Difference Sets: a Second Update

Dieter Jungnickel
Mathematisches Institut
Universität Augsburg
Universitätsstraße 14
D–86135 Augsburg
Germany

Bernhard Schmidt
Department of Mathematics
253-37 Caltech
Pasadena, CA 91125
USA

Abstract

In the 20 months after our previous update [36] of the first author's survey [33] had been finished there has been further rapid progress in the theory of difference sets. Therefore, a second update has become necessary.

1 Introduction

This paper is an update of the update [36] of the survey [33] of the first author. Many exciting theorems have been proven in the meantime we would like to report on. One of the reasons why we love to study difference sets is that, in this field, methods from combinatorics, geometry, algebra and number theory can be combined in an almost unparalleled way to a beautiful theory. The results surveyed in this paper will provide excellent examples.

In Section 2, we will treat a new general exponent bound for difference obtained by Schmidt [52]. His results combine a new approach to the absolute value problem for algebraic integers in cyclotomic fields with a refinement of the classical method of Turyn [56].

Section 3 is devoted to a new development in the theory of Singer-type difference sets initiated by Maschietti [41]. Maschietti proved that monomial hyperovals in $PG(2, 2^d)$ are equivalent to Singer-type difference sets in cyclic groups of order $2^d - 1$. In this way, the Segre hyperovals [53] and the Glynn hyperovals [21] give rise to three new infinite families of difference sets. The

difficult problem of showing that these families of difference sets are inequivalent to the previously known series was tackled by Evans, Krattenthaler and Xiang [20]. They reduced the problem to counting certain binary sequences and found a complete solution for the difference sets corresponding to the Segre hyperovals.

In Section 4, we sketch Chen's construction [8] of of a new infinite family of difference sets. We also discuss the new results on building sets, a fruitful concept introduced by Davis and Jedwab [11] which already has become a well established tool for the study of difference sets.

In Section 5, we give an exposition of Ionin's new method [30] for the construction of symmetric designs. By combining incidence matrices of symmetric designs corresponding to difference sets which can be built up from building sets with balanced generalized weighing matrices, Ionin obtained seven new infinite families of symmetric designs.

Some new results on Hadamard difference sets in elementary abelian 2-groups and on perfect binary sequences will be described in Sections 6 and 7, respectively. Finally, some miscellaneous recent results are collected in Section 8. The bibliography not only contains the papers mentioned in this survey, but also the papers quoted in our last survey which have appeared in the meantime.

A detailed exposition of the present state of art in the theory of difference sets will appear as Chapter VI of [2]. In particular, we recommend this source for a detailed treatment of Schmidt's exponent bound and its consequences as well as a complete exposition of the Davis-Jedwab theory of building blocks and its applications, including most of the known constructions for Hadamard difference sets and the new difference sets of Chen.

We conclude this section with some definitions. A (v, k, λ, n)-***difference set*** in a 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 parameter $n = k - \lambda$ is called the ***order*** of the difference set.

Difference sets with parameters of the form

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

are called ***Hadamard difference sets***.

If the parameters are of the form

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

for some prime power q and some postive integer d, we speak of ***Singer-type difference sets***.

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.

2 Existence theory without self-conjugacy

The existence theory of (v, k, λ, n)-difference sets in groups G concerns the problem of finding the solutions D of the group ring equation

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

which have coefficients 0 and 1 only. For abelian groups,there are two classical methods to tackle this problem, namely, Hall's multiplier concept [24] and Turyn's self-conjugacy approach [56]. 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 way has been found to overcome these difficulties. Recently, Schmidt [52] obtained a new method for the study of group ring equations which works under considerably weaker assumptions.

In order to understand Schmidt's method, it will be instructive to start with a brief discussion of the self-conjugacy condition. Turyn [56] demonstrated that the character method for the study of group ring equations works very nicely under this restriction. ERWAEHNEN Recall that a prime p is called ***self-conjugate*** modulo an integer m if there is an integer j with $p^j \equiv -1 \bmod m'$, and that a composite integer n is called ***self-conjugate*** modulo m if every prime divisor p of n has this property. In more number theoretic language, this just means that all prime ideals above n in the m-th 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 [56] 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 numberof distinct prime divisors of n and m, see [52, Remark 2.2]. 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 almost complete determination of the class group of the underlying cyclotomic field modulo the class group of its maximal real subfield [51, Proposition 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. Schmidt [52] presents a new approach to the absolute value problem. He shows 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, see Theorem 2.2. This is achieved by exploiting the decomposition groups of the prime ideals above n in K.

Using the reduction to subfields one can 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, Schmidt [52] obtains strong asymptotic exponent bounds for groups containing difference. In many cases, previously literally nothing had been known on the existence of these difference sets. Schmidt's results are a major steps towards Ryser's conjecture and the circulant Hadamard matrix conjecture.

By ξ_t, we denote a primitive complex t-th root of unity. The integer $F(n,m)$ defined below describes a subring $\mathbb{Z}[\xi_{F(n,m)}]$ 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. All results of this section are due to Schmidt [52].

Definition 2.1 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

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

We define $F(m,n) = \prod_{i=1}^{t} {p_i}^{b_i}$ to be the minimum multiple of the square-free part of m such that for every prime divisor q of n and $i = 1, .., t$, 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 $q^{o_{m_q}(q)} \not\equiv 1 \pmod{p_i^{b_i+1}}$.

The following basic result is very useful for virtually all combinatorial problems accessible to the character method. It can also be used to study the class groups of cyclotomic fields, see [51].

Theorem 2.2 *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.

In order to understand the significance of Theorem 2.2 it is important to note that the order of magnitude of $F(m,n)$ usually is the squarefree part of m, see [52, Remark 3.6]. A combination of Theorem 2.2 with a refinement of a method of Turyn [56] leads to the following bound on the absolute value of cyclotomic integers.

Theorem 2.3 *Let $X \in \mathbb{Z}[\xi_m]$ be of the form*

$$X = \sum_{i=0}^{m-1} a_i \xi_m^i, \tag{2}$$

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.

The application of Theorem 2.3 gives us the following general exponent bound.

Theorem 2.4 *Assume the existence of a (v,k,λ,n)-difference set in an abelian group G. Then*

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

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

Theorem 2.4 has many striking consequences, the nicest of which is as follows.

Theorem 2.5 *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.

Note that the bound in Theorem 2.5 is in some sense optimal, since there are infinite families of abelian groups G containing Hadamard difference sets such that $\exp(G) \geq C|G|^{1/2}$ for some constant C, see [2] or [11].

Ryser's conjecture [48, p. 139] asserts that there is no (v, k, λ, n)-difference set with $\gcd(v, n) > 1$ in any cyclic group. We want to apply Theorem 2.4 to the parameters of all known difference sets, as given in the following list.

