Perfect binary arrays and difference sets

Jonathan Jedwab

Hewlett-Packard Laboratories, Filton Road, Stoke Gifford, Bristol BS12 6QZ, UK

Chris Mitchell

Computer Science Department, Royal Holloway and Bedford New College, London University, Egham Hill, Egham, Surrey TW20 0EX, UK

Fred Piper and Peter Wild

Mathematics Department, Royal Holloway and Bedford New College, London University, Egham Hill, Egham, Surrey TW20 0EX, UK

Received 12 July 1991
Revised 15 May 1992

Abstract

A perfect binary array is an r-dimensional array with elements ± 1 such that all out-of-phase periodic autocorrelation coefficients are zero. Such an array is equivalent to a Menon difference set in an abelian group. We give recursive constructions for four infinite families of two-dimensional perfect binary arrays, using only elementary methods. Brief outlines of the proofs were previously given by three of the authors. Although perfect binary arrays of the same sizes as two of the families were constructed earlier by Davis, the sizes of the other two families are new.

1. Introduction

Let $A=(a_{ij})$, $0 \leqslant i < s$, $0 \leqslant j < t$, be an $s \times t$ array such that $a_{ij}=1$ or -1 for all i and j. A is called an $s \times t$ *binary array*, and is called *trivial* if $s=t=1$. Define the *periodic autocorrelation function* R_A of A by

$$R_A(u,v)=\sum_{i=0}^{s-1}\sum_{j=0}^{t-1} a_{ij}a_{i+u,j+v},$$

where u, v are integers. Here, and in the rest of this paper, we consider the sums $i+u$ and $j+v$ to be addition modulo s and t, respectively. A binary array A is called *perfect*

Correspondence to: Jonathan Jedwab, Hewlett-Packard Laboratories, Filton Road, Stoke Gifford, Bristol BS12 6QZ, UK.

SSDI 0012-365X(92)00202-B

if $R_A(u,v)=0$ for all $(u,v)\neq(0,0)$. We write PBA(s,t) to denote an $s\times t$ perfect binary array.

If A is a nontrivial PBA(s,t) then $st=4N^2$ for some integer N and A is equivalent to a $(4N^2, 2N^2-N, N^2-N)$-difference set in $\mathbb{Z}_s\times\mathbb{Z}_t$ [2, 9, 18]. We call a difference set with these parameters a *Menon difference set*, after Menon [22]. We refer the reader to Calabro and Wolf's paper [6] introducing perfect binary arrays, to Turyn's papers on the one-dimensional case [23, 24], and to subsequent work on perfect binary arrays, including the construction of a PBA(s,t) for small values of st: [1, 4, 5, 7–9, 16, 20, 25, 26]. For a general background on difference sets, see [3] or [15].

Davis [10, 11] gave a character-theoretic construction, later much simplified by Dillon [12], for a PBA$(2^y, 2^y)$ and a PBA$(2^{y+1}, 2^{y-1})$ $(y\geqslant 1)$. In this paper we give elementary constructions for perfect binary arrays of these sizes, and also construct a PBA$(2^y\cdot 3, 2^y\cdot 3)$ and a PBA$(2^{y+1}\cdot 3, 2^{y-1}\cdot 3)$ $(y\geqslant 1)$. The methods were briefly outlined by Jedwab and Mitchell [16] and Wild [26] (independently of Davis).

The basic idea is to construct a PBA$(2s,2t)$ from a PBA(s,t). The $4st$ entries of the PBA$(2s,2t)$ are made up of the st entries of the PBA(s,t), appearing twice, and the entries of another $s\times t$ binary array, which we call *rowwise quasiperfect* (or RQPBA(s,t)), which appear a second time with opposite sign. A similar construction is used to construct a RQPBA$(2s,2t)$ from a RQPBA(s,t) and another sort of $s\times t$ binary array, called *doubly quasiperfect* (or DQPBA(s,t)).

We prove, under certain conditions on s and t, an equivalence between a RQPBA(s,t) and a DQPBA(s,t). This means we can repeat the construction to obtain a PBA$(4s,4t)$, a RQPBA$(4s,4t)$ and a DQPBA$(4s,4t)$. By iterating the construction, we obtain a PBA$(2^y s, 2^y t)$ for each $y\geqslant 0$. At the same time we construct a PBA$(2^{y+2}s, 2^y t)$. The four families mentioned above are then obtained from a PBA$(1,1)$ and DQPBA$(1,1)$, and from a PBA$(6,6)$ and DQPBA$(6,6)$.

