Barker arrays I — even number of elements

Jonathan Jedwab

Hewlett-Packard Laboratories, Filton Road,

Stoke Gifford, Bristol BS12 6QZ, U.K.

Abstract

A Barker array is a two-dimensional array with elements ± 1 such that all out-of-phase aperiodic autocorrelation coefficients are 0, 1 or -1. No $s \times t$ Barker array with $s, t > 1$ and $(s,t) \neq (2,2)$ is known and it is conjectured that none exists. We define a class of arrays that includes Barker arrays. We prove nonexistence results for this class of arrays in the case st even, providing support for the Barker array conjecture. We demonstrate several connections, in the case st even, between this class of arrays and perfect, quasiperfect and doubly quasiperfect binary arrays.

Keywords Barker array, aperiodic autocorrelation, binary array, nonexistence, perfect, quasi-perfect, doubly quasiperfect.

AMS Subject Classification Primary 05B20, secondary 05B10

Abbreviated title Barker Arrays I

1 Introduction

An $s \times t$ *binary array* is a two-dimensional array (a_{ij}) for which

$$a_{ij} = \begin{cases} 1 \text{ or } -1 & \text{for all } 0 \le i < s, 0 \le j < t \\ 0 & \text{otherwise.} \end{cases}$$

Define the *aperiodic autocorrelation function* of a binary array (a_{ij}) by

$$C(u,v) = \sum_i \sum_j a_{ij} a_{i+u,j+v},$$

where u, v are integers. In this paper, summations will be over all integers unless otherwise stated. We shall write $C_A(u,v)$ to distinguish the aperiodic autocorrelation function of A from that of any other binary array. A binary array is called *Barker* if $|C(u,v)| \le 1$ for all $(u,v) \ne (0,0)$. The array $\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ is Barker, but no Barker array with $s,t > 1$ and $(s,t) \ne (2,2)$ is known. Alquaddoomi and Scholtz [1] conjectured that no such array exists, and proved the necessary conditions that neither s nor t is an odd prime, that st is a square when s or t is even, and that $2st - 1$ is a square when $st \equiv 1 \pmod 4$. Jedwab [6] proved that if s, t are even then $s = t$.

In this paper we define a property of binary arrays which we call *Barker structure*, which any $s \times t$ Barker array with $st > 2$ possesses. For an $s \times t$ binary array with Barker structure, we prove restrictions on the possible values of (s,t), as well as the array elements (a_{ij}), in the cases s,t even and s even, t odd. We also show that any such array is simultaneously perfect and quasiperfect, and that its existence implies the existence of larger arrays with restrictive autocorrelation properties. (For background material on perfect, quasiperfect and doubly quasiperfect arrays, we refer the reader to Jedwab *et al.* [9].)

In a further paper [8] we prove nonexistence results for binary arrays with Barker structure when s,t are odd.

2 Barker structure

Define the *rowwise* and *columnwise semi-periodic autocorrelation function* of an $s \times t$ binary array by

$$P^R(u,v) = C(u,v) + C(u,v-t), \text{ defined on } -s < u < s, 0 \leq v < t, \quad (1)$$

$$P^C(u,v) = C(u,v) + C(u-s,v), \text{ defined on } 0 \leq u < s, -t < v < t \quad (2)$$

respectively. Any expression involving $P^R(u,v)$ or $P^C(u,v)$ (or any other autocorrelation function referred to later in this paper) will implicitly refer only to values of (u,v) for which the function is defined. Given a binary array $A = (a_{ij})$, we call the values

$$x_i = \sum_j a_{ij}, \quad y_j = \sum_i a_{ij}$$

the *row sums* and *column sums* of A respectively. From Lemma 2 of [6] we have:

Lemma 1 *Let A be an $s \times t$ binary array and let (x_i) and (y_j) be respectively the row sums and column sums of A. Then*

$$\begin{aligned} \sum_{v=0}^{t-1} P^R(u,v) &= \sum_i x_i x_{i+u} \text{ for all } u, \\ \sum_{u=0}^{s-1} P^C(u,v) &= \sum_j y_j y_{j+v} \text{ for all } v. \end{aligned}$$

We now define the Barker structure property.

Definition 1 *Let A be an $s \times t$ binary array. A is said to have* Barker structure *if, for all $(u,v) \neq (0,0)$,*

(i) for s,t even,

$$\begin{aligned} P^R(u,v) &= 0, \\ P^C(u,v) &= 0. \end{aligned}$$

(*ii*) *for s even and t odd,*

$$P^R(u,v) = \begin{cases} 0 & \text{for } u \text{ even} \\ k(u) & \text{for } u \text{ odd,} \end{cases}$$

where $k(u) = 1$ *or* -1 *for all* $-s < u < s$, *and* $k(u) + k(u-s) = 0$ *for all* $0 < u < s$,

$$P^C(u,v) = 0.$$

(*iii*) *for* s, t *odd,*

$$P^R(u,v) = \begin{cases} k & \text{for } u \text{ even} \\ 0 & \text{for } u \text{ odd,} \end{cases}$$

$$P^C(u,v) = \begin{cases} k & \text{for } v \text{ even} \\ 0 & \text{for } v \text{ odd,} \end{cases}$$

where $k = 1$ *or* -1 *and* $k \equiv st \pmod 4$.

Theorem 1 (Alquaddoomi and Scholtz [1]) *Let* A *be an* $s \times t$ *Barker array with* $st > 2$. *Then* A *has Barker structure.*

Theorem 1 is implied by equations (21)–(23) of [1]. However we deliberately state the result in weaker form. In fact we shall derive all our results for arrays possessing only Barker structure.

We note some preliminary restrictions on the values of (s,t) for an $s \times t$ binary array with Barker structure.

