Towards Ryser's conjecture

Bernhard Schmidt

Abstract. Ryser's conjecture asserts that there is no (v,k,λ)-difference set with $\gcd(v,k-\lambda)>1$ in any cyclic group. We survey what is known on this conjecture and obtain progress towards it by improving the exponent bound for difference sets in [12]. As a consequence, with three possible exceptions, Ryser's conjecture is true for all parameters of known (v,k,λ)-difference sets with $k \le 5\cdot 10^{10}$. In particular, the circulant Hadamard matrix conjecture holds for orders $\le 10^{11}$, also with only three possible exceptions. Finally, we obtain the first necessary and sufficient condition known in the literature for the existence of an infinite class of difference sets not relying on the self-conjugacy assumption.

1. Introduction

In 1938, Singer discovered that the desarguesian projective geometry $\mathrm{PG}(n,q)$ admits a cyclic regular automorphism group, nowadays called the **Singer cycle** of $\mathrm{PG}(n,q)$. Such an automorphism group is equivalent to a certain *difference set* in a cyclic group. Here a $(\mathbf{v},\mathbf{k},\lambda)$**-difference set** means a k-subset D of a group G of order v such that every nonidentity element g of G has exactly λ representations $g=d_1d_2^{-1}$ with $d_1,d_2\in D$. We call D **abelian**, **cylic** etc. if G has this property. The parameter $n:=k-\lambda$ is called the **order** of D. For convenience, n sometimes is added to the parameters, and we speak of a (v,k,λ,n)-difference set. Difference sets with $n=0,1$ are called **trivial** and will be excluded from our considerations.

Singer's discovery of an infinite family of difference sets inspired the development of an existence theory for these objects. First only cyclic groups were considered, later the theory was extended to noncyclic finite groups. In this paper, we mainly will be interested in the cyclic case. Until recently, only two main methods for the study of difference sets were known: Hall's multiplier theorem [3, 1947] and Turyn's self-conjugacy approach [16, 1965]. Both methods work well for *small* parameters (v,k,λ,n). Thus it was possible to settle the existence problem for cyclic difference sets with $k\le 100$ already in the 60s [2, 1969]. These results and the fact that no cyclic (v,k,λ,n)-difference set with $\gcd(v,n)>1$ has ever been found motivate the following conjecture of Ryser [11] from 1963.

Conjecture 1.1 (Ryser's conjecture) *There is no cyclic (v,k,λ,n)-difference set with $\gcd(v,n)>1$.*

Ryser's conjecture is still open, only some partial results are known. Despite many efforts, there had not been any new results since Turyn's work [16, 1965] until substantial progress was obtained in [12]. In the present paper, we will improve upon [12].

Ryser's conjecture implies two further longstanding conjectures, namely, the Barker and the circulant Hadamard matrix conjecture. 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 conjecture** asserts that there are no Barker sequences of length $v > 13$. Storer and Turyn [15] proved the Barker conjecture for all odd v. The following is well known, see [1, Rem. 14.13].

Result 1.2 *Ryser's conjecture implies the circulant Hadamard matrix conjecture which in turn implies the Barker conjecture.*

In [12], the Barker conjecture was verified for $v \leq 4 \cdot 10^{12}$. In the present paper, we will show that the circulant Hadamard matrix conjecture holds for $v \leq 10^{11}$ with only three possible exceptions. We will also show that, again with only three possible exceptions, Ryser's conjecture is true for all parameters of known difference sets with $k \leq 5 \cdot 10^{10}$.

Let us briefly discuss the previous work related to Ryser's conjecture. Hall's table of difference sets [3, 1956] shows that Ryser's conjecture is true for $k \leq 50$ with eleven possible exceptions. These eleven cases were eliminated by the independent and overlapping work of Mann [6], Rankin [10], Turyn [16], and Yamamoto [18]. Thus, in 1965, it was known that Ryser's conjecture is true for $k \leq 50$. Baumert [2, 1969] extended the table for difference sets in cyclic groups to $k \leq 100$ and, in particular, showed that Ryser's conjecture holds in this range. The two most difficult cases $(v, k, \lambda) = (441, 56, 7)$ and $(891, 90, 9)$ were excluded by H. Rumsey (unpublished) by extensive computations, see [2]. Baumert's table was extended by Vera Lopez and Garcia Sanchez [17, 1997] to $k \leq 150$. Together with the previously known results, their table shows the following.

Result 1.3 *Ryser's conjecture is true for $k \leq 107$.*

To my knowledge, the following are the only open cases for Ryser's conjecture with $k \leq 150$: $(v, k, \lambda) = (429, 108, 27)$, $(715, 120, 20)$, $(351, 126, 45)$, $(465, 150, 50)$, see [17]. We will be able to exclude the third of these cases later.