We show that for the size $2^y\times 2^y$ $(y\geqslant 1)$, the recursive construction can be used to obtain a PBA for which the corresponding difference set is fixed by the multiplier -1, and a RQPBA and DQPBA for which certain symmetry properties hold. These properties of the construction have not previously been noted.

The constructions also generate infinite families of rowwise quasiperfect and doubly quasiperfect binary arrays with $2N^2$ elements, for integer N, as shown by Jedwab and Mitchell [17].

2. The construction

Let $A=(a_{ij})$ and $B=(b_{ij})$ be $s\times t$ binary arrays. We define the *periodic cross-correlation function* $R_{AB}(u,v)$ of A and B at displacement (u,v) by

$$R_{AB}(u,v)=\sum_{i=0}^{s-1}\sum_{j=0}^{t-1} a_{ij}b_{i+u,j+v},$$

where, as before, we identify the subscripts with the integers modulo s and modulo t. Note that $R_{BA}(u,v)=R_{AB}(s-u,t-v)$. Define an $s\times 2t$ binary array $C=(c_{ij})=\mathrm{ic}(A,B)$ by

$$c_{i,2j}=a_{ij} \quad \text{and} \quad c_{i,2j+1}=b_{ij} \qquad \text{for all } 0\leqslant i<s \quad \text{and} \quad 0\leqslant j<t.$$

We say C is obtained by *interleaving the columns of A and B*. Similarly, we define a $2s\times t$ binary array $D=(d_{ij})=\mathrm{ir}(A,B)$ obtained by *interleaving the rows of A and B*:

$$d_{2i,j}=a_{ij} \quad \text{and} \quad d_{2i+1,j}=b_{ij} \qquad \text{for all } 0\leqslant i<s \quad \text{and} \quad 0\leqslant j<t.$$

It is straightforward to prove the following lemma.

Lemma 2.1. *Let A and B be $s\times t$ binary arrays. Let $C=\mathrm{ic}(A,B)$ and $D=\mathrm{ir}(A,B)$. Then*

$$R_C(u,2v)=R_A(u,v)+R_B(u,v),$$

$$R_C(u,2v+1)=R_{AB}(u,v)+R_{AB}(s-u,t-v-1),$$

$$R_D(2u,v)=R_A(u,v)+R_B(u,v),$$

$$R_D(2u+1,v)=R_{AB}(u,v)+R_{AB}(s-u-1,t-v)$$

for all $0\leqslant u<s$, $0\leqslant v<t$.

Our aim is to construct perfect binary arrays C and D by interleaving appropriate arrays A and B.

Definition 2.2. Let A and B be $s\times t$ binary arrays. A and B are called *complementary* if

$$R_A(u,v)+R_B(u,v)=0 \quad \text{for all } (u,v)\neq(0,0),$$

and *uncorrelated* if

$$R_{AB}(u,v)=0 \quad \text{for all } u,v.$$

Theorem 2.3. *Let A and B be $s\times t$ binary arrays. Then $C=\mathrm{ic}(A,B)$ is a* PBA$(s,2t)$ *(respectively $D=\mathrm{ir}(A,B)$ is a* PBA$(2s,t)$*) if and only if A and B are complementary arrays such that*

$$R_{AB}(u,v)+R_{AB}(s-u,t-v-1)=0 \quad \textit{for all } u,v$$

$$(\textit{resp. } R_{AB}(u,v)+R_{AB}(s-u-1,t-v)=0 \quad \textit{for all } u,v).$$

Proof. This theorem follows immediately from Definition 2.2 and Lemma 2.1. □

Corollary 2.4. *Let A and B be $s\times t$ binary arrays which are complementary and uncorrelated. Then* $\mathrm{ic}(A,B)$ *is a* PBA$(s,2t)$ *and* $\mathrm{ir}(A,B)$ *is a* PBA$(2s,t)$.

Let $A=(a_{ij})$ and $B=(b_{ij})$ be $s\times t$ binary arrays. Define a $2s\times t$ binary array

$$C=(c_{ij})=\begin{bmatrix}A\\B\end{bmatrix}$$

by

$$c_{ij}=a_{ij} \quad \text{and} \quad c_{i+s,j}=b_{ij} \qquad \text{for all } 0\leqslant i<s \text{ and } 0\leqslant j<t,$$

and an $s\times 2t$ binary array $D=(d_{ij})=[A \;\; B]$ by

$$d_{ij}=a_{ij} \quad \text{and} \quad d_{i,j+t}=b_{ij} \qquad \text{for all } 0\leqslant i<s \text{ and } 0\leqslant j<t.$$

The following lemma, whose proof is straightforward, shows how to construct uncorrelated binary arrays.