Theorem 2 (Alquaddoomi and Scholtz [1]) *Let* A *be an* $s \times t$ *binary array with Barker structure. Then there exists a* (v,k,λ)*-difference set in* $\mathbb{Z}_s \times \mathbb{Z}_t$ *with parameters as follows:*

(*i*) *for s or t even,* $st = 4N^2$ *for some integer* N *and* $(v,k,\lambda) = (4N^2, 2N^2 - N, N^2 - N)$

(*ii*) *for* $st \equiv 1 \pmod 4$, $2st - 1 = (2N+1)^2$ *for some integer* N *and* $(v,k,\lambda) = (2N^2 + 2N + 1, N^2, N(N-1)/2)$

(iii) for $st \equiv 3 \pmod 4$*,* $st = 4N - 1$ *for some integer* N *and* $(v, k, \lambda) = (4N - 1, 2N - 1, N - 1)$.

Although Theorem 2 was obtained in [1] only for Barker arrays, the method clearly applies to arrays with Barker structure. The parameters in Theorem 2 (i) and (iii) are those of Menon and Hadamard difference sets respectively. (For a general treatment of difference sets, see [3] or [5].)

We shall obtain further restrictions on the dimensions of an $s \times t$ binary array with Barker structure by applying Lemma 1. This leads to equations in the row and column sums which are necessarily satisfied by such an array. In the following sections we shall examine the cases

(i) s, t even — the equations are straightforward to solve

(ii) s even and t odd — the equations reduce to a familiar unsolved problem.

We investigate the case s, t odd in a further paper [8] in which we do not solve the equations, but obtain conditions on s and t which are necessary for the equations to have a solution.

3 The case s, t even

3.1 Row and column sum equations

We first examine some consequences of the equations in the row and column sums that are necessarily satisfied by an $s \times t$ binary array with Barker structure, where s, t are even. Call an $s \times t$ binary array *positive* if $\sum_i \sum_j a_{ij} \geq 0$. Without loss of generality, we may take a binary array (a_{ij}) with Barker structure to be positive, since $(-a_{ij})$ also has Barker structure.

From Lemma 1 and Definition 1 (i), the row sums (x_i) satisfy

$$\sum_i x_i x_{i+u} = \begin{cases} 0 & \text{for all } u \neq 0 \\ st & \text{for } u = 0. \end{cases} \quad (3)$$

Using these equations and the corresponding equations in the column sums, Jedwab [6] used Lemma 2 to prove Theorem 3.

Lemma 2 *Let (x_i) be the row sums of an $s \times t$ binary array such that (3) is satisfied. Then $s \le t$ and, for some $0 \le I < s$,*

$$x_i = \begin{cases} 0 & \text{for all } i \neq I \\ \pm\sqrt{st} & \text{for } i = I. \end{cases}$$

Theorem 3 *Let A be an $s \times t$ binary array with Barker structure where s, t are even. Let (x_i) and (y_j) be the row and column sums of A. Then $s = t$ and for some $0 \le I < s$, $0 \le J < t$,*

$$\begin{aligned} x_i &= \begin{cases} 0 & \text{for all } i \neq I \\ kt & \text{for } i = I, \end{cases} \\ y_j &= \begin{cases} 0 & \text{for all } j \neq J \\ kt & \text{for } j = J, \end{cases} \end{aligned}$$

where $k = 1$ if A is positive and $k = -1$ otherwise.

We now obtain further conditions on t and (a_{ij}) with the help of the following lemma, whose proof is straightforward. This describes the transformation of the aperiodic and semi-periodic autocorrelation functions under change of sign of alternate rows or columns of a binary array.

Lemma 3 *Let $A = (a_{ij})$, $B = (b_{ij})$, $C = (c_{ij})$ be $s \times t$ binary arrays related by $b_{ij} = (-1)^j a_{ij}$, $c_{ij} = (-1)^i a_{ij}$ for all (i, j). Then for all (u, v),*

(i)

$$\begin{aligned} C_B(u,v) &= (-1)^v C_A(u,v), \\ P_B^R(u,v) &= \begin{cases} (-1)^v P_A^R(u,v) & \text{for } t \text{ even} \\ (-1)^v (C_A(u,v) - C_A(u,v-t)) & \text{for } t \text{ odd}, \end{cases} \\ P_B^C(u,v) &= (-1)^v P_A^C(u,v). \end{aligned}$$

(ii)

$$C_C(u,v) = (-1)^u C_A(u,v),$$

$$
\begin{aligned}
P_C^R(u,v) &= (-1)^u P_A^R(u,v), \\
P_C^C(u,v) &= \begin{cases} (-1)^u P_A^C(u,v) & \textit{for } s \textit{ even} \\ (-1)^u (C_A(u,v) - C_A(u-s,v)) & \textit{for } s \textit{ odd.} \end{cases}
\end{aligned}
$$

We can now establish further conditions on t and (a_{ij}).

Definition 2 *Let $A = (a_{ij})$ be an $s \times t$ binary array. Let (I, I', J, J') be a parameter set such that A has the following properties:*

(i) $0 \le I < s$, $0 \le I' < s$, $0 \le J < t$, $0 \le J' < t$

(ii) $I + I' \equiv J + J' \pmod 2$

(iii) $a_{Ij} = 1$ *for all* $0 \le j < t$

(iv) $a_{I'j} = (-1)^{j+J}$ *for all* $0 \le j < t$

(v) $a_{iJ} = 1$ *for all* $0 \le i < s$

(vi) $a_{iJ'} = (-1)^{i+I}$ *for all* $0 \le i < s$

(vii) $\sum_j a_{i,2j} = \sum_j a_{i,2j+1} = 0$ *for all* $i \ne I, I'$

(viii) $\sum_i a_{2i,j} = \sum_i a_{2i+1,j} = 0$ *for all* $j \ne J, J'$.

