1993

A Summary of Menon Difference Sets

James A. Davis
University of Richmond, jdavis@richmond.edu

Jonathan Jedwab

Recommended Citation
Davis, James A., and Jonathan Jedwab. "A Summary of Menon Difference Sets." *Congressus Numerantium* 93 (1993): 203-07.

A summary of Menon difference sets

James A. Davis, University of Richmond, VA 23173, U.S.A
Jonathan Jedwab, Hewlett-Packard Laboratories, Bristol BS12 6QZ, U.K.

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 nonidentity element of G exactly λ times. A difference set is called abelian, nonabelian or cyclic if the underlying group is. Difference sets are important in design theory because they are equivalent to symmetric (v,k,λ) designs with a regular automorphism group. Abelian difference sets arise naturally in the solution of many problems of signal design in digital communications, including synchronization, radar, coded aperture imaging and optical image alignment. A Menon difference set (MDS) has parameters of the form $(v,k,\lambda) = (4N^2, 2N^2 - N, N^2 - N)$; alternative names used by some authors are Hadamard difference set or H-set. The Menon parameters provide the richest source of known examples of difference sets. The central research question is: for each integer N, which groups of order $4N^2$ support a MDS? This question remains open, for abelian and nonabelian groups, despite a large literature spanning thirty years. 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 MDSs and several diverse branches of discrete mathematics. It is intended that a more detailed version of this survey will appear in a future publication.

The abelian case

A classical paper by Turyn [22] used character theory and algebraic number theory to establish an exponent bound on certain Sylow subgroups of an abelian group containing a MDS. In particular, a necessary condition for the existence of an abelian MDS with $N = 2^a$ is that the group exponent is at most 2^{a+2}. A succession of constructive results culminated in Kraemer's proof [11] that this condition is also sufficient.

A body of evidence had accumulated, involving both constructive and nonexistence results, supporting McFarland's conjecture that $N = 2^a 3^b$ is a necessary condition for a MDS. In particular Turyn [24] constructed a MDS in $Z_2^2 \times Z_3^{2b}$ and $Z_4 \times Z_3^{2b}$ by elementary methods, whereas McFarland [16] proved the nonexistence of an abelian MDS for $N > 3$ prime by combining techniques from finite geometry, algebraic number theory and character theory. Turyn [23] also proved the nonexistence of a cyclic MDS for $1 < N < 55$. But recently Xia [25] disproved the conjecture spectacularly

CONGRESSUS NUMERANTIUM 93(1993), pp.203–207

by explicitly constructing a MDS in $Z_4 \times Z_{p_1}^4 \times \ldots \times Z_{p_1}^4$, 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 equivalently studied as binary arrays (matrices with elements ± 1) with constant out-of-phase periodic autocorrelation. A binary supplementary quadruple (BSQ) is a set of four $s_1 \times \ldots \times s_r$ binary arrays possessing special correlation properties, from which Jedwab [10] recursively constructed a MDS in $G \times Z_{s_1} \times \ldots \times Z_{s_r}$ by elementary methods, where G is any abelian 2-group satisfying Turyn's exponent bound. Turyn [24] gave a product construction essentially for combining BSQs of size $s_1 \times \ldots \times s_r$ and $s_{r+1} \times \ldots \times s_{r+r'}$ to produce a BSQ of size $s_1 \times \ldots \times s_{r+r'}$.

In the array framework, Kraemer's result [11] arises from a trivial BSQ and Xia's result [25] 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.* [2] constructed a BSQ of size $3^b \times 3^b$, generalizing Turyn's result [24] for $b = 1$. Combining these results (for the first time), a MDS exists in $G \times Z_{3^{b_1}}^2 \times \ldots \times Z_{3^{b_r}}^2 \times Z_{p_1}^4 \times \ldots \times Z_{p_t}^4$, 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 no other abelian groups have been shown to contain a MDS.

Turyn's character theoretic technique [22] for proving nonexistence has been extended in several papers. McFarland [18] proved that if an abelian group contains a MDS, then certain subgroups must also contain a MDS. McFarland [17] gave restrictions on abelian 2-groups H for which there exists a MDS in $H \times Z_p \times Z_p$, where p is an odd prime. Chan and Siu [3] generalized to the abelian group $H \times P$ whose Sylow p-subgroup P has rank 2, where H is not necessarily a 2-group. Arasu *et al.* [1] considered P with unrestricted rank, proving in particular that a MDS exists 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 $Z_{3^b} \times Z_{3^b}$. Nevertheless the central existence question remains open for abelian groups, even for $N = 2^a 3^b$. The above result of Arasu *et al.* demonstrates that for general N, existence cannot be determined solely in terms of an exponent bound on the Sylow subgroups, in marked contrast to Kraemer's result [11] for the case $N = 2^a$.

