Difference Sets: an Update

Dieter Jungnickel
and
Bernhard Schmidt

Mathematisches Institut
Universität Augsburg
Universitätsstraße 15
86135 Augsburg

Abstract

In the last few years there has been rapid progress in the theory of difference sets. This is a survey of these fascinating new developments.

1 Introduction

This paper is an update of the survey of the first author [Jungnickel (1992)]. Recent surveys on related topics are Ma (1994) (partial difference sets) and Pott (1996) (relative difference sets). For the connections to coding theory, we refer the reader to Assmus, Key (1992, 1992a, to appear) and Pott (1992). A comprehensive introduction to difference sets can be found in Beth, Jungnickel, Lenz (1986) and Jungnickel (1992).

For the convenience of the reader, we recall the basic definition. A (v, k, λ)-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. We say that D is abelian, cyclic etc. if G has this property.

The known families of difference sets can be subdivided into three classes: **difference sets with Singer parameters**, **cyclotomic difference sets**

and **difference sets with** $(\mathbf{v}, \mathbf{n}) > \mathbf{1}$. The difference sets with Singer parameters include the classical Singer difference sets and the Gordon-Mills-Welch series. By cyclotomic difference sets we mean the Paley series consisting of the quadratic residues in $GF(q)$, $q \equiv 3 \bmod 4$, the families using higher order residues and also the twin prime power series. The families of difference sets with $(v, n) > 1$ are the Hadamard difference sets, the McFarland and Spence family and two new series, one found by Davis/Jedwab and one found by Chen. The construction methods for these three classes of difference sets are completely different: The Singer difference sets are cyclic and can be obtained from the action of a cyclic group of linear transformations on the one-dimensional subspaces of a finite field (viewed as a vector space over a suitable subfield), while cyclotomic difference sets live in elementary abelian groups (or the direct product of two such groups) and are unions of cosets of multiplicative subgroups of finite fields. The class of difference sets with $(v, n) > 1$ is by far the richest; only recently, in a major work of Davis and Jedwab (1996), it has been discovered that all these difference sets are in fact very similar. In their paper, Davis and Jedwab give a recursive construction which covers all abelian groups known to contain a difference set with $(v, n) > 1$ (a modification is needed to include Chen's series). The best way to describe their construction is in terms of (abelian) characters: The difference set is built up from smaller pieces, which are in some sense orthogonal to each other with respect to the character group.

In the **existence theory** of difference sets, usually the following kind of problem is considered. Given a parameter series (for instance the Singer series), which (abelian) groups can contain a difference set with these parameters? Here the group order is prescribed, and the task is to find necessary and sufficient conditions on the group structure for the existence of a difference set. This turns out to be an extremely difficult problem; up to now, it has been solved for only two infinite parameter series, namely for difference sets in abelian 2-groups [Davis (1991), Kraemer (1993)] and (almost) for McFarland difference sets under the self-conjugacy assumption [McFarland (1973), Ma, Schmidt (1995a, submitted)].

The existence theory for Singer and cyclotomic difference sets on one side and difference sets with $(v, n) > 1$ on the other side is clearly separated. While the main tool for the study of the Singer and cyclotomic difference sets is the multiplier theorem, almost all results on difference sets with $(v, n) > 1$ are exponent bounds and rely on the character theoretic approach introduced by Turyn (1965). Most of the nonexistence results presented in this survey

are of the latter type, since the research focussed on difference sets with $(v, n) > 1$ in the last few years.

In this context, we encounter a notion coming from algebraic number theory again and again. A prime p is called **self-conjugate** modulo a positive integer m, if there exists j, such that $p^j \equiv -1 \bmod m'$, where m' is the p-free part of m. If we study difference sets in an abelian group G, we usually say that the self-conjugacy assumption is satisfied, if every prime divisor of the order n is self-conjugate modulo $\exp(G)$.

2 Difference Sets with $(\mathbf{v}, \mathbf{n}) > \mathbf{1}$

There are five known families of difference sets with $(v, n) > 1$, namely the Hadamard difference sets (called Menon difference sets in Jungnickel (1992)), the McFarland and the Spence family, a series similar to the Spence difference sets discovered by Davis, Jedwab (1996), and a series generalizing Hadamard difference set found by Chen.

A striking fact that should be mentioned in such a survey is that all known abelian difference sets with $(v, n) > 1$ satisfy a common condition which might be called the **character divisibility property**: We say that an (v, k, λ)-difference set D of square order $n = k - \lambda$ in an abelian group G satisfies the character divisibility property if the character value $\chi(D)$ is divisible by $\sqrt{n}$ for all nontrivial characters χ of G. Although every known abelian difference set with $(v, n) > 1$ has this property we feel that it would not be a good idea to turn this observation into a conjecture as has been done in similar situations. Instead, we pose the following

Research Problem: Construct difference sets with $(v, n) > 1$ that do not have the character divisibility property.

In our exposition of the latest results, we begin with the Hadamard difference sets (HDSs) which form by far the richest and most important family. In parts of the sections on HDSs we have drawn from the survey Davis, Jedwab (1996a). For more details we refer the reader to this article which deals exclusively with HDSs.

2.1 Abelian HDSs

By a **Hadamard difference set (HDS)**, we mean a difference set with parameters

$$(v, k, \lambda) = (4N^2, 2N^2 - N, N^2 - N).$$

In the last few years, there has been rapid progress in the theory of HDSs. Perhaps this is best demonstrated by the following outdated conjecture which is usually (but erroneously) attributed to McFarland and was wiped out completely by the new results.

Conjecture 2.1 *If there is an abelian HDS with $v = 4N^2$, then $N = 2^r 3^s$ for some integers r, s.*

The reader should compare this conjecture with Theorem 2.4!

We first come to the new constructions and then summarize the recent nonexistence results. We call a difference set D in a group G **reversible** if $\{d^{-1} : d \in D\} = D$.

1) After working hard for about ten years, Xia (1992) found a construction for reversible HDSs in all groups

$$\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_{p_1}^4 \times \cdots \times \mathbf{Z}_{p_t}^4,$$

where each p_i is a prime with $p_i \equiv 3 \bmod 4$ We note that this also yields HDSs in $\mathbf{Z}_4 \times \mathbf{Z}_{p_1}^4 \times \cdots \times \mathbf{Z}_{p_t}^4$ (which are not reversible). Xia's sensational construction was the first result disproving Conjecture 2.1.

The proof of the correctness of Xia's construction was considerably simplified by Xiang and Chen (1996).

2) Using a recursive construction Jedwab (1992) showed that HDSs exist in all groups

$$H \times \mathbf{Z}_{s_1} \times \cdots \times \mathbf{Z}_{s_r}$$

(where H is an abelian 2-group of square order with $exp(H) \leq 2\sqrt{|H|}$) if there exists a binary supplementary quadruple (BSQ) (see Jedwab's paper for the definition) of size $s_1 \times \cdots \times s_r$.

A new and much clearer way of viewing this construction is presented in Davis, Jedwab (1996, Cor. 6.4). Because of its importance, we explain this approach in some detail. Davis and Jedwab introduce the notion of a **covering extended building set (covering EBS)**. An $(a, m, h, \pm)$ covering EBS 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 $j \neq i$.

