11-1993

New Constructions of Menon Difference Sets

K. T. Arasu

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

Jonathan Jedwab

Surinder K. Sehgal

Recommended Citation

Arasu, K. T., James A. Davis, Jonathan Jedwab, and Surinder K. Sehgal. "New Constructions of Menon Difference Sets." *Journal of Combinatorial Theory, Series A* 64, no. 2 (November 1993): 329-36. doi: 10.1016/0097-3165(93)90101-D.

JOURNAL OF COMBINATORIAL THEORY, Series A 64, 329–336 (1993)

Note

New Constructions of Menon Difference Sets

K. T. ARASU*

Wright State University, Dayton, Ohio 45435

JAMES A. DAVIS

University of Richmond, Richmond, Virginia 23173

JONATHAN JEDWAB

Hewlett–Packard Laboratories, Bristol BS12 6QZ, United Kingdom

AND

SURINDER K. SEHGAL

Ohio State University, Columbus, Ohio 43210

Communicated by William M. Kantor

Received October 4, 1991

Menon difference sets have parameters $(4N^2, 2N^2 - N, N^2 - N)$. These have been constructed for $N = 2^a 3^b$, $0 \leqslant a, b$, but the only known constructions in abelian groups require that the Sylow 3-subgroup be elementary abelian (there are some nonabelian examples). This paper provides a construction of difference sets in higher exponent groups, and this provides new examples of perfect binary arrays.

1. INTRODUCTION

Let G be a group of order v and D be a k-subset of G; then D is called a (v, k, λ) difference set (DS) provided that the differences dd'^{-1} for $d, d' \in D$, $d \neq d'$ contain every nonidentity element of G exactly λ times. We will restrict our attention in this paper to the abelian case. One heavily studied group of parameters are of the form $(4N^2, 2N^2 - N, N^2 - N)$ (these

* This work is partially supported by NSA Grant MDA 904-90-H-4008.

0097-3165/93 $5.00

582a/64/2-13

are called either Menon difference sets or Hadamard difference sets). If N is a power of 2, many constructions exist (see [4], [5], [7] and [9]). When N is of the form 2^a3^b, then number theoretic considerations put restrictions on the exponents of the Sylow 2-subgroup and the Sylow 3-subgroup. Let $G = Z_{2^{a_1}} \times \cdots \times Z_{2^{a_u}} \times Z_{3^{b_1}} \times \cdots \times Z_{3^{b_r}}$, where $\sum a_i = 2a+2$ and $\sum b_j = 2b$.

DEFINITION 1.1. Let G be the group above; p^{σ_p} is the exponent of the Sylow p-subgroup of G, and

$$\tau_2(x) = \begin{cases} \sum_{i:\, a_i > x} (a_i - x) & 1 \leqslant x < \sigma_2 \\ 0 & \sigma_2 \leqslant x \end{cases}$$

It has been shown in [6] that results of Turyn [10] imply the following exponent bounds.

LEMMA 1.1. *Let G be the group above. Then G has a difference set only if both of the conditions below hold.*

(i) $\sigma_2 \leqslant a+2$.

(ii) $3^{\sigma_3 - b} \leqslant 2^{\tau_2(2)}$.

Let H be any abelian 2-group meeting the exponent bound of Lemma 1.1(i). Menon difference sets have been constructed in groups of the form $H \times EA(3^{2b})$ where $EA(3^{2b})$ is the elementary abelian group of order 3^{2b} (see [5] or [11]). No constructions in other abelian groups are known, and there are many nonexistence results when N is not of the form 2^a3^b (in fact, McFarland has conjectured that $N = 2^a3^b$ is a necessary condition). The purpose of this paper is to mix techniques from character theory and the study of perfect binary arrays to prove that any group of the form $H \times Z_{3^{b_1}}^2 \times Z_{3^{b_2}}^2 \times \cdots \times Z_{3^{b_r}}^2$ has a Menon difference set.

One of the main reasons for studying DS involves their applications in generating designs. This is done by letting the points of the design be the elements of the group, and the blocks of the design be the translates of D. It is easy to check that this incidence structure forms an (v, k, λ) design (see [1] or [8]).