(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 any positive integer.

Note that 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 $u = 2^d$. Difference sets of type (iv) are known to exist only if f is even or $p \leq 3$, see [7, 8, 11]. However, in this section we will consider arbitrary f and p. The next theorem shows that Ryser's conjecture is true for most of the parameters of known difference sets.

Theorem 2.6
a) Assume the existence of a Hadamard difference set in a cyclic group of order $4u^2$. Then $F(4u^2, u^2) \geq 2^{-s+1}u^2$, where s is the number of distinct odd prime divisors of u.

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

c) No cyclic group can contain a difference set with either Spence or Chen/Davis/Jedwab parameters.

The ***circulant Hadamard matrix conjecture*** asserts that there is no Hadamard difference set in any cyclic group of order greater than 4. Among other things, Turyn [56] proved that u must be odd if a Hadamard difference set in the cyclic group of order $4u^2$ exists. Since Turyn's results in 1965, there had not been any progress toward the circulant Hadamard matrix conjecture. Recalling that the order of magnitude of $F(4u^2, u^2)$ usually is u, we see that part a) of Theorem 2.6 comes close to a proof of this conjecture.

3 Singer-type difference sets, hyperovals and codes

Maschietti [41] discovered a beautiful connection between monomial hyperovals in $\Pi := PG(2,q)$, where $q = 2^d$, and difference sets with Singer-type parameters $(v,k,\lambda) = (2^d-1, 2^{d-1}-1, 2^{d-2}-1)$. We recall that a ***hyperoval*** in Π is a set of $q+2$ points no three of which are collinear. By a result of Segre (see [25, Thm. 8.4.2]), every hyperoval in $PG(2,q)$ is projectively equivalent to some hyperoval of the form

$$H(f) = \{(1,x,f(x)) : x \in \mathbb{F}_q\} \cup \{(0,1,0),(0,0,1)\},$$

where f is a permutation polynomial over $\mathbb{F}_q$ of degree at most $q-2$ with $f(0)=0$ and $f(1)=1$ such that the map f_s defined by

$$f_s(0) = 0 \quad \text{and} \quad f_s(x) = \frac{f(x+s)+f(s)}{x} \text{ for } x \neq 0$$

is a permutation of $\mathbb{F}_q$ for every $s \in \mathbb{F}_q$. Conversely, if f satisfies all these conditions, then $H(f)$ is a hyperoval in $PG(2,q)$. If f is a monomial, then $H(f)$ is called a ***monomial*** hyperoval. The known monomial hyperovals are given in the following list. Glynn [21] conjectured that this list actually comprises *all* monomial hyperovals, but this conjecture remains unresolved.

- *Translation hyperovals* (see [54, 45]): $H(x^{2^n})$, $(n,d)=1$,
- *Segre hyperovals* [53]: $H(x^6)$, $d \geq 5$ odd,
- *Glynn hyperovals* [21]: $H(x^{\sigma+\gamma})$ and $H(x^{3\sigma+\gamma})$, where $d \geq 7$ is odd, $\sigma = 2^{(d+1)/2}$ and $\gamma = 2^m$ for $d = 4m-1$ and $\gamma = 2^{3m+1}$ for $d = 4m+1$.

The first step toward Maschietti's result is the following characterization [41] of the monomial hyperovals; its proof is just a straightforward verification.

Lemma 3.1 *The set $H(x^k)$ is a hyperoval in $PG(2,q)$ if and only if $(k(k-1), q-1) = 1$ and the mapping $\tau : \mathbb{F}_q \to \mathbb{F}_q, x \mapsto x^k + x$ is two-to-one (that is, the preimage of each $y \in \mathbb{F}_q$ is either empty or consists of two elements).*

Let $\tau(F_q)$ denote the image of F_q under τ, and write $D(x^k) := \tau(F_q) \setminus \{0\}$. Note $|D(x^k)| = 2^{d-1} - 1$ if τ is two-to-one. Using Lemma 3.1, geometric arguments and some counting, Maschietti [41] obtained the following beautiful result.

Theorem 3.2 *The set $H(x^k)$ is a hyperoval if and only if $D(x^k)$ is a $(2^d - 1, 2^{d-1} - 1, 2^{d-2} - 1)$-difference set in $\mathbb{F}_q^*$.*

Maschietti [41] also proved that $H(x^k)$ is a translation hyperoval if and only if $D(x^k)$ is the trace zero Singer difference set in $\mathbb{F}_q^*$. This shows that difference sets corresponding to nonequivalent hyperovals can be equivalent. However, in a profound paper, Evans, Krattenthaler and Xiang [20] show that, subject to the truth of some plausible conjectures, the difference sets corresponding to the Segre and Glynn hyperovals (except for the two Glynn hyperovals $H(x^{3\sigma+\gamma})$ for $d = 7$ or 9) are all inequivalent, and that they are also inequivalent to the previously known families of $(2^d-1, 2^{d-1}-1, 2^{d-2}-1)$-difference sets (that is, Singer, GMW, quadratic residue and Hall difference sets, see [33]). The results of Evans, Krattenthaler and Xiang [20] are based on the following neat proof of Maschietti's Theorem 3.2; we note that their approach is quite different from Maschietti's.

Partial proof of Theorem 3.2:

Assume that $H(x^k)$ is a hyperoval. Let χ be a nontrivial character of $\mathbb{F}_q^*$. We need to show $|\chi(D(x^k))|^2 = 2^{d-2}$. By Lemma 3.1, we have $(k(k-1), q-1) = 1$. Thus there is a character ψ of $\mathbb{F}_q^*$ with $\chi = \psi^{k-1}$. Recall that τ is a two-to-one mapping. We compute

$$\begin{aligned}
\chi(D(x^k)) &= \chi(\tau(\mathbb{F}_q)) \\
&= \frac{1}{2} \sum_{x \in F_q} \chi(x^k + x) \\
&= \frac{1}{2} \sum_{x \in F_q} \chi(x)\chi(x^{k-1} + 1) \\
&= \frac{1}{2} \sum_{x \in F_q} \psi(x^{k-1})\chi(x^{k-1} + 1)
\end{aligned}$$

$$= \frac{1}{2}\sum_{x\in F_q}\psi(x)\chi(x+1).$$

But $\sum_{x\in F_q}\psi(x)\chi(x+1)$ is a Jacobi sum of absolute value $2^{d/2}$ (see [59, Lemmas 6.1, 6.2]), so we are done. □

The above proof shows that all nontrivial character values of the difference sets $D(x^k)$are Jacobi sums. The prime ideal decomposition of the principal ideals of cyclotomic fields generated by Jacobi sums is known from Stickelberger's theorem, a classical number theoretic result, see [59, p. 96].In principle, this allows the computation the 2-ranks $C_2(d,k)$ of the incidence matrices of the designs corresponding to the difference sets $D(x^k)$ using the following lemma which is essentially due to MacWilliams and Mann [40].