Once a covering EBS is known, it is easy to construct difference sets corresponding to this covering EBS, as is shown in Davis, Jedwab (1996, Theorem 2.4):

Theorem 2.2 *Suppose there exists an $(a, m, h, \pm)$ covering EBS in an abelian group G. Then there exists an $(h|G|, ah \pm m, ah \pm m - m^2)$-difference set in any abelian group containing G as a subgroup of index h.*

The reason why covering EBSs are so useful is that there is a very powerful recursive construction for these objects. Using this method, Davis and Jedwab obtain a unified construction covering all abelian groups which are known to contain a difference set with $(v, n) > 1$.

3) Arasu, Davis, Jedwab, Sehgal (1993) constructed a BSQ of size $3^b \times 3^b$ for all $b \geq 1$. In the terminology of Davis and Jedwab this amounts to a $(3^b(3^b - 1)/2, 3^b, 4, +)$ covering EBS in $\mathbf{Z}_{3^b}^2$.

4) The most recent constructions yield reversible HDSs in $\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_p^4$ for <u>all</u> odd primes p (note that this also gives HDSs in $\mathbf{Z}_4 \times \mathbf{Z}_p^4$); in the setting of Davis and Jedwab this amounts to $(p^2(p^2 - 1)/2, p^2, 4, +)$ covering EBSs in $\mathbf{Z}_p^4$. This important new development began with the discovery of a reversible HDS in $\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_5^4$ by van Eupen and Tonchev (preprint) who found this difference set by a computer search. Wilson, Xiang (submitted, Theorem 2.2) gave a very general construction method for reversible HDSs in the groups $\mathbf{Z}_2^2 \times \mathbf{Z}_p^4$. They showed that the construction of an HDS in $H \times \mathbf{Z}_p^4$, where $H \cong \mathbf{Z}_4$ or $\mathbf{Z}_2^2$, can be reduced to the construction of a spread S in $PG(3, p)$ and two projective two-weight codes which are connected with S by certain intersection properties. We note that Xia's construction, whose original proof had been very involved, is an easy corollary to this result. By their method, Wilson and Xiang obtained HDSs in $\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_p^4$, $p = 13, 17$ (with the help of a computer search), and exponentially many inequivalent reversible HDSs in $\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_p^4$ for $p \equiv 3 \bmod 4$.

In an earlier version of this survey, we wrote that "it seems very likely that HDSs in $H \times \mathbf{Z}_p^4$, $H \cong \mathbf{Z}_4$ or $\mathbf{Z}_2^2$, exist for all primes $p \equiv 1 \bmod 4$" and that "a construction should probably use Theorem 2.2 of Wilson and Xiang". In the meantime, exactly this was done by Chen (submitted) in a brilliant work. And he did even more than this: he generalized his construction to get the following new series of difference sets.

Theorem 2.3 *Let r, s, t be any positive integers, and let $q = 3^r$ or $q = p^{2s}$ for any odd prime p. Then there exists a difference set with parameters*

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

in $K \times V$, where K is any abelian group of order $4\frac{q^{2t}-1}{q^2-1}$ and V is the elementary abelian group of order q^{2t}.

The state of knowledge about abelian HDSs on the existence side is summarized in the next theorem. No other abelian groups are known to contain an HDS. The best method to understand this result is described in Davis, Jedwab (1996, section 6); one has to apply their recursive procedure to the covering EBSs mentioned above to get the following.

Theorem 2.4 *Let H be an abelian group of order 2^{2a+2} ($a \geq 0$) with $exp(H) \leq 2^{a+2}$, let $b_1, ..., b_r$ be positive integers, and let $p_1, ..., p_t$ be (not necessarily distinct) odd primes. Then the group*

$$H \times \mathbf{Z}_{3^{b_1}}^2 \times \cdots \times \mathbf{Z}_{3^{b_r}}^2 \times \mathbf{Z}_{p_1}^4 \times \cdots \times \mathbf{Z}_{p_t}^4$$

contains an HDS. Here $r = 0$ or $t = 0$ is allowed and is interpreted in the obvious way.

On the nonexistence side, all new results rely on the character theoretic approach. In this section, we only mention the results which need the self-conjugacy assumption. More nonexistence results on HDSs can be found in Section 3.

Chan, Ma and Siu (1994) found necessary conditions for groups of p-rank two (p odd) to contain an HDS. This result was generalized by Arasu, Davis and Jedwab (1995) who proved part (a) of the following theorem. Part (b) was independently obtained by Davis, Jedwab (submitted (a)) and Ma, Schmidt (1995).

Theorem 2.5 *Let G be an abelian group with Sylow p-subgroup P of order p^{2a} (p odd) containing an HDS. Write $G = H \times P$. Assume that p is self-conjugate modulo $exp(G)$. Then the following hold.*

(a) $exp(P) \leq p^a$.

Furthermore, if $exp(P) = p^a$, then $P \cong \mathbf{Z}_{p^a} \times \mathbf{Z}_{p^a}$.

(b) If $P \cong \mathbf{Z}_{p^a} \times \mathbf{Z}_{p^a}$, then also each of the groups $H \times \mathbf{Z}_{p^b} \times \mathbf{Z}_{p^b}$ with $b < a$ contains an HDS.

Ray-Chaudhuri and Xiang (to appear (a)) obtained the following partial generalization of the result of Mann and McFarland (1973).

Theorem 2.6 *There are no HDSs in abelian groups* $\mathbf{Z}_2 \times \mathbf{Z}_2 \times P$*, where* $|P| = p^{2a}$*, a is odd and p is a prime congruent to* 1 mod 4*.*

2.2 Nonabelian HDSs

The recent research on nonabelian HDSs focussed on 2-groups and groups of order $4p^2$ (p an odd prime). Davis (1992) showed that Kraemer's method which settled the existence question for HDSs in abelian 2-groups can be modified to construct HDSs in nonabelian 2-groups. This result was generalized to non-2-groups by Meisner (1992, 1996a) who gave a recursive construction of nonabelian HDSs using relative difference sets. A research effort initiated by Dillon (1990) led to the decision of the existence question for HDSs for all 267 groups of order 64. Constructions were found for 258 of these groups and nonexistence was proved for 8. The last remaining case, the so-called modular group of exponent 32, was settled by Liebler and Smith (1993) who found a construction for HDSs in this group with the help of a representation theoretic sieve. Their construction was extended by Davis and Smith (1994) who proved that there exists a group of order 2^{2a+2} and exponent 2^{a+3} containing an HDS for every $a \geq 2$. Even higher exponents where achieved by a recent construction of Davis, Iiams (submitted). They showed that there is an HDS in a nonabelian group of order 2^{4d+2} and exponent 2^{3d+2} for every $d > 0$. By comparison with Turyn's exponent bound for abelian HDSs, this is not exactly what one would have expected!

Liebler (1993) used arguments of McFarland (1989) and techniques from representation theory to prove the following result.

Theorem 2.7 *If p is an odd prime and the group*

$$G = \langle x, y, z | x^p = y^p = z^4 = 1, yx = xy, z^{-1}xz = x^{-1}, z^{-1}yz = y^{-1} \rangle$$

contains an HDS, then $p = 3$*.*

Iiams (1995) extended Liebler's work to other groups of order $4p^2$ and obtained the following.