A is called balanced *with parameters (I, I', J, J').*

Theorem 4 *Let A be a positive $s \times t$ binary array with Barker structure where s, t are even. Then $s = t$ and A is balanced for some parameters (I, I', J, J'). If $t > 2$ then $t \equiv 0 \pmod 4$.*

Proof From Theorem 3 we have $s = t$ and for some $0 \le I < s$, $0 \le J < t$,

$$\sum_j a_{ij} = 0 \text{ for all } i \ne I, \tag{4}$$

$$\sum_i a_{ij} = 0 \text{ for all } j \ne J. \tag{5}$$

Since A is a positive array, Theorem 3 also gives

$$\begin{aligned} a_{Ij} &= 1 \text{ for all } 0 \le j < t, \\ a_{iJ} &= 1 \text{ for all } 0 \le i < s. \end{aligned} \tag{6}$$

These are balance properties (iii) and (v).

Now define $B = (b_{ij})$ by $b_{ij} = (-1)^j a_{ij}$. From Lemma 3 (i) and Definition 1 (i), B is also an $s \times t$ binary array with Barker structure where s, t are even. Hence, by Theorem 3, for some $0 \le I' < s$, $0 \le X < t$,

$$\sum_j b_{ij} = 0 \text{ for all } i \ne I', \tag{7}$$

$$\sum_i b_{ij} = 0 \text{ for all } j \ne X,$$

$$b_{I'j} = k \text{ for all } 0 \le j < t, \tag{8}$$

$$b_{iX} = k \text{ for all } 0 \le i < s, \tag{9}$$

where $k = \pm 1$. We next determine X and k. Rewrite (8) and (9) in terms of (a_{ij}),

$$a_{I'j} = (-1)^j k \text{ for all } 0 \le j < t, \tag{10}$$

$$a_{iX} = (-1)^X k \text{ for all } 0 \le i < s. \tag{11}$$

By comparing (11) with (5) and (6), we deduce that $X = J$ and $(-1)^X k = 1$, so that $k = (-1)^J$. Substitution in (10) gives

$$a_{I'j} = (-1)^{j+J} \text{ for all } 0 \le j < t, \tag{12}$$

which is balance property (iv).

Similarly, applying Lemma 3 (ii) to $C = (c_{ij})$, where $c_{ij} = (-1)^i a_{ij}$, establishes that for some $0 \le J' < t$,

$$a_{iJ'} = (-1)^{i+I} \text{ for all } 0 \le i < s, \tag{13}$$

which is balance property (vi). The ranges for I, I', J, J' given by Theorem 3 are those of balance property (i). Substitution of $j = J'$ in (12) and $i = I'$ in (13) gives two alternative expressions for $a_{I'J'}$,

$$a_{I'J'} = (-1)^{J'+J} = (-1)^{I'+I},$$

so that for consistency

$$I' + I \equiv J' + J \pmod 2,$$

which is balance property (ii).

Finally, suppose $t > 2$ so that there exists some $0 \le i < t$ for which $i \ne I, I'$. For any such i, from (4) and (7),

$$\begin{aligned} \sum_j a_{ij} &= 0, \\ \sum_j (-1)^j a_{ij} &= 0. \end{aligned}$$

Therefore

$$\sum_j a_{i,2j} = \sum_j a_{i,2j+1} = 0 \text{ for all } i \ne I, I', \tag{14}$$

which is balance property (vii). But $\sum_j a_{i,2j}$ is the sum of exactly $t/2$ non-zero terms, each of which is 1 or -1, so (14) implies that $t/2 \equiv 0 \pmod 2$, or equivalently

$$t \equiv 0 \pmod 4.$$

Balance property $(viii)$ is proved in a similar manner to property (vii). □

3.2 Perfect, quasiperfect and doubly quasiperfect binary arrays

We next show that the existence of an $s \times t$ binary array with Barker structure, where s, t are even, implies the existence of infinite families of binary arrays with restrictive autocorrelation properties.

We define the *periodic, periodic rowwise quasi-, periodic columnwise quasi-* and *periodic doubly quasi-* autocorrelation function of an $s \times t$ binary array on $0 \le u < s$, $0 \le v < t$, respectively

$$R(u,v) = C(u,v) + C(u,v-t) + C(u-s,v) + C(u-s,v-t),$$

$$\begin{aligned} Q^R(u,v) &= C(u,v) + C(u,v-t) - C(u-s,v) - C(u-s,v-t), \\ Q^C(u,v) &= C(u,v) - C(u,v-t) + C(u-s,v) - C(u-s,v-t), \\ D(u,v) &= C(u,v) - C(u,v-t) - C(u-s,v) + C(u-s,v-t). \end{aligned}$$

An $s \times t$ binary array for which the autocorrelation function is 0 for all $(u,v) \neq (0,0)$ is called respectively *perfect, rowwise quasiperfect, columnwise quasiperfect* and *doubly quasiperfect*, written respectively PBA(s,t), RQPBA(s,t), CQPBA(s,t) and DQPBA(s,t). For further details, see Jedwab *et al.* [9] (Wild [17] showed the above definitions to be equivalent to those in [9]).

Lemma 4 *Let A be an $s \times t$ binary array. Then*

$$\begin{aligned} P^R(u,v) &= 0 \textit{ for all } (u,v) \neq (0,0) \\ (\textit{respectively } P^C(u,v) &= 0 \textit{ for all } (u,v) \neq (0,0)) \end{aligned}$$

if and only if

(*i*) *A is a* PBA(s,t) *and*

(*ii*) *A is a* RQPBA(s,t) *(respectively* CQPBA(s,t)*).*

Proof Using (1) we may write, for all (u,v),

$$R(u,v) = \begin{cases} P^R(u,v) + P^R(u-s,v) & \text{for } u \neq 0 \\ P^R(u,v) & \text{for } u = 0, \end{cases}$$

$$Q^R(u,v) = \begin{cases} P^R(u,v) - P^R(u-s,v) & \text{for } u \neq 0 \\ P^R(u,v) & \text{for } u = 0. \end{cases}$$

Then for $(u,v) \neq (0,0)$,

$$P^R(u,v) = 0 \text{ for all } -s < u < s, 0 \leq v < t$$

if and only if

$$R(u,v) = Q^R(u,v) = 0 \text{ for all } 0 \leq u < s, 0 \leq v < t.$$

The second equivalence follows similarly from (2). □

We note that arrays for which $P^C(u,v) = 0$ for all $(u,v) \neq (0,0)$ (*i.e.* which are simultaneously perfect and columnwise quasiperfect) were previously studied under the name *aperiodic perfect* arrays by Lüke *et al.* [11] and, allowing array elements 0 as well as ± 1, by Antweiler *et al.* [2].

