative difference sets and all parameter series of known difference sets with $\gcd(v, n) > 1$ we have $n \approx v$ and the squarefree part v_0 of v is approximately $\sqrt{v}$ or less (again, "$\approx$" is not used in a strict sense here). For our reasoning we assume the worst, i.e. $v_0 \approx \sqrt{v}$. By Remark 3.6, we should have $F(v, n) \approx v_0$ in almost all cases. Since $2^{s-1} \approx 2^{\log\log v_0} < \log v_0$ and $n \approx v$, we get $\frac{2^{s-1}F(v,n)}{n} \approx v^{-\frac{1}{2}}$. We conclude that, loosely speaking, Theorem 5.3 shows

$$\exp(G) \le |G|^{3/4}$$

in almost all cases with $v_0 \approx \sqrt{v}$ and $n \approx v$.

6. Difference sets with $\gcd(v, n) > 1$

The most interesting test cases for our exponent bound are the parameter series corresponding to known families of difference sets. In this section, we apply Theorem 5.3 to all parameter series corresponding to known difference sets with $\gcd(v, n) > 1$. The following is a complete list of these series; see [28, 29].

(i) Hadamard parameters:

$$(v, k, \lambda, n) = (4u^2, 2u^2 - u, u^2 - u, u^2)$$

where u is any positive integer.

(ii) McFarland parameters:

$$(v, k, \lambda, n) = (q^{d+1}[\frac{q^{d+1} - 1}{q - 1} + 1], q^d \frac{q^{d+1} - 1}{q - 1}, q^d \frac{q^d - 1}{q - 1}, q^{2d})$$

where $q = p^f \neq 2$ and p is a prime.

(iii) Spence parameters:

$$(v, k, \lambda, n) = (3^{d+1} \frac{3^{d+1} - 1}{2}, 3^d \frac{3^{d+1} + 1}{2}, 3^d \frac{3^d + 1}{2}, 3^{2d})$$

where d is any positive integer.

(iv) Chen/Davis/Jedwab parameters:

$$(v, k, \lambda, n) = (4q^{2t} \frac{q^{2t} - 1}{q^2 - 1}, q^{2t-1}[\frac{2(q^{2t} - 1)}{q + 1} + 1], q^{2t-1}(q - 1)\frac{q^{2t-1} + 1}{q + 1}), q^{4t-2})$$

where $q = p^f$, p is a prime, and t is any positive integer.

We do not allow $q = 2$ for the McFarland parameters since then $(v, k, \lambda, n) = (2^{2d+2}, 2^{2d+1} - 2^d, 2^{2d} - 2^d, 2^{2d})$, and these are Hadamard parameters with $u = 2^d$. Hadamard difference sets are known to exist for every u of the form $u = 2^a 3^b r^2$ where $a, b \in \{0, 1\}$ and r is any positive integer; see [29]. Here we will consider arbitrary u. McFarland and Spence difference sets are known for any prime power q and any positive integer d; see [29]. Difference sets of type (iv) are known to exist only if f is even or $p \leq 3$; see [9, 12, 29]. However, in this section we will consider arbitrary f and p. We will first deal with Hadamard difference sets. A lot of work has been devoted to finding necessary conditions for the existence of Hadamard difference sets; see [1, 8, 7, 13, 37, 38, 39, 44, 51]. However, all these results rely either on the self-conjugacy condition or on very restrictive assumptions on the parameter u. In particular, almost nothing has been known on the existence of Hadamard difference sets for which u has many prime divisors. The following consequence of our exponent bound 5.3 changes this situation dramatically.

Theorem 6.1. *For any finite set P of primes there is a computable constant $C(P)$ such that*

$$\exp(G) \leq C(P)|G|^{1/2}$$

for any abelian group G containing a Hadamard difference set whose order u^2 is a product of powers of primes in P.

Proof. By Proposition 3.3 there is a constant $C_0(P)$ such that $F(4u^2,u^2)\le C_0(P)$ for all u which are products of powers of primes in P. Thus by Theorem 5.3

$$\exp(G)\le 2^{(|P|-1)/2}C_0(P)^{1/2}\cdot 4u = C(P)|G|^{1/2}$$

where $C(P)=2^{(|P|+1)/2}C_0(P)^{1/2}$. □

Theorem 6.2. *Let G be an abelian group containing a difference set whose parameters (v,k,λ,n) are of type (ii), (iii) or (iv) of the the above list. Then for any fixed $\varepsilon>0$ the following hold if v is large enough:*

a) $\exp(G)\le p^{-\frac{(1-\varepsilon)fd-1}{2}}|G|$ *for McFarland parameters,*

b) $\exp(G)\le 3^{-\frac{(1-\varepsilon)d}{2}}|G|$ *for Spence parameters,*

c) $\exp(G)\le p^{-f[t-\varepsilon(t-1)]+1/2}|G|$ *for Chen/Davis/Jedwab parameters.*