Difference sets are often studied in the context of a group ring $Z[G]$ and characters. The definition of a DS 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 $D^{(-1)} = \sum_{d \in D} d^{-1}$. Since we are only considering the abelian case, characters of the group are simply homomorphisms 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 $Z[G]$ satisfies the definition of a difference set if the character sum for the character χ on D yields 2 possible results: $\chi(D)=k$ if χ is the principal (all 1) character, and $|\chi(D)|=\sqrt{k-\lambda}$ for any nonprincipal χ. Another useful fact about characters is that if B is an element of $Z[G]$, then $\chi(B)=0$ for every nonprincipal character χ if and only if B is a multiple of G (this is because of the orthogonality relations for characters: see [10] for similar arguments). One final property of characters that we use is the fact that $G/\mathrm{Ker}(\chi)$ is a cyclic group. This is true because the induced character must be faithful (otherwise, the kernel would be bigger), and the only faithful characters are on cyclic groups.

A Menon difference set in an abelian group is equivalent to a perfect binary array. An $s_1\times s_2\times\cdots\times s_r$ binary array is a matrix $A=(a[j_1,j_2,\ldots,j_r])$, $0\leqslant j_i<s_i$ with $a[j_1,j_2,\ldots,j_r]=\pm 1$. If we have two $s_1\times s_2\times\cdots\times s_r$ binary arrays, say A and B, the periodic cross-correlation function of A with B is $R_{AB}(u_1,u_2,\ldots,u_r)=\sum_{j_1=0}^{s_1-1}\sum_{j_2=0}^{s_2-1}\cdots\sum_{j_r=0}^{s_r-1}a[j_1,j_2,\ldots,j_r]\,b[j_1+u_1,j_2+u_2,\ldots,j_r+u_r]$, where $0\leqslant u_i<s_i$ for all i (the sum j_i+u_i is mod s_i). The periodic autocorrelation function is R_{AA}, and we abbreviate that R_A. If $R_A(u_1,u_2,u_r)=0$ whenever $(u_1,u_2,\ldots,u_r)\neq(0,0,\ldots,0)$, then A is a perfect binary array (PBA). An $s_1\times s_2\times\cdots\times s_r$ PBA is equivalent to a $(4N^2,\ 2N^2-N,\ N^2-N)$ difference set in $Z_{s_1}\times Z_{s_2}\times\cdots\times Z_{s_r}$, where $\prod s_i=4N^2$. The equivalence comes from defining the subset $v(A)=\{(j_1,j_2,\ldots,j_r)\mid a[j_1,j_2,\ldots,j_r]=-1\}$ of $Z_{s_1}\times\cdots\times Z_{s_r}$; $v(A)$ is a difference set in this group. Perfect binary arrays have engineering applications in the theory of communications (see [2] or [5] for more on PBAs).

We will exhibit four candidate sets, and use character theory to establish that they correspond to what is called a binary supplementary quadruple (this definition can be found in [5]).

DEFINITION 1.2. Let A, B, C, D be $s_1\times\cdots\times s_r$ binary arrays (not necessarily perfect). $\{A,\ B,\ C,\ D\}$ is called an $s_1\times\cdots\times s_r$ binary supplementary quadruple (BSQ) if the following holds for all $0\leqslant u_i<s_i$;

(i) $(R_A+R_B+R_C+R_D)(u_1,u_2,\ldots,u_r)=0$ whenever $(u_1,u_2,\ldots,u_r)\neq(0,0,\ldots,0)$.

(ii) $(R_{WX}+R_{YZ})(u_1,\ldots,u_r)=0$ for all $\{W,X,Y,Z\}=\{A,B,C,D\}$.

There are many ways to combine PBAs to get new PBAs; we need the tensor product.

