HEWLETT PACKARD

A Survey of Hadamard Difference Sets

Jonathan Jedwab, James Davis[1]
Networks and Communications Laboratory
HP Laboratories Bristol
HPL-94-14
February, 1994

difference set, Hadamard

A (v,k,λ) difference set is a k-element subset D of a group G of order v for which the multiset $\{d_1d_2^{-1}: d_1,d_2 \in D,\ d_1 \neq d_2\}$ contains each nonidentity element of G exactly λ times. A Hadamard difference set (HDS) has parameters of the form $(v,k,\lambda) = (4N^2,2N^2-N,N^2-N)$. The Hadamard parameters provide the richest source of known examples of difference sets. The central question is: for each integer N, which groups of order $4N^2$ support a HDS? This question remains open, for abelian and nonabelian groups, despite an extensive literature. We survey the current state of knowledge of the subject.

Internal Accession Date Only
[1] University of Richmond, Richmond, VA 23173

1 Introduction

A (v, k, λ) difference set is a k-element subset D of a group G of order v for which the multiset $\{d_1 d_2^{-1} : d_1, d_2 \in D, d_1 \neq d_2\}$ contains each non-identity element of G exactly λ times. A difference set is called abelian, nonabelian or cyclic according to the properties of the underlying group. Difference sets are important in design theory because they are equivalent to symmetric (v, k, λ) designs with a regular automorphism group [29]. The study of difference sets is also deeply connected with coding theory because the code, over a field F, of the symmetric design corresponding to a (v, k, λ) difference set may be considered as the right ideal generated by D in the group algebra FG [26], [29]. Abelian difference sets arise naturally in the solution of many problems of signal design in digital communications, including synchronization [21], radar [1], coded aperture imaging [20], [47] and optical image alignment [37]. A difference set with parameters of the form $(v, k, \lambda) = (4N^2, 2N^2 - N, N^2 - N)$ is called a Hadamard difference set (HDS) because a group subset D is a HDS if and only if the $(+1, -1)$ incidence matrix of the design corresponding to D is a regular Hadamard matrix [26]. Although some authors have instead used the names Menon difference set or H-set we propose that for historical reasons and for consistency the more popular term Hadamard is preferable and should henceforth be used. (Unfortunately some confusion may remain because difference sets with parameters of the form $(v, k, \lambda) = (4n - 1, 2n - 1, n - 1)$ are also called Hadamard.) The Hadamard parameters provide the richest source of known examples of difference sets. The central question is: for each integer N, which groups of order $4N^2$ support a HDS? This question remains open, for abelian and nonabelian groups, despite an extensive literature. The techniques so far used include algebraic number theory, character theory, representation theory, finite geometry and graph theory as well as elementary methods and computer search. Considerable progress has been made recently, both in terms of constructive and nonexistence results. Indeed some of the most surprising advances currently exist only in preprint form, so one intention of this survey is to clarify the status of the subject and to identify future research directions. Another intention is to show the interplay between the study of HDSs and several diverse branches of discrete mathematics. Earlier surveys of HDSs have been given by Chan and Siu [6], Arasu [2] and Jungnickel [26]. A summary of this survey is scheduled for publication [12].

In this survey we assume, by referring to a HDS, that the underlying

group has order $4N^2$. Unless otherwise stated, a and b denote integers satisfying $a \geq 0$ and $b > 0$. The exponent of a group G is written as $\exp(G)$. For background material on group theory see [18], for example.

2 The abelian case

A classical paper by Turyn [50] used character theory and algebraic number theory to establish an exponent bound on certain Sylow subgroups of an abelian group containing a HDS. Given positive integers m and w we call m *self-conjugate mod* w if for each prime divisor p of m there exists an integer j_p such that $p^{j_p} \equiv -1 \pmod{w_p}$, where w_p is the largest divisor of w coprime to p. A central result of Turyn's paper, as restated by Lander [29], is:

Theorem 2.1 *Suppose there exists a HDS in an abelian group G. Let H be a subgroup of G of order h and index w. Suppose that m is a divisor of N, not coprime to w, and self-conjugate mod* $\exp(G/H)$, *such that for each prime p dividing m and w, the Sylow p-subgroup of G/H is cyclic. Then $m \leq 2^{r-1}h$, where r is the number of distinct prime divisors of* $\gcd(m, w)$.

In particular, a necessary condition for the existence of an abelian HDS with $N = 2^a$ is that the group exponent is at most 2^{a+2}. A succession of constructive results, notably those of Davis [8] and Dillon [17], culminated in Kraemer's proof [28] that this condition is also sufficient:

Theorem 2.2 *There exists a HDS in an abelian group G of order 2^{2a+2} if and only if* $\exp(G) \leq 2^{a+2}$.

