7-21-1997

Nested Hadamard Difference Sets

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

Jonathan Jedwab

Recommended Citation

Davis, James A., and Jonathan Jedwab. *Journal of Statistical Planning and Inference* 62, no. 1 (July 21, 1997): 13-20. doi: 10.1016/S0378-3758(96)00162-0.

Journal of Statistical Planning and
Inference 62 (1997) 13–20

journal of
statistical planning
and inference

Nested Hadamard difference sets

James A. Davis[a,*,1], Jonathan Jedwab[b]

[a] *Department of Mathematics, University of Richmond, Richmond, VA 23173, USA*
[b] *Hewlett-Packard Laboratories, Filton Road, Stoke Gifford, Bristol BS12 6QZ, UK*

Received 15 December 1995

Abstract

A Hadamard difference set (HDS) 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 multidimensional matrix with elements ± 1 such that all out-of-phase periodic autocorrelation coefficients are zero. We show that if a group of the form $H \times Z_{p^r}^2$ contains a $(hp^{2r}, \sqrt{h}p^r(2\sqrt{h}p^r-1), \sqrt{h}p^r(\sqrt{h}p^r-1))$ HDS (HDS), p a prime not dividing $|H| = h$ and $p^j \equiv -1 \pmod{\exp(H)}$ for some j, then $H \times Z_{p^t}^2$ has a $(hp^{2t}, \sqrt{h}p^t(2\sqrt{h}p^t-1), \sqrt{h}p^t(\sqrt{h}p^t-1))$ HDS for every $0 \leqslant t \leqslant r$. Thus, if these families do not exist, we simply need to show that $H \times Z_p^2$ does not support a HDS. We give two examples of families that are ruled out by this procedure.

AMS classification: primary 05 B 10; secondary 62 K 05

Keywords: Difference set; Perfect binary array

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 *Hadamard* or alternatively *Menon* difference sets) in an abelian group G. We will use the notation HDS for Hadamard difference sets as HDS.

Recently, HDSs have been constructed in all groups $H \times K \times L$ for which H is of the form $Z_{2^{a_1}} \times \cdots \times Z_{2^{a_u}}$, where $\sum_i a_i = 2a+2 \geqslant 2$ and $\max_i a_i \leqslant a+2$, K is of the form $Z_{3^{b_1}}^2 \times \cdots \times Z_{3^{b_r}}^2$ and L is of the form $Z_{p_1}^4 \times \cdots \times Z_{p_t}^4$, where each p_j is a prime satisfying $p_j \equiv 3 \pmod 4$ (Arasu et al., 1993; Davis and Jedwab; Jedwab, 1992; Xia, 1992). There are also many nonexistence results, in particular Chan et al. (to appear), Chan (1991), Lander (1983), McFarland (1989, 1990a,b), Turyn (1965).

[*] Corresponding author. Tel.: +1 804 2898094; fax: +1 804 2876444; e-mail: jad@mathcs.urich.edu.
[1] This work is partially supported by NSA grant # MDA 904-92-H-3067.

0378-3758/97/$17.00
PII S0378-3758(96)00162-0

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 HDS is the exponent bound $\exp(P) \leqslant p^{\alpha}$, which follows easily from Theorem 4.33 of Lander (1983) based on results of Turyn (1965). In this paper we restrict attention to the case $\exp(P) = p^{\alpha}$, and show that P must then have the form $Z_{p^\alpha} \times Z_{p^\alpha}$.

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 Chan and Siu (1991) or Jedwab (1992). An integer-valued r-dimensional matrix $A = (a[j_1,\ldots,j_r])$ with $0 \leqslant j_i < s_i$ $(1 \leqslant i \leqslant r)$ is called an $s_1 \times \cdots \times s_r$ *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 $(u_1,\ldots,u_r) \neq (0,\ldots,0)$, $0 \leqslant u_i < s_i$. The array is *binary* if each matrix element is ± 1. The invertible mapping from the binary array A to $v(A) = \{(j_1,\ldots,j_r)\colon a[j_1,\ldots,j_r] = -1\}$ gives rise to an equivalence between an $s_1 \times \cdots \times s_r$ perfect binary array and a HDS in $Z_{s_1} \times \cdots \times Z_{s_r}$, where $4N^2 = \prod_i s_i$ (Kopilovich, 1988).