Theorem 2.8 *Let* $p \geq 5$ *be a prime and let G be a group of order* $4p^2$ *containing an HDS. Then G has an irreducible complex representation of*

degree 4 or $G \cong \langle x, y, z | x^p = y^p = z^4 = 1,\ xy = yx,\ xz = zx,\ zyz^{-1} = y^{-1} \rangle$ *and* $p \equiv 1 \bmod 4$.

We note that Theorem 2.8 excludes 10 of the 16 isomorphism classes of groups of order $4p^2$ in the case $p \equiv 1 \bmod 4$ and 11 of the 12 isomorphism classes in the case $p \equiv 3 \bmod 4$. For both $p \equiv 1$ and 3 mod 4, McFarland (1989) had already excluded four of these classes (the abelian) and Liebler (1993) had excluded one nonabelian class, see Theorem 2.7.

There has also been an interesting discovery of a single nonabelian HDS by Smith (1995), namely an HDS in a group of order 100. McFarland (1989) had shown that an HDS in an abelian group of this order cannot exist. Smith's HDS gives the first example of a parameter triple (v, k, λ) such that a nonabelian but no abelian (v, k, λ)-difference set exists.

Finally, we note that the existence of abelian reversible HDSs implies the existence of certain nonabelian HDSs; for instance, a reversible HDS in $\mathbf{Z}_2^2 \times \mathbf{Z}_p^4$ leads to HDSs in all semi-direct products of $\mathbf{Z}_2^2$ and $\mathbf{Z}_p^4$. For related material, see Meisner (1992, 1996, 1996a).

2.3 McFarland difference sets

A **McFarland difference set** is a difference set with parameters

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

where $q = p^f$ is a prime power and d is a positive integer. A series of difference sets with these parameters was constructed by McFarland (1973) in his important paper. We will assume $(p, f) \neq (2, 1)$, as this is the case of Hadamard difference sets in 2-groups.

In the last years there has been a lot of progress in the existence theory of McFarland difference sets. Under the self-conjugacy assumption the existence problem for abelian McFarland difference sets has been solved almost completely by the work of Ma and Schmidt (1995a, submitted). A new construction in the case $q = 4$ is due to Davis and Jedwab (1996). It shows that the exponent bound of Ma and Schmidt (submitted) is necessary and sufficient in this case.

Let us first look at some previous results. Arasu, Sehgal (1995) constructed a McFarland difference set with $q = 4$ and $d = 1$ in $\mathbf{Z}_2 \times \mathbf{Z}_4^2 \times \mathbf{Z}_3$,

a group which is not covered by McFarland's original construction. Arasu, Sehgal (1995a) gave a nonexistence proof for two special cases of McFarland difference sets. In the case $d = 1$, Arasu, Davis, Jedwab, Ma and McFarland (1996) slightly improved the exponent bounds that can be obtained by the arguments of Turyn (1965). Finally, Ma and Schmidt (1995a, submitted) found the following exponent bounds which are best possible and almost completely solve the existence problem for abelian McFarland difference sets under the self-conjugacy assumption.

Theorem 2.9 *Assume that there exists a McFarland difference D set in an abelian group G of order $v = q^{d+1}[1 + (q^{d+1} - 1)/(q - 1)]$, where $q = p^f$ and p is 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 $exp(P) \leq 4$.

Note that by the construction of McFarland (1973) condition (a) of Theorem 2.9 is also sufficient. As mentioned above, the construction of Davis and Jedwab (1996) shows that condition (b) is also sufficient for $f = 2$; for $p = 2$ and $f > 2$ there are still a lot of open cases, and it is an interesting question if the methods of Davis, Jedwab (1996) and Ma, Schmidt (1995a) may be combined to solve this problem. It should be mentioned that Theorem 2.9 remains true if the self-conjugacy condition is replaced by the weaker assumption that D has the character divisibility property. This implies that, if the self-conjugacy condition does not hold, constructions of putative difference sets in groups exceeding the exponent bounds of Theorem 2.9 have to be extremely involved. It is a very important question if such constructions are possible.

In the case $f = 1$ of Theorem 2.9 (a) it is possible to determine **all** McFarland difference sets with the given parameters. Ma and Schmidt (1997) proved the following.

Theorem 2.10 *If $f = 1$ in the situation of Theorem 2.9 (a), then D is one of the difference sets constructed by McFarland.*

2.4 The Davis-Jedwab series

After Spence's work [Spence (1977)] who constructed a series of difference sets with parameters

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

the first discovery of a new parameter series of difference sets is due to Davis and Jedwab (1996). The new parameters are

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

where d is a positive integer. Davis and Jedwab (1996) constructed difference sets with these parameters in all abelian groups of the given order v which have a Sylow 2-subgroup P of exponent at most 4, with the single exception of $d = 1$ and $P \cong \mathbf{Z}_4^3$. This construction is a part of a unifying construction including all abelian groups known to contain a McFarland or Spence difference set, see Corollary 5.3 of Davis, Jedwab (1996). The method is the same as explained in Section 2.1: A recursive construction for covering EBSs combined with Theorem 2.2.

Previously, Ma and Schmidt (1995a) had proved that in the case $d = 1$, that is $(v, k, \lambda) = (320, 88, 24)$, an abelian group containing such a difference set must have a Sylow 2-subgroup of exponent at most 4. Schmidt (preprint) generalized this result and obtained the following. We call a difference set with the above parameters a **Davis-Jedwab difference set**.

Theorem 2.11 *Let G be an abelian group of order $2^{2d+4}(2^{2d+2}-1)/3$ with Sylow 2-subgroup P. With the possible exception of $d = 1$ and $P \cong \mathbf{Z}_4^3$, a Davis-Jedwab difference set in G that has the character divisibility property exists if and only if* $\exp(P) \leq 4$.

Roughly speaking, this result shows that Davis and Jedwab did a very good job and constructed everything which is possible without using extremely complicated character sums.

3 Difference sets without self-conjugacy

The best way to understand the importance of the self-conjugacy assumption is in terms of (abelian) characters. Let D be a k-subset of an abelian group G. If D is viewed as an element of the group ring $\mathbf{Z}G$, then D is a (v, k, λ)-difference set in G if and only if

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

for all nonprincipal characters χ of G, where $n = k - \lambda$ is the order of D. This approach to the study of difference sets was introduced in the classical paper of Turyn (1965). For simplicity, let us assume that n is a square, say $n = u^2$. It can be shown [see Turyn (1965)] that if n is self-conjugate modulo $\exp(G)$, then (3.1) implies that $\chi(D) = u\xi$, where ξ is a root of unity (let us call such solutions **trivial solutions**). This means that $\chi(D)$ can be determined explicitly from (3.1) under the self-conjugacy assumption. Together with the fact that $\chi(D)$ is the image of a subset of G this gives rise to necessary conditions for difference sets. This is the reason why difference sets are quite well understood today, if self-conjugacy is assumed.

Much less is known about difference sets without self-conjugacy, since in this case it is much more difficult to determine $\chi(D)$ from (3.1). How complicated matters can become is best demonstrated by McFarland's work [McFarland (1989)] on HDSs in abelian groups of order $4p^2$. He needed 70 pages to show that no such difference set exists if p is a prime $\equiv 1 \bmod 4$ (where self-conjugacy does not hold); the proof of the same result for primes $p \equiv 3 \bmod 4$, $p > 3$, (where self-conjugacy holds) only takes one page [see Mann, McFarland (1973)]!