Proof. a) Assume the existence of a difference set with McFarland parameters in an abelian group. We only deal with the case where p is odd. The case $p=2$ is similar. If we take $p_1=p$ in Definition 3.1, we see that $F(v,n)$ divides $p(\frac{q^{d+1}-1}{q-1}+1)$ since $b_1=1$. This implies

$$F(v,n)\le 2pq^d. \tag{13}$$

Let s be the number of odd prime divisors of v. Then

$$2^{s-1}\le 2^{\delta(\frac{q^{d+1}-1}{q-1}+1)}\le\frac{q^{\varepsilon d}}{2} \tag{14}$$

if v is large enough by Corollary 2.7 (generate the factor $1/2$ on the right hand side of (14) by the right interpretation of "large enough"). From Theorem 5.3 and (13), (14) we obtain part a) of Theorem 6.2. The proofs for parts b) and c) are similar. □

Ryser's conjecture [47, p. 139] asserts that there is no (v,k,λ,n)-difference set with $\gcd(v,n)>1$ in any cyclic group. The next application of Theorem 5.3 shows that Ryser's conjecture is true for most of the parameters of known difference sets.

Theorem 6.3. *a) If there is a Hadamard difference set in a cyclic group of order $4u^2$, then $F(4u^2,u^2)\ge 2^{-s+1}u^2$ where s is the number of distinct odd prime divisors of u.*

b) If there is a difference set with McFarland parameters in a cyclic group of order $q^{d+1}[\frac{q^{d+1}-1}{q-1}+1]$, $q=p^f$, then $d=f=1$.

c) There are no difference sets with Spence or Chen/Davis/Jedwab parameters in any cyclic groups.

Proof. a) This is immediate from Theorem 5.3.

b) Assume the existence of a difference set with McFarland parameters in a cyclic group G of order $v=q^{d+1}[\frac{q^{d+1}-1}{q-1}+1]$ where $q=p^f$, and p is a prime.

Claim 1: $fd\le 2$.

Proof: If we take $p_1=p$ in Definition 3.1, then $b_1=1$ if p is odd and $b_1=2$ if $p=2$. In both cases $F(v,n)$ divides $p(\frac{q^{d+1}-1}{q-1}+1)$ since $\frac{q^{d+1}-1}{q-1}+1$ is even for $p=2$. Thus

$$F(v,n)\le 2pq^d. \tag{15}$$

We denote the number of all divisors of a positive integer r by $D(r)$. Since the divisors of r occur in pairs $(x, r/x)$, $x \leq \sqrt{r}$, we have $D(r) < 2\sqrt{r}$ for any r. Since $2^{\delta(r)} \leq D(r)$, we get

$$2^{\delta(r)} < 2\sqrt{r} \tag{16}$$

for any positive integer r. Let s be the number of distinct odd prime divisors of v. Note $s \leq 1 + \delta(\frac{q^{d+1}-1}{q-1} + 1)$. Thus

$$2^{s-1} < 2\sqrt{2q^d} \tag{17}$$

by (16) and since $\frac{q^{d+1}-1}{q-1} + 1 \leq 2q^d$. Using (15), (17) and $\exp(G) = v$ together with Theorem 5.3 we get

$$4\sqrt{2}p > q^{d/2} = p^{fd/2}. \tag{18}$$

Thus one of the following cases must occur:

(1) $fd \leq 2$,
(2) $fd = 3$ and $p \leq 31$,
(3) $fd = 4$ and $p \leq 5$,
(4) $fd = 5$ and $p \leq 3$,
(5) $fd = 6$ and $p = 2$.

However, all triples (p, f, d) occurring in the cases (2)–(5) can be ruled out by a direct application of Theorem 5.3. Thus we have established Claim 1.

Claim 2: If $fd = 2$, then $p < 441$.

Proof: Assume $fd = 2$ and $p > 441$. Then $a := \frac{q^{d+1}-1}{q-1} + 1 > p^2 > 442^2 = 195,364$. Thus $a > \exp(\exp(1/\varepsilon))$ where $\varepsilon = 2/5$. By Corollary 2.7 we get $2^{\delta(a)} < a^{2/5}$. Also note $a \leq 2q^d$. Thus

$$2^{s-1} = 2^{\delta_{odd}(v)-1} \leq 2^{\delta(a)} < a^{2/5} < \sqrt{2}q^{2d/5}. \tag{19}$$

Since we assumed $\exp(G) = v$, we get $n = q^{2d} \leq 2^{s-1}F(v, n)$ from Theorem 5.3. Using (15), (19) and $q^d = p^{fd} = p^2$ we conclude $p^{1/5} < 2\sqrt{2}$, contradicting $p > 441$. This proves Claim 2.

