9-1995

A Nonexistence Result for Abelian Menon Difference Sets Using Perfect Binary Arrays

K. T. Arasu

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

Jonathan Jedwab

COMBINATORICA
Akadémiai Kiadó – Springer-Verlag

COMBINATORICA 15 (3) (1995) 311–317

A NONEXISTENCE RESULT FOR ABELIAN MENON DIFFERENCE SETS USING PERFECT BINARY ARRAYS

K. T. ARASU*, JAMES A. DAVIS† and J. JEDWAB

Received April 8, 1993
Revised August 13, 1993

A Menon difference set has the parameters $(4N^2, 2N^2-N, N^2-N)$. In the abelian case it is equivalent to a perfect binary array, which is a multi-dimensional matrix with elements ± 1 such that all out-of-phase periodic autocorrelation coefficients are zero. Suppose that the abelian group $H \times K \times Z_{p^\alpha}$ contains a Menon difference set, where p is an odd prime, $|K| = p^\alpha$, and $p^j \equiv -1 \pmod{\exp(H)}$ for some j. Using the viewpoint of perfect binary arrays we prove that K must be cyclic. A corollary is that there exists a Menon difference set in the abelian group $H \times K \times Z_{3^\alpha}$, where $\exp(H) = 2$ or 4 and $|K| = 3^\alpha$, if and only if K is cyclic.

1. Introduction

Let G be a multiplicative group of order v and D be a k-element subset of G; then D is called a (v,k,λ)-*difference set* in G provided that the differences dd'^{-1} for $d, d' \in D, d \neq d'$ contain every nonidentity element of G exactly λ times. We shall consider $(4N^2, 2N^2-N, N^2-N)$-difference sets (known as *Menon* or alternatively *Hadamard* difference sets) in an abelian group G.

Recently, Menon difference sets have been constructed in all groups $H \times K \times L$ for which H is of the form $Z_{2^{a_1}} \times \ldots \times Z_{2^{a_u}}$, where $\sum_i a_i = 2a+2 \geq 2$ and $\max_i a_i \leq a+2$, K is of the form $Z^2_{3^{b_1}} \times \ldots \times Z^2_{3^{b_r}}$, and L is of the form $Z^4_{p_1} \times \ldots \times Z^4_{p_t}$, where each p_j is a prime satisfying $p_j \equiv 3 \pmod 4$ [1], [5], [7], [16]. There are also many nonexistence results, in particular [2], [4], [10], [12], [13], [14] and [15].

Let m and w be positive integers; then m is called *semiprimitive* mod w if there exists an integer j such that $m^j \equiv -1 \pmod w$. Consider an abelian group $G = H \times P$, where $|P| = p^{2\alpha}$ and p is an odd prime semiprimitive mod $\exp(H)$.

A necessary condition for G to contain a Menon difference set is the exponent bound $\exp(P) \leq p^\alpha$, which follows easily from Theorem 4.33 of [10] based on results of Turyn [15]. In this paper we restrict attention to the case $\exp(P) = p^\alpha$, and show that P must then have the form $Z_{p^\alpha} \times Z_{p^\alpha}$.

Mathematics Subject Classification (1991): 05 B 10, 20

* This work is partially supported by NSA grant # MDA 904-92-H-3057 and by NSF grant # NCR-9200265. The author thanks the Mathematics Department, Royal Holloway College, University of London for its hospitality during the time of this research