DEFINITION 1.3. Let $A=(a[j_1,\ldots,j_r])$, $B=(b[j_{r+1},\ldots,j_{r+r'}])$ be respectively an $s_1\times\cdots\times s_r$ and an $s_{r+1}\times\cdots\times s_{r+r'}$ binary array. The tensor product of A with B is the $s_1\times\cdots\times s_{r+r'}$ binary array $\Pi(A,B)=(c[j_1,\ldots,j_{r+r'}])$ where $c[j_1,\ldots,j_{r+r'}]=a[j_1,\ldots,j_r]\,b[j_{r+1},\ldots,j_{r+r'}]$ for all $0\leqslant j_i<s_i$, $1\leqslant i\leqslant r+r'$.

We shall establish the existence of a $3^b \times 3^b$ BSQ. We shall then recursively use the following theorems to get new PBAs, which will give the difference sets that we are looking for (Theorem 1.1 was proved by Turyn [11], then generalized in [5]; Theorem 1.2 was proved by Jedwab [5]).

THEOREM 1.1. *Let* $\{A_1, B_1, C_1, D_1\}$ *and* $\{A_2, B_2, C_2, D_2\}$ *be, respectively, an* $s_1 \times \cdots \times s_r$ *BSQ and an* $s_{r+1} \times \cdots \times s_{r'}$ *BSQ. Let*

$$A = \Pi(A_1 + B_1, A_2) + \Pi(A_1 - B_1, B_2),$$
$$B = \Pi(A_1 + B_1, C_2) + \Pi(A_1 - B_1, D_2),$$
$$C = \Pi(C_1 + D_1, A_2) + \Pi(C_1 - D_1, B_2),$$
$$D = \Pi(C_1 + D_1, C_2) + \Pi(C_1 - D_1, D_2).$$

Then $\{A/2, B/2, C/2, D/2\}$ *is an* $s_1 \times \cdots \times s_{r+r'}$ *BSQ (where* $A/2$ *is obtained by dividing each element of* A *by* 2).

THEOREM 1.2. *If there exists an* $s_1 \times s_2 \times \cdots \times s_r$ *BSQ then there exists a (Menon) difference set in the group* $Z_{2^{a_1}} \times Z_{2^{a_2}} \times \cdots \times Z_{2^{a_u}} \times Z_{s_1} \times \cdots \times Z_{s_r}$, *where* $\sum a_i = 2a + 2 \geqslant 2$ *and* $a_i \leqslant a + 2$ *for all* i.

2. CONSTRUCTION

Let G be the group of the form $Z_{3^b}^2 \cong \langle y, z \rangle$, $y^{3^b} = z^{3^b} = 1$. We want to label the cyclic subgroups of order 3^b in a careful way. We use $D_{1,i} = \langle yz^i \rangle$, $i = 0, 1, \ldots, (3^{b+1}-1)/(3-1)-2$ and $D_{3j,1} = \langle y^{3j}z \rangle$, $j = 0, 1, \ldots, (3^b-1)/(3-1)$. It is worth noticing that $D_{1,m} = D_{1,m+3^b}$ and $D_{3n,1} = D_{3(n+3^{b-1}),1}$. Consider the multisets $D_k = \bigcup_{i=0}^{(3^b-1)/(3-1)-1} z^i D_{1,3i+k}$ for $k = 0$, 1, or 2, and $D_3 = \bigcup_{j=0}^{(3^b-1)/(3-1)} y^j D_{3j,1}$. We show that these sets correspond to a $3^b \times 3^b$ BSQ, and we will use Theorems 1.1 and 1.2 to build difference sets out of them. We break up the proof into the following series of lemmas.

LEMMA 2.1. D_k *has no repeated elements.*

Proof. Suppose there is a repeated element. We will consider the $k = 0$ case; all the other cases are the same. If there is a repeated element, there must be an i, i', m, m' so that $z^i(yz^{3i})^m = z^{i'}(yz^{3i'})^{m'}$. In order for this to occur, $m = m'$ (since the same power of y must be present). Considering the powers of z, we get $z^{i+3mi} = z^{i'+3mi'}$, or $i(1+3m) \equiv i'(1+3m) \pmod{3^b}$. Since $1 + 3m$ is invertible mod 3^b, we can conclude that $i \equiv i' \pmod{3^b}$; the restrictions on the i and i' imply that they are the same. Thus, these two elements are not really distinct, so there aren't any repeated elements. ∎