Lemma 2.5. *Let A and B be $s\times t$ binary arrays. Then*:
(i) $A'=\left[\begin{smallmatrix}A\\A\end{smallmatrix}\right]$ *and* $B'=\left[\begin{smallmatrix}B\\-B\end{smallmatrix}\right]$ *are uncorrelated,*
(ii) $A''=[A \;\; A]$ *and* $B''=[B \;\; -B]$ *are uncorrelated.*

Definition 2.6. Let B be an $s\times t$ binary array. B is called *rowwise quasiperfect* if

$$B'=\begin{bmatrix}B\\-B\end{bmatrix} \text{ has } R_{B'}(u,v)=0 \quad \text{for all } (u,v)\neq(0,0) \text{ or } (s,0).$$

B is called *columnwise quasiperfect* if

$$B''=[B \;\; -B] \text{ has } R_{B''}(u,v)=0 \quad \text{for all } (u,v)\neq(0,0) \text{ or } (0,t).$$

We write RQPBA(s,t) (respectively CQPBA(s,t)) for an $s\times t$ rowwise (resp. columnwise) quasiperfect binary array.

We shall state the construction theorems involving quasiperfect binary arrays using the rowwise form (as in [16, 17, 26]). Corresponding constructions using the columnwise form can easily be obtained by noting that B is a RQPBA(s,t) if and only if B^{T} is a CQPBA(t,s).

Also note that if $A=(a_{ij})$ and $B=(b_{ij})$ are related by $b_{ij}=(-1)^i a_{ij}$, then for s odd, A is a PBA(s,t) if and only if B is a RQPBA(s,t). The special case $t=1$ of this result is due to Geramita and Seberry [14].

Lemma 2.7. *Let A be a* PBA(s,t) *and B a* RQPBA(s,t). *Then*

$$A'=\begin{bmatrix}A\\A\end{bmatrix} \quad \text{and} \quad B'=\begin{bmatrix}B\\-B\end{bmatrix}$$

are complementary.

Proof. By Definition 2.6,

$$R_{B'}(u,v)=\begin{cases}0 & \text{for all } (u,v)\neq(0,0),\ (s,0),\\ -2st & \text{for } (u,v)=(s,0)\end{cases}$$

and it is simple to show that

$$R_{A'}(u,v)=\begin{cases}0 & \text{for all } (u,v)\neq(0,0),\ (s,0),\\ 2st & \text{for } (u,v)=(s,0).\end{cases}$$

Hence,

$$R_{A'}(u,v)+R_{B'}(u,v)=0 \quad \text{for all } (u,v)\neq(0,0). \qquad \square$$

Theorem 2.8. *If there exist a* PBA(s,t) *and* RQPBA(s,t) *then there exist a* PBA$(2s,2t)$ *and a* PBA$(4s,t)$.

Proof. Suppose A is a PBA(s,t) and B is a RQPBA(s,t). Then

$$A'=\begin{bmatrix}A\\A\end{bmatrix} \quad\text{and}\quad B'=\begin{bmatrix}B\\-B\end{bmatrix}$$

are complementary uncorrelated $2s\times t$ binary arrays, by Lemmas 2.5 and 2.7. Hence ic(A',B') is a PBA$(2s,2t)$ and ir(A',B') is a PBA$(4s,t)$, by Corollary 2.4. $\square$

Example 2.9.

$$A=\begin{bmatrix}+ & +\\ + & -\end{bmatrix}$$

is a PBA(2, 2) and a RQPBA(2, 2). By Theorem 2.8,

$$\mathrm{ic}\left(\begin{bmatrix}A\\A\end{bmatrix},\begin{bmatrix}A\\-A\end{bmatrix}\right)=\begin{bmatrix}+ & + & + & +\\ + & + & - & -\\ + & - & + & -\\ + & - & - & +\end{bmatrix}$$

is a PBA(4, 4), and

$$\mathrm{ir}\left(\begin{bmatrix}A\\A\end{bmatrix},\begin{bmatrix}A\\-A\end{bmatrix}\right)=\begin{bmatrix}+ & + & + & + & + & - & + & -\\ + & + & - & - & + & - & - & +\end{bmatrix}^{\mathrm{T}}$$

is a PBA(8, 2).

3. Quasiperfect binary arrays

Our aim now is to give a construction for rowwise quasiperfect binary arrays similar to Theorem 2.8.