Theorem 5 *Let A be an $s \times t$ binary array where s, t are even. Then A has Barker structure if and only if $s = t$ and A is simultaneously a* $\mathrm{PBA}(s,t)$, *a* $\mathrm{RQPBA}(s,t)$ *and a* $\mathrm{CQPBA}(s,t)$.

Proof Immediate from Theorem 3, Lemma 4 and Definition 1 (i). □

The simultaneous autocorrelation properties of A given in Theorem 5 allow the construction of infinite families of perfect, quasiperfect and doubly quasiperfect binary arrays. We note from Corollary 4 of [9] that the existence of a $\mathrm{DQPBA}(s,t)$ is equivalent to the existence of a $\mathrm{RQPBA}(s,t)$ if $t/\gcd(s,t)$ is odd, and to the existence of a $\mathrm{CQPBA}(s,t)$ if $s/\gcd(s,t)$ is odd.

Theorem 6 *Let A be an $s \times t$ binary array with Barker structure where s, t are even. Then there exists each of the following types of array, for each $y \geq 0$:*

$$\mathrm{PBA}(2^y t, 2^y t), \quad \mathrm{PBA}(2^{y+2} t, 2^y t), \quad \mathrm{DQPBA}(2^y t, 2^y t), \quad \mathrm{RQPBA}(2^y t, 2^{y+2} t),$$
$$\mathrm{DQPBA}(2^{y+1} t, 2^y t), \quad \mathrm{RQPBA}(2^{y+1} t, 2^{y+2} t), \quad \mathrm{RQPBA}(2^{y+1} t, 2^{y+4} t).$$

Proof From Theorem 5, A is simultaneously a $\mathrm{PBA}(t,t)$, a $\mathrm{RQPBA}(t,t)$ and a $\mathrm{CQPBA}(t,t)$. The existence of the first four families follows from Corollary 5 of [9]. The existence of the remaining families follows from Theorem 7 of [9], provided there exists a $\mathrm{RQPBA}(2t,t)$. To complete the proof, we now show that if A is simultaneously a $\mathrm{PBA}(s,t)$ and a $\mathrm{RQPBA}(s,t)$ then $B = \begin{bmatrix} A \\ A \end{bmatrix}$ is a $\mathrm{RQPBA}(2s,t)$.

From Lemma 4,

$$P_A^R(u,v) = 0 \text{ for all } (u,v) \neq (0,0).$$

For all $0 \leq u < 2s$, $0 \leq v < t$,

$$P_B^R(u,v) = \sum_{i=0}^{2s-1} \sum_j b_{ij} b_{i+u,(j+v) \bmod t}$$

$$= \sum_{i=0}^{s-1}\sum_j b_{ij}b_{i+u,(j+v)\bmod t} + \sum_{i=0}^{s-1}\sum_j b_{i+s,j}b_{i+s+u,(j+v)\bmod t}. \tag{15}$$

If $u \geq s$ then the second term of (15) is 0 and so

$$\begin{aligned} P_B^R(u,v) &= \sum_{i=0}^{s-1}\sum_j a_{ij}a_{i+u-s,(j+v)\bmod t} \\ &= P_A^R(u-s,v), \end{aligned}$$

whereas if $u < s$ then from (15)

$$\begin{aligned} P_B^R(u,v) &= 2\sum_{i=0}^{s-u-1}\sum_j a_{ij}a_{i+u,(j+v)\bmod t} + \sum_{i=s-u}^{s-1}\sum_j a_{ij}a_{i+u-s,(j+v)\bmod t} \\ &= \begin{cases} 2P_A^R(u,v) + P_A^R(u-s,v) & \text{if } u \neq 0 \\ 2P_A^R(u,v) & \text{if } u = 0. \end{cases} \end{aligned}$$

Therefore for $(u,v) \neq (0,0)$ or $(s,0)$, $P_B^R(u,v) = 0$ and hence $Q_B^R(u,v) = 0$. Also $P_B^R(s,0) = st$ and so $Q_B^R(s,0) = P_B^R(s,0) - P_B^R(0,0) = 0$.

Hence B is rowwise quasiperfect. □

Since the 2×2 array $\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ has Barker structure, we deduce that for $t = 2$ there exists each of the types of array listed in Theorem 6 for each $y \geq 0$, as previously constructed in [9] and [10].

3.3 Nonexistence results for small t

We now pursue the combinatorial constraints given by the balance properties for an $s \times t$ binary array with Barker structure, where s, t are even. We show how these constraints can be combined with the simultaneous autocorrelation properties to establish the nonexistence of such arrays for $t = 4$ and $t = 8$ and, subject to additional constraints on the structure of A, for $t = 12$ and $t = 16$.

Suppose $A = (a_{ij})$ is a positive $s \times t$ binary array with Barker structure where s, t are even and $t > 2$. Then by Theorem 4, $s = t = 4r$ for some r and A is balanced for some parameters (I, I', J, J'). From Theorem 5, A is simultaneously a PBA(t,t), a RQPBA(t,t) and a CQPBA(t,t).

Define $B = (b_{ij})$ by $b_{ij} = a_{i,(j+J)\bmod t}$ for all (i,j). Then it is straightforward to show from Definition 2 that B is balanced with parameters $(I, I', 0, J'')$, where $J'' = (J' - J) \bmod t$, and simple arguments show that B is simultaneously a PBA(t,t) and a RQPBA(t,t). Without loss of generality we may take $0 < J'' \leq t/2$ since $J \neq J'$ and, by Lemma 3 (i), we may if necessary first transform A via $a'_{ij} = (-1)^{i+I} a_{ij}$ for all (i,j) (so that the values of J, J' are interchanged) whilst preserving the Barker structure. Next define $C = (c_{ij})$ by $c_{ij} = b_{(i+I)\bmod t,j}$ for all (i,j). Then C is balanced with parameters $(0, I'', 0, J'')$, where $I'' = (I' - I) \bmod t$, and C is a PBA(t,t). We may similarly take $0 < I'' \leq t/2$. From balance property (ii), $I'' \equiv J'' \pmod 2$.