In order to complete the proof of part b) of Theorem 6.3 it remains to show that $fd = 2$ and $p \leq 439$ is impossible. A straightforward direct application of Theorem 5.3 rules out all these cases with the single exception of $(p, f, d) = (3, 1, 2)$, i.e. $(v, k, \lambda, n) = (2 \cdot 3^3 \cdot 7, 3^2 \cdot 13, 3^2 \cdot 4, 3^4)$. However, in this case, 3 is self-conjugate modulo v. Thus no difference set with these parameters can exist in the cyclic group by Result 2.10. This concludes the proof of part b).

c) In the case of Spence parameters we have $F(v, n) \leq 3(3^{d+1} - 1)/2$ and $s \leq d$ in Theorem 5.3 and thus $\exp(G) < (2/3)^{d-2}v$. This leaves only the case $d = 1$ where we have $(v, k, \lambda, n) = (36, 15, 6, 9)$. But 3 is self-conjugate modulo 36, and thus no difference set with these parameters can exist in the cyclic group by Result 2.10.

In order to prove the nonexistence of difference sets with Chen/Davis/Jedwab parameters in cyclic groups G we apply Result 2.10. First assume that p is odd. Denote the Sylow p-subgroup of G by S_p. Note that S_p is cyclic of order q^{2t}. Let U be the subgroup of G of order $2\frac{q^{2t}-1}{q^2-1}$. Then p is self-conjugate modulo

$e := \exp(G/U)$ since e is 2 times a power of p. Thus Result 2.10 implies

$$q^{2t} = \exp(S_p) \leq |U||S_p|/q^{2t-1} = 2q\frac{q^{2t}-1}{q^2-1}.$$

Thus $1 < 2q/(q^2-1)$, contradicting $q \geq 3$.

Finally, for $p = 2$ we take $|U| = \frac{q^{2t}-1}{q^2-1}$, and apply the same argument. □

A circulant Hadamard matrix of order m is a weighing matrix $W(m,m)$ that is invariant under the cyclic group $\mathbb{Z}_m$. Examples for such matrices are known only for $m = 1, 4$ (take (1), respectively $(1,1,1,-1)$, as the first row). It is well known that the order of a Hadamard matrix must be 1, 2 or a multiple of 4 [47, p. 106]. Moreover, we know from Lemma 2.14 that the order of a circulant Hadamard matrix must be a square. Thus $m = 4u^2$ for some $u \in \mathbb{Z}^+$ if a circulant Hadamard matrix of order $m > 1$ exists. Using Lemmas 2.9 and 2.13, it can be checked that a circulant Hadamard matrix M of order $4u^2$ exists if and only if there is a Hadamard difference set D in $\mathbb{Z}_{4u^2}$. For instance, if H is the group ring element corresponding to M, then $D := (G+H)/2$ is the desired Hadamard difference set.

The circulant Hadamard matrix conjecture asserts that there is no circulant Hadamard matrix of order greater than 4. This conjecture was first mentioned in Ryser's book [47, p. 134], but goes back further to obscure sources. Turyn [51, 52] proved that u must be odd if a circulant Hadamard matrix of order $4u^2$ exists and that the circulant Hadamard matrix conjecture is true for $u < 55$. However, since Turyn's work in the 60s there has not been any progress on this conjecture because of the lack of methods to overcome the failure of the self-conjugacy approach.

Using the equivalence to Hadamard difference sets in cyclic groups, we can apply Theorem 6.3 a) to the circulant Hadamard matrix conjecture. Remark 3.6 strongly suggests that part a) of Theorem 6.3 should rule out the existence of circulant Hadamard matrices for almost all u. We confirm this by the following result of a computer search.

Range of u (u odd)	# of cases not ruled out by Theorem 6.3 a)
$3 \leq u \leq 10^4$	26
$10^5 \leq u \leq 10^5 + 10^4$	2
$10^6 \leq u \leq 10^6 + 10^4$	1
$10^7 \leq u \leq 10^7 + 10^4$	1
$10^8 \leq u \leq 10^8 + 10^4$	0

By [51, Theorem 6], one can rule out 12 of the 26 cases with $u \leq 10,000$ not covered by Theorem 6.3 a). The remaining open cases with $u \leq 10,000$ are $u =$ 165, 231, 1155, 2145, 2805, 3255, 3905, 5115, 5187, 6699, 7161, 8151, 8645, 9867.