Definition 3.1. Let A and B be $s \times t$ binary arrays. Let

$$A' = \begin{bmatrix} A \\ -A \end{bmatrix} \quad \text{and} \quad B' = \begin{bmatrix} B \\ -B \end{bmatrix}.$$

A and B are called *quasicomplementary* if

$$R_{A'}(u,v) + R_{B'}(u,v) = 0 \quad \text{for all } (u,v) \neq (0,0), (s,0),$$

and *quasiuncorrelated* if A' *and* B' are uncorrelated.

Theorem 3.2. *Let A and B be $s \times t$ binary arrays. Let*

$$A' = \begin{bmatrix} A \\ -A \end{bmatrix} \quad \textit{and} \quad B' = \begin{bmatrix} B \\ -B \end{bmatrix}.$$

Then $C = \mathrm{ic}(A, B)$ is a RQPBA$(s, 2t)$ *(resp. $D = \mathrm{ir}(A, B)$ is a* RQPBA$(2s, t)$*) if and only if A and B are quasicomplementary arrays such that*

$$R_{A'B'}(u,v) + R_{A'B'}(2s-u, t-v-1) = 0 \quad \textit{for all } u, v,$$

$$(\textit{resp. } R_{A'B'}(u,v) + R_{A'B'}(2s-u-1, t-v) = 0 \textit{ for all } u, v).$$

Proof. This theorem follows by applying Lemma 2.1 to

$$C' = \begin{bmatrix} C \\ -C \end{bmatrix} = \mathrm{ic}(A', B')$$

$$(\text{resp. } D' = \begin{bmatrix} D \\ -D \end{bmatrix} = \mathrm{ir}(A', B')). \qquad \square$$

Corollary 3.3. *Let A and B be $s \times t$ binary arrays which are quasicomplementary and quasiuncorrelated. Then* ic(A, B) *is a* RQPBA$(s, 2t)$ *and* ir(A, B) *is a* RQPBA$(2s, t)$.

The following lemma shows how to construct quasiuncorrelated binary arrays.

Lemma 3.4. *Let A and B be $s \times t$ binary arrays. Then*

$$[A \quad A] \quad \textit{and} \quad [B \quad -B]$$

are quasiuncorrelated.

Proof. Apply Lemma 2.5(ii) to

$$\begin{bmatrix} A \\ -A \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} B \\ -B \end{bmatrix}. \qquad \square$$

Definition 3.5. Let C be an $s\times t$ binary array. C is called *doubly quasiperfect* if

$$C'=\begin{bmatrix} C & -C \\ -C & C \end{bmatrix} \text{ has } R_{C'}(u,v)=0 \quad \text{for all } (u,v)\neq(0,0),(s,0),(0,t),(s,t).$$

We write DQPBA(s,t) for an $s\times t$ doubly quasiperfect binary array.

Note that C is DQPBA(s,t) if and only C^{T} is a DQPBA(t,s). Note also that if $B=(b_{ij})$ and $C=(c_{ij})$ are related by $b_{ij}=(-1)^i c_{ij}$ then for t odd, C is a DQPBA(s,t) if and only if B is a RQPBA(s,t).

The proof of the following lemma is similar to the proof of Lemma 2.7.

Lemma 3.6. *Let B be a* RQPBA(s,t) *and C a* DQPBA(s,t). *Then* $[B\ \ B]$ *and* $[C\ \ -C]$ *are quasicomplementary.*

Theorem 3.7. *If there exist a* RQPBA(s,t) *and a* DQPBA(s,t) *then there exist a* RQPBA$(2s,2t)$ *and a* RQPBA$(s,4t)$.

Proof. Suppose B is a RQPBA(s,t) and C is a DQPBA(s,t). Then $B''=[B\ \ B]$ and $C''=[C\ \ -C]$ are quasicomplementary quasiuncorrelated $s\times 2t$ binary arrays, by Lemmas 3.4 and 3.6. Hence ir(B'',C'') is a RQPBA$(2s,2t)$ and ic(B'',C'') is a RQPBA$(s,4t)$, by Corollary 3.3. □

Example 3.8.

$$B=\begin{bmatrix} + & + \\ + & - \end{bmatrix}$$

is a RQPBA$(2,2)$ and

$$C=\begin{bmatrix} + & + \\ + & + \end{bmatrix}$$

is a DQPBA$(2,2)$. By Theorem 3.7,

$$\mathrm{ir}\,([B\ \ B],[C\ \ -C])=\begin{bmatrix} + & + & + & + \\ + & + & - & - \\ + & - & + & - \\ + & + & - & - \end{bmatrix}$$

is a RQPBA$(4,4)$, and

$$\mathrm{ic}\,([B\ \ B],[C\ \ -C])=\begin{bmatrix} + & + & + & + & + & - & + & - \\ + & + & - & + & + & - & - & - \end{bmatrix}$$

is a RQPBA$(2,8)$.