We can contract a binary array $A = (a_g\colon g \in G)$ corresponding to a difference set $v(A)$ 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 $A' = (a'_{g'}\colon g' \in G')$, where $a'_{g'} = \sum_{g:Ug=g'} a_g$. 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.

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

By using Ma's lemma (Arasu et al., to appear, Lemma 3.4) and some character theory, we can place restrictions on the contracted array values. In particular, we can show that when we contract a group of the form $H \times Z_{p^\alpha}^2$ by a cyclic subgroup of order p^α (p a prime that is semiprimitive mod $\exp(H)$), the contracted array values are congruent mod p^α in p-tuples. This was shown in Arasu et al. (to appear).

Proposition 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, 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 $g' \in G'$,*

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

Suppose that we are working with the group $H \times Z^2_{p^\alpha}$, so $\beta = \alpha$. Since the contraction is by a group of order p^α, the array values will all satisfy $-p^\alpha \leqslant a'_{g'} \leqslant p^\alpha$. The only way that the p-tuple of array values associated to $a'_{g'}$ can be unequal is if they are of the form $(a'_{g'}, a'_{g'z^{p^{\alpha-1}}}, \ldots, a'_{g'z^{(p-1)p^{\alpha-1}}}) = (-p^\alpha, \pm p^\alpha, \ldots, p^\alpha)$. For any of these contractions, we can get a count of how many p-tuples are of this form (see Arasu et al., to appear, for details).

Theorem 1. *Suppose that there is a PBA in the group $H \times Z^2_{p^\alpha}$. When we contract by a cyclic subgroup of order p^α, there will be at least $w = h/(p+1)$ p-tuples $(-p^\alpha, \pm p^\alpha, \ldots, p^\alpha)$ for any of these contractions.*

This explicit counting of the number of unequal p-tuples for any contraction of this form led to the calculation of what happens when we pull a p-tuple up to the original group and then push it down by a different contraction. This is possible because the pull up is completely determined by the array values: all of the elements of the original array that contract to p^α must have been $+1$ to start, and the same for $-p^\alpha$ pulling up to -1. This led to the following Lemma (see [1] for details).

Lemma 2 (Pull–push). *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 $b p^{\alpha-1}$ under contraction with respect to K, where b is odd.*

It is this technical lemma that we will generalize in this paper to get a nested family of PBAs once we get one example of a PBA. The main implication of the pull–push lemma in Arasu et al. is the following theorem.

Theorem 2. *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.*

Thus, we can restrict our attention to groups of the form $H \times Z^2_{p^\alpha}$ for the rest of the paper.

2. Nesting of HDS

In the previous section, we established several facts about the contractions of the PBA to smaller perfect arrays. We quoted the result about HDS with exponent p^α, so from this point on in the paper, we will only consider groups of the form $H \times Z^2_{p^\alpha}$. We assume that p is a prime and that p is semiprimitive mod the exponent of H. We will first make more precise the form of the array based on considering more than one contraction. The following lemma is a generalization of the push–pull lemma.

Lemma 3 (Generalized pull–push). *Suppose that there is a PBA in $H \times Z^2_{p^\alpha}$ where p is a prime that is semiprimitive mod the exponent of H. Let g be an element that is mapped to a p-tuple of the form $(-p^\alpha, \pm p^\alpha, \ldots, p^\alpha)$ when it is contracted by a cyclic subgroup H_1 of order p^α. If we contract the original array by a different cyclic subgroup H_2 of order p^α, then g cannot be mapped to a p-tuple of the form $(-p^\alpha, \pm p^\alpha, \ldots, p^\alpha)$.*

Proof. Suppose that there is an element of the group g that is mapped to a contracted value of $\pm p^\alpha$ under contraction by H_1, a cyclic subgroup of order p^α . Since g contracts to a p-tuple which is a mixture of $\pm p^\alpha$, there is another element $gz^{kp^{\alpha-1}}$ that will contract to the negative of g. Let H_2 be another cyclic subgroup of order p^α, and consider what happens to the subgroup H_2 when it is contracted by H_1. Since contraction is a homomorphism, H_2 maps to a subgroup of size at least p. Since G/H_1 is a cyclic group, there is a unique subgroup of order p inside G/H_1. Thus, H_2 maps onto this subgroup of order p, as does $\langle z^{p^{\alpha-1}} \rangle$. This implies that there is an element h_k of H_2 so that $h_k H_1 = z^{kp^{\alpha-1}} H_1$ for $0 \leqslant k \leqslant p-1$. Since $h_k \in h_k H_1$, h_k is also in $z^{kp^{\alpha-1}} H_1$, so we get that $gh_k H_2 \cap gz^{kp^{\alpha-1}} H_1 = gH_2 \cap gz^{kp^{\alpha-1}} H_1$ is not empty. Thus, when we contract g by H_2, there will be at least one element -1 and one element $+1$ contracting together. The only way for g to be mapped to a p-tuple of the form $(-p^\alpha, \pm p^\alpha, \ldots, p^\alpha)$ is for gH_2 to have all the same number contracting to it. This proves the lemma. □