The most important result on Ryser's conjecture aside from [12] is the following due to Turyn [16]. We recall that a prime p is called **self-conjugate** modulo

an integer w if -1 is a power of p modulo the p-free part of w. A composite integer m is called self-conjugate modulo w if every prime divisor of m has this property.

Result 1.4 *Assume the existence of a cyclic (v,k,λ,n)-difference set. Let m and w be positive integers with $(m,w)>1$ such that m^2 divides n, w divides v, and m is self-conjugate modulo w. Then*

$$m \le \frac{2^{r-1}v}{w}$$

where r is the number of prime divisors of (m,w).

Turyn's result shows that Ryser's conjecture is true in the case of self-conjugacy:

Corollary 1.5 *If there is a prime p dividing (v,n) which is self-cojugate modulo v, then there is no cylic (v,k,λ,n)-difference set.*

We note that the self-conjugacy assumption is very rarely satisfied if v has many prime divisors. In the present paper, we will obtain a result which does not need severe assumptions like self-conjugacy and thus is of broader applicability.

2. Characters

The standard method for the study of difference sets in abelian groups is the use of complex characters. We summarize the necessary facts here, see [7] for proofs. Let G be a finite abelian group. A complex character of G is a homomorphism $\chi : G \to \mathbb{C}^*$. The character χ_0 defined by $\chi_0(g)=1$ for all $g \in G$ is called the **trivial** character. The set of characters of G forms a group G^* isomorphic to G where the group operation is defined by $\chi_1\chi_2(g)=\chi_1(g)\chi_2(g)$. If χ is a character of G of order e, then $\chi(g)$ is a complex eth root of unity for all $g \in G$. Any character of G can be extended to the group ring $\mathbb{Z}[G]$ by linearity. A subset D of G will be identified with $\sum_{d\in D} d \in \mathbb{Z}[G]$. For $X=\sum_{g\in G} a_g g \in \mathbb{Z}[G]$ we write $X^{(-1)} := \sum_{g\in G} a_g g^{-1}$. We use the notation $\xi_t = e^{2\pi i/t}$.

Lemma 2.1 ([16]) *Let D be a (v,k,λ,n)-difference set in an abelian group G. Let χ be a character of G of order e. Then $\chi(D) \in \mathbb{Z}[\xi_e]$ and*

$$|\chi(D)|^2 = n.$$

3. The field descent

Lemma 2.1 has been used in dozens of papers for the study difference sets. Almost all of these results rely on the self-conjugacy assumption. The main merit of [12] is to provide a method free from this restrictive condition. The key to this method is the so-called "field descent", see [12, Thm. 3.5]. For the formulation of the field descent, we need a definition.

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*

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

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

Result 3.2 (Field descent) *Assume $|X|^2 = n$ 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.

In [12], Result 3.2 was used to obtain a general exponent bound for difference sets. In the Section 5, we will improve upon this bound considerably.

4. Bounding the absolute value

In this section, we will use Result 3.2 to obtain an upper bound on the absolute value of cyclotomic integers. This bound is an improvement upon [12, Thm. 4.2]. In the present paper, we will only give the applications of our new bound to abelian difference sets. Similar applications to relative difference sets, planar functions, and group invariant weighing matrices can be given [13, Chapter 3].

As a preparation for the proof of our bound, we need a simple lemma on conjugate characters. Two characters χ and τ of order e of an abelian group G are called **conjugate** if there is $\sigma \in \mathrm{Gal}(\mathbb{Q}(\xi_e)/\mathbb{Q})$ with $\chi(g) = \tau(g)^\sigma$ for all $g \in G$. Let φ denote the Euler totient function. The following is well known and easy to prove, see [9, p.6], for instance.

Lemma 4.1 *Let χ be a character of order e of an abelian group G. Then χ has exactly $\varphi(e)$ distinct conjugates. Furthermore, if $\chi(A) \in \mathbb{Q}$ for some $A \in \mathbb{Z}[G]$, then $\tau(A) = \chi(A)$ for all conjugates τ of χ.*

The following theorem on cyclotomic integers of prescribed absolute value is the main result of this paper.