In this context, it should be mentioned that, from the point of view of the character approach via equation (3.1), Ryser's conjecture (a (v, k, λ)-difference set with $(v, n) > 1$ cannot be cyclic) and Lander's conjecture (if a (v, k, λ)-difference set exists in an abelian group G and p is a prime divisor of (v, n), then the Sylow p-subgroup of G cannot be cyclic) are very dubious. The reason for this is that almost all "evidence" for these conjectures comes from cases where (3.1) has only the trivial solutions. If (3.1) has further solutions, then the situation changes considerably and very little is known about this. We remark that these important problems are closely connected to the question whether there exists a McFarland difference set exceeding the exponent bounds of Theorem 2.9.

A new approach to avoid the self-conjugacy assumption is due to Chan (1993); he showed that in some special cases equation (3.1) has only the trivial solutions, although the self-conjugacy assumption does not hold. This resulted in necessary conditions for the existence of HDSs in groups of the form $\mathbf{Z}_{2pq} \times \mathbf{Z}_{2pq}$ resp. $\mathbf{Z}_{2p} \times \mathbf{Z}_{2p} \times H$, where p, q are distinct prime numbers and H is an abelian q-group. In particular, he showed that an HDS in $\mathbf{Z}_{6p} \times \mathbf{Z}_{6p}$ can only exist if $p = 3$ or $p = 13$. Applications of Chan's method to divisible difference sets can be found in Arasu, Pott (1996).

The most difficult and most interesting problems arise in the cases where equation (3.1) has other solutions than the trivial ones. An example where equation (3.1) has three essentially distinct types of solutions, namely the case of abelian McFarland difference sets with $q = 9$ and $d = 1$ (i.e. $(891, 90, 9)$-difference sets) is studied in the remarkable work of Arasu and Ma (in preparation). Avoiding the explicit determination of these solutions, they prove that such a difference set can only exist if the exponent of the underlying group is 33 (by McFarland's construction [McFarland (1973)], this condition is also sufficient).

Some theorems which are very useful for the study of difference sets without self-conjugacy can be found in Ma's important work [Ma (to appear)] on relative $(n, n, n, 1)$-difference sets.

Another approach to difference sets without self-conjugacy was chosen by Schmidt (in preparation). He uses properties of the decomposition group of the prime ideal divisors of the order of the difference set together with arguments similar to those of McFarland (1989, section 4) to find restrictions on the solutions of (3.1). To give a flavor of these results, we mention the following special case. By ξ_t we denote a primitive complex t-th root of unity.

Theorem 3.1 *Let $d = p^a m$, where p is an odd prime and $m > 0$ is an odd integer relatively prime to p. If $X \in \mathbf{Z}[\xi_d]$ satisfies*

$$X\overline{X} = p,$$

then with suitable j either $\xi_d^j X \in \mathbf{Z}[\xi_m]$ or $X = \pm\xi_d^j Y$, where Y is a generalized Gauss sum (see Ireland, Rosen (1990)).

With the help of results similar to Theorem 3.1 it is often possible to find all solutions of equation (3.1). One of the most interesting applications concerns the following well-known conjecture on Hadamard matrices, see Jungnickel (1992, section 12).

Conjecture 3.2 *There is no circulant Hadamard matrix of order $m > 4$ (or, equivalently, there is no cyclic Hadamard difference set with $N > 1$).*

Here m and N are connected via $m = 4N^2$. Since Turyn's classical work [Turyn (1965)] it has been known that Conjecture 3.2 is true for $m < 12,100$. Since then there have been a lot of incorrect claims on this subject (and also on Conjecture 3.4 below), see Lin, Wallis (1993). We restrict our attention to the few results which have a chance to be correct. Schmidt (in preparation) extends the bound of $12,100$ for which Conjecture 3.2 is known to be true and also proves some general nonexistence theorems on Hadamard difference sets relying on the approach mentioned above and the sub-difference set method due to McFarland (1990).

A notion closely connected to cyclic HDSs is **Barker sequences**. These are finite sequences $a_1, ..., a_v$ of ones and minus ones, such that the so-called aperiodic autocorrelation

$$c_j = \sum_{i=1}^{v-j} a_i a_{i+j}$$

takes only the values 0 and ± 1 for $j = 1, ..., v-1$. The only known examples of Barker sequences have length $v \in \{2, 3, 4, 5, 7, 11, 13\}$. It is conjectured that these are all possible values of v.

Conjecture 3.3 *There is no Barker sequence of length $v > 13$.*

The following facts are well-known, see Jungnickel (1992, Section 12).

Theorem 3.4 *There is no Barker sequence of odd length $v > 13$. If there exists a Barker sequence of even length v, then $v = 4N^2$ for some N and there exists an HDS in the cyclic group of order $4N^2$.*

Hence Conjecture 3.3 is weaker than Conjecture 3.2. There is one important theorem on Barker sequences due to Eliahou, Kervaire, Saffari (1990) which is <u>not</u> known to be true for cyclic HDSs:

Theorem 3.5 *There is no Barker sequence of length $4N^2$ if N has a prime divisor congruent to* 3 mod 4.

Using this theorem together with the results of Turyn (1965), Eliahou, Kervaire (1992) showed that Conjecture 3.3 is true for $v < 1,898,884$. Some details of this paper were discussed in Jedwab, Lloyd (1992), Broughton (1994) and Eliahou, Kervaire (1994).

The results of Schmidt (in preparation) give some further restrictions on the length of Barker sequences which do not follow from Turyn's work or Theorem 3.5.

4 Miscellanea

4.1 Difference Sets with multiplier -1

A well-known conjecture of McFarland states that, up to a single exception, all abelian difference sets with multiplier -1 must be HDSs. This conjecture has been the main research problem in this field for many years. Recently, Cao (private communication) claimed to have a proof of McFarland's conjecture (we have not seen the paper yet). Hence the following might be true.

Theorem 4.1 *Let D be a (v, k, λ)-difference set with multiplier -1 (w.l.o.g. assume $k < v/2$ by complementation). Then either $(v, k, \lambda) = (4000, 775, 150)$ or D is a Hadamard difference set.*

Ma (1991) had shown that the proof of Theorem 4.1 can be reduced to the proof of two number theoretic conjectures on solutions of certain diophantine equations, see Jungnickel (1992, section 13). Le, Xiang (1996) could verify the first of these two conjectures. The key to their proof is the observation that a solution violating Ma's conjecture would lead to a fundamental solution of Pell's equation. Finally, Cao (private communication) claimed to have a proof of both of Ma's conjectures completing the proof of Theorem 4.1.

Concerning Hadamard difference sets with multiplier -1, Xiang (submitted) proved that no such difference sets exist in $\mathbf{Z}_2^2 \times \mathbf{Z}_9^2$ and $\mathbf{Z}_4^2 \times \mathbf{Z}_3^2$. This settled the last two open cases with $N < 10$, see Ma (1990).

The new constructions for difference sets with multiplier -1 were already mentioned in Section 2.2; the constructions of Xia (1992), van Eupen, Tonchev (preprint), Wilson, Xiang (submitted) and Chen (submitted) all provide reversible HDSs. Dillon (1990) constructed reversible HDSs in all groups $\mathbf{Z}_{2^t} \times \mathbf{Z}_{2^t}$. Putting all these examples together with the trivial HDS in $\mathbf{Z}_4$ and Turyn's reversible HDS in $\mathbf{Z}_2^2 \times \mathbf{Z}_3^2$ into the recursive constructions of Menon (1962) and Turyn (1984), one obtains the following theorem. No other abelian groups are known to contain a reversible HDS.

