Exponent Bounds

Bernhard Schmidt

We survey the presently known exponent bounds for difference sets and relative difference sets. The cases where these bounds are sufficient for the existence of the objects in question are discussed in some detail.

1 Introduction

One of the central themes of the theory of difference sets is to search for necessary and sufficient conditions on the group structure for the existence of difference sets. Most known necessary conditions have the form of *exponent bounds*. Here the **exponent** of a group means the order of its largest cyclic subgroup. An exponent bound gives an upper bound on the exponent of groups containing difference sets. Turyn's exponent bound [49] from 1965 is the most prominent example. Since Turyn's work, exponent bounds have played an important role in the study of difference sets.

Turyn's exponent bound has two important features: It relies on a *self-conjugacy assumption* and it is obtained by considering a *single homomorphic image* of a putative difference set.

Turyn's bound has been refined in two ways. Firstly, under the self-conjugacy assumption, one can try to improve Turyn's result by considering several homomorphic images simultaneously. It turns out that this approach, though it needs sophisticated arguments to combine information from different homomorphic images, often leads to striking results. In particular, necessary and sufficient conditions for the existence of several infinite families of difference sets can be derived in this way. For difference sets, only five results of this category are known: For Hadamard difference sets in abelian 2-groups (Turyn, Davis, Kraemer), McFarland difference

sets (McFarland, Ma/Schmidt, Davis/Jedwab), McFarland difference sets without self-conjugacy (Schmidt), Chen difference sets (Chen, Schmidt), and Davis-Jedwab difference sets (Davis-Jedwab, Schmidt). All these results will be treated in this paper.

The second, more important refinement of Turyn's method is to try to get rid of the very restrictive self-conjugacy assumption. Results in this direction have been obtained by McFarland [38], Chan [9] and Ma [32]. These results are remarkable, however, they only apply in quite special situations. Substantial progress has been obtained by the author [46, 47] by introducing the new method of *field descent*. These *field descent exponent bounds* are very general and do not rely on restrictive assumptions like self-conjugacy.

2 Preliminaries

In this section, we briefly mention the basic notions concerning difference sets. For thorough treatments see [7, Chapter VI] and [39].

Let G be a finite group of order nm, and let N be a subgroup of G of order n. A subset R of G is called an $(\mathbf{m}, \mathbf{n}, \mathbf{k}, \lambda)$ **difference set in G relative to N** if every $g \in G \setminus N$ has exactly λ representations $g = r_1 r_2^{-1}$ with $r_1, r_2 \in R$, and no nonidentity element of N has such a representation. The subgroup N is called the **forbidden subgroup**.

In the case $n = 1$, i.e., when the forbidden subgroup consists only of the identity element, we write v instead of m and speak of a $(\mathbf{v}, \mathbf{k}, \lambda)$ **difference set** in G. The nonnegative integer $n = k - \lambda$ is called the **order** of the difference set. If $n \in \{0, 1\}$, the difference set is called **trivial**. By a "difference set" we will always mean a nontrivial difference set. Sometimes it is useful to attach n to the parameters of a difference set. Thus we also speak of $(\mathbf{v}, \mathbf{k}, \lambda, \mathbf{n})$ **difference sets**.

3 Self-conjugacy exponent bounds

We first explain Turyn's classical exponent bound. Turyn's argument relies on the the so-called *self-conjugacy assumption*.

Definition 3.1 *Let m be a positive integer. A prime p is called* **self-conjugate** *modulo m if $p^j \equiv -1 \pmod{m'}$ for some j where*

m' is the p-free part of m. A composite integer is called self-conjugate modulo m if all its prime divisors are self-conjugate modulo m.

The following is a straightforward generalization of Turyn's result [49, Cor. 1] using projections. The most important applications will be given later.

Theorem 3.2 (Turyn) *Assume that there is an (m, n, k, λ) difference set in a (not necessarily abelian) group G relative to a subgroup N. Let U be a normal subgroup of G such that G/U is cyclic and let l be a positive integer self-conjugate modulo $|G/U|$ such that*
a) N is not contained in U and l^2 divides k or
b) N is contained in U, $k - \lambda n \neq 0$ and l^2 divides $k - \lambda n$.
Then

$$\frac{|U|}{|U \cap N|} \geq \frac{l}{2^{r-1}}$$

where $r = \max(1, s)$, and s is the number of prime divisors of $\gcd(l, |G/U|)$.