Lemma 3.3 *Let G be an abelian group of exponent e, let p be a prime not dividing e, and let $\mathcal{P}$ be a prime ideal above p in $\mathbb{Z}[\xi_e]$, $\xi_e = e^{2\pi i/e}$. Let D be a difference set in G. Then the p-rank of the incidence matrix of D is the number of complex characters χ of G with $\chi(D) \not\equiv 0 \pmod{\mathcal{P}}$.*

Proof Note that $F := \mathbb{Z}[\xi_e]/\mathcal{P}$ is a finite field of characteristic p which contains a primitive e-th root of unity (namely $\mathcal{P}+\xi_e$), see [31, Prop. 13.2.3]. Thus the lemma follows from the result of MacWilliams and Mann [40] (see also [2, Lemma 2.3.11]) by viewing the characters $G \to \mathbb{C}^*$ as characters $G \to F^*$. □

Thus the 2-ranks $C_2(d,k)$ are, in principle, given by Stickelberger's theorem and Lemma 3.3. However, it turns out that the enumeration of the characters χ with $\chi(D(x^k)) \not\equiv 0 \pmod{\mathcal{P}}$ actually leads to a difficult counting problem involving certain binary sequences. Evans, Krattenthaler and Xiang [20] solve this counting problem for the difference sets corresponding to the Segre hyperovals $H(x^6)$ and obtain the following surprising recursion for the 2-ranks $C_2(d,6)$ which had been conjectured by Xiang [63] on the basis of computational evidence.

Theorem 3.4 *The 2-rank $C_2(d,6)$ of the cyclic $(2^d-1, 2^{d-1}-1, 2^{d-2}-1)$-difference set corresponding to the Segre hyperoval in $PG(2,2^d)$ is divisible by d, and the numbers $A(d) := C_2(d,6)/d$ satisfy the recursion*

$$A(d) = A(d-2) + A(d-4) + 1$$

with initial values $A(2) = 0$, $A(3) = 1$, $A(4) = 1$ and $A(5) = 3$. Thus, for any positive integer m,

$$\begin{aligned} C_2(2m,6) &= 2m(F_m - 1) \text{ and} \\ C_2(2m+1,6) &= (2m+1)(2F_m - 1), \end{aligned}$$

where F_n is the n-th Fibonacci number.

Further interesting results on the difference sets corresponding to the Segre hyperovals can be found in the paper of Dillon, Dobbertin and Xiang [14]. In particular, these authors characterize the nonroots of the binary cyclic codes associated with the Segre difference sets. They also give a further alternative proof for the fact that $D(x^k)$ is a difference set if $H(x^k)$ is a hyperoval which makes use of Parseval's relation.

For the difference sets $D(x^k)$ corresponding to the Glynn hyperovals, the problem of counting the characters χ with $\chi(D(x^k)) \not\equiv 0 \pmod{\mathcal{P}}$ seems to be even more difficult and has not been solved yet. However, on the basis of "abundant computational evidence", Evans, Krattenthaler and Xiang [20] conjecture that the 2-ranks of these difference sets satisfy certain 5-term recurrence relations. They show that subject to the truth of this conjecture the difference sets corresponding to the Segre and Glynn hyperovals (except for the two Glynn hyperovals $H(x^{3\sigma+\gamma})$ for $d = 7$ and 9) are all inequivalent.

4 Chen difference sets and building sets

Chen [7] not only constructed Hadamard difference sets of order m^4 for every positive integer m, but also discovered a new infinite family of difference sets with parameters

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

where $q = p^f$ is a power of 3 or a square of an odd prime power and t is any positive integer. The family of Davis/Jedwab difference sets [11] has parameters

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

where $t \geq 2$ is a positive integer. If we set $q = 2$ in (3), we recover the parameters (4). Chen [8] concluded that there should be difference with parameters (3) for any power q of 2 — and proved it. In order to give a

flavor of this construction, we first recall the definition of covering extended building sets (CEBSs) which were introduced by Davis and Jedwab [11].

An $(a, m, h, \pm)$ CEBS in an abelian group G is a family $\{D_1, ..., D_h\}$ of subsets of G with the following properties.

a) $|D_1| = a \pm m$ and $|D_i| = a$ for $i = 2, ..., h$.

b) For every nonprincipal character χ of G there is exactly one i with $|\chi(D_i)| = m$ and $\chi(D_j) = 0$ if $j \neq i$.

¿From a CEBS in G one can construct difference sets in many groups which contain G as a subgroup.

Theorem 4.1 ([11], Thm. 2.4) *Suppose that $\{B_1, ..., B_h\}$ is an $(a, m, h, \pm)$ CEBS in an abelian group G. Let H be an abelian group containing G as a subgroup of index h, and let $\{g_1, ..., g_h\}$ be a complete system of coset representatives of G in H. Then*

$$D := \bigcup_{i=1}^{h} B_i g_i$$

is an $(h|G|, ah \pm m, ah \pm m - m^2)$-difference set in H.

Proof Surely, D is a subset of H with the right cardinality. Let χ be a nontrivial character of H. We have to show $|\chi(D)| = m$. If χ is nontrivial on G, this follows from condition a) in the definition of a CEBS. If χ is trivial on G, then $\sum_{i=1}^{h} \chi(h_i) = 0$ and thus $\chi(D) = \sum_{i=1}^{h} |B_i| \chi(h_i) = a \sum_{i=1}^{h} \chi(h_i) \pm m\chi(h_1) = \pm m\chi(h_1)$. Hence $|\chi(D)| = m$, since $\chi(h_1)$ is a root of unity. □

We now sketch Chen's construction [8] of difference sets with parameters (3) for all powers q of 2. This construction depends on the following consequence of Menon's direct product construction [43] for Hadamard difference sets and the existence of trivial Hadamard difference sets in $\mathbb{Z}_2 \times \mathbb{Z}_2$ and $\mathbb{Z}_4$.

Lemma 4.2 *Any abelian 2-group of square order and exponent at most 4 contains a Hadamard difference set.*

Of course, we know from the celebrated Davis/Kraemer theorem [37] that an abelian 2-group G of square order contains a Hadamard difference set if and only if $\exp G \leq 2\sqrt{|G|}$, but we only need the simple Lemma 4.2here.

Let A be an elementary abelian group of order $2q^{2t}$ and $m := \frac{q^{2t}-q^2}{q^2-1}$. Chen first finds subgroups $K_0, ..., K_{2m}$ of A with $|K_0| = q^{2t-2}$, $|K_i| = 2q^{2t-2}$ and $|K_i \cap K_0| = q^{2t-4}$ for $i = 1, ..., 2m$ such that every nonprincipal character of A is trivial on exactly one K_i, $0 \leq i \leq 2m$.