LEMMA 2.2. *If χ is a character of order 3^b on $\langle y, z\rangle$, then $|\chi(D_k)| = 3^b$ for one value of k, and 0 for the others.*

Proof. Let χ be a character of order 3^b. By the remarks in the introduction, $G/\mathrm{Ker}(\chi)$ is cyclic. Let $x\,\mathrm{Ker}(\chi)$ be a generator of $G/\mathrm{Ker}(\chi)$; the order of $x\,\mathrm{Ker}(\chi)$ is 3^b since that is the size of the factor group. This implies that the order of x must also be 3^b since that is the maximum order in G. The subgroups $\langle x\rangle$ and $\mathrm{Ker}(\chi)$ intersect only in the identity (no power of x smaller than 3^b can be in $\mathrm{Ker}(\chi)$), and their product is all of G; thus, G must be a direct product of $\langle x\rangle$ and $\mathrm{Ker}(\chi)$. The fact that G has rank 2 implies that $\mathrm{Ker}(\chi)$ must be cyclic of order 3^b.

Now that we have established the fact that $\mathrm{Ker}(\chi)$ is cyclic, we need to observe that all of the cyclic subgroups of G of order 3^b are of the form $D_{i,j}$ for some i, j. Thus, χ is principal on one $D_{i',j'}$ and nonprincipal on all of the others. If that $D_{i',j'}$ only appears once, then the character sum is (in modulus) the size of that set, which is 3^b. If it appears twice, then suppose that χ has order 3^b on the element z (it must have order 3^b on either y or z, and the y argument is the same). The character sum is 3^b times $\chi(z^i) + \chi(z^{i+3^{b-1}})$. Since χ is a homomorphism, this sum can be rewritten $\chi(z^i)(1+\chi(z^{3^{b-1}}))$; $\chi(z^{3^{b-1}})$ is a primitive third root of unity, so $|\chi(z^i)(1+\chi(z^{3^{b-1}}))| = 1$. Thus, the character sum is (in modulus) 3^b. ∎

LEMMA 2.3. *If χ is a character of $\langle y, z\rangle$ that is nonprincipal but of order less than 3^b, then $|\chi(D_k)| = 3^b$ for one k, and 0 for the others.*

Proof. Let ξ be a primitive 3^bth root of unity, and suppose that χ is a character of order less than 3^b. Then $\chi(y) = \xi^{e3^v}$, $\chi(z) = \xi^{f3^t}$, $1 \leqslant t$, $v \leqslant b$, but not both t and v are b, and e, f are nonzero integers not divisible by 3. Consider the case $v < t$ (the $v > t$, $v = t$ cases are similar). Nothing of the form yz^x is in the kernel of the character because there is no way to satisfy the equation $e3^v + xf3^t \equiv 0 \pmod{3^b}$ when $v < t$. Thus, χ is nonprincipal on every subgroup $D_{i,j}$ contained in the sets D_0, D_1, and D_2, so the character sum is 0 over these parts. The kernel does contain elements of the form $y^{3x}z$ whenever $3xe3^v + f3^t \equiv 0 \pmod{3^b}$, or whenever $x \equiv -fe^{-1}3^{t-v-1} \pmod{3^{b-v-1}}$. The character χ is principal on the subgroups $D_{3j,1}$ associated with those solutions, and nonprincipal on all the other subgroups $D_{3j,1}$ in D_3. There are q solutions x to this equation with $0 \leqslant x \leqslant (3^b - 1)/(3-1)$, where q is either $3^v + 3^{v-1} + \cdots + 3 + 1$ or $3^v + 3^{v-1} + \cdots + 3 + 1 + 1$. (In general the number of solutions to the congruence $x \equiv a \pmod{b}$ with $0 \leqslant x \leqslant c$ is $\lfloor c/b \rfloor$ or $\lfloor c/b \rfloor + 1$.) Thus, the character sum over D_3 is $3^b(\chi(y^x) + \chi(y^{x+3^{b-v-1}}) + \chi(y^{x+2\cdot 3^{b-v-1}}) + \cdots + \chi(y^{x+(q-1)3^{b-v-1}})) = 3^b\chi(y^x)(1 + \chi(y^{3^{b-v-1}}) + \cdots + \chi(y^{(q-1)\cdot 3^{b-v-1}}))$. Since $\chi(y) = \xi^{e3^v}$, we get