3.1 Difference sets

In the case of difference sets, Turyn's exponent bound reads as follows.

Corollary 3.3 (Turyn) *Assume the existence of a (v, k, λ, n) difference set in a group G. Let U be a subgroup of G such that G/U is cyclic, and let l^2 be a divisor of n which is self-conjugate modulo $|G/U|$. Then*

$$|U| \geq \frac{l}{2^{r-1}}$$

where $r = \max(1, s)$, and s is the number of prime divisors of $\gcd(l, |G/U|)$.

A **Hadamard difference set** is a difference set with parameters $(v, k, \lambda, n) = (4u^2, 2u^2 - u, u^2 - u, u^2)$ for some positive integer u. In the case $u = p^a$ for a prime p, the Turyn bound is quite strong since then p is always self-conjugate modulo $v/2$:

Corollary 3.4 *Assume that an abelian group G contains a Hadamard difference set with $u = p^a$ for some prime p. Then*

$$\exp G \le \begin{cases} 2^{a+2} & \text{if } p = 2, \\ p^a & \text{if } p > 2. \end{cases}$$

It took almost 30 years until it was shown by Davis [13] and Kraemer [28] that Turyn's bound is also *sufficient* for the existence of Hadamard difference sets in abelian 2-groups:

Theorem 3.5 (Davis, Kraemer) *A Hadamard difference set in an abelian 2-group G of order 2^{2a+2} exists if and only if $\exp G \le 2^{a+2}$.*

The case of *nonabelian* 2-groups is very different: Davis and Iiams [15] extended an example of Liebler and Smith [30] to an infinite family of difference sets in high exponent 2-groups.

Theorem 3.6 (Davis, Iiams) *For every positive integer t, there is a nonabelian group of order 2^{4t+2} and exponent 2^{3t+3} containing a Hadamard difference set.*

Iiams [23] proved that the exponent obtained in Theorem 3.6 is the highest possible under some conditions:

Theorem 3.7 (Iiams) *Let G be a 2-group of order 2^{4t+2^m}, $m \in \{1, 2\}$, with a normal cyclic subgroup $\langle x \rangle$ of order $\exp G$ such that x and x^{-1} are not conjugate in G. If G contains a Hadamard difference set, then $\exp G \le 2^{3t+m+1}$.*

The result of Davis and Kraemer is one of the few known necessary and sufficient conditions for the existence of an infinite family of difference sets. The following theorem on McFarland difference sets also belongs to this category. A **McFarland difference set** is a difference set with parameters

$$\begin{aligned} v &= q^{d+1}[1 + (q^{d+1} - 1)/(q - 1)], \\ k &= q^d(q^{d+1} - 1)/(q - 1), \\ \lambda &= q^d(q^d - 1)/(q - 1), \\ n &= q^{2d}, \end{aligned}$$

where $q = p^f$ is a prime power and d is a positive integer. McFarland [37] constructed such difference sets in all abelian groups G of order $v = q^{d+1}[1+(q^{d+1}-1)/(q-1)]$ which contain an elementary abelian subgroup order q^{d+1}.

Theorem 3.8 (Ma, Schmidt [35]) *Assume that there is a McFarland difference set in an abelian group G of order $q^{d+1}[1+(q^{d+1}-1)/(q-1)]$ where $q = p^f$ and p is a prime self-conjugate modulo $\exp G$. Let P be the Sylow p-subgroup of G. Then the following hold.*

a) If p is odd, then P is elementary abelian.

b) If $p = 2$ and $f \geq 2$, then $\exp P \leq 4$.

In view of McFarland's result mentioned above, part a of Theorem 3.8 is *sufficient* for the existence of a McFarland difference set. Davis and Jedwab [16] showed that part b is also sufficient for infinitely many cases.