† This work is partially supported by NSA grant # MDA 904-92-H-3067

We shall make use of the viewpoint of perfect binary arrays; for a general discussion of this topic and its applications in signal processing, see [3] or [7]. An integer-valued r-dimensional matrix $A=(a[j_1,\ldots,j_r])$ with $0 \le j_i < s_i$ $(1 \le i \le r)$ is called an $s_1 \times \ldots \times s_r$ *array*. The array is called *perfect* if the periodic autocorrelation coefficients

$$R_A(u_1,\ldots,u_r) = \sum_{j_1=0}^{s_1-1} \cdots \sum_{j_r=0}^{s_r-1} a[j_1,\ldots,j_r]a[(j_1+u_1) \bmod s_1,\ldots,(j_r+u_r) \bmod s_r]$$

are zero for all $(u_1,\ldots,u_r) \neq (0,\ldots,0)$, $0 \le u_i < s_i$. The array is *binary* if each matrix element is ± 1. The invertible mapping from the binary array A to $\nu(A) = \{(j_1,\ldots,j_r) : a[j_1,\ldots,j_r] = -1\}$ gives rise to an equivalence between an $s_1 \times \ldots \times s_r$ perfect binary array and a Menon difference set in $Z_{s_1} \times \ldots \times Z_{s_r}$, where $4N^2 = \prod_i s_i$ [9].

Difference sets are often studied in the context of a group ring $Z[G]$. The definition of a difference set immediately yields the group ring equation $DD^{(-1)} = (k-\lambda)+\lambda G$, where we identify the subset D of G with the group ring element $D = \sum_{d \in D} d$, and $D^{(-1)} = \sum_{d \in D} d^{-1}$.

Let U be a normal subgroup of G, so that we can form the factor group $G' = G/U$. The *contraction* of D with respect to U is the multiset $D' = D/U = \{Ud : d \in D\}$, which satisfies the equation $D'D'^{(-1)} = (k-\lambda)+\lambda|U|G'$ in the group ring $Z[G']$. We can write $D' = \sum_{g' \in G'} t_{g'} g'$ in $Z[G']$, where $t_{g'} = |g' \cap D|$ is the number of elements of D in the coset g' of U. The elements of the multiset $\{t_{g'} : g' \in G'\}$ are known as the *intersection numbers* of D relative to U, and satisfy the equations $\sum_{g' \in G'} t_{g'} = k$ and $\sum_{g' \in G'} t_{g'}^2 = k - \lambda + \lambda|U|$.

We can similarly contract a binary array $A = (a_g : g \in G)$ corresponding to a difference set $\nu(A)$ in G by summing the array elements a_g over values of g lying in the same coset of U. This yields the contracted array $A' = (a'_{g'} : g' \in G')$, where $a'_{g'} = \sum_{g : Ug = g'} a_g$. Since the coset g' of U comprises $t_{g'}$ elements of D and $|U| - t_{g'}$ elements not in D, the definition of the mapping ν shows that the contracted array values are related to the intersection numbers by the linear transformation

$$a'_{g'} = |U| - 2t_{g'} \text{ for all } g' \in G'. \tag{1}$$

It is straightforward to show that any contraction of a perfect binary array will also be perfect (though not necessarily binary). Defining the *energy* of an array to be the sum of the squares of the array elements we also obtain the following result, which is the central reason for using the transformation (1) in this paper:

Lemma 1.1. *The energy of an $s_1 \times \ldots \times s_r$ perfect binary array is $\prod_{i=1}^{r} s_i$, and remains constant under all contractions.*

In contrast, the sum of squares of the intersection numbers depends on the order of the subgroup U.

We will also make use of character theoretic results. Since we consider only abelian groups, a character of the group is simply a homomorphism from the group to the multiplicative group of complex roots of unity. Extending this homomorphism to the entire group ring yields a map from the group ring to the complex numbers. The element D of $Z[G]$ is then a (v,k,λ)-difference set in G if and only if

$$|\chi(D)| = \begin{cases} k & \text{if } \chi \text{ is the principal (all 1) character} \\ \sqrt{k-\lambda} & \text{otherwise.} \end{cases}$$

The element A of $Z[G]$ satisfies $\chi(A)=0$ for all nonprincipal characters χ of G if and only if A is a multiple of G. These properties follow from the orthogonality relations on characters; see [15] for similar arguments. Furthermore $G/Ker(\chi)$ is a cyclic group since it is isomorphic to a finite multiplicative subgroup of a field (the complexes).