4. Doubly quasiperfect binary arrays

We now give conditions under which the existence of a rowwise quasiperfect binary array is equivalent to the existence of a doubly quasiperfect binary array. This will allow us to use perfect binary arrays and doubly quasiperfect binary arrays as the basic structures of a recursive construction.

Definition 4.1. Let $A=(a_{ij})$ and $B=(b_{ij})$ be $s \times t$ binary arrays and let c be an integer. B is called the c-shear of A if $ct \equiv 0 \pmod{s}$ and

$$b_{ij}=a_{i-cj,j} \quad \text{for all } i,j.$$

Note that if B is the c-shear of A then A is the $(-c)$-shear of B.

Lemma 4.2. *Let A be an $s \times t$ binary array. If B is the c-shear of A then*

$$R_B(u,v)=R_A(u-cv,v) \quad \textit{for all } u,v.$$

Proof.

$$\begin{aligned} R_B(u,v) &= \sum_{i=0}^{s-1}\sum_{j=0}^{t-1} b_{ij}b_{i+u,j+v} \\ &= \sum_{i=0}^{s-1}\sum_{j=0}^{t-1} a_{i-cj,j}a_{i+u-c((j+v)\bmod t),j+v} \\ &= \sum_{i=0}^{s-1}\sum_{j=0}^{t-1} a_{i-cj,j}a_{i+u-cj-cv,j+v} \end{aligned}$$

for all u,v, since $ct \equiv 0 \pmod{s}$. Replacing $i-cj$ by i, for each fixed j, we obtain the result. □

Corollary 4.3. *Let A be a $2s \times 2t$ binary array and let B be the c-shear of A. Then*

$$R_A(u,v)=0 \quad \textit{for all } (u,v) \neq (0,0),\ (s,0),\ (0,t),\ (s,t)$$

if and only if

$$R_B(u,v)=0 \quad \textit{for all } (u,v) \neq (0,0),\ (s,0),\ (0,t),\ (s,t).$$

Proof. This corollary follows from Definition 4.1 and Lemma 4.2. □

Definition 4.4. Let A be an $s \times t$ binary array. Let

$$B=\begin{bmatrix} A & A \\ -A & -A \end{bmatrix}$$

and let $B'=(b'_{ij})$ be the c-shear of B. Define an $s \times t$ binary array $A'=(a'_{ij})$ by $a'_{ij}=b'_{ij}$ for all $0 \leqslant i < s$, $0 \leqslant j < t$. A' is called the c-transform of A.

Theorem 4.5. *Let A be an $s \times t$ binary array and let c satisfy $ct \equiv s \pmod{2s}$. Then A is rowwise quasiperfect if and only if the c-transform of A is doubly quasiperfect.*

Proof. Let

$$B = \begin{bmatrix} A & A \\ -A & -A \end{bmatrix}$$

and let B' be the c-shear of B. From the given form for B,

$$b_{ij} = b_{i,j+t} = -b_{i+s,j} = -b_{i+s,j+t}$$

for all $0 \leqslant i < s$, $0 \leqslant j < t$. By Definition 4.1 this implies that

$$b'_{i+cj,j} = b'_{i+cj+ct,j+t} = -b'_{i+s+cj,j} = -b'_{i+s+cj+ct,j+t}$$

for all $0 \leqslant i < s$, $0 \leqslant j < t$. Hence, using $ct \equiv s \pmod{2s}$,

$$b'_{ij} = -b'_{i,j+t} = -b'_{i+s,j} = b'_{i+s,j+t}$$

for all $0 \leqslant i < s$, $0 \leqslant j < t$. Therefore,

$$B' = \begin{bmatrix} A' & -A' \\ -A' & A' \end{bmatrix},$$

where A' is the c-transform of A. By Corollary 4.3, A is rowwise quasiperfect if and only if A' is doubly quasiperfect. □

We have now established conditions under which rowwise quasiperfect and doubly quasiperfect binary arrays are equivalent.

Corollary 4.6. *If $t/\gcd(s,t)$ is odd then there exists a* RQPBA(s,t) *if and only if there exists a* DQPBA(s,t).