Theorem 2.1 can also be used to derive exponent bounds for an abelian HDS when N is not of the form 2^a. For example, when $N = 3^b$, the Sylow 3-subgroup has exponent at most 3^b. When $N = 2^a 3^b$, the Sylow 2-subgroup again has exponent at most 2^{a+2} and the Sylow 3-subgroup has an exponent bound dependent on the Sylow 2-subgroup [23] (it is sometimes mistakenly stated that the exponent bound so derived is always 3^b). Turyn [50] also showed that for an abelian HDS with even N, the Sylow 2-subgroup cannot be cyclic.

A body of evidence had accumulated, involving both constructive and nonexistence results, supporting McFarland's conjecture (reported in [2]) that $N = 2^a 3^b$ $(a, b \geq 0)$ is a necessary condition for a HDS. In particular Turyn [52] used elementary methods to prove:

Theorem 2.3 *There exists a HDS in* $Z_2^2 \times Z_3^{2b}$ *and* $Z_4 \times Z_3^{2b}$.

On the nonexistence side, McFarland [39] combined techniques from finite geometry, algebraic number theory and character theory to establish:

Theorem 2.4 *There does not exist an abelian HDS for* $N > 3$ *prime.*

Turyn [51] also proved:

Theorem 2.5 *There does not exist a cyclic HDS for* N *even or* $1 < N < 55$.

But recently Xia [53] disproved McFarland's conjecture spectacularly by explicit construction:

Theorem 2.6 *There exists a HDS in* $Z_4 \times Z_{p_1}^4 \times \ldots \times Z_{p_t}^4$, *where each* p_j *is a prime satisfying* $p_j \equiv 3 \pmod 4$.

An approach that has proved fruitful is to combine the group theoretic viewpoint with insights gained from the engineering literature, in which abelian difference sets are studied as binary arrays (matrices with elements ± 1) with constant out-of-phase periodic autocorrelation. Jedwab [25] defined a binary supplementary quadruple (BSQ) to be a set of four $s_1 \times \ldots \times s_\tau$ binary arrays possessing special correlation properties, and used an elementary recursive construction method to prove:

Theorem 2.7 *If there exists an* $s_1 \times \ldots \times s_\tau$ *BSQ then there exists a HDS in* $G \times Z_{s_1} \times \ldots \times Z_{s_\tau}$, *where* G *is any abelian 2-group satisfying Turyn's exponent bound (of Theorem 2.2).*

Turyn [52] gave a product construction essentially for combining BSQs:

Theorem 2.8 *If there exists an* $s_1 \times \ldots \times s_\tau$ *BSQ and an* $s_{\tau+1} \times \ldots \times s_{\tau+\tau'}$ *BSQ then there exists an* $s_1 \times \ldots \times s_{\tau+\tau'}$ *BSQ.*

In the array framework, Kraemer's Theorem 2.2 arises from a trivial BSQ and Xia's Theorem 2.6 can be viewed as constructing a BSQ of size $p \times p \times p \times p$, where p is a prime congruent to 3 mod 4. Arasu *et al.* [4] constructed a BSQ of size $3^b \times 3^b$, which in the case $b = 1$ implies Turyn's Theorem 2.3. Combining these results (for the first time) in Theorems 2.7 and 2.8 gives:

Theorem 2.9 *There exists a HDS in* $G \times Z_{3^{b_1}}^2 \times \ldots \times Z_{3^{b_\tau}}^2 \times Z_{p_1}^4 \times \ldots \times Z_{p_t}^4$, *where* G *is any abelian 2-group satisfying Turyn's exponent bound and each* p_j *is a prime congruent to* 3 *mod* 4.

To our knowledge Theorem 2.9 describes all abelian groups which have been shown to contain a HDS.

Turyn's character theoretic technique [50] for proving nonexistence has been extended in several papers. McFarland [41] proved that under certain conditions the existence of a HDS in an abelian group implies the existence of a HDS in a subgroup:

Theorem 2.10 *Suppose there exists a HDS in an abelian group $H \times L$, where $|H|$ is even and* $\gcd(|H|, |L|) = 1$. *If $|L|$ is self-conjugate mod* $\exp(H)$ *then there exists a HDS in H.*

Many authors have obtained additional results under the hypotheses of Theorem 2.10 by restricting L to be a Sylow p-subgroup of order p^{2b}, where p is an odd prime. The exponent bound $\exp(L) \leq p^b$ then follows directly from Theorem 2.1. Arasu *et al.* [3] used the binary array viewpoint to show that in the case $\exp(L) = p^b$, L must have the form $Z_{p^b}^2$:

Theorem 2.11 *Suppose there exists a HDS in an abelian group $H \times K \times Z_{p^b}$, where $|K| = p^b$ and p is an odd prime self-conjugate mod* $\exp(H)$. *Then K is cyclic.*

A corollary in the case $p = 3$ is that there exists a HDS in an abelian group of order $2^{2a+2}3^{2b}$ and exponent either $2 \cdot 3^b$ or $4 \cdot 3^b$ if and only if the Sylow 3-subgroup is $Z_{3^b}^2$. In particular, there exists a HDS in $H \times Z_9^2$ but not in $H \times Z_3^2 \times Z_9$, where $H = Z_2^2$ or Z_4. This demonstrates that for general N, the existence of an abelian HDS cannot be determined solely in terms of an exponent bound on the Sylow subgroups, in marked contrast to Kraemer's Theorem 2.2 for the case $N = 2^a$. Recently Davis and Jedwab [11] strengthened Theorem 2.11 by showing the existence of a HDS in the stated group implies the existence of a HDS in each of a nested sequence of subgroups; this theorem contains earlier results of McFarland [40] and Chan *et al.* [5]:

Theorem 2.12 *Suppose there exists a HDS in an abelian group $H \times Z_{p^b}^2$ of order hp^{2b}, where $p > 3$ is a prime self-conjugate mod* $\exp(H)$. *Then $(p+1) \mid h$ and $h > (p+1)^2$, and there exists a HDS in $H \times Z_{p^c}^2$ for each nonnegative integer $c \leq b$.*

Theorem 2.12 suggests that abelian groups of the form $H \times Z_p^2$ are good candidates for future study. Chan [7] obtained a further nonexistence result for groups of this form without assuming a self-conjugate condition:

Theorem 2.13 *Suppose there exists a HDS in an abelian group* $Z_2^2 \times Z_p^2 \times Q$ *of order* $4p^2q^{2b}$, *where* p *and* q *are distinct odd primes for which* $\mathrm{ord}_p(q)$ *is odd. Then* $p \leq 2q^b(p-1)/\mathrm{ord}_p(q)$.

The result is obtained by showing the implied existence of a HDS in the subgroup $Z_2^2 \times Z_p^2$ and then invoking McFarland's Theorem 2.4.

Nevertheless, despite all these results, the central existence question remains open for abelian groups, even for $N = 2^a3^b$.

3 The nonabelian case

Many of the techniques used to analyse the existence of abelian HDSs can be carried over directly to the nonabelian case. But the surprising results of several recent papers have been reached by developing new techniques, which have shown that existence criteria in nonabelian groups differ markedly from those in abelian groups. Indeed a number of recent results have overturned much of the conventional thinking about HDSs. We will start by outlining nonexistence results and then examine existence results.

Turyn's character theoretic technique [50], leading to an exponent bound for abelian groups containing a HDS, can be adapted to the nonabelian case by considering abelian quotient groups:

Theorem 3.1 *Suppose there exists a HDS in a group* G. *Let* H *be a normal subgroup of* G *of order* h *and index* w *for which* G/H *is abelian. Suppose that* m *is a divisor of* N, *not coprime to* w, *and self-conjugate mod* $\exp(G/H)$, *such that for each prime* p *dividing* m *and* w, *the Sylow* p*-subgroup of* G/H *is cyclic. Then* $m \leq 2^{r-1}h$, *where* r *is the number of distinct prime divisors of* $\gcd(m, w)$. *In particular, if* $N = 2^a$ *then* $|H| \geq 2^a$.

The proof of Theorem 3.1 relies on the presence of an abelian factor group in which to carry out the same combination of character theoretic and number theoretic arguments as for the abelian case.

Dillon [16] and Fan *et al.* [19] independently proved:

Theorem 3.2 *If the dihedral group of order* $4N^2$ *contains a HDS then so does* C_{4N^2}.

Therefore from Theorem 2.5 the group $\langle x, y \mid x^8 = y^2 = 1, yxy = x^{-1} \rangle$ does not contain a HDS, which demonstrates that an exponent bound is not a necessary and sufficient existence condition for a HDS in a general 2-group

(unlike Theorem 2.2 for the abelian case). Leung *et al.* [31] proved under the hypothesis of Theorem 3.2 that N must have several distinct prime divisors:

Theorem 3.3 *Suppose the dihedral group of order $4N^2$ contains a HDS. Then N is odd and $\prod_{p|N\,:\,p \text{ prime}}(1-1/p) \leq (1-1/P^2)/2$, where P is the smallest prime divisor of N. In particular, N has at least four distinct prime divisors.*

Leung and Ma [30] gave the following nonexistence result for a 2-group with a large dihedral quotient:

Theorem 3.4 *Suppose there exists a HDS in a group G of order 2^{2a+2}. If H is a normal subgroup of G for which G/H is dihedral, then $|H| \geq 2^a$.*

For nonabelian 2-groups, Theorems 3.1 and 3.4 provide the only known nonexistence results. These results are sufficient to identify all groups of order 16 [27] and 64 [14], [33] which do not contain a HDS. However the determination of complete nonexistence criteria for larger 2-groups remains an important open question.