2. Congruences for contracted array elements

In this section we derive congruences that constrain the intersection numbers of a contracted difference set. This gives corresponding restrictions on the elements of a contracted array. We require two lemmas for the proof of Proposition 2.1.

Lemma 2.1. (Chan *et al.* [2]; Turyn [15]) *Let p be a prime and $G=H\times P$ be an abelian group, where P is the Sylow p-subgroup of G and p is semiprimitive mod $\exp(H)$. Let χ be a nonprincipal character of G and let α be a positive integer. Suppose $A\in Z[G]$ satisfies $\chi(A)\overline{\chi(A)}\equiv 0 \pmod{p^{2\alpha}}$. Then $\chi(A)\equiv 0 \pmod{p^{\alpha}}$.* ∎

Lemma 2.2. (Ma [11], Lemma 3.4) *Let p be a prime and G be an abelian group with a cyclic Sylow p-subgroup. If $A\in Z[G]$ satisfies $\chi(A)\equiv 0 \pmod{p^{\alpha}}$ for all nonprincipal characters χ of G, then there exist $x_1,x_2\in Z[G]$ such that*

$$A = p^{\alpha}x_1 + Qx_2,$$

where Q is the unique subgroup of G of order p. ∎

Proposition 2.1. *Let D be a (v,k,λ)-difference set in an abelian group G and let U be a subgroup of G. Let p be a prime and suppose that $G'=G/U=H\times Z_{p^{\alpha}}$, where $Z_{p^{\alpha}}=\langle z\rangle$ and p is semiprimitive mod $\exp(H)$. Let D' be the contraction of D with respect to U, write $D'=\sum_{g'\in G'} t_{g'}g'$ in $Z[G']$, and let $A'=(a'_{g'})$ be the contracted array corresponding to D'. If $p^{2\beta}|k-\lambda$ for some positive integer β then for all $g'\in G'$,*

$$t_{g'} \equiv t_{g'z^{p^{\alpha-1}}} \equiv \cdots \equiv t_{g'z^{(p-1)p^{\alpha-1}}} \pmod{p^{\beta}}$$
$$a'_{g'} \equiv a'_{g'z^{p^{\alpha-1}}} \equiv \cdots \equiv a'_{g'z^{(p-1)p^{\alpha-1}}} \pmod{2p^{\beta}}.$$

Proof. Since D' is a contracted difference set, $D'D'^{(-1)}=(k-\lambda)+\lambda|U|G'$ in $Z[G']$. Therefore for every nonprincipal character χ of G',

$$\chi(D')\overline{\chi(D')} = k-\lambda \equiv 0 \pmod{p^{2\beta}}.$$

By Lemma 2.1 this implies $\chi(D') \equiv 0 \pmod{p^\beta}$ and so by Lemma 2.2, there exist $x_1, x_2 \in Z[G']$ such that $D' = p^\beta x_1 + \langle z^{p^{\alpha-1}} \rangle x_2$. Multiplying both sides by $1 - z^{p^{\alpha-1}}$ and substituting for D',

$$\sum_{g' \in G'} t_{g'} g'(1 - z^{p^{\alpha-1}}) \equiv 0 \pmod{p^\beta}.$$

The result follows from comparison of coefficients and the transformation (1). ∎

3. Main Result

Henceforth, consider the abelian group $G = H \times K \times Z_{p^\alpha}$ to contain a Menon difference set D, where p is an odd prime, $|K| = p^\alpha$, $|H| = h$, and p is semiprimitive mod $\exp(H)$. In this section we will use Proposition 2.1 to prove that K is cyclic.