Proof. We note that $ct \equiv s \pmod{2s}$ if and only if $t/\gcd(s,t)$ is odd and c is an odd multiple of $s/\gcd(s,t)$. The result follows from Theorem 4.5. □

Suppose $t/\gcd(s,t)$ is odd and A is a RQPBA(s,t). The above proof gives a procedure for obtaining a DQPBA(s,t) A'. Put

$$B = \begin{bmatrix} A & A \\ -A & -A \end{bmatrix} \quad \text{and} \quad c = s/\gcd(s,t).$$

Form B', the c-shear of B, by cycling column j of B by cj places for $j = 0, \ldots, 2t-1$. Then the first s rows and t columns of B' are A', the c-transform of A.

Example 4.7. Let $s = t = 4$, so $t/\gcd(s,t) = s/\gcd(s,t) = 1$. Let A be the RQPBA$(4,4)$ constructed in Example 3.8. Since $s/\gcd(s,t) = 1$, we cycle column j of the corresponding

B by j places to obtain

$$B' = \begin{bmatrix} + & - & - & + & - & + & + & - \\ + & + & + & + & - & - & - & - \\ + & + & + & + & - & - & - & - \\ + & - & - & + & - & + & + & - \\ - & + & + & - & + & - & - & + \\ - & - & - & - & + & + & + & + \\ - & - & - & - & + & + & + & + \\ - & + & + & - & + & - & - & + \end{bmatrix}.$$

Then

$$A' = \begin{bmatrix} + & - & - & + \\ + & + & + & + \\ + & + & + & + \\ + & - & - & + \end{bmatrix}$$

is a DQPBA(4, 4).

5. Infinite families of perfect binary arrays

The relationship between rowwise quasiperfect and doubly quasiperfect binary arrays described in Corollary 4.6 allows us to restate Theorems 2.8 and 3.7 as follows.

Theorem 5.1. *If there exist a* PBA(s,t) *and a* DQPBA(s,t) *then there exist a* PBA$(2s,2t)$ *and a* DQPBA$(2s,2t)$. *If* $t/\gcd(s,t)$ *is odd, there also exist a* PBA$(4s,t)$ *and a* RQPBA$(s,4t)$.

Corollary 5.2. *If there exist a* PBA(s,t) *and a* DQPBA(s,t) *then there exist a* PBA$(2^y s, 2^y t)$ *and a* DQPBA$(2^y s, 2^y t)$ *for each* $y \geqslant 0$. *If* $t/\gcd(s,t)$ *is odd, there also exist a* PBA$(2^{y+2}s, 2^y t)$ *and a* RQPBA$(2^y s, 2^{y+2}t)$ *for each* $y \geqslant 0$.

Corollary 5.3. *There exist the following infinite famililes of two-dimensional perfect binary arrays*:

$$\text{PBA}(2^y, 2^y), \quad \text{PBA}(2^{y+1}, 2^{y-1}), \quad \text{PBA}(2^y.3, 2^y.3),$$

$$\text{PBA}(2^{y+1}.3, 2^{y-1}.3) \qquad (y \geqslant 1).$$

There exist the following infinite families of doubly quasiperfect and rowwise quasiperfect binary arrays:

$$\mathrm{DQPBA}(2^y,2^y),\quad \mathrm{DQPBA}(2^y.3,2^y.3),\quad \mathrm{RQPBA}(2^{y-1},2^{y+1}),$$
$$\mathrm{RQPBA}(2^{y-1}.3,2^{y+1}.3)\qquad (y\geqslant 1).$$

Proof. There exist a PBA(1,1) and a DQPBA(1,1), and a PBA(6,6) and a DQPBA(6,6) [16]. The existence of the above eight families follows by putting $s=t=1$ and $s=t=6$ in Corollary 5.2, with the exception of a PBA(12,3) and a RQPBA(3,12) (represented by the case $y=1$ of the fourth and eighth families). A PBA(12,3) is given in [9] and therefore, by the remark preceding Lemma 2.7, there exists a RQPBA(3,12). □

As shown by Jedwab and Mitchell [17], we can also use Theorem 3.7 and Corollary 4.6 to prove the following.

Theorem 5.4. *If there exists a* DQPBA$(2t,t)$ *then for each* $y\geqslant 0$ *there exist a* DQPBA$(2^{y+1}t,2^yt)$, *a* RQPBA$(2^{y+1}t,2^{y+2}t)$, *and a* RQPBA$(2^{y+1}t,2^{y+4}t)$.

Corollary 5.5. *There exist the following infinite families of doubly quasiperfect and rowwise quasiperfect binary arrays*:

$$\mathrm{DQPBA}(2^y,2^{y-1}),\quad \mathrm{RQPBA}(2^y,2^{y+1}),\quad \mathrm{RQPBA}(2^y,2^{y+3})\qquad (y\geqslant 1).$$

6. Symmetry properties

If we recursively apply the construction methods of Theorems 2.8 and 3.7 and Corollary 4.6, beginning with the trivial array [+], we can obtain a family of perfect, rowwise quasiperfect and doubly quasiperfect binary arrays of size $2^y\times 2^y$ $(y\geqslant 1)$ with special structure.