Recently, Liebler [32] began a systematic use of representation theory to study the existence of HDSs. This is a natural generalization of the character theoretic technique initiated by Turyn for the abelian case. Iiams [22] used this approach to generalize McFarland's Theorem 2.4 for $N > 3$ prime to some nonabelian cases. The method is to list all groups of order $4p^2$ ($p > 3$ a prime) and to calculate their representations. The representation sums then place restrictions on the possible difference sets and so eliminate many groups from the list:

Theorem 3.5 *Suppose there exists a HDS in a group G of order $4p^2$, where $p > 3$ is prime. Then all Sylow 2-subgroups of G are cyclic. Moreover if G does not have an irreducible complex representation of degree 4 then $G \cong \langle x, y, z \mid x^p = y^p = z^4 = 1, xy = yx, xz = zx, zyz^{-1} = y^{-1} \rangle$ and $p \equiv 1 \pmod 4$.*

The authors are not aware of any further nonexistence results for nonabelian groups.

Turning now to the existence question, the earliest result is due to Kesava Menon [46] who proved by elementary construction that the set of groups containing a HDS is closed under direct products:

Theorem 3.6 *If G_1 and G_2 each contain a HDS then so does $G_1 \times G_2$.*

Much of the early attention was focussed on nonabelian 2-groups. Indeed the first known family of nonabelian HDSs was constructed by McFarland [38] in 2-groups. Dillon [16] extended this result to:

Theorem 3.7 *There exists a HDS in any group of order 2^{2a+2} whose center contains Z_2^{a+1}.*

Dillon's method is one which occurs frequently in the construction of HDSs, namely to use the subgroup structure of the group to construct the difference set. In this example, the building blocks are the $2^{a+1}-1$ subgroups of order 2^a (the hyperplanes). Dillon [15] conjectured that a sufficient condition for a group of order 2^{2a+2} to support a HDS is that it has a normal subgroup Z_2^{a+1}. The conjecture remains undecided although there are partial results due to Davis [9] and Meisner [44]. Davis [10] showed that Kraemer's techniques, which settled the existence question for abelian 2-groups, could be modified to construct HDSs in nonabelian groups of order 2^{2a+2} when the center contains a subgroup of order 2^{a+1} (not necessarily elementary abelian as in Theorem 3.7).

Dillon [14] proposed a research programme to settle the existence question for a HDS in all 267 groups of order 64. Constructions were found for 258 of these groups and nonexistence was proved for 8, leaving just the "modular group" of exponent 32. Contrary to most expectations, Liebler and Smith [33] succeeded in constructing a HDS in this group by introducing a representation theoretic algorithm for the efficient sieving of possible solutions to certain equations in finite group rings:

Theorem 3.8 *There exists a HDS in the group $\langle x, y \mid x^{32} = y^2 = 1, yxy = x^{17} \rangle$.*

In groups of order 64, for the abelian case a HDS exists if and only if the group exponent is at most 16 (by Theorem 2.2), whereas for the nonabelian case there is a group of exponent 16 which does not contain a HDS (by Theorem 3.4) and yet a group of exponent 32 which does (by Theorem 3.8)! Turyn's exponent bound for abelian 2-groups is therefore neither necessary nor sufficient in the nonabelian case. Smith [49] observed that the automorphism group for the design associated with the difference set of Theorem 3.8 is the modular group itself, and that this is a new design.

Subsequently Davis and Smith [13] found a new way to interpret the difference set of Theorem 3.8 and so were able to generalize the construction to an infinite family of HDSs in 2-groups each exceeding the abelian exponent bound:

Theorem 3.9 *There exists a HDS in the group* $\langle x, y \mid x^{2^{a+3}} = y^{2^{a-1}} = 1, yxy^{-1} = x^{2^{a+2}+1} \rangle$ *for every* $a \geq 2$.

It is not known whether 2^{a+3} is an upper bound for the exponent of a group of order 2^{2a+2} containing a HDS. The smallest 2-groups in which the existence question is currently unresolved have order 256.