Theorem 4.2 *There exist reversible HDS in G and $G \times \mathbf{Z}_2^2 \times \mathbf{Z}_3^{2a} \times \mathbf{Z}_{p_1}^4 \times \cdots \times \mathbf{Z}_{p_s}^4$ for all groups $G = \mathbf{Z}_4^b \times \mathbf{Z}_{2^{c_1}}^2 \times \cdots \times \mathbf{Z}_{2^{c_r}}^2$, where the p_i are (not necessarily distinct) odd primes with and $a, b, c_1, ..., c_r$ are nonnegative integers.*

4.2 Skew Paley-Hadamard difference sets

By **Paley-Hadamard difference sets** we mean difference sets with parameters $(v, k, \lambda) = (4n-1, 2n-1, n-1)$. These were called just Hadamard difference sets in Jungnickel (1992); we have switched to "Paley-Hadamard" to avoid confusion with the HDSs from Sections 2.1 and 2.2. A Paley-Hadamard difference set in a group G is called a **skew Paley-Hadamard difference set** if G is the disjoint union of D, $D^{(-1)} := \{d^{-1} : d \in D\}$ and the identity element. It is well known (see Jungnickel (1992, section 9)) that a skew Paley-Hadamard difference set in an abelian group of order v can only exist if $v = p^m \equiv 3 \bmod 4$ for some prime p and some positive integer m. The following is a longstanding open conjecture.

Conjecture 4.3 *If there exists an abelian skew Paley-Hadamard difference set in a group G of order $v = p^m \equiv 3 \bmod 4$, then G must be elementary abelian.*

Chen, Xiang, Sehgal (1994) made some progress towards Conjecture 4.3. They proved the following result which, in particular, shows that Conjecture 4.3 is true for $m \leq 5$.

Theorem 4.4 *Let G be an abelian p-group, where p is a prime with $p \equiv 3 \bmod 4$, and write $|G| = p^m$, $exp(G) = p^s$. If G admits a skew Paley-Hadamard difference set and $s \geq 2$, then $s \leq (m+1)/4$.*

4.3 Dihedral difference sets

Leung, Ma, Wong (1992) derived strong necessary conditions for the existence of difference sets in dihedral groups lending support to the following conjecture.

Conjecture 4.5 *No nontrivial difference sets exist in dihedral groups.*

Using a computer search, Leung, Ma and Wong verified Conjecture 4.5 for all parameter triples (v, k, λ) with $k - \lambda \leq 10^6$, except five undecided cases. In this context, we mention the following observation of Schmidt (submitted).

Special cases of this result were previously obtained by Fan, Ma and Siu (1985) for dihedral difference sets and by Shiu (1996) for arbitrary difference sets.

Theorem 4.6 *There is no nontrivial symmetric (v, k, λ)-design with $v = 2p^m$ for any odd prime p and any positive integer m. In particular, there is no nontrivial difference set in any group of order $2p^m$.*

4.4 Multipliers

There have been some attempts to make progress towards Hall's multiplier conjecture, see Qiu (1993, 1994, 1995, 1995a, 1996, submitted (a), submitted (b)); let us first recall this conjecture.

Conjecture 4.7 *If D is a (v, k, λ)-difference set in an abelian group and t is a divisor of $n = k - \lambda$ relatively prime to v, then t is a multiplier of D.*

Maybe the most interesting result in this direction is the following obtained by Muzychuk (submitted). It finishes the case $n = 2p^a$ which was first considered by Turyn (1964) and Mann, Zaremba (1969), but not completely settled.

Theorem 4.8 *Let D be a (v, k, λ)-difference set in an abelian group, where $n = 2p^a$ for some odd prime p and $(p, |G|) = 1$. Then p is a multiplier of D.*

A unified theorem containing most of the numerous variations of Hall's multiplier theorem is due to Arasu and Xiang (1995). There are also some new results concerning the structure of multiplier groups. Xiang (1994) used techniques from algebraic number theory to get restrictions on the numerical multiplier group of difference sets. Xiang and Chen (1995) obtained the following upper bound for the size of the multiplier group of a cyclic difference set.

Theorem 4.9 *The multiplier group M of a cyclic (v, k, λ)-difference set D has cardinality at most k, unless D is the Singer difference set belonging to $PG(2, 4)$ (in which case $|M| = 6$).*

4.5 Planar difference sets

By a planar difference set we mean a difference set with parameters $(v, k, \lambda) = (n^2 + n + 1, n + 1, 1)$. Such a difference set is equivalent to a projective plane with a regular automorphism group (Singer group), see Beth, Jungnickel, Lenz (1986). The structure of the multiplier groups of planar difference sets was studied by Ho in a sequence of papers [Ho (1993, 1993a, 1993b, 1994, 1995, submitted (a))]; to give an impression of his results, we mention the following.

Theorem 4.10 *Let Π be a projective plane of order n with Singer group G (not necessarily abelian) and difference set $D \subset G$, and let M be the multiplier group of D. Then the Sylow 2-subgroup S of M is a cyclic direct factor of M, and hence M is solvable. Moreover, the following hold.*

a) Write $n = m^{2^a}$, where m is not a square. Then $|S| \leq 2^a$; if M is abelian, then actually $|S| = 2^a$ and $|M| \leq (m+1)2^a$.

b) M fixes a line of Π.

c) If M has even order, then each subgroup of G is invariant under the unique involution in M, except possibly if $n = 16$ and G is nonabelian.

d) Let H be an abelian subgroup of M. If H has odd order, then $|H| \leq n + 1$. If $|H| = n + 1$, then $n^2 + n + 1$ is a prime.

e) If M is abelian, then either $|M| \leq n + 1$ or n is a square.

f) If G is abelian, then $|M| \leq n + 1$ except for $n = 4$, where $|M| = 6$.

g) If M is abelian and n is a square, then the Sylow 3-subgroup of M is cyclic.

Recently, Ho (submitted (b)) obtained the following generalization of Ott's celebrated theorem, see Ott (1975).

Theorem 4.11 *A finite projective plane admitting more than one abelian Singer group is Desarguesian.*

Gordon (1994, submitted) provides some computational results on the prime power conjecture which states that the order of an abelian planar difference set must be prime power. He uses the known nonexistence results and a computer to show that the prime power conjecture is true for all orders $n \leq 2,000,000$ and to extend the list of integers that cannot divide the order of an abelian planar difference set; the previous version of this list can be found in Jungnickel (1992, Theorem 8.7).

An application of the Singer difference set of $\Pi = PG(2,q)$ was found by Jungnickel (1991); he used this difference set for the construction of a **anti-polarity** in Π, i.e. a bijection α between the points and lines of Π satisfying $p \in \alpha(q) \Rightarrow q \notin \alpha(p)$.

4.6 The geometry of Singer and GMW difference sets

It is well-known that $-D$ is an oval of the projective plane corresponding to an abelian planar difference set D, see Jungnickel (1992). In the classical case, one can say more.