Theorem 6.1. *Let* $t=2^y$, *where* $y\geqslant 0$. *There exist arrays* $A=(a_{ij})$, $B=(b_{ij})$ *and* $C=(c_{ij})$, *which are, respectively, a* PBA(t,t), *a* RQPBA(t,t) *and a* DQPBA(t,t), *for which the following properties hold for all* $0\leqslant i,j<t$:

(i) $a_{ij}=a_{t-i,t-j}$,

(ii) $b_{0j}=b_{0,t-j-1}$, $b_{ij}=-b_{t-i,t-j-1}(i\neq 0)$, $b_{ij}=b_{t-i,j}$ $(i\neq 0)$,

(iii) $c_{ij}=c_{i,t-j-1}$, $c_{ij}=c_{t-i-1,j}$.

Proof. We use induction on y. The case $y=0$ is given trivially by $A=B=C=[+]$. Assume that arrays A, B, C with the desired properties exist for some $y\geqslant 0$ and that

$$D'=(d'_{ij})=\begin{bmatrix} C & -C\\ -C & C\end{bmatrix}$$

is the 1-shear of

$$D=(d_{ij})=\begin{bmatrix} B & B \\ -B & -B \end{bmatrix}.$$

From the proof of Theorems 2.8 and 3.7

$$A'=(a'_{ij})=\text{ic}\left(\begin{bmatrix} A \\ A \end{bmatrix}, \begin{bmatrix} B \\ -B \end{bmatrix}\right)$$

is a PBA$(2t,2t)$ and $B'=(b'_{ij})=\text{ir}([B\ \ B],[C\ \ -C])$ is a RQPBA$(2t,2t)$. From the proof of Corollary 4.6, $C'=(c'_{ij})$ is a DQPBA$(2t,2t)$, where

$$E'=(e'_{ij})=\begin{bmatrix} C' & -C' \\ -C' & C' \end{bmatrix}$$

is the 1-shear of

$$E=(e_{ij})=\begin{bmatrix} B' & B' \\ -B' & -B' \end{bmatrix}.$$

Property (i) for A' and property (ii) for B' follow easily from the inductive hypothesis.

We now prove the first part of property (iii) for C'. By definition of E' we must show that for all $0\leqslant i<4t$, $0\leqslant j<2t$,

$$e'_{ij}=-e'_{i,4t-j-1}.$$

Now by Definition 4.1, $e'_{ij}=e_{i-j,j}$ and so this is equivalent to

$$e_{i-j,j}=-e_{i+j+1,4t-j-1}.$$

Replacing $i-j$ by $2i$ and then by $2i+1$, we require that for all $0\leqslant i,j<2t$,

$$e_{2i,j}=-e_{2i+2j+1,4t-j-1} \quad \text{and} \quad e_{2i+1,j}=-e_{2i+2j+2,4t-j-1}.$$

But by construction of B', $E=\text{ir}([D\ \ D],[D'\ \ D'])$ and so this is equivalent to

$$d_{ij}=-d'_{i+j,2t-j-1} \quad \text{and} \quad d'_{ij}=-d_{i+j+1,2t-j-1}.$$

Both of these hold provided $d'_{ij}=-d'_{i,2t-j-1}$ for all $0\leqslant i,j<2t$, since $d_{ij}=d'_{i+j,j}$ by Definition 4.1. By definition of D', this relation is given by (iii). A similar argument gives the second part of property (iii) for C'. □

7. Comments

The parameter set $\{s,t\}$ of every PBA(s,t) and DQPBA(s,t), and the parameter set (s,t) of every RQPBA(s,t), known to the authors, belongs to one of the infinite families constructed in Corollaries 5.3 and 5.5. When st is a power of 2 the only possible values of $\{s,t\}$ for a PBA(s,t) are those of the first two families of Corollary 5.3 [19, 23]. To the authors' knowledge the smallest value of st for which the existence of PBA(s,t) is undecided, using the nonexistence theorems of Turyn [23], Lander [19] and McFarland [21], occurs at $\{s,t\}=\{18,18\}$ and $\{9,36\}$.