A Barker sequence of length l is a sequence $(a_i)_{i=1}^l$ with $a_i = \pm 1$ such that $|\sum_{i=1}^{l-k} a_i a_{i+k}| \leq 1$ for $1 \leq k \leq l-1$. It is known that the existence of a Barker sequence of length $l > 13$ implies the existence of a circulant Hadamard matrix of size l; see [51, 52]. Thus $l = 4u^2$ where u is odd. Furthermore, it is shown in [17] that l cannot have a prime divisor $p \equiv 3 \bmod 4$ if $l > 13$ is the length of a Barker sequence. Combining these two results with Theorem 6.3 a) we get the following

bound by a computer search. It improves the previously known bound [16, p. 363] by a factor greater than 10^6. We do not need Turyn's inequality [51, Thm. 6] to obtain this result.

Theorem 6.4. *There is no Barker sequence of length l with*

$$13 < l \leq 4 \cdot 10^{12}.$$

7. Relative difference sets, quasiregular projective planes and planar functions

In this section, we utilize our results on cyclotomic integers to obtain a nonexistence theorem on relative difference sets. No results of comparable generality have previously been known. A treatment of most of the previously known results can be found in [43, Chapters 4,5]. In particular, we will obtain new necessary conditions for the existence of relative $(n, n, n, 1)$-difference sets which are equivalent to quasiregular projective planes of type b) of the Dembowski/Piper classification [14]; see Proposition 7.2 below. We will combine this result with a further new nonexistence theorem on relative $(n, n, n, 1)$-difference sets to derive a strong asymptotic exponent bound on abelian groups admitting planar functions.

If the prime power conjecture for projective planes is true, then, in particular, n must be a prime power if a relative $(n, n, n, 1)$-difference set exists. It is known that n must be a power of 2 if a relative $(n, n, n, 1)$-difference set with even n exists in an abelian group; see [18] or [27]. In an important paper, Ma [33] proved that there is no relative $(n, n, n, 1)$-difference set in an abelian group if n is a product of two primes. However, aside from Ma's result and a simple exponent bound [43, Thm. 4.1.1] very little had been known about the existence of relative $(n, n, n, 1)$-difference sets in general – especially if n has many prime divisors; see [43, Section 5.4]. As for the Hadamard difference sets, our results are the first to tackle these cases.

Theorem 7.1. *Assume the existence of an (m, n, k, λ)-difference set R in a group G relative to N. Let U be any subgroup of G not containing N such that G/U is cyclic of order e. Then*

$$|U \cap N| \leq \left(\frac{2^{s-1}F(e,k)}{k}\right)^{1/2} |U|$$

where s is the number of distinct odd prime divisors of e.

Proof. Let $\rho : G \to G/U$ be the canonical epimorphism, and let χ be a character of G/U of order e. Note that χ is nontrivial on $N_U := NU/U$ since U does not contain N. Since any coset of N contains at most one element of R and since χ has a trivial kernel, we have $\chi(\rho(R)) = \sum_{i=0}^{e-1} a_i \xi_e^i$ with $0 \leq a_i \leq C$ where $C = |U|/|U \cap N|$. Since χ is nontrivial on N_U we get

$$k = \chi(\rho(R))\overline{\chi(\rho(R))} \leq 2^{s-1}F(e,k)|U|^2/|U \cap N|^2$$

from Lemma 2.11 and Theorem 4.2, proving the theorem. □

Now we are going to study relative $(n, n, n, 1)$-difference sets corresponding to quasiregular projective planes of type b) of the Dembowski/Piper classification [14]. These projective planes (of order n) admit a quasiregular collineation group of order n^2 with exactly three point orbits whose sizes are $1, n, n^2$. Here a collineation group G is called quasiregular if it induces a regular operation on all its point

orbits, i.e. if all points in any fixed orbit of G have the same stabilizer. Since the conjugates of a point stabilizer coincide with the stabilizers of the points in the same orbit, a collineation group G is quasiregular if and only if all its point stabilizers are normal subgroups of G. In particular, any abelian collineation group is quasiregular. Next, we describe the connection between quasiregular projective planes and relative $(n, n, n, 1)$-difference sets. For the convenience of the reader, we sketch the proof.

Proposition 7.2. *There is a projective plane of order n with a quasiregular collineation group G of order n^2 and point orbits of size $1, n, n^2$ if and only if there is an $(n, n, n, 1)$-difference set R in G relative to a normal subgroup N.*

Proof. Assume that there is a projective plane of order n with a collineation group G as described in the assertion. By [14, Thm. 4] the orbits of size $1, n$ form an incident point-line pair (p_0, L_0). Since G acts regularly on the point orbit $\mathcal{O}$ of size n^2, we may identify G with $\mathcal{O}$. Let $p \neq p_0$ be a point incident with L_0, and let $L \neq L_0$ be a line through p. Then $N := G_p$ is a normal subgroup of G of order n, and a straightforward verification shows that $L \setminus \{p\}$ is an $(n, n, n, 1)$-difference set in G relative to N. The converse is proven by reversing this construction. □

The next theorem will be needed for the proof of our asymptotic exponent bound for groups admitting planar functions. It is the only result of this paper which does not rely on the methods developed in Sections 3 and 4.