$$\chi(D_3)=\begin{cases}3^b\chi(y^x)(1+\xi^{e3^{b-1}}+\xi^{2\cdot e3^{b-1}}+1+\cdots & \\ \quad +\xi^{2\cdot e3^{b-1}}+1) & q\equiv 1 \pmod 3\\ 3^b\chi(y^x)(1+\xi^{e3^{b-1}}+\xi^{2\cdot e3^{b-1}}+1+\cdots & \\ \quad +\xi^{2\cdot e3^{b-1}}+1+\xi^{e3^{b-1}}) & q\equiv 2 \pmod 3\end{cases}$$

$$=\begin{cases}3^b\chi(y^x) & q\equiv 1 \pmod 3\\ 3^b\chi(y^x)(1+\xi^{e3^{b-1}}) & q\equiv 2 \pmod 3\end{cases}$$

In either case, the modulus of this sum is 3^b since $(1+\xi^{e3^{b-1}})=-\xi^{2\cdot e3^{b-1}}$ has modulus 1. Thus, $|\chi(D_3)|=3^b$ and all the others are 0. ∎

We consider the four binary arrays $A=v^{-1}(D_0)$, $B=v^{-1}(D_1)$, $C=v^{-1}(D_2)$, and $D=v^{-1}(D_3)$ that correspond to our subsets of G.

LEMMA 2.4. *The sets* $\{A, B, C, D\}$ *form a* $3^b\times 3^b$ *BSQ.*

Proof. We need to translate the definition of BSQ into character theoretic terms. The first condition, $(R_A+R_B+R_C+R_D)(u_1,u_2)=0$, can be shown by considering the group ring expression $D_0D_0^{(-1)}+D_1D_1^{(-1)}+D_2D_2^{(-1)}+D_3D_3^{(-1)}-3^{2b}$. By Lemmas 2.2 and 2.3, any nonprincipal character on G has a sum of 3^b (in modulus) on one of the D_k, and it will be 0 on the others. Thus, the character sum on the expression is 0, and the remarks in the introduction imply that the group ring expression is cG for some c. The fact that $|D_0|=|D_1|=|D_2|=3^b(3^b-1)/2$ and $|D_3|=3^b(3^b+1)/2$ implies that $c=\{\sum|D_i|^2-3^{2b}\}/|G|=\{3\cdot 3^{2b}(3^b-1)^2/4+3^{2b}(3^b+1)^2/4-3^{2b}\}/3^{2b}=3^{2b}-3^b$. The number of times that the non-identity element (u_1,u_2) appears in the expression is $3^{2b}-3^b$, and this corresponds to the number of times that $X[j_1,j_2]=X[j_1+u_1,j_2+u_2]=-1$ in the autocorrelation equation, for $X=A, B, C,$ or D (we call these $(-1,-1)$ pairs). There are $2\cdot 3^{2b}-3^b$ times when $X[j_1,j_2]=-1$, so there are $2\cdot 3^{2b}-3^b-(3^{2b}-3^b)=3^{2b}$ pairs of the form $(-1,1)$ and $(1,-1)$. Finally, there are a total of $4\cdot 3^{2b}$ pairs, and so there are $4\cdot 3^{2b}-3^{2b}-3^{2b}-(3^{2b}-3^b)=3^{2b}+3^b$ $(1,1)$ pairs. Thus, the autocorrelation equation becomes $(R_A+R_B+R_C+R_D)(u_1,u_2)=(3^{2b}-3^b)(-1)(-1)+3^{2b}(-1)(1)+3^{2b}(1)(-1)+(3^{2b}+3^b)(1)(1)=0$ for all $(u_1,u_2)\neq(0,0)$.