Theorem 3.9 (Ma/Schmidt, Davis/Jedwab) *A McFarland difference set in an abelian group G of order $2^{2d+3}(2^{2d+1}+1)/3$ exists if and only if the Sylow 2-subgroup of G has exponent at most 4.*

Quite recently, two new families of difference sets were discovered by Chen [11] and Davis, Jedwab [16]. Chen's difference sets have parameters

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

where $q = p^f$ is a power of 3 or a square of an odd prime power and t is a positive integer. For $t = 1$, such a difference set is a Hadamard difference set. For $t \geq 2$, *any* difference set with the above parameters, for *any* prime power q, will be called a **Chen**

difference set. Chen's construction requires the underlying groups to have an elementary abelian Sylow p-subgroup.

The second recent series of difference sets was constructed by Davis and Jedwab [16] and has parameters

$$\begin{aligned} v &= 2^{2t+2}(2^{2t}-1)/3, \\ k &= 2^{2t-1}(2^{2t+1}+1)/3, \\ \lambda &= 2^{2t-1}(2^{2t-1}+1)/3, \\ n &= 2^{4t-2} \end{aligned}$$

where $t \geq 2$ is an integer. *Any* difference set with such parameters will be called a **Davis-Jedwab difference set**. Note that Davis-Jedwab difference sets are also Chen difference sets (put $q = 2$). Davis and Jedwab [16] constructed Davis-Jedwab difference sets in all abelian groups of order $2^{2t+2}(2^{2t}-1)/3$ which have a Sylow 2-subgroup S_2 of exponent at most 4, with the single exception of $t = 2$ and $S_2 \cong \mathbb{Z}_4^3$. This exception was removed by Arasu and Chen [1] who constructed the necessary difference set in $\mathbb{Z}_4^3 \times \mathbb{Z}_5$. If we apply Turyn's bound 3.3 to Chen difference sets, we get the following.

Theorem 3.10 (Turyn) *Let $q = p^f$ be a prime power, and let G be an abelian group of order $4q^{2t}(q^{2t}-1)/(q^2-1)$ containing a Chen difference set. Assume that p is self-conjugate modulo $\exp G$. Denote the Sylow p-subgroup of G by S_p. Then the following hold.*

a) If p is odd, then $\exp S_p \leq q$.

b) If $p = 2$, then $\exp S_2 \leq 4q$.

Schmidt [45] improved Turyn's bound for Chen difference sets.

Theorem 3.11 (Schmidt) *Let $q = p^f$ be an odd prime power, and let t, f be integers ≥ 2. Let G be an abelian group of order $4q^{2t}(q^{2t}-1)/(q^2-1)$ containing a Chen difference set. Assume that p is self-conjugate modulo $\exp G$. Then the Sylow p-subgroup of G has exponent at most p^{f-1}.*

Schmidt's result leads to the following necessary and sufficient conditions for the existence of Chen difference set for infinitely many cases.

Corollary 3.12 (Chen, Schmidt) *Let p be an odd prime. Let G be an abelian group of order $4p^8(p^4+1)$ whose Sylow 2-subgroup is elementary abelian. Then G contains a Chen difference set if and only if its Sylow p-subgroup is elementary abelian.*

For the formulation of the next result, we need a definition. See [7, Chapter VI] for the terminology.

Definition 3.13 *Let D be a (v,k,λ,n) difference set in an abelian group. We say that D has the* **character divisiblilty property** *if $\chi(D)$ is divisible by $\sqrt{n}$ for all nontrivial characters χ of G.*

Theorem 3.14 (Davis/Jedwab, Schmidt, Arasu/Chen) *Let G be an abelian group of order $2^{2t+2}(2^{2t}-1)/3$ with $t \geq 2$. A Davis-Jedwab difference set in G with the character divisibility property exists if and only if the Sylow 2-subgroup of G has exponent at most 4.*

3.2 Relative difference sets

Turyn's Theorem 3.2 provides a useful exponent bound for relative difference sets. In the following, we concentrate on **semiregular** relative diffference sets, i.e., relative (m,n,k,λ) difference sets with $n > 1$ and $m = k$. For this family, there is a further exponent bound due to Pott [39, Thm. 4.1.1].