Theorem 7.3. *Let G be an abelian group containing an $(n, n, n, 1)$-difference set R relative to N. Let p be a prime divisor of n, and let S be the Sylow p-subgroup of N. If p^a is the exact power of p dividing n, then*

$$\exp(S) \leq p^{\lceil a/2 \rceil}$$

where $\lceil x \rceil$ denotes the smallest integer $\geq x$.

Proof. Let $o(g)$ denote the order of an element g of G. Assume $e := \exp(S) \geq p^{\lceil a/2 \rceil + 1}$ and let $S = \langle a_1 \rangle \times \cdots \times \langle a_t \rangle$, $o(a_1) = e$, be a decomposition of S into a direct product of cyclic groups. Let $G = \langle b_1 \rangle \times \cdots \times \langle b_s \rangle$ be a decomposition of G into cyclic groups of prime power order and write $a_1 = \prod_{j=1}^{s} b_j^{t_j}$ where w.l.o.g. $o(b_1^{t_1}) = e$.

Define $\chi \in G^*$ by $\chi(b_1) = \xi_{o(b_1)}$ and $\chi(b_j) = 1$ for $j > 1$ and write $K := \operatorname{Ker}\ \chi$. Then G/K is a cyclic p-group whose order is at least $p^{\lceil a/2 \rceil + 1}$ since $o(b_1) \geq o(b_1^{t_1}) = e \geq p^{\lceil a/2 \rceil + 1}$. Furthermore, $|S \cap K| = |\operatorname{Ker}\ \chi|_S| = p^a/e$.

Let $\rho : G \to G/K$ be the canonical automorphism. We have $\chi(\rho(R))\overline{\chi(\rho(R))} \in \{0, n\}$ by Lemma 2.11 implying $\chi(\rho(R))\overline{\chi(\rho(R))} \equiv 0 \pmod{p^a}$ for every nontrivial $\chi \in (G/K)^*$. Since p is self-conjugate modulo any power of p and thus modulo $\exp(G/K)$, we get $\chi(\rho(R)) \equiv 0 \pmod{p^{\lfloor a/2 \rfloor}}$ for every nontrivial $\chi \in (G/K)^*$ from Corollary 2.3. This congruence also holds for the trivial character χ_0 of G/K since $\chi_0(\rho(R)) = |R| = n$. Thus we can apply Lemma 2.8 and get (using the notation of Lemma 2.8)

$$\rho(R) = p^{\lfloor a/2 \rfloor} X_0 + p^{\lfloor a/2 \rfloor - 1} P_1 X_1 + \cdots + X_{\lfloor a/2 \rfloor} P_{\lfloor a/2 \rfloor}.$$

Thus $p^{\lfloor a/2 \rfloor}$ divides $\rho(R)\rho(R)^{(-1)}$. From Lemma 2.11 we get

$$\rho(R)\rho(R)^{(-1)} = n - |S \cap K|N + |K|G.$$

Thus $p^{\lfloor a/2 \rfloor}$ divides $|S \cap K| = p^a/e$, contradicting $e \geq p^{\lceil a/2 \rceil + 1}$. □

It is known that a planar function from $\mathbb{Z}_n$ to $\mathbb{Z}_n$ cannot exist if n is even, not squarefree or the product of two primes or if there are two prime divisors p, q of n such that p is self-conjugate modulo q; see [33, Thm. 1.1, Cor. 4.4]. However, very little has been known about planar functions $f : H \to N$ for which H and N are noncyclic abelian groups. Our next result provides an asymptotic exponent bound on H and N.

Theorem 7.4. *For any finite set P of primes there is a computable constant $C(P)$ such that*

$$\exp(H), \exp(N) \leq C(P)\sqrt{n}$$

for any abelian groups H, N admitting a planar function $f : H \to N$ whose degree n is a product of powers of primes in P.