The family of perfect binary arrays A constructed in Theorem 6.1 corresponds to a family of Menon difference sets in $\mathbb{Z}_{2^y}\times\mathbb{Z}_{2^y}$ $(y\geqslant 1)$, each of which is fixed by the multiplier -1. Such a family was previously obtained by Dillon [12]. However, the rotational and reflective symmetry properties of the rowwise quasiperfect and doubly quasiperfect binary arrays B and C constructed in Theorem 6.1 have not previously been noted. The arrays C are particularly interesting in this respect, having reflective symmetry about both a horizontal and vertical axis.

The construction methods presented here have recently been generalised in several ways: to perfect binary arrays in any number of dimensions, to perfect arrays with any integer elements, and to Menon difference sets in nonabelian groups. In a different notation, the constructions of Theorems 2.8 and 3.7 can be unified.

Using the definition of relative difference set given in [13] and arguments similar to those used by Chan et al. [9], it can be shown that a nontrivial RQPBA(s,t) is equivalent to a relative difference set in $\mathbb{Z}_{2s}\times\mathbb{Z}_t$ relative to $\langle(s,0)\rangle$ and a nontrivial DQPBA(s,t) is equivalent to a relative difference set in $\mathbb{Z}_{2s}\times\mathbb{Z}_{2t}/\langle(s,t)\rangle$ relative to $\langle(s,0),(0,t)\rangle/\langle(s,t)\rangle$, the parameters in both cases being $(st, 2, st, st/2)$.

Acknowledgment

This work was carried out while the first author was studying for a Mathematics Ph.D. at Royal Holloway and Bedford New College, University of London. The authors thank Sheelagh Lloyd and Miranda Mowbray of HP Labs Bristol, and the referees, for their helpful comments on the manuscript.

References

[1] K.T. Arasu and J. Reis, On abelian groups of order 64 that have difference sets, Tech. Report 1987.10, Wright State Univ., 1987.

[2] L.D. Baumert, Cyclic Difference Sets, Lecture Notes in Mathematics, Vol. 182 (Springer, New York, 1971).

[3] T. Beth, D. Jungnickel and H. Lenz, Design Theory (Cambridge Univ. Press, Cambridge, 1986).

[4] L. Bömer and M. Antweiler, Perfect binary arrays with 36 elements, Electron. Lett. 23 (1987) 730–732.

[5] L. Bömer and M. Antweiler, Two-dimensional perfect binary arrays with 64 elements, IEEE Trans. Inform. Theory 36 (1990) 411–414.

[6] D. Calabro and J.K. Wolf, On the synthesis of two-dimensional arrays with desirable correlation properties, Inform. Control 11 (1968) 537–560.

[7] W.-K. Chan and M.-K. Siu, Authors' correction to 'Summary of perfect $s\times t$ arrays, $1\leqslant s\leqslant t\leqslant 100$', Electron. Lett. 27 (1991) 1112.

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

[9] Y.K. Chan, M.K. Siu and P. Tong, Two-dimensional binary arrays with good autocorrelation, Inform. Control 42 (1979) 125–130.

[10] J. Davis, Difference sets in abelian 2-groups, J. Combin. Theory Ser. A 57 (1991) 262–286.

[11] J. Davis, Difference sets in abelian 2-groups, Ph.D. Thesis, Univ. of Virginia, 1987.

[12] J.F. Dillon, Difference sets in 2-groups, Contemp. Math. 111 (1990) 65–72.

[13] J.E.H. Elliott and A.T. Butson, Relative difference sets, Illinois J. Math. 10 (1966) 517–531.

[14] A.V. Geramita and J. Seberry, Orthogonal Designs: Quadratic forms and Hadamard matrices (Marcel Dekker, New York, 1979).

[15] D.R. Hughes and F.C. Piper, Design Theory (Cambridge Univ. Press, Cambridge, 1985).

[16] J. Jedwab and C.J. Mitchell, Constructing new perfect binary arrays, Electron. Lett. 24 (1988) 650–652.

[17] J. Jedwab and C. Mitchell, Infinite families of quasiperfect and doubly quasiperfect binary arrays, Electron. Lett. 26 (1990) 294–295.

[18] L.E. Kopilovich, On perfect binary arrays, Electron. Lett. 24 (1988) 566–567.

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

[20] H.D. Lüke, L. Bömer and M. Antweiler, Perfect binary arrays, Signal Process. 17 (1989) 69–80·.

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

[22] P.K. Menon, On difference sets whose parameters satisfy a certain relation, Proc. Amer. Math. Soc. 13 (1962) 739–745.

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

[24] R.J. Turyn, Sequences with small correlation, in: H.B. Mann, ed., Error Correcting Codes (Wiley, New York, 1968) 195–228.

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

[26] P. Wild, Infinite families of perfect binary arrays, Electron. Lett. 24 (1988) 845–847.