Theorem 3.15 (Pott) *If a relative (m,n,m,λ) difference set exists in an abelian group G with $|G| > 4$, then $\exp G$ divides m. In particular, there is no semiregular relative difference set in any cyclic group of order > 4.*

In the following, we focus on semiregular relative difference sets with **prime power parameters**, i.e., relative difference sets with parameters of the form $(m,n,k,\lambda) = (p^a, p^b, p^a, p^{a-b})$, p prime. In this case, Turyn's exponent bound can be improved dramatically. The major result here is the following from [36] improving previous work of Ma/Pott [33] and Schmidt [43, 44].

Theorem 3.16 (Ma, Schmidt) *Let p be an odd prime. If a relative (p^a, p^b, p^a, p^{a-b}) difference set exists in an abelian group G, then*

$$\exp G \leq p^{\lfloor a/2 \rfloor + 1}$$

where $\lfloor a/2 \rfloor$ denotes the largest integer not exceeding $a/2$.

The bound in Theorem 3.16 is sharp in the sense that it can be attained for all triples (p, a, b) with $b \leq \lfloor a/2 \rfloor$, see [39, Chapter 4].

For $p = 2$, the situation is quite different. We have the following results due to Ma/Pott [33] and Schmidt [43, 44].

Theorem 3.17 (Ma, Pott, Schmidt)

a) Assume the existence of a $(2^{2a}, 2^b, 2^{2a}, 2^{2a-b})$ relative difference set in an abelian group G relative to N. Then $\exp N \leq 2^a$ and $\exp G \leq 2^a \exp N$. Furthermore, if $b > a$, then N is not a direct factor of G.

b) Assume the existence of a $(2^{2a+1}, 2^b, 2^{2a+1}, 2^{2a-b+1})$ relative difference set in an abelian group G relative to N. Then $\exp G \leq 2^{a+2}$ and $\exp N \leq 2^{a+1+\delta}$ where $\delta = 1$ if $\exp G = \exp N$ and $\delta = 0$ otherwise.

Davis and Jedwab [16, Cor. 8.2] partially improved results of Davis [14] and Ma and Schmidt [34, 43] to show that the bounds in Theorems 3.16 and 3.17 are essentially *sufficient* in the case $b = 1$:

Theorem 3.18 (Ma/Schmidt, Davis/Jedwab) *Let p be prime. With the possible exceptions $G \cong \mathbb{Z}_{p^{c+1}}^2$ or $\mathbb{Z}_{p^{c+1}} \times \mathbb{Z}_{p^c} \times \mathbb{Z}_p$, p odd, $c \geq 1$, an abelian p-group G containes a (p^a, p, p^a, p^{a-1}) relative difference set if and only if $\exp G \leq p^{\lfloor a/2 \rfloor + 1 + \delta}$ where $\delta = 1$ if $p = 2$ and $a \equiv 1 \pmod 2$ and $\delta = 0$ otherwise.*

Semiregular relative difference sets with parameters of the form $(n, n, n, 1)$ are of special interest since they can be used to construct quasiregular projective planes of order n, see [39, Chapter 5]. It is conjectured that an $(n, n, n, 1)$ relative difference set exists if and only if n is a prime power and the underlying group is an elementary abelian p-group. The following result from [33] can be interpreted as a result on collineation groups of projective planes.

Theorem 3.19 (Ma, Pott) *Let p be an odd prime. If a relative $(p^2, p^2, p^2, 1)$ difference set exists in an abelian group G, then G must be elementary abelian.*

4 Field descent exponent bounds

Aside from the Theorem 3.15, all exponent bounds we have seen depend on a self-conjugagy argument. This is very restrictive: It can be seen that self-conjugacy "almost never" holds if the group order has many prime divisors, for instance, see [46]. Thus more general exponent bounds are desirable. Such bounds have been obtained by the author of the present paper by the new method of *field descent*. We describe the most important results concerning the field descent here. First we need a definition.

Definition 4.1 *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 $q^{\mathrm{ord}_{m_q}(q)} \not\equiv 1 \pmod{p_i^{b_i+1}}$.

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

Proposition 4.2 *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 $m, n \in Q$.

Now we are ready to state the field descent result from [46].

Theorem 4.3 (Schmidt) *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.

The field descent leads to the following general exponent bounds proved in [47].