Proof. Assume that there is a planar function $f : H \to K$ where H and K are abelian groups of order n, and n is a product of powers of primes in P. By Lemma 2.12 there is an $(n, n, n, 1)$-difference set in $G := H \times N$ relative to N. From Theorem 7.3 we get

$$\exp(N) \leq \sqrt{n} \prod_{p \in P} \sqrt{p}. \tag{20}$$

Let χ be a character of G of order $e := \exp(H)$ with $|\ker \chi \cap N| = n/p$ where p is some prime divisor of n. Write $U := \ker \chi$ and note $|U| = n^2/e$. Then G/U is cylic of order e and thus

$$|U \cap N| = n/p \leq \left(\frac{2^{|P|-1} F(e, n)}{n} \right)^{1/2} n^2/e$$

by Theorem 7.1. Thus

$$e = \exp(H) \leq C' \sqrt{n} \tag{21}$$

where $C' = p \left(2^{|P|-1} C(P)\right)^{1/2}$ and $C(P)$ is the constant from Proposition 3.3.

Now the assertion follows from (20) and (21). □

8. Group invariant weighing matrices

In this final section, we apply Theorem 4.2 to group invariant weighing matrices and give an example of a strong asymptotic exponent bound that can be derived in this way. Very little has been known about the existence of group invariant weighing matrices. The case which has attracted the most attention is that of circulant weighing matrices, i.e. matrices $W(m, n)$ which are invariant under the cyclic group $\mathbb{Z}_m$; see [15, 40, 41, 49]. It is known that circulant weighing matrices $W(q^2 + q + 1, q^2)$ exist for all prime powers q [49]. On the nonexistence side, it has been shown that there are no circulant weighing matrices $W(m, m-1)$ for $m > 2$ [41] and that a circulant weighing matrix $W(m, n)$ with odd m can only exist if $(m-n)^2 - (m-n) \geq n-1$ [19]. Further nonexistence results can be obtained using multiplier theorems or Turyn's self-conjugacy approach. However, these methods only work under severe restrictions on the parameters m and n and, as usual, fail in

most cases when m or n have many prime divisors. As a consequence of Theorem 4.2 we obtain the following result which is of much broader applicability. Recall that by Lemma 2.14 a group invariant weighing matrix $W(m,n)$ can only exist if n is a square.

Theorem 8.1. *Assume the existence of a G-invariant weighing matrix $H = W(m,s^2)$ where s is a positive integer. Let U be a subgroup of G such that G/U is cyclic of order e. Then*

$$s \le \left(2^t F(e,s)\right)^{1/2} |U|$$

where t is the number of distinct prime divisors of e.

In particular, the existence of a circulant weighing matrix $W(m,s^2)$ implies

$$s^2 \le 2^r F(m,s)$$

where r is the number of distinct prime divisors of m.

Proof. Let $\rho : G \to G/U$ be the canonical epimorphism, and let χ be a character of G/U of order e. If we view H as an element of $\mathbb{Z}[G]$ (see the paragraph preceding Lemma 2.13), then $\rho(H) = \sum_{g\in G/U} a_g g$ with $|a_g| \le |U|$ for all g since H has coefficients $-1,0,1$ only. As χ has a trivial kernel, we get $\chi(\rho(H)) = \sum_{i=0}^{e-1} b_i \xi_e^i$ with $|b_i| \le |U|$ for all i. Now we apply Lemma 2.13 and Theorem 4.2 and get

$$s^2 = \chi(\rho(H))\overline{\chi(\rho(H))} \le 2^t |U|^2 F(e,s)$$

(note $F(e,s) = F(e,s^2)$), proving the assertion. □

Note that Theorem 8.1 is weaker than Theorem 6.3 a) in the case of circulant Hadamard matrices since we had to deal with coefficients $-1,0,1$ instead of just $-1,1$. As an example illustrating the power of Theorem 8.1 we give an application to the family of group invariant weighing matrices $W(2s^2,s^2)$ where s is a positive integer. This is a rich and interesting family since examples for such matrices are known for any square s: There are Hadamard difference sets of order $n = s^2$ in suitable abelian groups G for any square s [9]. If D is such a Hadamard difference set (viewed as a group ring element) and $\rho : G \to G/U$ is a projection onto a subgroup U of G of order 2, then $\rho(D) - (G/U) \in \mathbb{Z}[G/U]$ describes a G/U-invariant weighing matrix $W(2s^2,s^2)$. It is straightforward to verify this using Lemma 2.9.

Corollary 8.2. *Let P be any finite set of primes, and let Q be the set of all products of powers of primes in P. Then there is a computable constant $C(P)$ such that*

$$\exp(G) \le C(P)s$$

for any $s \in Q$ and any abelian group G of order $2s^2$ for which a G-invariant weighing matrix $W(2s^2,s^2)$ exists.

In particular, a circulant weighing matrix $W(2s^2,s^2)$ can only exist for finitely many $s \in Q$.

Proof. This is immediate from Proposition 3.3 and Theorem 8.1. □

Acknowledgement

I would like to thank M. Matsumoto for guidance and encouragement, and M. Hagita for interesting discussions.