The proof of the second condition involves studying the group ring expression $D_0D_1^{(-1)}+D_2D_3^{(-1)}$. Using the same arguments as above, we find that the character sum over this equation is 0 for any nonprincipal character. By the remarks in the introduction, this implies that $D_0D_1^{(-1)}+D_2D_3^{(-1)}=cG$ for some c. A counting argument yields that $c=(3^{2b}-3^b)/2$, and this number is also the number of $(-1,-1)$ pairs (by this we mean the number of times that $X[j_1,j_2]=Y[j_1+u_1,j_2+u_2]=-1$ for $(X,Y)=(A,B)$ or (C,D)) in the sum $R_{AB}+R_{CD}$. Since $|D_0|=(3^{2b}-3^b)/2$, and

$|D_2| = (3^{2b} - 3^b)/2$, there are $((3^{2b} - 3^b)/2 + (3^{2b} - 3^b)/2) - (3^{2b} - 3^b)/2 = (3^{2b} - 3^b)/2$ $(-1, 1)$ pairs. Similar counts yield $(3^{2b} + 3^b)/2$ $(1, -1)$ pairs and $(3^{2b} + 3^b)/2$ $(1, 1)$ pairs. Thus, $R_{AB} + R_{CD}(u_1, u_2) = (3^{2b} - 3^b)/2(-1)$ $(-1) + (3^{2b} - 3^b)/2(-1)(1) + (3^{2b} + 3^b)/2(1)(-1) + (3^{2b} + 3^b)/2(1)(1) = 0$ for every (u_1, u_2). We can shuffle the four sets any way we want, and we will get the same result for the autocorrelation equation. Thus, these four sets satisfy the definition of a BSQ. ▮

Putting all this together, we get the following

THEOREM 2.1. *Any group of the form* $Z_{2^{a_1}} \times Z_{2^{a_2}} \times \cdots \times Z_{2^{a_u}} \times Z^2_{3^{b_1}} \times Z^2_{3^{b_2}} \times \cdots \times Z^2_{3^{b_r}}$, *where* $\sum a_i = 2a + 2$, $a \geqslant 0$, $a_i \leqslant a + 2$, $\sum b_i = 2b \geqslant 0$, *has a Menon difference set with* $N = 2^a 3^b$.

Proof. Combining Lemma 2.4 and Theorem 1.1, we see that we have a $3^{b_1} \times 3^{b_1} \times 3^{b_2} \times 3^{b_2} \times \cdots \times 3^{b_r} \times 3^{b_r}$ BSQ. Theorem 1.2 uses that BSQ to build the difference set that we want. ▮

In two dimensions, Theorem 2.1 shows the existence of a perfect binary array of size $2^{a+2}3^b \times 2^a 3^b$ and $2^{a+1}3^b \times 2^{a+1}3^b$ for all $a, b \geqslant 0$. This removes 6 cases from the updated version [6] of Chan and Siu's [2, 3] table, leaving 21 undecided $s \times t$ cases, $1 \leqslant s,\ t \leqslant 100$. The smallest remaining cases are 10×40 and 20×20. It is interesting to note that Theorem 2.1 and Lemma 1.1 leave undecided cases for $N = 2^a 3^b$, the smallest of which are 8×72 and 16×36 (in the 2-dimensional case).

We remark here that similar arguments to those used in Lemma 2.4 will show that the binary arrays A, B, C, D satisfy $R_{AB}(u_1, u_2) = R_{AC}(u_1, u_2) = -R_{AD}(u_1, u_2) = 1$ for all (u_1, u_2). Thus these arrays have optimal periodic correlation properties in the sense that the cross-correlation function of any pair is constant with minimal magnitude, and the sum of the four autocorrelation functions is zero except at the zero shift. It may also be shown that these mutual correlation properties carry through, under Theorem 1.1, to each BSQ constructed in this paper. Furthermore the $(+1, -1)$ incidence matrices corresponding to each BSQ form a quadruple of (non-symmetric) multicirculant binary matrices $\{\bar{A}, \bar{B}, \bar{C}, \bar{D}\}$ satisfying $\bar{A}\bar{A}^T + \bar{B}\bar{B}^T + \bar{C}\bar{C}^T + \bar{D}\bar{D}^T = 4.3^{2b}I$ and $XY^T = YX^T$ for $X, Y \in \{\bar{A}, \bar{B}, \bar{C}, \bar{D}\}$, $X \neq Y$. The incidence matrices therefore provide new infinite families of Williamson matrices of order 4.3^{2b}, as well as Hadamard matrices of the same order arising from the Goethals-Seidel construction (see [11, 12]).