Theorem 4.4 (Schmidt) *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*

$$e \le \frac{vF(e,n)}{2\sqrt{n\varphi(F(e,n))}}$$

where φ denotes the Euler totient function and F is defined as in 4.1.

It is worth to state the abelian case separately.

Theorem 4.5 *Assume the existence of a (v,k,λ,n)-difference 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

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

For relative difference sets, we get the following exponent bound [47].

Theorem 4.6 (Schmidt) *Assume the existence of an (m,n,k,λ)-difference set 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*

$$|U \cap N| \le \frac{|U|F(e,k)}{2\sqrt{k\varphi(F(e,k))}}.$$

The field descent also can be applied to group invariant weighing matrices and other problems which can be studied by character methods. Here we only mention the most striking applications to difference sets, circulant Hadamard matrices and Barker sequences which can be found in [46, 47].

Theorem 4.7 (Schmidt) *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.

Ryser's conjecture asserts that there is no (v, k, λ, n) difference set with $\gcd(v, n) > 1$ in any cyclic group. It is interesting to check Ryser's conjecture for the parameters of known difference sets with $\gcd(v, n) > 1$. These are the Hadamard, McFarland, Spence, Chen, and Davis-Jedwab parameters, cf. [7].

Theorem 4.8 (Schmidt)

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

$$\frac{p+2}{\varphi(p+2)} \geq 4 - \frac{12}{p+2} \tag{4.1}$$

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.

By computer search, one can check that Theorem 4.8 implies the following.

Theorem 4.9 (Schmidt) *For $k \leq 5 \cdot 10^{10}$, Ryser's conjecture is true for all parameters (v, k, λ, n) of known difference sets with the possible exception of $(v, k, \lambda) = (4u^2, 2u^2 - u, u^2 - u)$ with $u \in \{165, 11715, 82005\}$.*

McFarland difference sets with $p = 3$, $f = 2$ and $d = 1$ were studied thoroughly by Arasu and Ma [4]. This case is very difficult since the self-conjugacy condition does not hold. Their result is the following.

Theorem 4.10 (Arasu, Ma) *A McFarland difference set in an abelian group G of order* 891 *exists if and only if the Sylow* 3*-subgroup of G is elementary abelian.*

In [47], a necessary and sufficient condition for the existence of McFarland difference sets with $f = d = 1$ was obtained. This is the first example of a 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.

Theorem 4.11 (Schmidt) *Let p be an odd prime such that $p+2$ is squarefree and*

$$\frac{p+2}{\varphi(p+2)} < 4 - \frac{12}{p+2}. \tag{4.2}$$

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

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

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 [48] proved the Barker conjecture for all odd v. It is well known [7, VI. §14] that the existence of a Barker sequence of even length v implies the existence of a circulant Hadamard matrix of order v which in turn is equivalent to the existence of a Hadamard difference set in a cyclic group of order v. Together with other known results, Theorem 4.8 a implies the following.

Theorem 4.12 (Schmidt)
a) There is no circulant Hadamard matrix of order v, $4 < v \leq 10^{11}$, *with the possible exceptions* $v = 4u^2$, $u \in \{165, 11715, 82005\}$.
b) There is no Barker sequence of length v *with* $13 < v < 4 \cdot 10^{12}$.

References

[1] K.T. Arasu, Y.Q. Chen: A difference set in $(\mathbb{Z}/4\mathbb{Z})^3 \times \mathbb{Z}/5\mathbb{Z}$. *Des. Codes Cryptogr.*, to appear.

[2] 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.

[3] 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 et al., DeGruyter Verlag, Berlin/New York 1996, 129-143.

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

[5] K.T. Arasu, S.K. Sehgal: Difference sets in abelian groups of p-rank two. *Des. Codes Cryptogr.* **5** (1995), 5-12.

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

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

[8] Z.I. Borevich, I.R. Shafarevich: *Number Theory.* Academic Press, New York/San Francisco/London 1966.

[9] W.K. Chan: Necessary Conditions for Menon Difference Sets. *Des. Codes Cryptogr.* **3** (1993), 147-154.

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

[11] 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.

[12] C.W. Curtis, I. Reiner: *Representation Theory of Finite Groups and Associative Algebras.* Wiley, New York/London 1962.