Nonabelian HDSs have also been found in groups other than 2-groups. Meisner [45] modified Jedwab's recursive construction of Theorem 2.7 for application to the nonabelian case, proving:

Theorem 3.10 *Suppose that a group* G *of order* $4N^2$ *contains a HDS, and a group* H *of order* $8N^2$ *contains a relative difference set* B *with parameters* $(4N^2, 2, 4N^2, 2N^2)$. *Suppose further that there is a central element* x *in* H *of order* 2 *such that* $G \cong H/\langle x \rangle$ *and* $xB = H \setminus B$. *Then any group* K *of order* $16N^2$ *with* H *as a subgroup and* x *as a central element will contain a HDS.*

Thus a larger HDS is constructed from a smaller HDS plus a relative difference set. A similar theorem is used to construct a larger relative difference set from a smaller relative difference set and so establish the recursive construction. This leads to new nonabelian HDSs, for example in all groups of the form $D_3 \times C_{2^{a+1}} \times C_{3 \cdot 2^a}$, where D_3 is the dihedral group of order 6. By further application of this recursive construction, Meisner found many new families of nonabelian HDSs and unified several previous construction methods, including that of Turyn [52] in [42], those of Davis [10] and Jedwab [25] in [43], and those of Davis [9] and Dillon [17] in [44].

Perhaps the most unexpected recent result of all is the discovery by Smith [48], using computer search and representation theory, of a HDS in a nonabelian group of order 100:

Theorem 3.11 *There exists a HDS in the group* $\langle x, y, z \mid x^5 = y^5 = z^4 = [x, y] = 1, zx = x^2 z, zy = y^2 z \rangle$.

This result is especially remarkable because of McFarland's Theorem 2.4 showing that no abelian group of order 100 supports a HDS. This is the first demonstration that a nonabelian (v, k, λ) difference set can exist even when an abelian (v, k, λ) difference set cannot. Smith's theorem is also interesting because it shows that McFarland's conjecture, proved false for abelian groups by Xia's Theorem 2.6, also fails for nonabelian groups. Furthermore the difference set of Theorem 3.11 is reversible (see the following section).

4 Reversibility

Besides the central existence question, an active research area is the determination of those groups G supporting a HDS D which is reversible, meaning that $\{d^{-1} : d \in D\} = D$. A difference set with this structure is alternatively called symmetric because the corresponding incidence matrix (whose rows and columns are indexed by G and whose (g_1, g_2) entry is 1 if $g_1 \in g_2 D$ and 0 otherwise) is symmetric. The property of reversibility is motivated by the correspondence, in the abelian case, to the existence of a numerical multiplier -1 fixing the difference set [29]. Indeed, one of the oldest tools used to construct or rule out abelian difference sets is to infer the existence of numerical multipliers from the parameter set (v, k, λ) alone and so constrain the difference set. This section borrows heavily from the survey of reversible difference sets (not necessarily with Hadamard parameters) given by Ma [34].

Reversibility of HDSs is preserved under Kesava Menon's direct product construction of Theorem 3.6. Several constructions for abelian reversible HDSs are known. A reversible HDS exists in Z_4 trivially, and in $Z_{2^{a+1}}^2$ by an explicit construction of Dillon [17]:

Theorem 4.1 *Let $\tau : Z_{2^{a+1}} \mapsto \{0, 1\}$ map the residue x to $\lfloor x/2^a \rfloor$ and let $\pi : Z_{2^{a+1}} \mapsto Z_{2^{a+1}}$ map the residue $2^r t$ (t odd) to the residue $2^r t'$, where $tt' \equiv 1 \pmod{2^{a+1}}$. Then $\{(x, y) : \tau(\pi(x)y) = 1\}$ is a reversible HDS in $Z_{2^{a+1}}^2$.*

Now if the four incidence matrices corresponding to a $s_1 \times \ldots \times s_r$ BSQ are each symmetric then there exists a reversible HDS in $Z_2^2 \times Z_{s_1} \times \ldots \times Z_{s_r}$, and furthermore Turyn's BSQ product construction of Theorem 2.8 preserves this symmetry property. Since the four incidence matrices corresponding to Turyn's 3×3 BSQ and Xia's $p \times p \times p \times p$ BSQ are each symmetric, we can combine these results to obtain [34]:

Theorem 4.2 *There exists a reversible HDS in G and in $G \times Z_2^2 \times Z_3^{2b} \times Z_{p_1}^4 \times \ldots \times Z_{p_t}^4$, where $G = Z_4^c \times Z_{2^{a_1+1}}^2 \times \ldots \times Z_{2^{a_r+1}}^2$ and each p_j is a prime congruent to 3 mod 4.*

To our knowledge Theorem 4.2 describes all abelian groups which have been shown to support a reversible HDS. In contrast there is only one known example, due to McFarland [38], of a non-Hadamard parameter set (v, k, λ) for which there exists an abelian reversible difference set.