In terms of the group theory, this implies that the cosets of cyclic subgroups of size p^α that are used to build the difference set do not overlap. The next result shows that the difference set is completely built by cosets like this.

Theorem 3. *Suppose that there is a difference set in $H \times Z^2_{p^\alpha}$ where p is a prime that is semiprimitive* mod *the exponent of H. Every element of the group will contract down to exactly one p-tuple of the form $(-p^\alpha, \pm p^\alpha, \ldots, p^\alpha)$ under the contractions by cyclic subgroups of order p^α. The number of such p-tuples for every contraction is exactly $h/(p+1)$.*

Proof. We have $p^\alpha + p^{\alpha-1}$ subgroups H_i that will have contractions onto a group isomorphic to $H \times Z_{p^\alpha}$. Each of these contractions will have at least $h/(p+1)$ p-tuples of the form listed above. Since the p-tuples do not use any of the same elements by the above lemma, each p-tuple uses up $p \cdot p^\alpha$ elements of the original. If we count how many elements are being used, we get at least $(p^\alpha + p^{\alpha-1})(h/(p+1))(p \cdot p^\alpha) = hp^{2\alpha}$; since that is all of the elements in the group, we must have that every element is used exactly once. This also implies that the inequality mentioned above must be equality, and that implies that $w = h/(p+1)$. □

This theorem implies that every -1 in the array belongs to a coset of a cyclic subgroup of order p^α. Since these cosets cannot overlap because of the lemmas, this implies that the difference set is a union of cosets of these cyclic subgroups. By considering a different type of contraction, we get the following result.

Theorem 4 (Nested difference sets). *Suppose that there is a difference set in $H \times Z_{p^\alpha}^2$ where p is a prime that is semiprimitive mod the exponent of H. Then there is a difference set in $H \times Z_{p^{\alpha-1}}^2$.*

Proof. Consider what happens to an array value of ± 1 when it is contracted by the unique subgroup H_i that takes it to a p-tuple of the form $(-p^\alpha, \pm p^\alpha, \ldots, p^\alpha)$. The subgroup H_i has a unique subgroup Q isomorphic to Z_p, and Q is a subgroup of the unique subgroup of G that is isomorphic to Z_p^2. When G is contracted by Q, the array value that we have picked out will map to a p-tuple of the form $(-p, \pm p, \ldots, p)$. If we contract this p-tuple by the subgroup generated by any element q of Z_p^2 that is not in Q, we take this p-tuple and add its elements together. This is because the p-tuple is separated by the element q, so contraction by $\langle q \rangle$ amounts to collapsing the p-tuple on itself. Thus, the element that we started with contracts to an odd multiple of p under contraction by Z_p^2. This is true of every element of the array, so we have a perfect array in $H \times Z_{p^{\alpha-1}}^2$ where all of the elements are divisible by p (and they are not 0). Since the energy of this array must be $hp^{2\alpha}$, this forces all of the odd multiples to be ± 1. Therefore, if we divide the array by p, we get an array of ± 1 that is perfect, so this is a PBA with the correct parameters. □

This theorem can be applied repeatedly to show that a HDS in the group $H \times Z_{p^\alpha}^2$ implies a HDS in the group $H \times Z_p^2$. If we can show that there is no HDS in $H \times Z_p^2$, then there will not be an HDS in any group of the form $H \times Z_{p^\alpha}^2$. We will use this version of the theorem in the next section to show nonexistence of some new families of HDS.

It is worth noting that this reduction to the Z_p^2 case does not work for lower exponent Sylow-p subgroups. For example, $Z_2^2 \times Z_7^2$ does not have a HDS, but $Z_2^2 \times Z_7^4$ does have a HDS (Xia, 1992). In this lower exponent case, the HDS is not forced to be a union of cosets of subgroups, and the argument breaks down because of this.