Let U be any subgroup of G for which $G/U = G' = H \times Z_{p^\alpha}$, and let $Z_{p^\alpha} = \langle z \rangle$. Let $D' = \sum_{g' \in G'} t_{g'} g'$ be the contraction of D with respect to U, and let $A' = (a'_{g'} : g' \in G')$ be the contracted array corresponding to D'. Application of Proposition 2.1 with $N^2 = k - \lambda = hp^{2\alpha}/4$ gives

$$a'_{g'} \equiv a'_{g' z^{p^{\alpha-1}}} \equiv \cdots \equiv a'_{g' z^{(p-1)p^{\alpha-1}}} \pmod{2p^\alpha} \tag{2}$$

for all $g' \in G'$. By definition, each intersection number $t_{g'}$ satisfies $0 \le t_{g'} \le |U|$ and so from (1), each contracted array element $a'_{g'}$ is bounded by

$$-p^\alpha \le a'_{g'} \le p^\alpha. \tag{3}$$

For any $g' \in G'$, consider the set of array elements $\{a'_{g'}, a'_{g' z^{p^{\alpha-1}}}, \ldots, a'_{g' z^{(p-1)p^{\alpha-1}}}\}$, which we call a *$p$-tuple*. This set is indexed by the coset $g'Q$, where Q is the unique subgroup of order p in G'. It follows from (2) and (3) that if the elements of a p-tuple are not all equal, they must each be $\pm p^\alpha$. We now bound the number of such p-tuples of unequal elements.

Lemma 3.1. *When D is contracted with respect to U, the number w of p-tuples consisting of unequal elements $\pm p^\alpha$ satisfies $w \ge h/(p+1)$.*

Proof. By Lemma 1.1, the contracted array A' has energy $hp^{2\alpha}$. The contribution to the energy from the w p-tuples of unequal elements is $wp \cdot p^{2\alpha}$, and that from the remaining p-tuples of equal elements is R, say:

$$wp^{2\alpha+1} + R = hp^{2\alpha}. \tag{4}$$

Now consider a further contraction with respect to Q, giving a contracted difference set in $H \times Z_{p^{\alpha-1}}$. The corresponding contracted array still has energy $hp^{2\alpha}$. Each of the w p-tuples of unequal elements will collapse to an odd multiple of p^α, giving a total contribution to the energy of at least $wp^{2\alpha}$. The remaining p-tuples of equal elements will each collapse to p times their constant value, so that a previous contribution of $x^2 + \ldots + x^2 = px^2$ from a p-tuple will now be replaced by a contribution $(px)^2 = p^2x^2$. Therefore the total contribution to the energy from p-tuples of equal elements is pR, so that

$$wp^{2\alpha} + pR \leq hp^{2\alpha}. \tag{5}$$

Elimination of R from (4) and (5) gives the desired bound $w \geq h/(p+1)$. ∎

We remark that this bound implies $w \geq 1$, and since $R \geq 0$ we can deduce from (4) that $w \leq h/p$, giving $p \leq h$. In fact a simple argument excludes the possibility $R=0$ to give the necessary condition $p < h$, as obtained by Chan *et al.* [2] for the case K cyclic using similar methods.

Now write $K = \langle k_1, \ldots, k_r \rangle$, where $k_i^{p^{\alpha_i}} = 1$ for $i = 1, \ldots, r$ and $\sum_{i=1}^r \alpha_i = \alpha$. Consider the characters χ of $K \times Z_{p^\alpha}$ that send each k_i to a pth root of unity (or 1), and that sends z to a specific primitive p^αth root of unity, say ζ. There are p^r such characters; the kernel of χ will be of the form $\langle k_1 z^{c_1 p^{\alpha-1}}, \ldots, k_r z^{c_r p^{\alpha-1}} \rangle$ where $c_i = 0, 1, \ldots p-1$. We can use these characters to define homomorphisms $\psi_\chi : G \to G/\mathrm{Ker}(\chi)$ by $\psi_\chi(g) = g\mathrm{Ker}(\chi)$. By the remark at the end of Section 1, $K \times Z_{p^\alpha}/\mathrm{Ker}(\chi)$ is cyclic and therefore isomorphic to Z_{p^α}. Hence the map ψ_χ will produce a contracted difference set $\psi_\chi(D) = D'$ in $G' = H \times Z_{p^\alpha}$.