On the nonexistence side, McFarland [41] proved:

Theorem 4.3 *Suppose there exists a reversible HDS in an abelian group. Then the square-free part of N divides 6.*

McFarland [41] also showed that certain subgroups of an abelian group containing a reversible HDS must also contain a reversible HDS:

Theorem 4.4 *Suppose there exists a reversible HDS in an abelian group $H \times L$, where $|H|$ is even and $\gcd(|H|, |L|) = 1$. Then there exists a reversible HDS in H.*

Ma [36] constrained the structure of certain Sylow subgroups of an abelian group containing a reversible HDS, using Cayley polynomial digraphs:

Theorem 4.5 *Suppose there exists a reversible HDS in an abelian group G whose Sylow p-subgroup has exponent p^b, where p is prime and $p^b \neq 4$. Then G contains a subgroup $Z_{p^b} \times Z_{p^b}$.*

To our knowledge only one nonabelian group has been shown to contain a reversible HDS, as given by Smith's Theorem 3.11. This provides another example of a theorem derived for abelian groups, namely McFarland's Theorem 4.3, failing in the nonabelian case. On the other hand there are known to be infinite families of nonabelian reversible difference sets with non-Hadamard parameters [35].

5 Open Problems

The authors hope this survey explains the context for some of the new directions being pursued by researchers in HDSs. We now give a personal selection of ten open problems which we hope may serve as a starting point for further exciting discoveries.

1. Which abelian groups of order $2^{2a+2}3^{2b}$ contain a HDS? In particular does $Z_2^2 \times Z_9^3$ or $Z_4 \times Z_9^3$ contain a HDS?

2. Is there an abelian group of the form $H \times Z_p^2$ containing a HDS, where $p > 3$ is a prime not dividing $|H|$?

3. Is there an explicit construction for a HDS in all abelian 2-groups satisfying Turyn's exponent bound, as given by Dillon's Theorem 4.1 in the rank 2 case?

4. Is there a $p \times p \times p \times p$ BSQ for some prime p congruent to 1 mod 4? Can Xia's construction of Theorem 2.6 be modified to settle this, or other nonabelian or non-elementary abelian cases?

5. Which groups of order 256 support a HDS?

6. Can the Turyn exponent bound for abelian 2-groups be exceeded in the nonabelian case to the extent that a group of order 2^{2a+2} and exponent 2^{a+4} contains a HDS (see Theorem 3.9)? A good candidate group to study is $\langle x, y \mid x^{256} = y^4 = 1, yxy^{-1} = x^{65} \rangle$.

7. Are there any further nonexistence results for nonabelian 2-groups, apart from those relying on the presence of a large cyclic or dihedral factor group (Theorems 3.1 and 3.4)?

8. Is Dillon's conjecture on the existence of HDSs in certain 2-groups true?

9. Is there a nonabelian group of order $4p^2$ containing a HDS, where $p > 5$ is prime (see Iiams's Theorem 3.5 and Smith's Theorem 3.11)?

10. Which abelian 2-groups support reversible HDSs?

We conclude by listing the smallest open cases in several categories, beginning with the smallest order abelian groups in which the existence of a HDS is currently undecided. For $N < 20$, there are eight such groups [3], [4], [24, Prop. 3.5.1]:

$$Z_2^2 \times Z_4 \times Z_5^2, \quad Z_2 \times Z_8 \times Z_5^2, \quad Z_4^2 \times Z_5^2, \quad Z_2^2 \times Z_{16} \times Z_9,$$
$$Z_4 \times Z_{16} \times Z_9, \quad Z_8^2 \times Z_9, \quad Z_4 \times Z_3^2 \times Z_5^2, \quad Z_2 \times Z_8 \times Z_3^2 \times Z_9.$$

It is also interesting, from the binary array viewpoint, to consider the values (s, t) with $s \leq t$ for which the existence of a HDS in $Z_s \times Z_t$ is currently undecided. For $t \leq 100$ there are nineteen such values [4], [6]; the previously unresolved values $(56, 56)$ and $(44, 99)$ are removed by Theorem 2.12 (since $7^1 \equiv -1 \pmod 8$ and $11^3 \equiv -1 \pmod{36}$):

$$(10,40), \ (20,20), \ (8,72), \ (16,36), \ (15,60), \ (16,100), \ (20,80),$$
$$(40,40), \ (22,88), \ (32,72), \ (25,100), \ (52,52), \ (40,90), \ (60,60),$$
$$(68,68), \ (78,78), \ (80,80), \ (88,88), \ (100,100).$$

There are two abelian groups in which the existence of a reversible HDS with $N < 10$ is undecided [36], namely $Z_4^2 \times Z_3^2$ and $Z_2^2 \times Z_9^2$. There are four values of $N \leq 100$ for which the existence of a reversible HDS in one or more abelian groups of order $4N^2$ is undecided [41], [53], namely 25, 50, 75, and 100.