3. The $H \times Z_p \times Z_p$ case

In this section, we will show the nonexistence of PBAs under certain conditions on the size and exponent of H. When we combine this with the results of the previous section, this will give the nonexistence of the family of groups $H \times Z_{p^\alpha}^2$. We will use the PBA viewpoint in this section, and we will assume that p is a prime that is semiprimitive mod the exponent of H.

Suppose we have a $H \times p \times p$ PBA. If we contract this by any subgroup of order p, we get a perfect $H \times p$ array, call it A. From work in the Introduction, we see that A has $w = h/(p+1)$ p-tuples of the form $(-p, \pm p, \ldots, p)$ and $wp = hp/(p+1)$ p-tuples of the form $(\pm 1, \pm 1, \ldots, \pm 1)$. When we contract A by the subgroup of order p, we get

p times a PBA which we call A'. We want to isolate the impact on the autocorrelation of the p-tuples $(-p, \pm p, \ldots, p)$ when they are mapped onto themselves. In order to do this, define a ternary array B by replacing all of the ± 1 in A with 0 and dividing the remaining $\pm p$ values by p (the values in B will be 0, $+1$, and -1). Define B' to be the contraction of B by the subgroup of order p. B' will also be a ternary array with values 0, $+1$, and -1 because the p-tuples of ± 1 contract exactly the same way as the p-tuples $(-p, \pm p, \ldots, p)$ from A going to A'. With these new arrays, we get the following lemma.

Lemma 1. *Any nonzero autocorrelation of B' will be divisible by p.*

Proof. In order to show this, we need to calculate any nonzero autocorrelation of A by using the other arrays. Let $(u_1, \ldots, u_r) \neq (0, \ldots, 0)$ be an element in H. When we only consider p-tuples $(-p, \pm p, \ldots, p)$ in A being mapped onto other p-tuple of the same form, the contribution will be $p^2 R_B(u, u_1, \ldots, u_r)$ (the u in the front is from the subgroup of order p associated to A and B). When we consider what happens in either of the other cases ($\pm p$s to ± 1s or ± 1s to ± 1s), these calculations are going to be multiples of p, and they are best done in A'. However, A' will still contain the information of $\pm p$ to $\pm p$ which we have already counted, so we want to use B' to subtract that out. The contribution of either of the other 2 cases is $p(R_{A'}(u_1, \ldots, u_r) - R_{B'}(u_1, \ldots, u_r))$. This describes the autocorrelation of A, so we get the following equation:

$$R_A(u, u_1, \ldots, u_r) = p^2 R_B(u, u_1, \ldots, u_r) + p[R_{A'}(u_1, \ldots, u_r) - R_{B'}(u_1, \ldots, u_r)].$$

Both A and A' are perfect, so their autocorrelations are both 0. Thus, the equation reduces to $R_{B'}(u_1, \ldots, u_r) = pR_B(u, u_1, \ldots, u_r)$. Since autocorrelations are integral, this proves the lemma. □

If B' were perfect (every nonzero autocorrelation is 0), then this lemma would not help us. To see why B' is not perfect, notice that the sum of the autocorrelations would simply be the sum of the all 0 autocorrelation, which is the number of nonzero entries in B'. There are $w = h/(p+1)$ nonzero entries. This must be the square of the sum of the array by Jedwab (1991), so $h/(p+1)$ is a square. Since h is a square, this implies that $p+1$ is also a square, and the only prime where this works is $p = 3$. Since we are not including $p = 3$, B' cannot be perfect. By the above lemma, $|R_{B'}(u_1, \ldots, u_r)| \geqslant p$ for some nonzero $(u_1, \ldots, u_r)$. This implies the following, which was first shown in Chan (1991).