Therefore from Lemma 3.1, contraction of D with respect to any of the p^r subgroups $U = \mathrm{Ker}(\chi)$ results in at least $h/(p+1)$ p-tuples of unequal elements $\pm p^\alpha$. The array values a_g which sum to elements of these p-tuples are thereby completely determined, and we can examine what happens when we contract D with respect to a different subgroup of the form $\mathrm{Ker}(\chi)$. Thus, we can "pull" the p-tuples of unequal elements up to the original group $H \times K \times Z_{p^\alpha}$ and "push" them back down to $H \times Z_{p^\alpha}$ using a different subgroup. This is the key to the nonexistence result, and is described in the next lemma.

Lemma 3.2. *(push-pull) Each p-tuple of unequal elements $\pm p^\alpha$ arising from contraction with respect to the subgroup $\langle k_1 z^{c_1 p^{\alpha-1}}, \ldots, k_r z^{c_r p^{\alpha-1}} \rangle \neq K$ produces a p-tuple of equal elements $bp^{\alpha-1}$ under contraction with respect to K, where b is odd.*

Proof. Denote the subgroup $\langle k_1 z^{c_1 p^{\alpha-1}}, \ldots, k_r z^{c_r p^{\alpha-1}} \rangle \neq K$ by $\mathrm{Ker}(\chi)$. When we contract with respect to this subgroup, every element $-p^\alpha$ in the p-tuple of unequal elements $\pm p^\alpha$ corresponds to a coset $g\mathrm{Ker}(\chi)$ of the subgroup in the difference set. When this coset is contracted with respect to K, we get $p^{\alpha-1}$ copies of $g\langle z^{p^{\alpha-1}} \rangle$ (in $H \times Z_{p^\alpha}$). This means that we get a contribution of $-p^{\alpha-1}$ in each of the positions of the original p-tuple. Similarly, each element p^α in the original p-tuple will give a contribution of $p^{\alpha-1}$ in each position under the pull-push procedure. Thus every element of the final p-tuple receives the same total contribution, namely the sum of an odd number of values $\pm p^{\alpha-1}$. Furthermore, this accounts for all the p^α values of ± 1 that must contract onto each position of the final p-tuple, completing the proof. ∎

We are now ready to prove the main result of the paper.

Theorem 3.1. *If the abelian group $H\times K\times Z_{p^\alpha}$ contains a Hadamard difference set, where p is an odd prime, $|K|=p^\alpha$, and p is semiprimitive mod $\exp(H)$, then K is cyclic.*

Proof. Consider the contracted array corresponding to the contraction of D with respect to K. By Lemma 3.1, this array contains at least $h/(p+1)$ p-tuples of (unequal) elements $\pm p^\alpha$. By Lemmas 3.1 and 3.2, it also contains at least $h/(p+1)$ p-tuples of (equal) elements of the form $bp^{\alpha-1}$, b odd, for each of the p^r-1 subgroups $\mathrm{Ker}(\chi)\neq K$. The energy constraint of Lemma 1.1 then gives

$$\frac{h}{p+1}\left(p^{2\alpha+1}+(p^r-1)p^{2\alpha-1}\right)\leq hp^{2\alpha}.$$

This implies $p^r\leq p+1$, forcing $r=1$ and proving that K is cyclic. ∎

Combining Theorem 3.1 with the existence result stated in the introduction we can give necessary and sufficient conditions for the existence of Menon difference sets in many classes of abelian groups, for example:

Corollary 3.1. *A Menon difference set exists in the abelian group $H\times K\times Z_{3^\alpha}$, where $\exp(H)=2$ or 4 and $|K|=3^\alpha$, if and only if K is cyclic.* ∎

In particular this gives a theoretical proof for the nonexistence of a Menon difference set in $F\times Z_3^2\times Z_9$, where $F=Z_2^2$ or Z_4, previously established in [8] using computer search together with a preliminary version of the method presented here. The exclusion of these two groups is interesting because Menon difference sets exist in both $F\times Z_3^4$ and $F\times Z_9^2$. This demonstrates that, in contrast to the case of a 2-group, the exponent alone does not in general determine whether an abelian group contains a Menon difference set.