Proposition 4.12 *Let D be a Singer difference set corresponding to $PG(2,q)$, where q is odd, and let r be any integer. Then $rD := \{rd : d \in D\}$ is a conic provided that one of the following conditions holds for some integers i, j, k:*
(a) $rp^k(q^i + q^j) \equiv 1 \bmod q^2 + q + 1$;
(b) $rp^k \equiv 2 \bmod q^2 + q + 1$.

This result is due to Jackson, Quinn and Wild (1996). Similar questions have also been investigated in higher dimensions. In the context of constructing perfect ternary sequences, it is of interest for which values of r the set rD obtained from a difference set D corresponding to $\Pi = PG(d,q)$ is a quadric in Π. This has been shown to hold whenever there are integers i, j, k satisfying $rp^k(q^i + q^j) \equiv 1 \bmod (q^{d+1} - 1)/(q-1)$; however, no necessary and sufficient conditions on r are known in general, and it is also not known for which values of r the resulting quadric is non-degenerate. We refer the reader to Høholdt, Justesen (1983), Games (1986), Jackson, Wild (1992) and Jackson, Quinn, Wild (1996).

Jackson, Wild (to appear) characterized the designs arising from the Gordon-Mills-Welch difference sets as the $(\frac{q^n-1}{q-1}, \frac{q^{n-1}-1}{q-1}, \frac{q^{n-2}-1}{q-1})$-designs admitting
$GL(m, q^t)$ as an automorphism group for appropriate m, t with $mt = n$.

An interesting connection between hyperovals in $PG(2, 2^d)$ and difference sets with Singer parameters $(v, k, \lambda) = (2^d - 1, 2^{d-1} - 1, 2^{d-2} - 1)$ was discovered by A. Maschietti (submitted). In particular, this yields a method to construct three infinite series of difference sets with Singer parameters some of which are probably non-equivalent to the known ones.

4.7 Tables

The table concerning the existence of abelian difference sets with $n \leq 30$ in Jungnickel (1992) contained three open entries belonging to the parameters $(v, k, \lambda) = (90, 20, 4)$. The table is now complete, since these entries have been answered: Arasu, Sehgal (1995a) and Arasu, Davis, Jedwab, Ma, McFarland (1996) showed that in two of these cases ($\mathbf{Z}_4 \times \mathbf{Z}_8 \times \mathbf{Z}_3$ and $(\mathbf{Z}_2)^2 \times \mathbf{Z}_8 \times \mathbf{Z}_3$) no difference set can exist. The remaining case ($\mathbf{Z}_2 \times (\mathbf{Z}_4)^2 \times \mathbf{Z}_3$) was settled via construction by Arasu, Sehgal (1995).

There are some new tables available. The CRC handbook of combinatorial designs contains a table of abelian difference sets [Jungnickel, Pott (1996)] as well as of nonabelian difference sets [Smith (1996)]; these tables do not only deal with the existence question, but also provide a lot of explicit examples of difference sets.

Further tables of difference sets are Kopilovich (1989) [abelian noncyclic difference sets with $k \leq 100$] and Vera Lopez, Garcia Sanchez (to appear) [abelian difference sets with $100 < k \leq 150$].

Up to our knowledge, the only open cases of abelian (v, k, λ)-difference sets with $k \leq 100$ are the following.

$$\begin{aligned} (640, 72, 8), &\quad \mathbf{Z}_2 \times \mathbf{Z}_4^3 \times \mathbf{Z}_5; \\ (640, 72, 8), &\quad \mathbf{Z}_2^3 \times \mathbf{Z}_4^2 \times \mathbf{Z}_5; \\ (320, 88, 24), &\quad \mathbf{Z}_4^3 \times \mathbf{Z}_5. \end{aligned}$$

This is an update of the table in Jungnickel, Pott (1996). The updates are:

a) Iiams (in preparation) excluded the following cases.

$$\begin{aligned} (288, 42, 6), &\quad \mathbf{Z}_4 \times \mathbf{Z}_8 \times \mathbf{Z}_3^2; \\ (288, 42, 6), &\quad \mathbf{Z}_2^2 \times \mathbf{Z}_8 \times \mathbf{Z}_3^2; \\ (189, 48, 12), &\quad \mathbf{Z}_3^3 \times \mathbf{Z}_7; \\ (176, 50, 14), &\quad \mathbf{Z}_4^2 \times \mathbf{Z}_{11}; \\ (176, 50, 14), &\quad \mathbf{Z}_2^2 \times \mathbf{Z}_4 \times \mathbf{Z}_{11}; \\ (176, 50, 14), &\quad \mathbf{Z}_2^4 \times \mathbf{Z}_{11}. \end{aligned}$$

b) The cases $(160, 54, 18)$, $\mathbf{Z}_2 \times \mathbf{Z}_{16} \times \mathbf{Z}_5$ and $\mathbf{Z}_4 \times \mathbf{Z}_8 \times \mathbf{Z}_5$ were excluded by Ma, Schmidt (1997).

c) Abelian $(320, 88, 24)$-difference sets were constructed by Davis, Jedwab (1996) in all abelian groups of order 320 and exponent not exceeding 20, except in $\mathbf{Z}_4^3 \times \mathbf{Z}_5$.

d) Arasu and Ma (in preparation) showed that no abelian $(891, 90, 9)$-difference sets exist in groups of exponent exceeding 33.

e) The case of a $(783, 69, 6)$-difference set in $\mathbf{Z}_3^3 \times \mathbf{Z}_{29}$ was excluded by Schmidt (to appear).

Acknowledgement
The authors are grateful to J.A. Davis, J. Jedwab, S.L. Ma and Q. Xiang for several useful suggestions concerning this survey.

5 References

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.

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

K.T. Arasu, J.A. Davis, J. Jedwab, S.K. Sehgal: New constructions of Menon difference sets, J. Combin. Theory A 64 (1993), 329-336.

K.T. Arasu, S.L. Ma: Abelian Groups Admitting McFarland Difference Sets of Order 81. In preparation.

K.T. Arasu, A. Pott: Impossibility of a certain cyclotomic equation with applications to difference sets. Designs, Codes and Cryptography 8 (1996), 23-28.

K.T. Arasu, S.K. Sehgal: Some new difference sets. J. Combin. Theory (A) 69 (1995), 170-172.

K.T. Arasu, S.K. Sehgal: Difference sets in abelian groups of p-rank two. Designs, Codes and Cryptography 5 (1995a), 5-12.

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

E.F. Assmus, J.D. Key: Hadamard matrices and their designs: a coding theoretic approach. Trans. Amer. Math. Soc. 330 (1992), 269-293.

E.F. Assmus, J.D. Key: Designs and their codes: Cambridge University Press, Cambridge (1992a).

E.F. Assmus, J.D. Key: Designs and codes: an update. Designs, Codes and Cryptography 9 (1996), 7-27.

T. Beth, D. Jungnickel, H. Lenz: Design Theory. Cambridge University Press, Cambridge (1986).

W.J. Broughton: A note on Table 1 of "Barker sequences and difference sets".

L'Enseignement Math. 50 (1994), 105-107.

Z. Cao: Two number-theoretic conjectures and abelian difference sets with multiplier -1. Private communication.

W.K. Chan: Necessary Conditions for Menon Difference Sets. Designs, Codes and Cryptography 3 (1993), 147-154.

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

Y.Q. Chen: On the Existence of Abelian Hadamard Difference Sets and Generalized Hadamard Difference Sets. Submitted.