Let G be an abelian group containing A as a subgroup of index 2. Note $\exp G \leq 4$. The quotient group $H_0 := G/K_0$ has order $4q^2$ and thus there is a Hadamard difference set D_0 in H_0 by Lemma 4.2. For the same reason, there are also Hadamard difference sets D_i in A/H_i for $i = 1, ..., 2m$. Now let $U_0 \subset G$ be the preimage of D_0, and let $U_i \subset A$, $i = 1, ..., 2m$, be the preimage of D_i. Choose $g \in G \setminus A$. Then $\{U_0, U_1 \cup U_2 g, ..., U_{2m-1} \cup U_{2m} g\}$ is a $(2q^{2t-1}(q-1), q^{2t-1}, \frac{q^{2t}-q^2}{q^2-1}, +)$-CEBS in G. Thus Theorem 4.1 yields

Theorem 4.3 *Let q be any power of 2, let t be any positive integer, and let G be an abelian group of order $4q^{2t}\frac{q^{2t}-1}{q^2-1}$ which contains an elementary abelian subgroup of order $2q^{2t}$. Then there is a difference set with parameters (3) in G.*

Theorem 4.3 is an example demonstrating how fruitful the concept of building sets of Davis and Jedwab [11] is. Further examples are provided by Hou and Sehgal [27] who found an abundant number of new building sets. The focus of their work is on *secondary* (or second hand) building sets, i.e. building sets which can be obtained from other building sets by contraction or extension. A thorough analysis of these methods led Hou and Sehgal to the construction of many new families of semiregular relative difference sets. The maximum exponent of the abelian p-groups covered by their method is in general significantly higher than in all previously known constructions.

Up to now, only a few nonexistence results on CEBS have been obtained. Surely, this is a topic which deserves more attention. The only significant result known at present is due to Chen [9] who studied the family of CEBSs in abelian groups G with parameters of the form $(a, |G| - 2a, h, +)$. He calls these CEBSs (a, h)-***covering systems***. There are two known families of such systems corresponding to Hadamard and Spence difference sets. Chen obtained the following useful restrictions on the parameters of a covering system.

Theorem 4.4 *Let G be an abelian group with an (a, h)-covering system. Then there are nonnegative integers u and v, where u odd, such that*

$$\begin{aligned} |G| &= u^2[1 + v(u^2-1)/4, \\ a &= \frac{u(u-1)}{2}[1 + v(u^2-1)/4], \\ h &= u^2 v + 4. \end{aligned}$$

In particular, G is of odd order. Furthermore,

$$\varphi(\exp G) \leq (u^2-1)/4,$$

where φ denotes the Euler φ-function.

5 Ionin's construction of symmetric designs

Ionin [28, 29, 30] discovered a powerful technique for the construction of symmetric designs which uses difference sets with $(v,k) > 1$ as an essential ingredient. In this way, he found seven new infinite families of symmetric designs. Because of its importance, we describe Ionin's method in somne detail. His construction starts with an incidence matrix M of a (smaller) symmetric (v,k,λ)-design. Let K be a set of $v \times v$ matrices with entries 0 and 1 containing the zero matrix, where each matrix in $K \setminus \{0\}$ is obtained from M by some "harmless" modification, for instance, by applying the same cylic shift to each row of M.

Strategy: Try to arrange the matrices from K into a block matrix T such that T becomes an incidence matrix of a larger symmetric design. The crucial point here, of course, is to find sufficient conditions on K and T to make this construction work. Before we describe Ionin's conditions, we need to recall the following definition.

A ***balanced generalized weighing matrix*** $BGW(w,l,\mu)$ over a group G is a $w \times w$ matrix $W = (g_{ij})$ with entries from $\overline{G} := G \cup \{0\}$ such that each row of W contains exactly l nonzero entries, and for every $a, b \in \{1, ..., w\}$, $a \neq b$, the multiset $\{g_{ai} g_{bi}^{-1} : 1 \leq i \leq w, g_{ai}, g_{bi} \neq 0\}$ contains exactly $\mu/|G|$ copies of each element of G.

Ionin's sufficient conditions are given in the following theorem. By I and J we denote the identity matrix and the all-one matrix of the appropriate sizes, respectively.

Theorem 5.1 *Let K be a set of $v \times v$ matrices with entries 0-1 containing the zero matrix. Let G be any group of order $w := |K| - 1$ and write $K = \{M_g : g \in \overline{G}\}$, where M_0 is the zero matrix. Assume that there is some $BGW(w,l,\mu)$ over G, say $W = (g_{ij})$. Then the block matrix $T := (M_{g_{ij}})_{i,j=1}^{w}$ is an incidence matrix of a symmetric $(vw, kl, \lambda l)$- design, provided that the following conditions are satisfied.*

(i) M_1 *is an incidence matrix of a symmetric (v,k,λ)-design, that is* $M_1 M_1^T = (k-\lambda)I + \lambda J$

(ii) $M_{gk} M_{hk}^T = M_g M_h^T$ *for all* $g, h, k \in G$,

(iii) $\sum_{g \in G} M_g = \frac{k|G|}{v} J$,

(iv) $k^2 \mu = v \lambda l$.

The proof is by straightforward computation. For instance, for $a \neq b$, we have to show $\sum_{i=1}^{w} M_{g_{ai}} M_{g_{bi}}^T = \lambda l J$. Let us verify this:

$$\begin{aligned}
\sum_{i=1}^{w} M_{g_{ai}} M_{g_{bi}}^T &\overset{(ii)}{=} \sum_{i=1}^{w} M_{g_{ai} g_{bi}^{-1}} M_1^T \\
&\overset{BGW}{=} \frac{\mu}{|G|} (\sum_{g \in G} M_g) M_1^T \\
&\overset{(iii)}{=} \frac{\mu k |G|}{|G| v} J M_1^T \\
&\overset{(i),(iv)}{=} \lambda l J. \quad \square
\end{aligned}$$

The first ingredient needed to satisfy the conditions of Theorem 5.1 are the well known BGWs which can be obtained from the classical relative difference sets associated with affine spaces.