We therefore use the following algorithm to search for a positive $s \times t$ binary array (a_{ij}) with Barker structure, $s = t = 4r$.

Algorithm 1

(A) *For each pair* (I'', J'') *satisfying* $0 < I'' \leq t/2$, $0 < J'' \leq t/2$, $I'' \equiv J'' \pmod 2$, *generate all possible* $t \times t$ *binary arrays* (c_{ij}) *that are balanced with parameters* $(0, I'', 0, J'')$.

(B) *Retain only those arrays* (c_{ij}) *that are perfect.*

(C) *For each* $0 \leq I < t$ *and each array* (c_{ij}) *remaining from Step* (B), *let* $b_{ij} = c_{(i-I)\bmod t,j}$ *for all* (i,j) *and retain only those arrays* (b_{ij}) *that are rowwise quasiperfect.*

(D) *For each* $0 \leq J < t$ *and each array* (b_{ij}) *remaining from Step* (C), *let* $a_{ij} = b_{i,(j-J)\bmod t}$ *for all* (i,j) *and retain only those arrays* (a_{ij}) *that are columnwise quasiperfect.*

For each pair (I'', J''), Step (A) is implemented as the following branching algorithm, which fixes successive elements of the array so that at each stage no balance property is violated.

Algorithm 2

(A) *Set*

$$a_{0j} = 1, a_{I''j} = (-1)^j \quad \text{for all } 0 \leq j < t,$$

$$a_{i0} = 1, a_{iJ''} = (-1)^i \quad \text{for all } 0 \leq i < t.$$

(*B*) *If there exists an* (i, j) *for which* a_{ij} *is not yet set then branch, setting* $a_{ij} = 1$ *for one branch and* $a_{ij} = -1$ *for the other branch. Otherwise output* (a_{ij}) *and terminate this branch.*

(*C*) *If either of the balance properties* (*vii*) *and* (*viii*) *determines consistently the value of one or more unset array elements, set these elements accordingly and go to Step* (*C*). *If however balance properties* (*vii*) *and* (*viii*) *lead to an inconsistent assignment of unset array elements, discard* (a_{ij}) *and terminate this branch. If no unset array elements are determined go to Step* (*B*).

For the case $t = 4$ Algorithm 1 was implemented by hand, whereas for the case $t = 8$ computer search was used. In both cases all arrays remaining after Step (B) had $I'' = J'' = t/2$, and no array remained after Step (C). Therefore for $t = 4, 8$ there is no perfect and rowwise quasiperfect balanced $t \times t$ binary array. This implies:

Proposition 1 *There is no* 4×4 *or* 8×8 *binary array with Barker structure.*

(Although for $t = 4, 8$ there does not exist a perfect and rowwise quasiperfect balanced $t \times t$ binary array, we note that for $t = 2^r$ and for each $r \geq 1$ there exists a perfect $t \times t$ binary array that is balanced with parameters $(0, t/2, 0, t/2)$. Such a family of arrays can be obtained using the recursive construction of Theorem 8 of [9].)

The cases $t = 12, 16$ contain too many possibilities to allow exhaustive search using Algorithm 1, but we can prove nonexistence subject to additional constraints on the elements (a_{ij}).

Given $s \times t$ binary arrays $A = (a_{ij})$, $B = (b_{ij})$, define the *columnwise interleaving* of A with B to be the $2s \times t$ binary array $C = (c_{ij}) = \mathrm{ic}(A, B)$ given by

$$c_{i,2j} = a_{ij}, \quad c_{i,2j+1} = b_{ij} \quad \text{for all } (i, j).$$

We observe that in the cases $t = 4, 8$ each array remaining after Step (B) of Algorithm 1 is of *interleaved form*, namely $\mathrm{ic}\left(\begin{bmatrix} X \\ X \end{bmatrix}, \begin{bmatrix} Y \\ -Y \end{bmatrix}\right)$, for some component arrays X, Y. If we assume

A to have interleaved form, we can derive necessary conditions on the component arrays X, Y from the balance and autocorrelation properties of A.

Definition 3 *Let $A = (a_{ij})$ be an $s \times t$ binary array. Let (I, J, J') be a parameter set such that A has the following properties:*

(i) $0 \le I < s$, $0 \le J < t$, $0 \le J' < t$

(ii) $a_{Ij} = 1$ *for all* $0 \le j < t$

(iii) $a_{iJ} = 1$ *for all* $0 \le i < s$

(iv) $a_{iJ'} = (-1)^{i+I}$ *for all* $0 \le i < s$

(v) $\sum_j a_{ij} = 0$ *for all* $i \ne I$

(vi) $\sum_i a_{2i,j} = \sum_i a_{2i+1,j} = 0$ *for all* $j \ne J, J'$.

A is called partially balanced *with parameters (I, J, J').*

Note that an $s \times t$ binary array that is balanced for some parameters (I, I', J, J') is partially balanced with parameters (I, J, J').

