PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 00, Number 0, Pages 000–000
S 0002-9939(XX)0000-0

# PROOF OF THE BARKER ARRAY CONJECTURE

JAMES A. DAVIS, JONATHAN JEDWAB, AND KEN W. SMITH

(Communicated by John R. Stembridge)

ABSTRACT. Using only elementary methods, we prove Alquaddoomi and Scholtz's conjecture of 1989, that no $s \times t$ Barker array having $s, t > 1$ exists except when $s = t = 2$.

## 1. INTRODUCTION

Binary sequences and arrays whose out-of-phase aperiodic autocorrelations are collectively small are particularly useful in digital communication systems, especially synchronisation and radar. The search for such sequences and arrays dates from the 1950s [2], [16] and continues to the present day [7], [9], [13], [14]. We define an $s \times t$ *array* to be a two-dimensional array $(a_{ij})$ of complex-valued elements satisfying

$$a_{ij} = 0 \quad \text{unless } 0 \leq i < s \text{ and } 0 \leq j < t.$$

The array is *binary* if all nonzero elements $a_{ij}$ take values in $\{1, -1\}$. The *aperiodic autocorrelation function* of an $s \times t$ array $A = (a_{ij})$ is given by

$$C_A(u, v) = \sum_i \sum_j a_{ij} \overline{a_{i+u,j+v}} \quad \text{for integer } u,\ v \text{ satisfying } |u| < s \text{ and } |v| < t.$$

We refer to an $s \times 1$ array as a *sequence of length* $s$, abbreviating the array $(a_{i0})$ to $(a_i)$ and its aperiodic autocorrelation function $C_A(u, 0)$ to $C_A(u)$.

Alquaddoomi and Scholtz [1] defined an $s \times t$ *Barker array* to be an $s \times t$ binary array $A$ for which

$$|C_A(u, v)| \leq 1 \quad \text{for all } (u, v) \neq (0, 0).$$

This generalises the notion of a *Barker sequence* from one dimension (the case $s = 1$ or $t = 1$) to two dimensions; see [10] and [11] for recent nonexistence results for Barker sequences. The $2 \times 2$ array $\begin{bmatrix} + & + \\ + & - \end{bmatrix}$ is a Barker array, but it is conjectured that there are no other sizes for a (truly two-dimensional) Barker array:

Received by the editors 25 October 2005 (revised 9 March 2006).

2000 *Mathematics Subject Classification.* Primary 05B10, Secondary 94A99.

*Key words and phrases.* Barker array, difference set, relative difference set, perfect array, quasiperfect array.

Grant # MDA904-03-1-0032 (NSA).

Grant # 31-611394 (NSERC Canada).

Sabbatical support from Central Michigan University and the gracious hospitality of the University of Richmond.

**Conjecture 1.1** (Alquaddoomi and Scholtz 1989 [1]). *If an $s \times t$ Barker array exists for $s, t > 1$ then $s = t = 2$.*

In this paper we prove Conjecture 1.1 using only elementary methods. We include short proofs of key auxiliary results obtained elsewhere, in order to make the paper self-contained. Theorem 1.2 summarises the previous state of knowledge regarding Conjecture 1.1.

**Theorem 1.2** (Jedwab [6], Jedwab, Lloyd and Mowbray [8]). *Let $A$ be an $s \times t$ Barker array with $s, t > 1$. Then*

Case 1. $s, t$ even: $s = t$. *If $t > 2$ then $t \equiv 0 \pmod 4$ and $t \geq 12$.*
Case 2. $s$ even, $t > 1$ odd: $s > t$. *$s = 4S^2$ and $t = T^2$ for integers $S, T$. There exists a Barker sequence of length $s$.*
Case 3. $s, t > 1$ odd: $st \geq 3^{11}$. *Write $t = \prod_j p_j^{\alpha_j}$, where the $\{p_j\}$ are distinct primes and $\alpha_j \geq 1$ for all $j$. Then $\alpha_j \geq 2$ for all $j$ and $\alpha_k > 2$ for some $k$. If $st \equiv 1 \pmod 4$ then $p_j \equiv 1 \pmod 4$ for all $j$.*

Following [1], define the following function for an $s \times t$ array $A = (a_{ij})$:

$$P_A(u, v) = C_A(u, v) + C_A(u, v - t) \quad \text{for } -s < u < s \text{ and } 0 \leq v < t. \tag{1.1}$$