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

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

with $0 \le a_i \le C$ *for some constant* C *and assume that* $n := X\overline{X}$ *is an integer. Then*

$$n \le \frac{C^2 F(m,n)^2}{4\varphi(F(m,n))}.$$

Proof. By Theorem 3.2, we can assume $X \in \mathbb{Z}[\xi_f]$ where $f := F(m,n)$. Since $1, \xi_m, ..., \xi_m^{m/f-1}$ are independent over $\mathbb{Q}(\xi_f)$, we have $X = \sum_{i=0}^{f-1} b_i \xi_f^i$ where $b_i := a_{im/f}$. Now we view X also as an element of the group ring $\mathbb{Z}[G]$ where $G = \langle \xi_f \rangle$. Since $X\overline{X} = n \in \mathbb{Q}$, we have

$$\chi(X)\overline{\chi(X)} = n \tag{1}$$

for all $\varphi(f)$ characters χ of G of order f by Lemma 4.1. Write $l := \sum_{i=0}^{f-1} b_i$. The coefficient of 1 in $XX^{(-1)}$ is $\sum_{i=0}^{f-1} b_i^2$. From the Fourier inversion formula, we get $f\sum_{i=0}^{f-1} b_i^2 = \sum_{\tau \in G^*} |\tau(X)|^2$. Using (1) and $\chi_0(X) = l$ for the trivial character χ_0 of G, we get

$$f\sum b_i^2 \ge l^2 + \varphi(f)n. \tag{2}$$

Since $0 \le b_i \le C$, we have $\sum b_i^2 \le Cl$. Thus $f\sum b_i^2 - l^2 \le fCl - l^2 \le f^2C^2/4$. Combining this with (2) gives the assertion. □

5. A field descent exponent bound

We now apply Theorem 4.2 to obtain a general exponent bound on abelian groups containing difference sets. By φ we denote the Euler totient function.

Theorem 5.1 *Assume the existence of a* (v,k,λ,n)*-difference* D *set in an abelian group* G*. Then*

$$\exp G \le \frac{vF(v,n)}{2\sqrt{n\varphi(F(v,n))}}.$$

In particular, if G *is cyclic, then*

$$n \le \frac{F(v,n)^2}{4\varphi(F(v,n))}.$$

Proof. Let χ be a character of G of order $e := \exp G$. By Lemma 2.1, we have $|\chi(D)|^2 = n$. Also, since the kernel of χ on G has order v/e, we have

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

with $0 \le a_i \le v/e$. Thus, from Theorem 4.2, we get the assertion. □

6. Application to Ryser's conjecture

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 5.1 to all parameter series corresponding to known difference sets with $\gcd(v,n)>1$. The following is a complete list of these series, see [4, 5] or [1].

(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 $u=2^a3^br^2$ where $a,b\geq 0$ and r is any positive integer, see [5]. Here we will consider arbitrary positive integers u. McFarland and Spence difference sets are known for any prime power q and any positive integer d, see [5]. Difference sets of type (iv) are known to exist only if f is even or $p\leq 3$, see [1, 5]. However, here we will consider arbitrary f and p.

Now we come to the application of Theorem 5.1. The next theorem shows that Ryser's conjecture is true for most parameters of known difference sets.

Theorem 6.1

a) If there is a Hadamard difference set in a cyclic group of order $v=4u^2$ then $F(v,u)^2/\varphi(F(v,u))\geq v$.

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 $p>2$, $d=f=1$ and

$$\frac{p+2}{\varphi(p+2)}\geq 4-\frac{12}{p+2} \tag{3}$$

In particular, $p+2$ has at least 20 distinct prime divisors and $p>2\cdot 10^{28}$.

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

Proof. a) This is immediate from Theorem 5.1.

c) See [12, Thm. 6.3].

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. We first show $f = d = 1$.

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 $f := F(v, n)$ 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

$$f \leq 2p^{fd+1}. \tag{4}$$

Since $2 \cdot 3 \cdot 5/(1 \cdot 2 \cdot 4) < 4$, and since $r^{2/25} > r/(r-1)$ for all $r \geq 7$, we have

$$\frac{x}{4\varphi(x)} < x^{2/25}$$

for all integers $x > 1$. From Theorem 5.1 and (4) we thus get

$$p^{2fd} < (2p^{fd+1})^{27/25}.$$

This implies $fd = 1$ or $fd = 2$ and $p = 2$. In the latter case we have $f = 2$ and $d = 1$ since we assumed $q = p^f \neq 2$ for McFarland parameters. A direct application of Theorem 5.1 shows that this case cannot occur. Thus we have shown $fd = 1$.