Y.Q. Chen, Q. Xiang, S.K. Sehgal: An Exponent Bound on Skew Hadamard Abelian Difference Sets. Designs, Codes and Cryptography, 4 (1994), 313-317.

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

J.A. Davis (1992): A generalization of Kraemer's result on difference sets. J. Combin. Theory (A) 59, 187-192.

J.A. Davis, J.E. Iiams: Hadamard difference sets in nonabelian 2-groups with high exponent. Submitted.

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

J.A. Davis, J. Jedwab: A summary of Hadamard difference sets. In: Groups, Difference Sets, and the Monster. Eds. K.T. Arasu, J.F. Dillon, K. Harada, S.K. Sehgal, R.L. Solomon. DeGruyter Verlag, Berlin/New York (1996a), 145-156.

J.A. Davis, J. Jedwab: Nested Hadamard Difference Sets. Submitted.

J.A. Davis, J. Jedwab: Recent developments in difference sets. In preparation.

J.A. Davis, K.W. Smith: A construction of difference sets in high exponent 2-groups using representation theory. J. Alg. Comb. 3 (1994), 137-151.

J.F. Dillon: A survey of difference sets in 2-groups. Presented at the Marshall Hall Memorial Conference, Vermont (1990).

J.F. Dillon: Difference sets in 2-groups. In: Finite Geometries and Combinatorial Designs. Contemp. Math. 111 (1990a), 65-72.

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

S. Eliahou, M. Kervaire: Corrigendum to "Barker sequences and difference sets". L'Enseignement Math. 40 (1994), 109-111.

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

M. van Eupen, V.D. Tonchev: Linear Codes and the Existence of a Reversible Hadamard Difference Set in $\mathbf{Z_2} \times \mathbf{Z_2} \times \mathbf{Z_5^4}$. Preprint.

C.T. Fan, S.L. Ma, M.K. Siu: Difference sets in dihedral groups and interlocking difference sets. Ars Comb. 20 A (1985), 99-107.

R.A. Games: The geometry of quadrics and correlation of sequences. IEEE Trans. Inform. Th. 32 (1986), 423-426.

D. Ghinelli: Regular groups on generalized quadrangles and nonabelian difference sets with multiplier -1. Geo. Ded. 41 (1992), 165-174.

D.M. Gordon: The Prime Power Conjecture is True for $n < 2,000,000$. Electron. J. Comb. 1, R6 (1994).

D.M. Gordon: Some Restrictions on Orders of Abelian Planar Difference Sets. Submitted.

C.Y. Ho: Planar Singer groups with even order multiplier groups. In: Finite geometry and combinatorics. Eds. A. Beutelspacher, F. Buekenhout et al. Cambridge University Press, Cambridge (1993), 187-198.

C.Y. Ho: Projective planes with a regular collineation group and a question about powers of a prime. J. Algebra 154 (1993a), 141-151.

C.Y. Ho: Singer groups, an approach from a group of multipliers of even order. Proc. Amer. Math. Soc. 119 (1993b), 925-930.

C.Y. Ho: Subplanes of a tactical decomposition and Singer groups of a projective plane. Geom. Ded. 53 (1994), 307-326.

C.Y. Ho: Some basic properties of planar Singer groups. Geom. Ded. 55 (1995), 59-70.

C.Y. Ho: Arc subgroups of planar Singer groups. Submitted (a).

C.Y. Ho: Finite Projective Planes with Abelian Transitive Collineation Groups. Submitted (b).

T. Høholdt, J. Justesen: Ternary sequences with perfect periodic autocorrelation. IEEE Trans. Inform. Th. 29 (1983), 597-600.

J.E. Iiams: On difference sets in groups of order $4p^2$. J. Comb. Th. (A) 72 (1995), 256-276.

J.E. Iiams: Lander's Tables are Complete. In Preparation.

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

W.-A. Jackson, K.A.S. Quinn, P.R. Wild: Quadrics and difference sets. Ars Comb. 42 (1996), 97-106.

W.-A. Jackson, P.R. Wild: Relations between two perfect ternary sequence constructions. Designs, Codes and Cryptography 2 (1992), 325-332.

W.-A. Jackson, P.R. Wild: On GMW designs and cyclic Hadamard designs. Designs, Codes and Cryptography 10 (1997), 185-192.

J. Jedwab (1992): Generalized perfect arrays and Menon difference sets. Designs,

Codes and Cryptography 2, 19-68.

J. Jedwab: Non-existence of certain perfect binary arrays. Electron. Letters 29 (1993), 99-101.

J. Jedwab, S. Lloyd: A note on the non-existence of Barker sequences. Designs, Codes and Cryptography 2 (1992), 93-97.

D. Jungnickel: An anti-polarity in $PG(2, q)$. Bull. ICA 3 (1991), 78.

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

D. Jungnickel, A. Pott: Difference sets: abelian. In: The CRC handbook of combinatorial designs. Eds. C.J. Colbourn, J. Dinitz. CRC Press, Boca Raton (1996), 297-307.

L.E. Kopilovich: Difference Sets in non-cyclic groups. Kibernetika 2 (1989), 20-23.

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

M. Le, Q. Xiang: A result on Ma's conjecture. J. Comb. Theory (A) 73 (1996), 181-184.

K.H. Leung, S.L Ma, Y.L. Wong (1992): Difference Sets in Dihedral Groups. Designs, Codes and Cryptography 1, 333-338.

R.A. Liebler: The Inversion Formula. J. Comb. Math. Comb. Computing 13 (1993), 143-160.

R.A. Liebler, K.W. Smith: On difference sets in certain 2-groups. In: Coding Theory, Design Theory, Group Theory. Eds. D.Jungnickel, S.A. Vanstone. Wiley, New York (1993), 195-212.

C. Lin, W.D. Wallis: On the circulant Hadamard conjecture. In: Coding theory, design theory, group theory. Eds. D. Jungnickel, S.A. Vanstone. Wiley, New York (1993), 213-217.

S.L. Ma: Polynomial addition sets and symmetric difference sets. In: IMA Vol. Math. Appl. 21: Coding Theory and Design Theory, Ed. D. Ray-Chaudhuri. Springer-Verlag, New York (1990), 273-279.

S.L. Ma: McFarland's conjecture on abelian difference sets with multiplier minus one. Designs, Codes and Cryptography 1 (1991), 312-332.

S.L. Ma: A survey of partial difference sets. Designs, Codes and Cryptography 4 (1994), 221-261.

S.L. Ma: Planar Functions, Relative Difference Sets and Character Theory. J. Algebra, to appear.

S.L. Ma, B. Schmidt: On (p^a, p, p^a, p^{a-1})-Relative Difference Sets. Designs, Codes and Cryptography 6 (1995), 57-71.

S.L. Ma, B. Schmidt: The Structure of Abelian Groups Containing McFarland

Difference Sets. J. Comb. Theory (A) 70 (1995a), 313-322.

S.L. Ma, B. Schmidt: A sharp exponent bound for McFarland difference sets with $p = 2$. Submitted.

S.L. Ma, B. Schmidt: Difference Sets Corresponding to a Class of Symmetric Designs. Designs, Codes and Cryptography 10, (1997), 223-236.