Any expression involving $P_A(u, v)$ or $C_A(u, v)$ will implicitly refer only to values of $(u, v)$ for which the function is defined. In terms of the array elements $a_{ij}$ we have

$$P_A(u, v) = \sum_i \sum_{j=0}^{t-1} a_{ij} \overline{a_{i+u,(j+v) \bmod t}}. \tag{1.2}$$

Alquaddoomi and Scholtz [1] established Lemma 1.3 for binary arrays, and then used it to prove Proposition 1.4 for Barker arrays. This generalised the approach taken by Tuyrn and Storer in their classical paper [15] on the one-dimensional (sequence) case.

**Lemma 1.3** (Alquaddoomi and Scholtz [1]). *Let $A$ be an $s \times t$ binary array. Then*

$$P_A(u, v) \equiv P_A(u, v') \pmod 4 \quad \textit{for all } (u, v, v').$$

*Proof.* Let $u, v, v'$ satisfy $-s < u < s$ and $0 \leq v, v' < t$. From (1.2), $P_A(u, v)$ is the sum of $(s - |u|)t$ nonzero terms, of which exactly $[(s - |u|)t - P_A(u, v)]/2$ are $-1$ and $[(s - |u|)t + P_A(u, v)]/2$ are $+1$. But from (1.2), the product of these nonzero terms is independent of $v$. Therefore

$$(-1)^{[(s-|u|)t - P_A(u,v)]/2}$$

is independent of $v$, which implies $P_A(u, v) \equiv P_A(u, v') \pmod 4$. □

**Proposition 1.4** (Alquaddoomi and Scholtz [1]). *Let $A$ be an $s \times t$ Barker array with $st > 2$. Then*

Case 1. $s, t$ even:

$$P_A(u, v) = 0 \quad \textit{for } (u, v) \neq (0, 0).$$

Case 2. $s$ even and $t$ odd:

$$\begin{aligned} P_{A^T}(v, u) &= 0 \quad \textit{for } (u, v) \neq (0, 0), \\ P_A(u, v) &= \begin{cases} 0 & \textit{for } u \textit{ even and } (u, v) \neq (0, 0) \\ k(u) & \textit{for } u \textit{ odd,} \end{cases} \end{aligned}$$

*where $k(u) = 1$ or $-1$.*

Case 3. $s, t$ odd:

$$P_A(u,v) = \begin{cases} k & \textit{for } u \textit{ even and } (u,v) \neq (0,0) \\ 0 & \textit{for } u \textit{ odd,} \end{cases}$$

*where* $k = 1$ *or* $-1$.

*Proof.* For all $u, v$ satisfying $|u| < s$ and $|v| < t$, $C_A(u,v)$ is the sum of $(s-|u|)(t-|v|)$ nonzero terms, each of which is $\pm 1$. Therefore $C_A(u,v) \equiv (s+u)(t+v) \pmod 2$. The Barker array property then implies

$$C_A(u,v) = \pm(((s+u)(t+v)) \bmod 2) \quad \text{for } (u,v) \neq (0,0). \tag{1.3}$$

*Case* 1. *$s, t$ even:* From (1.3) we have

$$C_A(u,v) = 0 \quad \text{for } u \text{ or } v \text{ even and } (u,v) \neq (0,0).$$

Then by (1.1),

$$P_A(u,v) = 0 \quad \text{for } u \text{ or } v \text{ even and } (u,v) \neq (0,0).$$

Lemma 1.3 then implies that

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

*Case* 2. *$s$ even, $t$ odd:* From (1.3) we have

$$C_A(u,v) = \pm((u(1+v)) \bmod 2) \quad \text{for } (u,v) \neq (0,0). \tag{1.4}$$

It follows from (1.1) that

$$P_A(u,v) = \begin{cases} 0 & \text{for } u \text{ even and } (u,v) \neq (0,0) \\ \pm 1 & \text{for } u \text{ odd.} \end{cases}$$

Lemma 1.3 then implies that

$$P_A(u,v) = \begin{cases} 0 & \text{for } u \text{ even and } (u,v) \neq (0,0) \\ k(u) & \text{for } u \text{ odd,} \end{cases} \tag{1.5}$$

where $k(u) = 1$ or $-1$, as required.