Theorem 5.2 *Let q be a prime power, and let s be a divisor of $q-1$. Then there is a $BGW(\frac{q^{d+1}-1}{q-1}, q^d, q^d - q^{d-1})$ over $\mathbb{Z}_s$ for every positive integer d.*

The construction of these BGWs is easy: Let R be the set of elements of $\mathbb{F}_{q^{d+1}}$ of trace 1 relative to $\mathbb{F}_q$. Then R is a $(\frac{q^{d+1}-1}{q-1}, q-1, q^d, q^{d-1})$-difference set in $\mathbb{F}_{q^{d+1}}^*$ relative to $\mathbb{F}_q^*$. By projection, one obtains $(\frac{q^{d+1}-1}{q-1}, s, q^d, \frac{q^{d-1}(q-1)}{s})$-difference sets R_s relative to $N_s = \mathbb{F}_q^*/U_s$ for every divisor s of $q-1$, where U_s is the subgroup of F_q^* of index s.Let α be a primitive element of $\mathbb{F}_{q^{d+1}}$. We define a $(\frac{q^{d+1}-1}{q-1} \times \frac{q^{d+1}-1}{q-1})$-matrix $W = (n_{ij})$ with entries in $N_s \cup \{0\}$ as follows. If there is a (necessarily unique) element r of $R_s \alpha^i$ in the coset $N_s \alpha^j$,then we set $n_{ij} = \alpha^{-j} r$, and otherwise $n_{ij} = 0$. Then W is the desired BGW.

The second ingredient is incidence matrices of symmetric designs corresponding to difference sets with $(v, n) > 1$. The unifying construction [11] of Davis and Jedwab shows that such difference sets in direct products $R \times S$ of abelian groups R and S can be obtained in the form

$$D = \bigcup_{s \in S} B_s s$$

with $B_s \subset R$ such that $\{B_s : s \in S\}$ is a covering extended building set on R, see Thorem 4.1. This means that — with an appropriate ordering of the points and blocks — the incidence matrix M of the symmetric design corresponding to such a difference set is an $(|S| \times |S|)$-block matrix, where each block is an $(|R| \times |R|)$-matrix corresponding to some building block

$B_s \subset R$ such that each building block is represented exactly once in each row of M.

Now, we take $M_1 := M$ in Theorem 5.1. Then condition (i) is satisfied. The main problem here is to satisfy condition (iii). This can be done by deriving the matrices M_g from M by "harmless" operations not violating (ii) such that (iii) will be fulfilled. Examples of such harmless operations are applying the same cyclic shift to each row of the block matrix M or replacing each building block B_s by a translate of B_s in R. Let's consider the nicest examples, namely, the designs Ionin constructed from McFarland difference sets.

Let t be any prime power, and let a be any positive integer. McFarland difference sets can be obtained in groups $R \times S$, where R is the additive group of an $(a+1)$-dimensional vector space over $\mathbb{F}_t$ and where S is any group of order $r+1$; here $r = \frac{t^{a+1}-1}{t-1}$ is the number of hyperplanes of R. Define $B_1 := \emptyset$ and let $\{B_s : s \in S, s \neq 1\}$ be the set hyperplanes of R. Then $D := \cup_{s \in S} B_s s$ is a difference set in $R \times S$ with parameters

$$(v, k, \lambda) = (t^{a+1}(r+1), t^a r, t^{a-1}(r-1));$$

this fact was discovered by McFarland [42] in 1973. Now, the incidence matrix M of the symmetric design corresponding to such a difference set can be chosen as an $((r+1) \times (r+1))$-block matrix such that every row contains exactly one zero block (coming from $B_1 = \emptyset$) and r blocks corresponding to all the hyperplanes of R. For each hyperplane B_s, let $\{B_{s1}, ..., B_{st}\}$ be the set of all translates of B_s in R. We construct matrices M_{xy}, $x = 0, ..., r$, $y = 1, ..., t$, from M as follows.

To get M_{xy} from M, shift each row (of blocks) of M cyclically by x positions and replace each hyperplane B_s, $s \in S \setminus \{1\}$, by B_{sy}.

In this way, we get a set K of $(r+1)t$ matrices such that $\sum_{X \in K} X$ is a multiple of the all-one matrix. The reason for this is that the translates of a hyperplane cover each point of R exactly once and that the zero block occurs exactly once in each position during the cyclic shifting.

Now, let G be *any* group of order $(r+1)t$, and write $K = \{M_g : g \in G\}$ with $M_1 = M$. It is not difficult to verify that K satisfies the conditions $(i) - (iii)$ of Theorem 5.1. Suppose that $r = \frac{t^{a+1}-1}{t-1}$ is a prime power. Let $q := r^2$. Then $(r+1)t$ divides $q - 1 = (r+1)\frac{t^{a+1}-t}{t-1}$, and thus there is a $BGW(\frac{q^{d+1}-1}{q-1}, q^d, q^d - q^{d-1})$ over $\mathbb{Z}_{(r+1)t}$ for every $d \geq 1$ by Theorem 5.2. Also note $k^2\mu = t^{2a}r^2(q^d - q^{d-1}) = [t^{a+1}(r+1)][t^{a-1}(r-1)]q^d = v\lambda l$, that is, condition (iv) of Theorem 5.1 is satisfied, too.

Taking $G = \mathbb{Z}_{(r+1)t}$ and applying Theorem 5.1, we get Ionin's first infinite family of symmetric designs. We remark that this generalizes a construction

of Jungnickel and Pott [34] who obtained Theorem 5.3 under the more restrictive assumption that t is a prime.

Theorem 5.3 *Let t be a prime power, and let a be a positive integer such that $r := \frac{t^{a+1}-t}{t-1}$ is also a prime power. Then there is a symmetric design with parameters*

$$(v, k, \lambda) = (t^{a+1}\frac{r^{2d+2}-1}{r-1}, t^a r^{2d+1}, (r-1)r^{2d}t^{a-1})$$

for every positive integer d.

Applying the method leading to Theorem 5.3 to the complements of McFarland difference sets, Spence and Davis/Jedwab difference sets and their complements, and to Hadamard difference sets of order $4^d \cdot 9$, $d \geq 0$, Ionin [30] obtained six further infinite families of symmetric designs. All these constructions use Theorems 5.1 and 5.2.

6 Elementary Hadamard difference sets

An ***elementary Hadamard difference set*** (EHDS) is a difference set with parameters$(v, k, \lambda) = (2^{2t}, 2^{2t-1} \pm 2^{t-1}, 2^{2t-2} \pm 2^{t-1})$ in the elementary abelian group $EA(2^{2t})$. Sometimes these difference sets are (but shouldn't be) called ***bent functions***. EHDSs were studied intensively in Dillon's thesis [13]. Since then, several new constructions of EHDSs have been found. Dobbertin [15] and Xiang [62] used maximally nonlinear functions on $\mathbb{F}_{2^t}$ for the construction of EHDSs in $EA(2^{2t})$. Carlet [3] introduced the concept of generalized partial spreads for the construction and characterization of EHDSs. A ***generalized partial spread*** in $G = EA(2^{2t})$ is a subset S of G for which there are integers $\lambda_1, ..., \lambda_r$ and subgroups $U_1, ..., U_r$ of order 2^t of G with

$$S = -2^{t-1} + \sum_{i=1}^{r} \lambda_i U_i$$

in the group ring $\mathbb{Z}[G]$. It can be checked that a subset D of G is an EHDS if and only if $\chi(D) \equiv 2^{t-1} \pmod{2^t}$ for all characters χ of G, see [3, Lemma 1], for instance. Note that $\chi(U_i) \equiv 0 \pmod{2^t}$, by the orthogonality relations. Thus we have

Lemma 6.1 *Any generalized partial spread is also an EHDS.*

This fact was used in [3] to construct a new family of EHDSs. Carlet and Guillot [4, 5] gave characterizations of EHDSs in terms of generalized partial spreads. These results were improved considerably by Guillot [22] who obtained the following nice theorem.