We also remark that using the methods in [5] and the BSQs constructed here, we can obtain new existence and nonexistence results for divisible difference sets. For example, let G be the group $Z_{2^{z_1+a_1}} \times Z_{2^{z_2+a_2}} \times \cdots \times Z_{2^{z_u+a_u}} \times Z^2_{3^{b_1}} \times Z^2_{3^{b_2}} \times \cdots \times Z^2_{3^{b_r}}$, where $z_i = 0$ or 1, $\sum z_i > 0$, $\sum a_i = x \geqslant 2$, $\sum b_i = 2b > 0$. Let H be the subgroup $\{(y_1 2^{a_1}, ..., y_u 2^{a_u}, 0, ..., 0) \mid y_i = 0$ or

$z_i\}$ of G and let K be the subgroup $\{(y_1 2^{a_1}, ..., y_u 2^{a_u}, 0, ..., 0) \mid y_i = 0 \text{ or } z_i, \sum y_i \text{ even}\}$ of H. Then there exists a divisible difference set with the parameters $(E, 2, E, 0, E/2)$ in G/K relative to H/K, where $E = 2^x 3^{2b}$, provided

$$a_i \leqslant \begin{cases} \lceil x/2 \rceil & \text{when} \quad z_i = 1 \\ \lceil x/2 \rceil + 1 & \text{when} \quad z_i = 0, \end{cases}$$

and only if $a_i \leqslant \lceil x/2 \rceil$ when $z_i = 1$. Further results along similar lines follow from [5].

REFERENCES

1. T. BETH, D. JUNGNICKEL, AND H. LENZ, "Design Theory," Cambridge Univ. Press, Cambridge, 1986.
2. W. K. CHAN AND M. K. SIU, Summary of perfect $s \times t$ arrays, $1 \leqslant s \leqslant t \leqslant 100$, *Electron. Lett.* **27**, No. 9 (1991), 709–710.
3. W. K. CHAN AND M. K. SIU, Author's correction to "Summary of perfect $s \times t$ arrays, $1 \leqslant s \leqslant t \leqslant 100$," *Electron. Lett.* **27**, No. 12 (1991), 1112.
4. J. F. DILLON, Variations on a scheme of McFarland for noncyclic difference sets, *J. Combin. Theory Ser. A* **40** (1985), 9–21.
5. J. JEDWAB, Generalized perfect arrays and Menon difference sets, *Designs Codes Cryptogr.*, to appear.
6. J. JEDWAB, Nonexistence of perfect binary arrays, *Electron. Lett.* **27**, No. 14 (1991), 1252–1253.
7. R. G. KRAEMER, Proof of a conjecture on Hadamard 2-groups, submitted for publication.
8. E. S. LANDER, "Symmetric Designs: An Algebraic Approach," Cambridge Univ. Press, Cambridge, 1983.
9. R. L. MCFARLAND, A family of difference sets in non-cyclic groups, *J. Combin. Theory Ser. A* **15** (1973), 1–10.
10. R. J. TURYN, Character sums and difference sets, *Pacific J. Math.* **15**, No. 1 (1965), 319–346.
11. R. J. TURYN, A special class of Williamson matrices and difference sets, *J. Combin. Theory Ser. A* **36** (1984), 111–115.
12. R. J. TURYN, Hadamard matrices, Baumert–Hall units, four-symbol sequences, pulse compression, and surface wave encodings, *J. Combin. Theory Ser. A* **16** (1974), 313–333.