References

[1] S. Alquaddoomi and R.A. Scholtz, "On the nonexistence of Barker arrays and related matters," *IEEE Trans. Inform. Theory* vol. 35, pp. 1048–1057, 1989.

[2] K.T. Arasu, "Recent results on difference sets," in D. Ray-Chaudhuri, editor, *The IMA Volumes in Mathematics and its Applications, Vol. 21: Coding Theory and Design Theory*, Springer-Verlag, New York, 1990, pp. 1–23.

[3] K.T. Arasu, J.A. Davis, and J. Jedwab, "A nonexistence result for abelian Menon difference sets using perfect binary arrays," *Combinatorica.* To appear.

[4] K.T. Arasu, J.A. Davis, J. Jedwab, and S.K. Sehgal, "New constructions of Menon difference sets," *J. Combin. Theory (A)* vol. 64, pp. 329–336, 1993.

[5] W.-K. Chan, S.-L. Ma, and M.-K. Siu, "Non-existence of certain perfect arrays," *Discrete Math.* To appear.

[6] W.-K. Chan and M.-K. Siu, "Summary of perfect $s \times t$ arrays, $1 \leq s \leq t \leq 100$," *Electron. Lett.* vol. 27, pp. 709–710, 1991 (Correction *Electron. Lett.* vol. 27, p. 1112, 1991).

[7] W.K. Chan, "Necessary conditions for Menon difference sets," *Designs, Codes and Cryptography* vol. 3, pp. 147–154, 1993.

[8] J.A. Davis, "Difference sets in abelian 2-groups," *J. Combin. Theory (A)* vol. 57, pp. 262–286, 1991.

[9] J.A. Davis, "A result on Dillon's conjecture in difference sets," *J. Combin. Theory (A)* vol. 57, pp. 238–242, 1991.

[10] J.A. Davis, "A generalization of Kraemer's result on difference sets," *J. Combin. Theory (A)* vol. 59, pp. 187–192, 1992.

[11] J.A. Davis and J. Jedwab, "Nested Hadamard difference sets." In preparation.

[12] J.A. Davis and J. Jedwab, "A summary of Menon difference sets," *Congressus Numerantium.* Proceedings of 24rd Southeastern International Conference on Combinatorics, Graph Theory and Computing. To appear.

[13] J.A. Davis and K.W. Smith, "A construction of difference sets in high exponent 2-groups using representation theory," *J. Algebraic Combin.* vol. 3, no. 2, 1994.

[14] J.F. Dillon, "A survey of difference sets in 2-groups." Presented at Marshall Hall Memorial Conference, Vermont, 1990.

[15] J.F. Dillon, *Elementary Hadamard difference sets*, PhD thesis, University of Maryland, 1974.

[16] J.F. Dillon, "Variations on a scheme of McFarland for noncyclic difference sets," *J. Combin. Theory (A)* vol. 40, pp. 9–21, 1985.

[17] J.F. Dillon, "Difference sets in 2-groups," *Contemporary Math.* vol. 111, pp. 65–72, 1990.

[18] D.S. Dummit and R.M. Foote, *Abstract Algebra*, Prentice-Hall, New Jersey, 1991.

[19] C.T. Fan, M.K. Siu, and S.L. Ma, "Difference sets in dihedral groups and interlocking difference sets," *Ars Combinatoria* vol. 20-A, pp. 99–107, 1985.

[20] E.E. Fenimore and T.M. Cannon, "Coded aperture imaging with uniformly redundant arrays," *Applied Optics* vol. 17, pp. 337–347, 1978.

[21] J.E. Hershey and R. Yarlagadda, "Two-dimensional synchronisation," *Electron. Lett.* vol. 19, pp. 801–803, 1983.

[22] J.E. Iiams, "On difference sets in groups of order $4p^2$, part I." Preprint, Colorado State University.

[23] J. Jedwab, "Nonexistence of perfect binary arrays," *Electron. Lett.* vol. 27, pp. 1252–1254, 1991.

[24] J. Jedwab, *Perfect arrays, Barker arrays and difference sets*, PhD thesis, University of London, 1991.