Theorem 6.2 *There exists a set $\mathcal{U}$ of $2^{2t}-1$ subgroups of $G = EA(2^{2t})$ of order 2^t such that up to translation any EHDS in can be written in the form*

$$D = -2^{t-1} + \sum_{U \in \mathcal{U}} \lambda_U U$$

with uniquely determined integers λ_U.

7 Perfect binary sequences

Cyclic difference sets are intimately related to certain periodic sequences, a fact which is still not as well known as it should be — such sequences have many extremely important real world applications. The "autocorrelation function" of a sequence is a measure for how much the given sequence differs from its translates. Periodic binary sequences with good correlation properties are needed for applications in various areas of engineering. In order to explain the connection to difference sets, we have to recall a few definitions.

A sequence $\mathbf{a} = (a_i)_{i=0,1,2...}$ is called ***periodic*** with ***period*** v provided that $a_i = a_{i+v}$ for all i. We will only consider ***binary*** sequences, that is, all entries are either $+1$ or -1. The ***(periodic) autocorrelation function*** C of $\mathbf{a}$ is defined by

$$C(t) := \sum_{i=0}^{v-1} a_i a_{i+t}.$$

Note that the sequence $\mathbf{C} = C(t)$ is again periodic with period v, so that it suffices to consider the ***autocorrelation coefficients*** $C(t)$ for $t = 0, ..., v-1$. As already mentioned, the autocorrelation function is a measure for how much the original sequence differs from its ***translates***: $C(t)$ just counts the number of agreements of $\mathbf{a}$ with its translate by a shift of t minus the number of disagreements. In particular, $C(0) = v$. All other autocorrelation coefficients are called ***nontrivial*** or the ***off-peak*** autocorrelation coefficients. In what follows, we shall always denote the number of entries $+1$ contained in one period of $\mathbf{a}$ by k.

For practical applications, one requires sequences with a ***two-level autocorrelation function***, that is, all nontrivial autocorrelation coefficients

equal some constant γ. Such sequences turn out to be equivalent to cyclic difference sets, as the following simple but fundamental result shows.

Lemma 7.1 *A periodic binary sequence with period v, k entries $+1$ per period and two-level autocorrelation function (with all nontrivial autocorrelation coefficients equal to γ) is equivalent to a cyclic (v, k, λ)-difference set, where $\gamma = v - 4(k - \lambda)$.*

For some applications, it is more natural to use sequences with entries 0 and 1, instead of entries ± 1. If we replace every entry -1 in a periodic binary sequence $\mathbf{a}$ by 0, we obtain a 0/1-sequence $\hat{\mathbf{a}}$. Formally applying the definition of the autocorrelation function C of $\mathbf{a}$ to $\hat{\mathbf{a}}$, we obtain another periodic function which we will denote by $\hat{C}$. Fortunately, these two functions are related in a very simple manner:

Lemma 7.2 *Let $\mathbf{a}$ be a periodic binary sequence with period v, and let $\hat{\mathbf{a}}$ be the corresponding 0/1-sequence. Let k be the number of entries $+1$ in one period of $\mathbf{a}$. Then the autocorrelation coefficients $C(t)$ and $\hat{C}(t)$ are related as follows:*

$$C(t) \;=\; v - 4(k - \hat{C}(t).$$

Corollary 7.3 *Let $\mathbf{a}$ be a periodic binary sequence with period v. Then all autocorrelation coefficients $C(t)$ are congruent to v modulo 4.*

A ± 1-sequence (a_i) of period v is called ***perfect*** if it has a two-level autocorrelation function where the off-peak autocorrelation coefficients γ are as small as theoretically possible (in absolute value). It is not at all clear that perfect sequences exist, and indeed for many values of v no such sequences can exist. In order to determine the (theoretically) smallest values, we have to distinguish the period v of the sequence modulo 4, since always $\gamma \equiv v \bmod 4$, by Corollary 7.3. Not surprisingly, we call the difference sets corresponding to perfect sequences ***perfect*** difference sets. Let n denote the order of such a difference set D. Using the connection between the autocorrelation coefficients γ and the parameters of D given in Lemma 7.1, we have

$$n = \frac{v - \gamma}{4}.$$

Hence we obtain the following table.

	off-peak autocorrelation γ	order n of difference set
$v \equiv 0 \bmod 4$	0	$\frac{v}{4}$
$v \equiv 1 \bmod 4$	1	$\frac{v-1}{4}$
$v \equiv 2 \bmod 4$	2 or -2	$\frac{v-2}{4}$ or $\frac{v+2}{4}$
$v \equiv 3 \bmod 4$	-1	$\frac{v+1}{4}$

Thus there are five different classes of perfect difference sets, corresponding to the five different nontrivial autocorrelation coefficients. In the older literature, only the sequences with period $\equiv 1 \bmod 4$ were called perfect, but this seems a bit arbitrary. Given the size v and the order n of a difference set, the k-value has to be a solution of the trivial equation $k^2 - k = (k-n)(v-1)$ connecting the parameters of a difference set; hence

$$k \;=\; \frac{v}{2} \pm \sqrt{\frac{v^2}{4} - n(v-1)}\,.$$

Without loss of generality, we can choose the negative square root (the other sign corresponds to the complementary difference set). The different orders n yield the following parameters:

I $\left(v, \dfrac{v-\sqrt{v}}{2}, \dfrac{v-2\sqrt{v}}{4}\right)$ of order $\dfrac{v}{4}$

II $\left(v, \dfrac{v-\sqrt{2v-1}}{2}, \dfrac{v+1-2\sqrt{2v-1}}{4}\right)$ of order $\dfrac{v-1}{4}$

IIIa $\left(v, \dfrac{v-\sqrt{2-v}}{2}, \dfrac{v-2-2\sqrt{2-v}}{4}\right)$
of order $\dfrac{v+2}{4}$ (autocorrelation -2)

IIIb $\left(v, \dfrac{v-\sqrt{3v-2}}{2}, \dfrac{v+2-2\sqrt{3v-2}}{4}\right)$
of order $\dfrac{v-2}{4}$ (autocorrelation $+2$)

IV $\left(v, \dfrac{v-1}{2}, \dfrac{v-3}{4}\right)$ of order $\dfrac{v+1}{4}$

We shall discuss only the two most interesting cases, namely types **I** and **IV**. For more details and a discussion of the remaining cases, we refer the reader to the recent survey [35]; this paper also treats variations on the notion of perfectness (perfect ternary sequences, almost perfect sequences, perfect arrays etc.) and describes a specific real world application in some detail.