Besides the central existence question, an active research area is the determination of those groups supporting a MDS D which is reversible, meaning that $\{d^{-1} : d \in D\} = D$. An abelian difference set with this structure is alternatively called symmetric (because the corresponding incidence matrix is symmetric), or "fixed by the multiplier -1". Using a construction of Kesava Menon [20], the set of groups supporting a reversible MDS is closed under direct products. A reversible MDS exists in Z_4 trivially, and in $Z_{2^a+1}^2$ by an explicit construction of Dillon [7]. 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, and because this property is preserved under Turyn's product construction [24] for BSQs, there also exists a reversible MDS in $Z_2^2 \times Z_3^{2b} \times Z_{p_1}^4 \times \ldots \times Z_{p_t}^4$, where each p_j is a prime congruent to 3 mod 4. In contrast there is only one known example, due to McFarland [15], of a parameter set (v, k, λ) for which there exists an abelian reversible difference set that is not a MDS. On the nonexistence side, McFarland [18] proved that if an abelian group contains a reversible MDS then the square-free part of N divides 6, and showed that certain subgroups must also contain a reversible MDS. Ma [14] gave an exponent bound on certain Sylow subgroups of such a group by regarding the problem in terms of Cayley polynomial digraphs.

The nonabelian case

Turyn's character theoretic technique [22], leading to an exponent bound for abelian groups containing a MDS, can be adapted to the nonabelian case by considering abelian quotient groups. Dillon [6] and Fan *et al.* [9] proved that if the cyclic group of order $4N^2$ does not contain a MDS then neither does the dihedral group of order $4N^2$, and Leung and Ma [12] showed further that a 2-group with a large dihedral quotient does not contain a MDS. More recently, Liebler and Iiams used representation theoretic techniques to generalize McFarland's nonexistence result [16] for N prime to some nonabelian cases.

A great deal of attention has been focussed on nonabelian 2-groups. Indeed the first known family of nonabelian MDSs was constructed by McFarland [15] in 2-groups. Dillon [6] extended this result, showing that any group of order 2^{2a+2} whose center contains Z_2^{a+1} supports a MDS. Dillon conjectured that a sufficient condition for a group of order 2^{2a+2} to support a MDS is that it has a normal subgroup Z_2^{a+1}; despite partial results the conjecture remains undecided. Davis [4] showed that Kraemer's techniques [11], which settled the existence question for abelian 2-groups, could be modified to construct MDSs in nonabelian 2-groups. Furthermore, by Kesava Menon's elementary construction [20], the set of groups containing a MDS is closed under direct products.

Dillon [8] proposed a research effort to settle the existence question for a MDS 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 [13] succeeded in constructing a MDS in this group, demonstrating that Turyn's exponent bound for abelian 2-groups can be exceeded in the nonabelian case. Their method introduced a representation theoretic algorithm for the efficient sieving of possible solutions to certain equations in finite group rings. Subsequently Davis and Smith [5] extended this to show that for every a there exists a group of order 2^{2a+2} and exponent 2^{a+3} containing a MDS.

Nonabelian MDSs have also been found in groups other than 2-groups. Meisner [19] modified Jedwab's recursive method [10] to show that for every a there exists a group of order $2^{2a+2}3^2$, containing the dihedral group of order 6 as a direct factor, which supports a MDS. Using computer search and representation theory, Smith [21] recently discovered a MDS in a nonabelian group of order 100. This result is especially remarkable because of McFarland's proof [16] that no abelian group of order 100 supports a MDS. 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 example is also interesting because the difference set is reversible, and because it shows that McFarland's conjecture fails for nonabelian as well as abelian groups.

References

[1] K.T. Arasu, J.A. Davis, and J. Jedwab, A nonexistence result for abelian Menon difference sets using perfect binary arrays. Submitted.

[2] K.T. Arasu, J.A. Davis, J. Jedwab, and S.K. Sehgal, New constructions of Menon difference sets, *J. Combin. Theory (A)*. To appear.

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

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

[5] J.A. Davis and K.W. Smith, A construction of difference sets in high exponent 2-groups using representation theory. In preparation.

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

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

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

[9] 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.

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

[11] R.G. Kraemer, Proof of a conjecture on Hadamard 2-groups. Preprint.

[12] K.H. Leung and S.L. Ma, Partial difference triples. Preprint.

[13] R.A. Liebler and K.W. Smith, On difference sets in certain 2-groups, in *Proc. Marshall Hall Memorial Conference, Vermont, 1990.* In press.

[14] 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.

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

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

[17] 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.

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

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

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

[21] K.W. Smith, Non-abelian Hadamard difference sets. Preprint.

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

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

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

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