Lemma 2. *If we meet all of the conditions above, then $h \geqslant (p+1)^2$.*

Proof. If $|R_{B'}(u_1, \ldots, u_r)| \geqslant p$, there must be at least p nonzero elements in B'. Since w is the number of nonzero elements of B', this implies that $h/(p+1) \geqslant p$. The fact that h is a square implies that equality cannot hold here, so $h/(p+1) \geqslant p+1$. □

We now consider the case $h=(p+1)^2$. This means that there will be $p+1$ elements ± 1 in the array B', and they must be arranged in such a way that one of the nonzero autocorrelations $R_{B'}(u_1,\dots,u_r) = R_{B'}(u) = \pm p$. Thus, if $V = \{v_1, v_2, \dots, v_{p+1}\}$ is the set of elements where B' has a ± 1, then $v_i + u \in V$ for all $v_i \in V$ except one. If $c = \mathrm{ord}(u)$, the set V breaks up into r cycles with c elements and 1 cycle with $0 < d < c$ elements (d cannot be 0 because if it were then $R_{B'}(u) = \pm w = \pm(p+1)$ which is not divisible by p) and $rc + d = w = p + 1$.

Theorem 5. *If we meet all of the conditions above, then* $h > (p+1)^2$.

Proof. We break up the proof into 3 cases.

Case 1: $c = 2$, $d = 1$. Note here that $rc + d = 2r + 1$ is odd and $w = p + 1$ is even. Since they are supposed to be equal, this cannot happen.

Case 2: $c > 2$, $d < c - 1$. If we calculate $R_{B'}(2u)$, the r cycles of length c will have an autocorrelation of rc (even if there are ± 1 in the cycles, when we go by $2u$ they must match signs). The cycle that has only d elements of V in it will have an autocorrelation of $d - 2$. These are the only places where we can get nonzero autocorrelation, so $R_{B'}(2u) = rc + d - 2 = p - 1$. This is not divisible by p, so this cannot happen.

Case 3: $c > 2$, $d = c - 1$. In this case, $rc + d = (r+1)c - 1 = p + 1$, so $(r+1)c = p + 2$. This implies that c divides $p + 2$, but we know that c divides $(p+1)^2$. Since $p+2$ and $(p+1)^2$ are coprime, this cannot happen. □

This theorem shows that we get the nonexistence of two 2-dimensional PBAs with both s and t less than 100: 56 x 56 and 44 x 99. In fact, we have shown that any group H of order 64 with exponent less than or equal to 8 will not have a PBA. When we combine this with Theorem 4, this shows that the group $H \times 7^{\alpha} \times 7^{\alpha}$ will not have a PBA for any value of α. There is an analogous family with $p = 11$ coming from the 44 x 99 example.

References

Arasu, K.T., J.A. Davis and J. Jedwab. A nonexistence result for abelian Menon difference sets using perfect binary arrays. *Combinatorica* 15(3) (1995) 311–317.

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

Chan, W.K. (1991). Perfect arrays and Menon difference sets, M.Phil. Thesis.

Chan, W.-K., S.-L. Ma and M.-K. Siu. Non-existence of certain perfect arrays. *Discrete Math.* 125 (1994) 167–113.

Chan, W.-K. and M.-K. Siu (1991). Summary of perfect $s \times t$ arrays, $1 \leqslant s \leqslant t \leqslant 100$. *Electron. Lett.* **27**, 709–710.

Davis, J.A. and J. Jedwab. A survey of Hadamard difference sets. Groups, difference sets and the monster, Proc. Conf. on Difference Sets, Walter de Gruyter, New York, 1996.

Jedwab, J. (1991). Perfect arrays, Barker arrays and difference sets, Ph.D. Thesis, University of London.

Jedwab, J. (1992). Generalized perfect arrays and Menon difference sets. *Des. Codes Cryptography* **2**, 19–68.

Jedwab, J. and J.A. Davis (1993). There is no $2 \times 2 \times 3 \times 3 \times 9$ or $4 \times 3 \times 3 \times 9$ perfect binary array. *Electronic. Lett.* **29**, 99–100.

Kopilovich, L.E. (1988). On perfect binary arrays. *Electronic. Lett.* **24**, 566–567.

Lander, E.S. (1983). *Symmetric Designs: an Algebraic Approach*, London Mathematical Society Lecture Notes Series, Vol. 74, Cambridge Univ. Press, Cambridge.

Ma, S.L. (1985). Polynomial addition sets and polynomial digraphs. *Linear. Algebra. Appl.* **69**, 213–230.

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

McFarland, R.L. (1990a). Necessary conditions for Hadamard difference sets. In: D. Ray-Chaudhuri, Ed., *The IMA Volumes in Mathematics and its Applications, Coding Theory and Design Theory*, Vol. 21, Springer, New York, 257–272.

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

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

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