There remain eight abelian groups in which the existence of a $(4N^2,2N^2-N,N^2-N)$-difference set with $N<20$ is currently undecided [6 Proposition 3.5.1], namely

$$\begin{array}{llll} Z_2^2\times Z_4\times Z_5^2, & Z_2\times Z_8\times Z_5^2, & Z_4^2\times Z_5^2, & Z_2^2\times Z_{16}\times Z_9,\\ Z_4\times Z_{16}\times Z_9, & Z_8^2\times Z_9, & Z_4\times Z_3^2\times Z_5^2, & Z_2\times Z_8\times Z_3^2\times Z_9. \end{array}$$

References

[1] K.T. ARASU, J.A. DAVIS, J. JEDWAB, and S.K. SEHGAL: New constructions of Menon difference sets, *J. Comb. Theory (A)*, **64** 329–336, 1993.

[2] W.-K. CHAN, S.-L. MA, and M.-K. SIU: Non-existence of certain perfect arrays, *Discrete Math.* To appear.

[3] W.-K. CHAN, and M.-K. SIU: Summary of perfect $s\times t$ arrays, $1\leq s\leq t\leq 100$, *Electron. Lett.*, **27** 709–710, 1991. (Correction *Electron. Lett.* **27** 1112, 1991).

[4] W.K. CHAN: Perfect arrays and Menon difference sets, 1991, M. Phil. thesis.

[5] J.A. DAVIS, and J. JEDWAB: A survey of Hadamard difference sets. Submitted.

[6] J. JEDWAB: *Perfect arrays, Barker arrays and difference sets*, PhD thesis, University of London, 1991.

[7] J. JEDWAB: Generalized perfect arrays and Menon difference sets, *Designs, Codes and Cryptography*, **2** 19–68, 1992.
[8] J. JEDWAB, and J.A. DAVIS: Nonexistence of certain perfect binary arrays, *Electron. Lett.*, **29** 99–101, 1993.
[9] L.E. KOPILOVICH: On perfect binary arrays, *Electron. Lett.*, **24** 566–567, 1988.
[10] E.S. LANDER: *Symmetric Designs: an Algebraic Approach*, London Mathematical Society Lecture Notes Series 74. Cambridge University Press, Cambridge, 1983.
[11] S.L. MA: Polynomial addition sets and polynomial digraphs, *Linear Algebra and its Applications*, **69** 213–230, 1985.
[12] R.L. MCFARLAND: Difference sets in abelian groups of order $4p^2$, *Mitt. Math. Sem. Giessen*, **192** 1–70, 1989.
[13] 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*, 257–272. Springer-Verlag, New York, 1990.
[14] R.L. MCFARLAND: Sub-difference sets of Hadamard difference sets, *J. Comb. Theory (A)*, **54** 112–122, 1990.
[15] R.J. TURYN: Character sums and difference sets, *Pacific J. Math.*, **15** 319–346, 1965.
[16] M.-Y. XIA: Some infinite classes of special Williamson matrices and difference sets, *J. Comb. Theory (A)*, **61** 230–242, 1992.

K. T. Arasu

Department of Mathematics and Statistics, Wright State University, Dayton, Ohio 45435, USA

James A. Davis

Department of Mathematics, University of Richmond, Richmond, Virginia 23173, USA
jad@newton.urich.edu

Jonathan Jedwab

Hewlett-Packard Laboratories, Filton Road, Stoke Gifford, Bristol BS12 6QZ, U.K.