References

[1] K.T. Arasu, J.A. Davis, J. Jedwab: A nonexistence result for abelian Menon difference sets using perfect binary arrays. Combinatorica 15 (1995), 311-317. MR **96i:**05031

[2] K.T. Arasu, J.A. Davis, J. Jedwab, S.L. Ma, R.L. McFarland: Exponent bounds for a family of abelian difference sets. In: Groups, Difference Sets, and the Monster. Eds. K.T. Arasu, J.F. Dillon, K. Harada, S.K. Sehgal, R.L. Solomon. DeGruyter Verlag, Berlin/New York (1996), 129-143. MR **98b:**05014

[3] K.T. Arasu, Q. Xiang: Multiplier Theorems. J. Comb. Des. 3 (1995), 257-267. MR **96b:**05032

[4] L.D. Baumert: Cyclic Difference Sets. Springer Lecture Notes 182, Springer, Berlin (1971). MR **44:**97

[5] T. Beth, D. Jungnickel, H. Lenz: Design Theory. Cambridge University Press, Cambridge (1986). MR **88b:**05021

[6] A.I. Borevich, I.R. Shafarevich: Number Theory. Academic Press, New York/San Francisco/London (1966). MR **33:**4001

[7] W.K. Chan: Necessary Conditions for Menon Difference Sets. Designs, Codes and Cryptography 3 (1993), 147-154. MR **94c:**05015

[8] W.K. Chan, S.L. Ma, M.K. Siu: Non-existence of certain perfect arrays. Discrete Math. 125 (1994), 107-113. MR **94k:**05038

[9] Y.Q. Chen: On the existence of abelian Hadamard difference sets and a new family of difference sets. Finite Fields Appl. 3 (1997), 234-256. MR **98h:**05036

[10] R. Craigen: The structure of weighing matrices having large weights. Designs, Codes and Cryptography 5 (1995), 199-216. MR **96a:**05030

[11] R. Craigen, H. Kharaghani: Hadamard matrices from weighing matrices via signed groups. Designs, Codes and Cryptography 12 (1997), 49-58. MR **98m:**05029

[12] J.A. Davis, J. Jedwab: A unifying construction of difference sets. Technical Report HPL-96-31, Hewlett-Packard Labs., Bristol (1996).

[13] J.A. Davis, J. Jedwab: Nested Hadamard Difference Sets. J. Stat. Plann. Inf. 62 (1997), 13-20. MR **98h:**05037

[14] P. Dembowski, F. Piper: Quasiregular collineation groups of finite projective planes. Math. Zeitschrift 99 (1967), 53-75. MR **35:**6576

[15] P. Eades, R.M. Hain: On Circulant Weighing Matrices. Ars Comb. 2 (1976), 265-284. MR **55:**7808

[16] S. Eliahou, M. Kervaire: Barker sequences and difference sets. L'Enseignement Math. 38 (1992), 345-382. MR **93i:**11018

[17] S. Eliahou, M. Kervaire, B. Saffari: A new restriction on the length of Golay complementary sequences. J. Comb. Theory (A) 55 (1990), 49-59. MR **91i:**11020

[18] M.J. Ganley: On a paper of Dembowski and Ostrom. Arch. Math. 27 (1976), 93-98. MR **54:**13716

[19] A.V. Geramita, J.M. Geramita, J. Seberry: Orthogonal Designs. J. Lin. Multilin. Algebra 3 (1975/76), 281-306. MR **54:**12548

[20] A.V. Geramita, J. Seberry: Orthogonal designs III. Weighing matrices. Utilitas Math. 6 (1974), 209-236. MR **54:**12551

[21] M. Gysin, J. Seberry: On the weighing matrices of order $4n$ and weight $4n-2$ and $2n-1$. Australas. J. Combin. 12 (1995), 157-174. MR **96e:**05032

[22] M. Hall: Cyclic projective planes. Duke Math. J. 14 (1947), 1079-1090. MR **9:**370b

[23] G.H. Hardy, E.M. Wright: An Introduction to the Theory of Numbers. Fifth Edition. Oxford University Press (1979). MR **81i:**10002

[24] A.E. Ingham: The distribution of prime numbers. Cambridge Tract. No. 30. Cambridge University Press (1932).