Now let $fd = 1$. Then $p \neq 2$ since $q \neq 2$, and we have $v = p^2(p+2)$. Thus $f := F(v, n)$ divides $p(p+2)$. Theorem 5.1 gives $p^2 \leq p^2(p+2)^2/[4\varphi(p(p+2))]$ proving (3). Let $Y = 3 \cdot 5 \cdots 73$ be the product of the 20 smallest odd primes. Then $Y/\varphi(Y) < 3.97$ and $Y > 2 \cdot 10^{28}$. This implies the remaining assertions of part b. □

Remark 6.2

a) Theorem 6.1 eliminates the open case $(v, k, \lambda) = (351, 126, 45)$ mentioned in the introduction since these are Spence parameters with $d = 2$. The nonexistence of a cyclic difference set with these parameters also follows directly from Theorem 5.1 since $F(351, 81) = 39$.

b) A heuristic argument [12, Rem. 3.6] shows that the order of magnitude of $F(v, n)$ "usually" is the product of the primes dividing v. This indicates that Theorem 6.1 a should rule out "almost all" cyclic Hadamard difference sets. The next result, in particular, confirmes this claim.

Corollary 6.3 *For $k \leq 5 \cdot 10^{10}$, Ryser's conjecture is true for all parameters (v, k, λ) of known difference sets (see the list (i)-(iv) above) with the possible exception of $(v, k, \lambda) = (4u^2, 2u^2 - u, u^2 - u)$ with $u \in \{165, 11715, 82005\}$.*

Proof. For McFarland, Spence and Chen/Davis/Jedwab parameters, this immediately follows from Theorem 6.1. For Hadamard parameters, the result follows from a computer search using Result 1.4 and Theorem 6.1 a. □

Corollary 6.4 *There is no circulant Hadamard matrix of order v, $4 < v \leq 10^{11}$, with the possible exceptions $v = 4u^2$, $u \in \{165, 11715, 82005\}$.*

Proof. The existence of a circulant Hadamard matrix of order v implies the existence of a Hadamard difference set in the cyclic group of order v, see [1, Rem. 14.13]. Thus the assertion follows from Corollary 6.3. □

We conclude this paper with a necessary and sufficient condition for the existence of McFarland difference sets with $f = d = 1$. It is the first necessary and sufficient condition for a (presumably) infinite family of difference sets known in the literature which does not rely on the self-conjugacy argument.

Corollary 6.5 *Let p be an odd prime such that $p+2$ is squarefree and*

$$\frac{p+2}{\varphi(p+2)} < 4 - \frac{12}{p+2}. \tag{5}$$

Then a $(p^2(p+2), p(p+1), p+1)$-difference set in an abelian group G exists if and only if

$$G \cong (\mathbb{Z}/p\mathbb{Z})^2 \times (\mathbb{Z}/(p+2)\mathbb{Z}).$$

Proof. The existence of a $(p^2(p+2), p(p+1), p+1, p^2)$-difference set in $(\mathbb{Z}/p\mathbb{Z})^2 \times (\mathbb{Z}/(p+2)\mathbb{Z})$ is due to McFarland [8]. The necessary part follows directly from Theorem 6.1 b. □

References

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

[2] L.D. Baumert: Difference sets. *SIAM J. Appl. Math.* **17** (1969), 826-833.

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

[4] D. Jungnickel: Difference Sets. *In: Contemporary Design Theory: A Collection of Surveys. Eds. J.H. Dinitz and D.R. Stinson*, Wiley, New York 1992, 241-324.

[5] 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 et al.*, Cambridge University Press 1997, 89-112.

[6] H.B. Mann: Balanced incomplete block designs and abelian difference sets. *Illinois J. Math.* **8** (1964), 252-261.

[7] H.B. Mann: *Addition Theorems.* Wiley, New York 1965.

[8] R.L. McFarland: A family of difference sets in non-cyclic groups. *J. Comb. Theory Ser. A* **15** (1973), 1-10.

[9] R.L. McFarland: Difference sets in abelian groups of order $4p^2$. *Mitt. Math. Sem. Giessen* **192** (1989), 1-70.

[10] R. A. Rankin: Difference sets. *Acta Arith.* **9** (1964), 161-168.

[11] H.J. Ryser: *Combinatorial Mathematics.* Wiley, New York 1963.

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

[13] B. Schmidt: Characters and cyclotomic fields in finite geometry. Habilitation thesis, Universität Augsburg. In preparation.

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

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

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

[17] A. Vera Lopez, M.A. Garcia Sanchez: On the existence of abelian difference sets with $100 < k \leq 150$. *J. Comb. Math. Comb. Comp.* **23** (1997), 97-112.

[18] K. Yamamoto: Decomposition fields of difference sets. *Pacific J. Math.* **13** (1963), 337-352.

Department of Mathematics,
University of Augsburg,
Universitätsstraße 14,
86135 Augsburg, Germany
E-mail address: schmidt@math.uni-augsburg.de