Theorem 7 *Let A be a positive $s \times t$ binary array with Barker structure where s, t are even and $t > 4$. Let A be of interleaved form with component arrays X and $Y = (y_{ij})$. Then $s = t = 8r$ for some r, X is partially balanced for some parameters (L, K, K'), and X is simultaneously a* $\mathrm{PBA}(4r, 4r)$ *and a* $\mathrm{CQPBA}(4r, 4r)$*. Also*

$$y_{Lj} \quad = \quad k \text{ for all } 0 \le j < 4r,$$

where $k = 1$ or -1,

$$\sum_j y_{ij} \quad = \quad 0 \text{ for all } i \ne L,$$

and Y is simultaneously a $\mathrm{RQPBA}(4r, 4r)$ *and a* $\mathrm{DQPBA}(4r, 4r)$*.*

Proof (Outline) By Theorem 4, $s = t = 4r'$ for some r' and A is balanced for some parameters (I, I', J, J'). The partial balance properties of X and the constraints on Y are derived directly from the balance properties of A. The constraint $r' \equiv 0 \pmod 2$ follows from partial balance property (vi) of X, using an argument similar to that at the end of the proof of Theorem 4. By Theorem 5, A is simultaneously a PBA(t, t) and a CQPBA(t, t). The autocorrelation properties of X and Y are then given by the following partial converse to Theorems 2 and 4 of [9], which is straightforward to verify. Assuming A has interleaved form with component arrays X and Y, if A is perfect then X is perfect and Y is rowwise quasiperfect, and if A is columnwise quasiperfect then X is columnwise quasiperfect and Y is doubly quasiperfect. □

Assume that A has interleaved form. By Proposition 1 and Theorem 7, the smallest case is $t = 16$, for which the component array X has size 8×8. We see from Theorem 7 that the partial balance and autocorrelation properties required of X are weaker than those previously required of A. Nevertheless, a search procedure similar to that of Algorithms 1 and 2 shows that there is no perfect and columnwise quasiperfect 8×8 partially balanced binary array. (In fact the set of 8×8 perfect binary arrays that are partially balanced with parameters $(0, 0, K'')$, for each $0 < K'' \leq 4$, is no larger than that remaining after Step (B) of Algorithm 1, despite the relaxation in balance conditions.) We therefore have the following result.

Proposition 2 *There is no* 16×16 *binary array of interleaved form with Barker structure.*

Finally, we drop the assumption that A has interleaved form. Consideration of the balance and autocorrelation properties that are required with respect to both the rows and the columns of A suggests that restriction of the search to symmetric arrays might be helpful. Indeed, in the cases $t = 4, 8$ the set of arrays remaining after Step (B) of Algorithm 1 contains a large subset of symmetric arrays. It is straightforward to modify Algorithms 1 and 2 to search for a symmetric positive $4r \times 4r$ binary array with Barker structure. Computer search for the case $t = 12$ shows there is no symmetric perfect balanced 12×12 binary array. This implies the following result.

Proposition 3 *There is no symmetric* 12×12 *binary array with Barker structure.*

We conclude this section by summarising the main results for the case s, t even.

Theorem 8 *Let* A *be an* $s \times t$ *binary array with Barker structure where* s, t *are even. Then* $s = t$*,* A *is simultaneously a* $\mathrm{PBA}(t,t)$*, a* $\mathrm{RQPBA}(t,t)$ *and a* $\mathrm{CQPBA}(t,t)$*, and there exists each of the following types of array, for each* $y \geq 0$*:*

$$\mathrm{PBA}(2^y t, 2^y t), \quad \mathrm{PBA}(2^{y+2} t, 2^y t), \quad \mathrm{DQPBA}(2^y t, 2^y t), \quad \mathrm{RQPBA}(2^y t, 2^{y+2} t),$$
$$\mathrm{DQPBA}(2^{y+1} t, 2^y t), \quad \mathrm{RQPBA}(2^{y+1} t, 2^{y+2} t), \quad \mathrm{RQPBA}(2^{y+1} t, 2^{y+4} t).$$

If $t > 2$ *then* $t \equiv 0 \pmod 4$ *and* $t \geq 12$*. If* A *is a positive array then* A *is balanced for some parameters* (I, I', J, J')*. If* A *is symmetric then* $t \geq 16$*. If* A *is of interleaved form then* $t \equiv 0 \pmod 8$ *and* $t \geq 24$*.*

The nonexistence of a $\mathrm{PBA}(t,t)$ with $t \equiv 0 \pmod 4$ in the range $t \leq 100$ has been shown by McFarland for $t = 28, 44, 76, 92$ [12] and for $t = 84$ [13]. Therefore there does not exist a $t \times t$ binary array with Barker structure for these values of t.

4 The case s even, t odd

In this section we use methods similar to those of Section 3 to deduce restrictions on an $s \times t$ binary array with Barker structure, where s is even and t is odd.

From Lemma 1 and Definition 1 (ii), the row sums (x_i) and column sums (y_j) satisfy

$$\sum_i x_i x_{i+u} = \begin{cases} 0 & \text{for all } u \text{ even and } u \neq 0 \\ k(u)\, t & \text{for all } u \text{ odd} \\ st & \text{for } u = 0, \end{cases} \tag{16}$$

where $k(u) = 1$ or -1 for all $-s < u < s$, and $k(u) + k(u - s) = 0$ for all $0 < u < s$,

$$\sum_j y_j y_{j+v} = \begin{cases} 0 & \text{for all } v \neq 0 \\ st & \text{for } v = 0. \end{cases} \tag{17}$$

The solution of equations (17) is given by Lemma 2. We now show that if equations (16) have a solution then there exists a Barker sequence of length s. We refer the reader to [7] for a summary of results on Barker sequences. We note in particular that the only known even lengths for a Barker sequence are 2 and 4, and that any length $s > 13$ must satisfy $s = 4S^2$ for some odd S, where S is not a prime power and $S \geq 689$ [4], [7], [15], [16]. We also note that Ryser's conjecture [14] on cyclic difference sets, if true, would imply that there is no even length Barker sequence of length $s > 4$.

Lemma 5 *Let $s \geq 2$ and $(x_i : 0 \leq i < s)$ be integers and let p be a prime. Let*

$$p \,|\, \sum_i x_i x_{i+u} \text{ for all } 0 < u < s. \tag{18}$$

Then $p \not| \, x_i$ for at most one $0 \leq i < s$.