We next consider the function

$$P_{A^T}(v,u) = C_A(u,v) + C_A(u-s,v). \tag{1.6}$$

From (1.4),

$$P_{A^T}(v,u) = 0 \quad \text{for } u \text{ even and } (u,v) \neq (0,0). \tag{1.7}$$

Lemma 1.3 applied to $A^T$ states that

$$P_{A^T}(v,u) \equiv P_{A^T}(v,u') \pmod 4 \quad \text{for all } (u,u',v),$$

giving

$$P_{A^T}(v,u) = 0 \quad \text{for } (u,v) \neq (0,0), \text{ except when } s = 2 \text{ and } (u,v) = (1,0) \tag{1.8}$$

(since, when $s = 2$ and $v = 0$, there is no value of $u$ satisfying the conditions of (1.7)).

To complete the proof of Case 2, we now derive a contradiction for the case $s = 2$, so that (1.8) holds without the exception. By assumption $st > 2$ and $s = 2$, so $t > 1$ and we can choose an even value of $v$ satisfying $0 < v < t$. From (1.5),

$$k(1) = P_A(1,v) = P_A(1,t-v)$$

and so from (1.1) and (1.4),

$$\pm 1 = C_A(1,v) = C_A(1,-v). \tag{1.9}$$

But by (1.8), $P_{A^T}(v,1) = 0$ and so from (1.6) we get

$$\begin{aligned} 0 &= C_A(1,v) + C_A(-1,v) \\ &= C_A(1,v) + C_A(1,-v) \end{aligned}$$

since $C_A(u,v) = C_A(-u,-v)$ for all $u,v$. This contradicts (1.9).

*Case* 3. *$s,t$ odd:* From (1.3) we have

$$C_A(u,v) = \pm(((1+u)(1+v)) \bmod 2) \quad \text{for } (u,v) \neq (0,0).$$

Then by (1.1),

$$P_A(u,v) = \begin{cases} \pm 1 & \text{for } u \text{ even and } (u,v) \neq (0,0) \\ 0 & \text{for } u \text{ odd.} \end{cases}$$

Lemma 1.3 then implies that

$$P_A(u,v) = \begin{cases} k(u) & \text{for } u \text{ even and } (u,v) \neq (0,0) \\ 0 & \text{for } u \text{ odd,} \end{cases}$$

where $k(u) = 1$ or $-1$. By symmetry in $s$ and $t$ we also obtain

$$P_{A^T}(v,u) = \begin{cases} k'(v) & \text{for } v \text{ even and } (u,v) \neq (0,0) \\ 0 & \text{for } v \text{ odd,} \end{cases}$$

where $k'(v) = 1$ or $-1$. But, for $u,v$ even and $(u,v) \neq (0,0)$, by (1.3) the single nonzero contribution to $P_A(u,v) = C_A(u,v) + C_A(u,v-t)$ and to $P_{A^T}(v,u) = C_A(u,v) + C_A(u-s,v)$ is the same term $C(u,v)$, and so $k(u) = k'(v) = k$.

□

Proposition 1.4 is implied by Theorem 2 and equations (21)–(23) of [1]. Lemma 3.5 of [6] shows that an $s \times t$ binary array $A$ having $P_A(u,v) = 0$ for all $(u,v) \neq (0,0)$ is equivalent to $A$ being simultaneously a perfect binary array and a "quasiperfect" binary array. This in turn is equivalent to the $-1$ elements of $A$ corresponding to a $(4N^2, 2N^2 - N, N^2 - N)$-difference set in $\mathbb{Z}_s \times \mathbb{Z}_t$, where $st = 4N^2$ (see [4], for example); and the $-1$ elements of $\begin{bmatrix} A \\ -A \end{bmatrix}$ corresponding to an $(st, 2, st, st/2)$ relative difference set in $\mathbb{Z}_{2s} \times \mathbb{Z}_t = \langle x \rangle \times \langle y \rangle$, where $x^{2s} = y^t = 1$, relative to $\langle x^s \rangle$ (see [17]). See [3] or [12] for background on difference sets and relative difference sets.

## 2. Proof of the Conjecture

We begin with two lemmas.