[25] J. Jedwab, "Generalized perfect arrays and Menon difference sets," *Designs, Codes and Cryptography* vol. 2, pp. 19–68, 1992.

[26] D. Jungnickel, "Difference sets," in J.H. Dinitz and D.R. Stinson, editors, *Contemporary Design Theory: a collection of surveys*, Wiley, New York, 1992, pp. 241–324.

[27] R.E. Kibler, "A summary of noncyclic difference sets, $k < 20$," *J. Comb. Theory* vol. A25, pp. 62–67, 1978.

[28] R.G. Kraemer, "Proof of a conjecture on Hadamard 2-groups," *J. Combin. Theory (A)* vol. 63, pp. 1–10, 1993.

[29] E.S. Lander, *Symmetric Designs: an Algebraic Approach*, London Mathematical Society Lecture Notes Series 74. Cambridge University Press, Cambridge, 1983.

[30] K.H. Leung and S.L. Ma, "Partial difference triples." Preprint, National University of Singapore.

[31] K.H. Leung, S.L. Ma, and Y.L. Wong, "Difference sets in dihedral groups," *Designs, Codes and Cryptography* vol. 1, pp. 333–338, 1992.

[32] R.A. Liebler, "The inversion formula," *J. Combin. Math. and Combin. Computing* vol. 13, pp. 143–160, 1993.

[33] R.A. Liebler and K.W. Smith, "On difference sets in certain 2-groups," in D. Jungnickel and S.A. Vanstone, editors, *Coding Theory, Design Theory, Group Theory*, Wiley, New York, 1993, pp. 195–212.

[34] S.L. Ma, "A survey of partial difference sets," *Designs, Codes and Cryptography.* To appear.

[35] S.L. Ma, "A family of difference sets having -1 as an invariant," *European J. Combinatorics* vol. 10, pp. 273–274, 1989.

[36] S.L. Ma, "Polynomial addition sets and symmetric difference sets," in D. Ray-Chaudhuri, editor, *The IMA Volumes in Mathematics and its Applications, Vol. 21: Coding Theory and Design Theory*, Springer-Verlag, New York, 1990, pp. 273–279.

[37] S.J. Martin, M.A. Butler, and C.E. Land, "Ferroelectric optical image comparator using PLZT thin films," *Electron. Lett.* vol. 24, pp. 1486–1487, 1988.

[38] R.L. McFarland, "A family of difference sets in non-cyclic groups," *J. Combin. Theory (A)* vol. 15, pp. 1–10, 1973.

[39] R.L. McFarland, "Difference sets in abelian groups of order $4p^2$," *Mitt. Math. Sem. Giessen* vol. 192, pp. 1–70, 1989.

[40] R.L. McFarland, "Necessary conditions for Hadamard difference sets," in D. Ray-Chaudhuri, editor, *The IMA Volumes in Mathematics and its Applications, Vol. 21: Coding Theory and Design Theory*, Springer-Verlag, New York, 1990, pp. 257–272.

[41] R.L. McFarland, "Sub-difference sets of Hadamard difference sets," *J. Combin. Theory (A)* vol. 54, pp. 112–122, 1990.

[42] D.B. Meisner, "A difference set construction of Turyn adapted to semi-direct products." Preprint.

[43] D.B. Meisner, "New classes of groups containing Menon difference sets." Preprint.

[44] D.B. Meisner, *Menon designs and related difference sets*, PhD thesis, University of London, 1991.

[45] D.B. Meisner, "Families of Menon difference sets," *Annals of Discrete Math.* vol. 52, pp. 365–380, 1992.

[46] P. Kesava Menon, "On difference sets whose parameters satisfy a certain relation," *Proc. Amer. Math. Soc.* vol. 13, pp. 739–745, 1962.

[47] G.K. Skinner, "X-ray imaging with coded masks," *Scientific American* vol. 259, pp. 66–71, August 1988.

[48] K.W. Smith, "Non-abelian Hadamard difference sets." Preprint, Central Michigan University.

[49] K.W. Smith, Private communication, 1992.

[50] R.J. Turyn, "Character sums and difference sets," *Pacific J. Math.* vol. 15, pp. 319–346, 1965.

[51] R.J. Turyn, "Sequences with small correlation," in H.B. Mann, editor, *Error Correcting Codes*, Wiley, New York, 1968, pp. 195–228.

[52] R.J. Turyn, "A special class of Williamson matrices and difference sets," *J. Combin. Theory (A)* vol. 36, pp. 111–115, 1984.

[53] M.-y. Xia, "Some infinite classes of special Williamson matrices and difference sets," *J. Combin. Theory (A)* vol. 61, pp. 230–242, 1992.