H.B. Mann, R.L. McFarland: On Hadamard difference sets. In: J.N. Srivastava et. al. (eds.), A Survey of Combinatorial Theory. North-Holland, Amsterdam (1973), 333-334.

H.B. Mann, S.K. Zaremba: On multipliers of difference sets. Illinois J. Math. 13 (1969), 378-382.

A. Maschietti: Difference sets and hyperovals. Submitted.

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

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

R.L. McFarland: Sub-difference sets of Hadamard difference sets. J. Comb. Theory (A) 54 (1990), 112-122.

D.B. Meisner: Families of Menon difference sets. Ann. Discrete Math. 52 (1992), 365-380.

D.B. Meisner: A difference set construction of Turyn adapted to semi-direct products. In: Groups Difference Sets and the Monster. Eds. K.T. Arasu, J.F. Dillon, K. Harada, S.K. Sehgal, R.L. Solomon. DeGruyter Verlag, Berlin/New York (1996), 169-174.

D.B. Meisner: New Classes of Groups Containing Menon Difference Sets. Designs, Codes and Cryptography 8 (1996a), 319-325.

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

M. Muzychuk: Difference Sets with $n = 2p^m$. Submitted.

U. Ott: Endliche zyklische Ebenen. Math. Z. 144 (1975), 195-215.

A. Pott: On abelian difference set codes. Designs, Codes and Cryptography 2 (1992), 263-271.

A. Pott: Finite geometry and character theory. Springer, New York (1995).

A. Pott: A survey on relative difference sets. In: Groups, Difference Sets, and the Monster. Eds. K.T. Arasu, J.F. Dillon, K. Harada, S.K. Sehgal, R.L. Solomon. DeGruyter Verlag, Berlin/New York (1996), 195-232.

W. Qiu: Proving the multiplier theorem using representation theory of groups. Northeast. Math. J. 9 (1993), 169-172.

W. Qiu: The multiplier conjecture for elementary abelian groups. J. Comb. Des.

2 (1994), 117-129.
W. Qiu: On the multiplier conjecture. Acta. Math. Sinica, New Series 10 (1994), 49-58.
W. Qiu: A method of studying the multiplier conjecture and some partial solutions to it. Ars. Comb. 39 (1995), 5-23.
W. Qiu: The multiplier conjecture for the case $n = 4n_1$. J. Comb. Des. 3 (1995), 393-397.
W. Qiu: A necessary condition on the existence of abelian difference sets. Discrete Math. 137 (1995a), 383-386.
W. Qiu: Further results on the multiplier conjecture for the case $n = 2n_1$. J. Comb. Math. Comb. Comp. 20 (1996), 27-31.
W. Qiu: A character approach to the multiplier conjecture and a new result on it. Submitted (a)
W. Qiu: Further results on the multiplier conjecture for $2 = 2n_1$ and $n = 3n_1$. Submitted (b).
D.K. Ray-Chaudhuri, Q. Xiang: Constructions of Partial Difference Sets and Relative Difference Sets Using Galois Rings. Designs, Codes and Cryptography 8 (1996), 215-228.
D.K. Ray-Chaudhuri, Q. Xiang: New Necessary Conditions for Abelian Hadamard Difference Sets. J. Stat. Plan. Infl., to appear (a).
B. Schmidt: Nonexistence of a $(783, 69, 6)$-difference set. To appear in Discrete Math.
B. Schmidt: There are no symmetric (v, k, λ)-designs with $v = 2p^m$. Submitted.
B. Schmidt: Decomposition Groups, Class Groups and Difference Sets. In preparation.
B. Schmidt: Nonexistence Results for Chen and Davis-Jedwab difference sets. Preprint.
W.C. Shiu: Difference sets in groups containing subgroups of index 2. Ars Comb. 42 (1996), 199-205.
K.W. Smith: Non-abelian Hadamard difference sets. J. Comb. Theory (A) 70 (1995), 144-156.
K.W. Smith: Difference sets: Nonabelian. In: The CRC handbook of combinatorial designs. Eds. C.J. Colbourn, J. Dinitz. CRC Press, Boca Raton (1996), 308-312.
R.J. Turyn: The multiplier theorem for difference sets. Canad. J. Math. 16 (1964), 386-388.
R.J. Turyn: Character sums and difference sets. Pacific J. Math. 15 (1965), 319-346.

R.J. Turyn: A special class of Williamson matrices and difference sets. J. Comb. Theory (A) 36 (1984), 195-228.

A. Vera Lopez, M.A. Garcia Sanchez: On the existence of abelian difference sets with $100 < k \leq 150$. J. Comb. Math. Com. Comp., to appear.

R. Wilson, Q. Xiang: Constructions of Hadamard Difference Sets. Submitted.

M.Y. Xia: Some infinite classes of special Williamson matrices and difference sets, J. Combin. Theory (A) 61 (1992), 230-242.

Q. Xiang: Some results on -1 multiplier of difference lists. Ann. Discrete Math. 52 (1994), 559-566.

Q. Xiang: Some Results on Multipliers and Numerical Multiplier Groups of Difference Sets. Graphs and Combinatorics 10 (1994), 293-304.

Q. Xiang: On Reversible Abelian Hadamard Difference Sets. Submitted.

Q. Xiang, Y.Q. Chen: On the Size of the Multiplier Groups of Cyclic Difference Sets. J. Comb. Theory (A) 69 (1995), 168-169

Q. Xiang, Y.Q. Chen: On Xia's Construction of Hadamard Difference Sets. Finite Fields Appl. 2 (1996), 86-95.

6 "Old" References

The following are references of papers which had been mentioned in the previous survey Jungnickel (1992), but had not appeared at that time.

K.T. Arasu, V.C. Mavron: Biplanes and Singer groups. In: Coding theory, design theory, group theory. Eds. D. Jungnickel, S.A. Vanstone. Wiley, New York (1993), 111-119.

J.A. Davis: A note on non-abelian $(64, 28, 12)$-difference sets. Ars. Comb. 32 (1991), 311-314.

S. Gao, W. Wei: On non-abelian group difference sets. Discrete Math. 112 (1993), 93-102.

D. Hachenberger: On the existence of translation nets. J. Algebra 152 (1992), 207-229.

D. Hachenberger: On a combinatorial problem in group theory. J. Comb. Th. (A) 64 (1993), 79-101.

J.W.P. Hirschfeld: Projective spaces of square size. Simon Stevin 65 (1991), 319-329.

C.Y. Ho: On bounds for groups of multipliers of planar difference sets. J. Algebra 148 (1992), 325-336.

J. Jedwab, C. Mitchell, F. Piper, P. Wild: Perfect binary arrays and difference sets. Discrete Math. 125 (1994), 241-254.

D. Jungnickel: On Lander's multiplier theorem for difference lists. J. Comb. Inf. System Sc. 17 (1992), 123-129.

K.H. Leung, S.L. Ma: Constructions of partial difference sets and relative difference sets on p-groups. Bull. London Math. Soc. 22 (1990), 533-539.

S. Long: A generalization of the notion of ovals to symmetric designs. In: Coding theory, design theory, group theory. Eds. D. Jungnickel, S.A. Vanstone. Wiley, New York (1993), 219-225.

A. Pott: A generalization of a construction of Lenz. Sankhya (A) 54 (1992), 315-318.

A. Pott: New necessary conditions for abelian difference sets. Combinatorica 12 (1992), 89-93.