[25] K. Ireland, M. Rosen: A Classical Introduction to Modern Number Theory. Graduate Texts in Math. No. 84. Springer Verlag, Berlin/New York/Heidelberg (1990). MR **92e:**11001

[26] N. Jacobson: Basic Algebra I. Second edition. W. H. Freeman and Company, New York (1985). MR **86d:**00001

[27] D. Jungnickel: On a theorem of Ganley. Graphs and Comb. 3 (1987), 141-143. MR **89e:**05042

[28] D. Jungnickel: Difference Sets. In: J.H. Dinitz and D.R. Stinson, eds., Contemporary Design Theory: A Collection of Surveys. Wiley, New York (1992), 241-324. CMP 92:17

[29] D. Jungnickel, B. Schmidt: Difference Sets: An Update. In: Geometry, Combinatorial Designs and Related Structures. Proceedings of the First Pythagorean Conference, Eds. J.W.P. Hirschfeld, S.S. Magliveras, M.J. de Resmini. Cambridge University Press (1997), 89-112.
[30] C. Koukouvinos, J. Seberry: Weighing matrices and their applications. J. Stat. Plann. Inf. 62 (1997), 91-101. MR **98c:**62143
[31] E.S. Lander: Symmetric Designs: An Algebraic Approach. London Math. Soc. Lect. Notes 75, Cambridge University Press, Cambridge (1983). MR **85d:**05041
[32] W. de Launey: On the nonexistence of generalized weighing matrices. Ars Comb. 17 (1984), 117-132. MR **85j:**05011
[33] S.L. Ma: Planar Functions, Relative Difference Sets and Character Theory. J. Algebra 185 (1996), 342-356. MR **98b:**05016
[34] H.B. Mann: Introduction to Algebraic Number Theory. Ohio State University Press, Columbus, Ohio (1955). MR **17:**240e
[35] H.B. Mann: Addition Theorems. Wiley, New York (1965). MR **31:**5854
[36] R.L. McFarland: On multipliers of abelian difference sets. Ph.D. Dissertation, Ohio State University (1970).
[37] R.L. McFarland: Difference sets in abelian groups of order $4p^2$. Mitt. Math. Sem. Giessen 192 (1989), 1-70. MR **90g:**05048
[38] R.L. McFarland: Sub-difference sets of Hadamard difference sets. J. Comb. Theory (A) 54 (1990), 112-122. MR **91f:**05022
[39] R.L. McFarland: Necessary conditions for Hadamard difference sets. In: Coding theory and design theory, Part II, IMA Vol. Math. Appl., 21. Springer, New York (1990), 257-272. MR **91g:**05020
[40] R.C. Mullin: A note on balanced weighing matrices. In: Combinatorial Mathematics III, Springer, Berlin/Heidelberg/New York (1975), 28-41. MR **51:**12573
[41] R.C. Mullin, R.G. Stanton: On the non-existence of a class of circulant balanced weighing matrices. SIAM J. Appl. Math. 30 (1976), 98-102. MR **53:**12994
[42] H. Ohmori: Classification of weighing matrices of order 12 and weight 9. Discrete Math. 116 (1993), 55-78. MR **94g:**05021
[43] A. Pott: Finite geometry and character theory. Springer Lecture Notes 1601, New York (1995). MR **98j:**05032
[44] D.K. Ray-Chaudhuri, Q. Xiang: New Necessary Conditions for Abelian Hadamard Difference Sets. J. Stat. Plann. Inf. 62 (1997), 69-79. MR **98m:**05021
[45] P. Ribenboim: Algebraic Numbers. Wiley, New York (1972). MR **49:**4968
[46] J.B. Rosser, L. Schoenfeld: Approximate Formulas for some Functions of Prime Numbers. Illinois J. Math. 6 (1962), 64-94. MR **25:**1139
[47] H.J. Ryser: Combinatorial Mathematics. Wiley, New York (1963). MR **27:**51
[48] B. Schmidt: Cyclotomic Integers of Prescribed Absolute Value and the Class Group, J. Number Theory 72 (1998), 269–281. CMP 99:04
[49] J. Seberry, A.L. Whiteman: Some results on weighing matrices. Bull. Austral. Math. Soc. 12 (1975), 433-447. MR **52:**144
[50] J. Storer, R. Turyn: On binary sequences. Proc. Amer. Math. Soc. 12 (1961), 394-399. MR **23:**A2333
[51] R.J. Turyn: Character sums and difference sets. Pacific J. Math. 15 (1965), 319-346. MR **31:**3349
[52] R.J. Turyn: Sequences with small correlation. In: H.B. Mann (ed.), Error Correcting Codes, Wiley, New York (1969), 195-228. MR **39:**3897
[53] Q. Xiang: On reversible abelian Hadamard difference sets. J. Statist. Plann. Inference 73 (1998), 409–416. CMP 99:04

Department of Mathematics, 253-37 Caltech, Pasadena, California 91125
E-mail address: schmidt@cco.caltech.edu
Current address: Am alten Hof 12, 63683 Ortenberg, Germany