Proof We use induction on s. The case $s = 2$ is equivalent to

$$p \,|\, x_0 x_1 \quad \Rightarrow \quad p \,|\, x_0 \text{ or } p \,|\, x_1,$$

which is true because p is prime. Assume now that the result is true for the case $s - 1$. Taking $u = s - 1$ in (18), we have $p \,|\, x_0 x_{s-1}$. Since p is prime, without loss of generality

$$p \,|\, x_{s-1}. \tag{19}$$

Then from (18),

$$p \,|\, \sum_{i=0}^{s-u-2} x_i x_{i+u} \text{ for all } 0 < u < s - 1.$$

By the inductive hypothesis, $p \not| \, x_i$ for at most one $0 \leq i < s - 1$. Together with (19), this establishes the result for the case s and the induction is complete. □

Theorem 9 *Let (x_i) be the row sums of an $s \times t$ binary array where s is even and t is odd. Suppose (x_i) satisfy (16), where $k(u) = 1$ or -1 for all $-s < u < s$. Then $t = T^2$ for some odd T and there exists a Barker sequence (z_i) of length s satisfying $x_i = T z_i$ for all i.*

Proof Let p be a prime dividing t. From (16) we see that

$$p \,|\, \sum_i x_i x_{i+u} \text{ for all } 0 \le u < s. \tag{20}$$

Therefore by Lemma 5, $p \not| \, x_i$ for at most one $0 \le i < s$. Taking $u = 0$ in (20) then shows that $p \,|\, x_i$ for all $0 \le i < s$. Write $x_i = p x'_i$ for all i and $t = p^2 t'$, so that (16) becomes

$$\sum_i x'_i x'_{i+u} = \begin{cases} 0 & \text{for all } u \text{ even and } u \ne 0 \\ k(u)\, t' & \text{for all } u \text{ odd} \\ st' & \text{for } u = 0. \end{cases}$$

The equations for (x'_i) have the same form as (16) so we may apply the above argument repeatedly to each prime factor of t. This leads to

$$t = T^2 \text{ for some odd } T, \quad x_i = T z_i \text{ for all } i, \tag{21}$$

where (z_i) satisfies

$$\sum_i z_i z_{i+u} = \begin{cases} 0 & \text{for all } u \text{ even and } u \ne 0 \\ k(u) & \text{for all } u \text{ odd} \\ s & \text{for } u = 0, \end{cases} \tag{22}$$

and where $k(u) = 1$ or -1 for all $-s < u < s$. Taking $u = 0$ in (22),

$$\sum_{i=0}^{s-1} z_i^2 = s. \tag{23}$$

Write the array as (a_{ij}). Now t is odd and so from (21),

$$z_i = x_i / T = \sum_{j=0}^{t-1} a_{ij}/T \ne 0 \text{ for all } 0 \le i < s.$$

Therefore (23) implies that $z_i = 1$ or -1 for all $0 \le i < s$. Hence (z_i) is a binary sequence of length s satisfying (22), which are the defining equations for a Barker sequence of even length. □

Corollary 1 *Let A be an $s \times t$ binary array with Barker structure where s is even and t is odd. Let (x_i) and (y_j) be the row and column sums of A. Then $s = 4S^2$ and $t = T^2$ for some odd S, T*

where S is not a prime power, $2S > T$, and if $S > 1$ then $S \geq 689$. Furthermore there exists a Barker sequence (z_i) of length s satisfying

$$x_i = Tz_i \text{ for all } i.$$

For some $0 \leq J < t$,

$$y_j = \begin{cases} 0 & \text{for all } j \neq J \\ 2kST & \text{for } j = J, \end{cases}$$

where $k = 1$ if A is positive and $k = -1$ otherwise.

Proof (x_i) and (y_j) satisfy equations (16) and (17) respectively. Applying Lemma 2 to equations (17), $s \geq t$ and for some $0 \leq J < t$,

$$y_j = \begin{cases} 0 & \text{for all } j \neq J \\ \pm\sqrt{st} & \text{for } j = J. \end{cases} \tag{24}$$

Since s is even and t is odd, $s \geq t$ becomes

$$s > t. \tag{25}$$

Applying Theorem 9 to equations (16),

$$t = T^2 \tag{26}$$

for some odd T, and there exists a Barker sequence (z_i) of length s satisfying

$$x_i = Tz_i \text{ for all } i.$$

Using the quoted results on Barker sequences, either $s = 2$ (but then $t = 1$ from (25) and, trivially, no array A with the required properties exists) or else

$$s = 4S^2 \tag{27}$$

for some odd S where S is not a prime power, and if $S > 1$ then $S \geq 689$. Substitution of (26) and (27) in (24) and (25) gives the result. □

Taking the value $S = 1$ in Corollary 1 gives the parameter values for a Barker sequence of length 4. The existence of an array of the desired type with $S > 1$ implies the existence of an unknown Barker sequence.

Using a similar method to the proof of Theorem 3, we can obtain the following additional restrictions on (a_{ij}).

Lemma 6 *Let $A = (a_{ij})$ be an $s \times t$ binary array with Barker structure where $s = 4S^2$ is even and $t = T^2$ is odd. Then for some $0 \leq J < t$,*

$$\begin{aligned} \sum_i a_{2i,j} = \sum_i a_{2i+1,j} &= 0 \text{ for all } j \neq J, \\ \left\{ \sum_i a_{2i,J}, \sum_i a_{2i+1,J} \right\} &= \{0, 2kST\}, \\ \sum_j a_{ij} &= Tz_i \text{ for all } i, \end{aligned} \tag{28}$$

where $k = 1$ if A is positive and $k = -1$ otherwise, and (z_i) is a Barker sequence of length s.

Let $B = (b_{ij})$ be the $s \times t$ binary array related to A by $b_{ij} = (-1)^j a_{ij}$ for all (i, j). If B has Barker structure then constraints (28) strengthen to

$$\left\{ \sum_j a_{i,2j}, \sum_j a_{i,2j+1} \right\} = \{0, Tz_i\} \text{ for all } i. \tag{29}$$

(The reason that (29) depends on B having Barker structure is that the value of $P^R(u, v)$ does not change in a simple way under the transformation $b_{ij} = (-1)^j a_{ij}$ when t is odd. If A is an $s \times t$ Barker array with $st > 2$ then the condition on B certainly holds.)