Of course, difference sets of type **I** are just Hadamard difference sets, since v has to be an even square, say $v = 4u^2$. Then we can write the parameters in the more familiar way

$$(4u^2, 2u^2 - u, u^2 - u).$$

The circulant Hadamard matrix conjecture already discussed at the end of Section 2 states that the only cyclic Hadamard difference set occurs for $u = 1$, so that the only perfect sequence of a period v divisble by 4 has $v = 4$. Note that Schmidt's Theorem 2.6 immediately yields the following asymptotic result:

Corollary 7.4 *Let Q be any finite set of odd primes. Then there are only finitely many cyclic Hadamard difference sets of order u^2, where all prime divisors of u are in Q.*

Actually, Theorem 2.6 should prove the circulant Hadamard catrix conjecture for almost all large u. Schmidt [52] confirmed this hinch by the following results of a computer search.

Range of u (u odd)	**# of cases not ruled out by Theorem 2.6 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 the results of Turyn [56], one can rule out 12 of the 26 cases with $u \leq 10,000$ which are not covered by Theorem 2.6 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. In particular, the smallest integer u for which the nonexistence of a cyclic Hadamard difference set is still open is $u = 165$. Schmidt's results also have strong implications for a related problem, namely the ***Barker sequence conjecture***.

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 Hadamard difference set in the cyclic group of order l, see [56, 57]. 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 2.6 a), Schmidt [52] gets the following bound by a computer search. It improves the previously known bound [16, p. 363] by a factor greater than 10^6. Note that Turyn's inequality [56, Thm. 6] is not needed to obtain this result.

Theorem 7.5 *There is no Barker sequence of length l for $13 < l \leq 4 \cdot 10^{12}$.*

Difference sets of type **IV** are called ***Paley-Hadamard difference sets***. The known series of cyclic Paley-Hadamard difference sets (and their associated perfect sequences) are given in the following list, cf. [33] or [2].

(1) *Singer difference sets (m-sequences)*:
$(2^m - 1, 2^{m-1} - 1, 2^{m-2} - 1)$

(2) *Paley difference sets (Legendre sequences)*:
$\left(p, \frac{p-1}{2}, \frac{p-3}{4}\right)$, where p is a prime.

(3) *Twin prime difference sets (Uniformly redundant arrays)*:
$\left(p(p+2), \frac{p(p+2)-1}{2}, \frac{p(p+2)-3}{4}\right)$, where both p and $p+2$ are primes. (It is quite usual in the engineering literature to write the perfect sequence as an array in this case, corresponding to writing the underlying cyclic group in the form $\mathbb{Z}_p \times \mathbb{Z}_{p+2}$.)

A recent systematic investigation of cyclic Paley-Hadamard difference sets is in [55]. It is generally conjectured that every such difference set has parameters as in one of the three series above (but there are, of course, further nonequivalent examples); this conjecture has been verified in [55] for orders $n < 10,000$ with 17 possible exceptions:

Theorem 7.6 *Assume the existence of a Paley-Hadamard difference set D in a cyclic group of order v, where $v < 10,000$. Then v is either of the form $2^m - 1$, or a prime $\equiv 3$ mod 4, or the product of two twin primes, with the possible exceptions of $v =$* 1295, 1599, 1935, 3135, 3439, 4355, 4623, 5775, 7395, 7743, 8227, 8463, 8591, 8835, 9135, 9215, 9423.

A concrete application of the perfect sequences corresponding to the cyclic twin prime difference sets in Applied Optics ("Coded aperture imaging") is discussed in [35, Section 8].

8 Miscellanea

Difference sets with $(v, n) > 1$ seem to prefer to live in groups with low exponent and high rank. This phenomenon can be viewed as the central theme of most papers on difference sets, but is not completely understood

yet. Of course, the character method shows that the exponent of an abelian group containing a difference set with $(v, n) > 1$ usually has to be rather small, see Section 2. Moreover, many constructions of difference sets with $(v, n) > 1$ only work for groups with high rank. However, in most cases we do not know why (if at all) this has to be the case. An interesting contribution to the understanding of these phenomena is due to M. Hagita [23]. Roughly speaking, he shows that in some cases the existence of a difference set in an abelian group G implies the existence of difference sets in all abelian groups of the same order which have a higher rank and whose exponent does not exceed the exponent of G.

Some new nonexistence criteria for difference sets using the classical self-conjugacy approach can be found in the paper [18] of Enomoto, Hagita and Matsumoto. Arasu and Sehgal [1] filled ten missing entries of the table [58] by showing nonexistence in all these cases. Finally, we mention that Jia [32] proved that a difference set with Spence parameters $(v, k, \lambda, n) = (351, 126, 45, 81)$ in an abelian group G exists if and only if $\exp(G) = 39$. His proof uses the techniques developed by Ma [38].

References

[1] K.T. Arasu and S.K. Sehgal: Nonexistence of some difference sets. Preprint.

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

[3] C. Carlet: Generalized partial spreads. *IEEE Trans. Inform. Theory* **41** (1995), 1482-1487.

[4] C. Carlet: A construction of bent functions. In: *Finite fields and aplli-cations* (Eds. S.D. Cohen and H.Niederreiter), Cambridge University Press, Cambridge (1996), pp. 47–58.

[5] C. Carlet and P. Guillot: A characterization of binary bent functions. *J. Combin. Theory A* **76** (1996), 328–335.

[6] C. Carlet and P. Guillot: An alternate characterization of the bentness of binary functions, with uniqueness. *Designs, Codes and Cryptography* **14** (1998), 133–140.

[7] 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.

[8] Y.Q. Chen: A construction of difference sets. *Designs, Codes and Cryptography* **13** (1998), 247–250.

[9] On a family of covering extended building sets. *Designs, Codes and Cryptography* (to appear).

[10] J.A. Davis and J.E. Iiams: Hadamard difference sets in nonabelian 2-groups with high exponent. *J. Algebra* **199** (1998), 62–87.

[11] J.A. Davis and J. Jedwab: A unifying construction of difference sets. *J. Combin. Theory A* **80** (1997), 13–78.