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

[14] J.A. Davis: Constructions of relative difference sets in p-groups. *Discrete Math.* **103** (1992), 7-15.

[15] J.A. Davis, J. Iiams: Hadamard difference sets in non-abelian 2-groups with high exponent. *J. Algebra* **199** (1998), 62-87.

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

[17] J.A. Davis, J. Jedwab: Nested Hadamard Difference Sets. *J. Statist. Plann. Inference* **62** (1997), 13-20.

[18] J.F. Dillon: Variations on a scheme of McFarland for non-cyclic difference sets. *J. Combin. Theory Ser. A* **40** (1985), 9-21.

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

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

[21] M. Hall: A survey of difference sets. *Proc. Amer. Math. Soc.* **7** (1956), 975-986.

[22] J.E. Iiams: On Difference Sets in Groups of Order $4p^2$. *J. Comb. Theory Ser. A* **72** (1995), 256-276.

[23] J.E. Iiams: A note on certain 2-groups with Hadamard difference sets. Submitted.

[24] K. Ireland, M. Rosen: *A Classical Introduction to Modern Number Theory.* Graduate Texts in Math. 84, Springer, Berlin/Heidelberg/New York 1990.

[25] 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.

[26] 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.

[27] D. Jungnickel and B. Schmidt: Difference sets: A second update. Rend. Circ. Mat. Palermo (2) Suppl. **53** (1998), 89-118.

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

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

[30] R.A. Liebler, K.W. Smith: On difference sets in certain 2-groups. In: *Coding Theory, Design Theory, Group Theory: Proceedings of the Marshall Hall Conference.* Wiley, New York 1993, 195-212.

[31] S.L. Ma: *Polynomial addition sets.* Ph.D. thesis, University of Hong Kong, 1985.

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

[33] S.L. Ma, A. Pott: Relative difference sets, planar functions and generalized Hadamard matrices. *J. Algebra* **175** (1995), 505-525.

[34] S.L. Ma, B. Schmidt: On (p^a, p, p^a, p^{a-1})-relative difference sets. *Des. Codes Cryptogr.* **6** (1995), 57-72.

[35] S.L. Ma, B. Schmidt: A Sharp Exponent Bound for McFarland Difference Sets with $p = 2$. *J. Combin. Theory Ser. A* **80** (1997), 347-352.

[36] S.L. Ma, B. Schmidt: Relative (p^a, p^b, p^a, p^{b-a})-difference sets: A Unified Exponent Bound and a Local Ring Construction. *Finite Fields Appl.*, to appear.

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

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

[39] A. Pott: *Finite geometry and character theory.* Lecture Notes 1601, Springer, Berlin/Heidelberg/New York 1995.

[40] A. Pott: A survey on relative difference sets. In: *Groups, Difference Sets and the Monster.* Eds. K.T. Arasu et al., De-Gruyter Verlag, Berlin/New York 1996, 195-233.

[41] D.K. Ray-Chaudhuri, Q. Xiang: New Necessary Conditions for Abelian Hadamard Difference Sets. *J. Statist. Plann. Inference* **62** (1997), 69-79.

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

[43] B. Schmidt: *Differenzmengen und relative Differenzmengen.* Dissertation. Verlag Dr. Wißner, Augsburg 1995.

[44] B. Schmidt: On (p^a, p^b, p^a, p^{a-b})-relative difference sets. *J. Alg. Combin.* **6** (1997), 279-297.

[45] B. Schmidt: Nonexistence Results on Chen and Davis-Jedwab Difference Sets. *J. Algebra* **202** (1998), 404-413.

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

[47] B. Schmidt: Towards Ryser's conjecture. Proc. 3ecm (2000).

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

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

[50] R.J. Turyn: Sequences with small correlation. In: *Error Correcting Codes*. Ed. H.B. Mann, Wiley, New York 1969, 195-228.

[51] K. Yamamoto: Decomposition fields of difference sets. *Pacific J. Math.* **13** (1963), 337-383.

Bernhard Schmidt
Mathematisches Institut
Universiät Augsburg
86135 Augsburg
Germany
schmidt@math.uni-augsburg.de