We finally show that the existence of an $s \times t$ binary array with Barker structure, where s is even and t is odd, implies the existence of certain perfect and quasiperfect binary arrays.

Theorem 10 *Let A be an $s \times t$ binary array with Barker structure where s is even and t is odd. Then A is simultaneously a* PBA(s, t) *and a* CQPBA(s, t)*, and there exist a* PBA$(2s, 2t)$*, a* PBA$(s, 4t)$ *and a* CQPBA$(s, 2t)$*.*

Proof By Lemma 4 and Definition 1 (ii), A is simultaneously a PBA(s,t) and a CQPBA(s,t). Then from Theorem 2 of [9], there exist a PBA$(2s,2t)$ and a PBA$(s,4t)$. Following the proof of Theorem 6, $\begin{bmatrix} A & A \end{bmatrix}$ is a CQPBA$(s,2t)$. □

We note from Corollary 1 that $s = 4S^2$ for some odd S, so we cannot deduce the existence of a doubly quasiperfect binary array from the existence of a CQPBA(s,t) or a CQPBA$(s,2t)$ using Corollary 4 of [9].

We conclude this section by summarising the main results for the case s even and t odd.

Theorem 11 *Let A be an $s \times t$ binary array with Barker structure where s is even and t is odd. Then $s = 4S^2$ and $t = T^2$ for some odd S, T where S is not a prime power, $2S > T$, and if $S > 1$ then $S \geq 689$. A is simultaneously a* PBA(s,t) *and a* CQPBA(s,t)*, and there exist a* PBA$(2s,2t)$*, a* PBA$(s,4t)$ *and a* CQPBA$(s,2t)$*. There exists a Barker sequence of length s.*

We remark that in the case s even and t odd, Alquaddoomi and Scholtz's conjecture on the nonexistence of Barker arrays with $s, t > 1$ and $(s,t) \neq (2,2)$ would be implied by Ryser's conjecture applied to Barker sequences, if the latter were true.

5 Comments

If A is an $s \times t$ Barker array with $st > 2$ then A has Barker structure. The results of Theorems 8 and 11 seem to provide good reason to doubt the existence of an $s \times t$ binary array with Barker structure where $st > 4$ is even. In the case s, t even, the simultaneous autocorrelation properties required appear highly restrictive. In the case s even, t odd, the existence of such an array would disprove Ryser's long-standing conjecture on cyclic difference sets.

The smallest even value of $st > 4$ for which $t > 1$ and the nonexistence of an $s \times t$ binary array with Barker structure has not been determined occurs for s, t even at $(s,t) = (12,12)$ and for s even, t odd at $(s,t) = (4.689^2, 9)$.

We consider the case s, t odd in a further paper [8].

6 Acknowledgements

This work was carried out while studying for a Mathematics PhD at Royal Holloway and Bedford New College, University of London. I am very grateful to Fred Piper, Chris Mitchell and Peter Wild of RHBNC, and to Sheelagh Lloyd and Miranda Mowbray of HP Labs Bristol, for their invaluable assistance and encouragement throughout my research and for contributing many helpful ideas and comments to this paper.

References

[1] S. ALQUADDOOMI AND R.A. SCHOLTZ, *On the nonexistence of Barker arrays and related matters*, IEEE Trans. Inform. Theory, 35 (1989), pp. 1048–1057.

[2] M.F.M. ANTWEILER, L. BÖMER, AND H.-D. LÜKE, *Perfect ternary arrays*, IEEE Trans. Inform. Theory, 36 (1990), pp. 696–705.

[3] T. BETH, D. JUNGNICKEL, AND H. LENZ, *Design Theory*, Cambridge University Press, Cambridge, 1986.

[4] S. ELIAHOU, M. KERVAIRE, AND B. SAFFARI, *A new restriction on the lengths of Golay complementary sequences*, J. Combin. Theory (A), 55 (1990), pp. 49–59.

[5] D.R. HUGHES AND F.C. PIPER, *Design Theory*, Cambridge University Press, Cambridge, 1985.

[6] J. JEDWAB, *Nonexistence results for Barker arrays*, The Institute of Mathematics and its Applications Conference Series (New Series) No. 33: Cryptography and Coding II, Oxford University Press, New York, 1992, pp. 121–126.

[7] J. JEDWAB AND S. LLOYD, *A note on the nonexistence of Barker sequences*, Designs, Codes and Cryptography, 2 (1992), pp. 93–97.

[8] J. JEDWAB, S. LLOYD, AND M. MOWBRAY, *Barker arrays II — odd number of elements*, SIAM J. Discrete Math., to appear.

[9] J. JEDWAB, C. MITCHELL, F. PIPER, AND P. WILD, *Perfect binary arrays and difference sets*, 1991, submitted.

[10] J. JEDWAB AND C.J. MITCHELL, *Infinite families of quasiperfect and doubly quasiperfect binary arrays*, Electron. Lett., 26 (1990), pp. 294–295.

[11] H.D. LÜKE, L. BÖMER, AND M. ANTWEILER, *Perfect binary arrays*, Signal Processing, 17 (1989), pp. 69–80.

[12] R.L. McFARLAND, *Necessary conditions for Hadamard difference sets*, The IMA Volumes in Mathematics and its Applications, Vol 21: Coding Theory and Design Theory, Springer-Verlag, New York, 1990, pp. 257–272.

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

[14] H.J. RYSER, *Combinatorial Mathematics*, Carus Mathematical Monographs No. 14, Mathematical Association of America, Washington, DC, 1963.

[15] R.J. TURYN, *Character sums and difference sets*, Pac. J. Math., 15 (1965), pp. 319–346.

[16] R.J. TURYN, *Sequences with small correlation*, H.B. Mann, ed., Error Correcting Codes, Wiley, New York, 1968, pp. 195–228.

[17] P. WILD, *Infinite families of perfect binary arrays*, Electron. Lett., 24 (1988), pp. 845–847.