[12] J.A. Davis and J. Jedwab: Nested Hadamard Difference Sets. *J. Statist. Plann. Inf.* **62** (1997), 13–20.

Preprint.

[13] J.F. Dillon: *Elementary Hadamard difference sets.* Ph.D. thesis, University of Maryland (1974).

[14] J.F. Dillon, H. Dobbertin and Q. Xiang: Hyperovals, cyclic difference sets and codes. Preprint.

[15] H. Dobbertin: Constructions of bent functions and balanced Boolean functions with high nonlinearity. Lecture Notes in Computer Science **1008**, Springer, Berlin (1995), 61–74.

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

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

[18] H. Enomoto, M. Hagita and M. Matsumoto: A Note on Difference Sets. *J. Combin. Theory A* (to appear).

[19] M. van Eupen and V.D. Tonchev: Linear codes and the existence of a reversible Hadamard difference set in $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5^4$. *J. Combin. Theory A* **79** (1997), 161–167.

[20] R. Evans, C. Krattenthaler and Q. Xiang: Gauss Sums, Jacobi Sums, and p-ranks of Cyclic Difference Sets. Preprint.

[21] D.G. Glynn: Two new sequences of ovals in finite Desarguesian planes of even order. In: *Combinatorial mathematics*, Lecture Notes in Math. **1036**, Springer, Berlin/New York (1983), pp. 217-229

[22] P. Guillot: Completed GPS covers all bent functions. Submitted.

[23] M. Hagita: Foldings of difference sets in abelian groups. *Graphs and Combinatorics* (to appear).

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

[25] J.W.P. Hirschfeld: *Projective geometries over finite fields (2nd edition).* Oxford University Press (1998).

[26] C.Y. Ho: Arc subgroups of planar Singer groups. In: *Mostly finite geometries* (Ed. N.L. Johnson). Lecture Notes in Pure and Appl. Math. **190**, Dekker, New York (1997), pp.227-233.

[27] X.-D. Hou and S.K. Sehgal: Building sets and semi-regular divisible difference sets. Preprint.

[28] Y.J. Ionin: A technique for constructing symmetric designs. *Designs, Codes and Cryptography* **14** (1998), 147–158.

[29] Y.J. Ionin: New symmetric designs from regular Hadamard matrices. *Electronic J. of Comb.* **5** (1998), R1.

[30] Y.J. Ionin: Building symmetric designs with building sets. Preprint.

[31] K. Ireland and M. Rosen: *A Classical Introduction to Modern Number Theory.* Springer, Berlin/New York/Heidelberg (1990).

[32] Z. Jia: On $(351, 126, 45)$-difference sets. Preprint.

[33] D. Jungnickel: Difference sets. In: *Contemporary design theory: A collection of surveys* (Eds. J.H. Dinitz and D.R. Stinson). Wiley, New York (1992), pp. 241–324.

[34] D. Jungnickel and A. Pott: A new class of symmetric $(v, k\lambda)$-designs. *Designs, Codes and Cryptography* **4** (1994), 319–325.

[35] D. Jungnickel and A. Pott: Perfect and almost perfect sequences. Preprint.

[36] D. Jungnickel and B. Schmidt: Difference sets: An update. In: *Geometry, combinatorial designs and related structures* (Eds. J.W.P. Hirschfeld, S.S. Magliveras and M.J. de Resmini). Cambridge University Press (1997), pp. 89–112.

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

[38] S.L. Ma: Planar functions, relative difference sets and character theory. *J. Algebra* **185** (1996), 342–356.

[39] S.L. Ma and B. Schmidt: A sharp exponent bound for McFarland difference sets with $p = 2$. *J. Combin. Theory A* **80** (1997), 347–352.

[40] J. MacWilliams and H.B. Mann: On the p-rank of the design matrix of a difference set. *Inform. Control* **12** (1968), 474–488.

[41] A. Maschietti: Difference sets and hyperovals. *Designs, Codes and Cryptography* **14** (1998), 89–98.

[42] R.L. McFarland: A family of difference sets in non-cyclic abelian groups. *J. Comb. Th. (A)* **15** (1973), 1–10.

[43] P.K. Menon: On difference sets whose parameters satisfy a certain relation. *Proc. Amer. Math. Soc.* **13** (1962), 739–745.

[44] M. Muzychuk: Difference Sets with $n = 2p^m$. *J. Algebraic Combin.* **7** (1998), 77–89.

[45] S.E. Payne: A complete determination of translation ovoids in finite desarguesian planes. *Atti Acad. Naz. Lincei Rend.* **51** (1971), 328–331.

[46] W. Qiu: A character approach to the multiplier conjecture and a new result for the case $n = 3n_1$. *J. Combin. Des.* **5** (1997), 81–93.

[47] D.K. Ray-Chaudhuri and Q. Xiang: New necessary conditions for abelian Hadamard difference sets. *J. Stat. Plann. Inf.* **62** (1997), 69–79.

[48] H.J. Ryser: *Combinatorial mathematics.* Wiley, New York (1963).

[49] B. Schmidt: Nonexistence of a $(783, 69, 6)$-difference set. *Discrete Math.* **178** (1998), 283–285.

[50] B. Schmidt: Nonexistence Results for Chen and Davis-Jedwab difference sets. *J. Algebra* **202** (1998), 404–413.

[51] B. Schmidt: Cyclotomic integers of prescribed absolute value and the class group. Preprint.

[52] B. Schmidt: Cyclotomic integers and finite geometry. *J. Amer. Math. Soc.* (to appear).

[53] B. Segre: Ovals in a finite projective plane. *Canad. J. Math.* **7** (1955), 414–416.

[54] B. Segre and U. Bartocci: Ovali ed altre curve nei piani di Galois di caratteristica due. *Acta Arith.* **8** (1971), 423–449.

[55] H.Y. Song and S.W. Golomb: On the existence of cyclic Hadamard difference sets. *IEEE Trans. Inf. Th.* **40** (1994), 1266–1268.

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

[57] R.J. Turyn: Sequences with small correlation. In: *Error correcting codes* (Ed. H.B. Mann). Wiley, New York (1969), pp. 195–228.

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

[59] L.C. Washington: *Introduction to cyclotomic fields.* Springer, Berlin/New York/Heidelberg (1997).

[60] R. Wilson and Q. Xiang: Constructions of Hadamard difference sets. *J. Combin. Theory A* **77** (1997), 148–160.

[61] Q. Xiang: On reversible abelian Hadamard difference sets. *J. Stat. Plann. Inf.* (in press).

[62] Q. Xiang: Maximally nonlinear functions and bent functions. *Designs, Codes and Cryptography* (to appear).

[63] Q. Xiang: On balanced binary sequences with two-level autocorrelation functions. *IEEE Trans. Inform. Theory* (to appear).