**Lemma 2.1.** *Let $A = (a_{ij})$ be an $s \times t$ binary array and let $\zeta$ be a (not necessarily primitive) $t^{\text{th}}$ root of unity. Let $X = (x_i)$ be the complex-valued sequence of length $s$ given by*

$$x_i = \sum_j a_{ij} \zeta^j. \tag{2.1}$$

*Then*

$$C_X(u) = \sum_{v=0}^{t-1} P_A(u,v)\zeta^{-v} \quad \textit{for all } u.$$

*Proof.* From (1.2), for all $u$,

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

writing $k = (j+v) \bmod t$ and using $\zeta^t = 1$. Hence, for all $u$,

$$\begin{aligned}\sum_{v=0}^{t-1} P_A(u,v)\zeta^{-v} &= \sum_i\sum_j a_{ij}\zeta^j\overline{\sum_k a_{i+u,k}\zeta^k} \\ &= \sum_i x_i\overline{x_{i+u}} \\ &= C_X(u),\end{aligned}$$

as required. □

**Lemma 2.2.** *Let $X = (x_i)$ be a complex-valued sequence of length $s$ for which*

$$C_X(u) = 0 \quad \textit{for } u \neq 0.$$

*Then, for some $I$ satisfying $0 \le I < s$,*

$$|x_i|^2 = \begin{cases} 0 & \textit{for } i \neq I, \\ C_X(0) & \textit{for } i = I. \end{cases}$$

*Proof.* By the definition of aperiodic autocorrelation, we are given that

$$\sum_i x_i\overline{x_{i+u}} = 0 \quad \text{for } 0 < u < s. \tag{2.2}$$

We prove by induction on $s$ that, for some $I$ satisfying $0 \le I < s$,

$$|x_i|^2 = 0 \quad \text{for } i \neq I.$$

The case $s = 1$ is immediate (take $I = 0$). Assume case $s-1$ to be true. Put $u = s-1$ in (2.2) to give $x_0\overline{x_{s-1}} = 0$. This implies, without loss of generality, that $x_{s-1} = 0$. Then from (2.2) we have

$$\sum_{i=0}^{s-u-2} x_i\overline{x_{i+u}} = 0 \quad \text{for } 0 < u < s-1.$$

By the inductive hypothesis it follows that, for some $I$ satisfying $0 \le I < s-1$, $|x_i|^2 = 0$ for $i \neq I$. Combining this with $x_{s-1} = 0$ gives the case $s$, completing the induction.

Furthermore, by the definition of aperiodic autocorrelation, $C_X(0) = \sum_i |x_i|^2$ and so $C_X(0) = |x_I|^2$, as required. □

The case $\zeta = 1$ of Lemma 2.1 was used as a starting point in [5], [6] and [8] to derive equations in the row sums $\sum_j a_{ij}$ of an $s \times t$ Barker array from Proposition 1.4, leading eventually to Theorem 1.2. We will now use the case where $\zeta$ is a primitive $t^{\text{th}}$ root of unity to prove Conjecture 1.1.

**Theorem 2.3.** *If an $s \times t$ Barker array $A = (a_{ij})$ exists for $s, t > 1$ then $s = t = 2$.*

*Proof.* Let $\zeta$ be a primitive $t^{\text{th}}$ root of unity and define $X = (x_i)$ as in (2.1). We will show that the case $s, t$ even forces the result $s = t = 2$, whereas the case $s$ even, $t$ odd and the case $s, t$ odd both result in a contradiction. These three cases are exhaustive, because the transpose of a Barker array is also a Barker array.

*Case* 1. *$s, t$ even:* Proposition 1.4 and Lemma 2.1 together give

$$C_X(u) = \begin{cases} 0 & \text{for } u \neq 0 \\ st & \text{for } u = 0, \end{cases}$$

using $P_A(0,0) = C(0,0) = st$. Then by Lemma 2.2 there is some $I$ satisfying $0 \leq I < s$ for which

$$|x_I|^2 = st. \tag{2.3}$$

But by (2.1),

$$\begin{aligned} |x_I|^2 &= \left| \sum_{j=0}^{t-1} a_{Ij}\zeta^j \right|^2 \\ &\leq \left( \sum_{j=0}^{t-1} |a_{Ij}\zeta^j| \right)^2 \\ &= t^2. \end{aligned}$$

It follows from (2.3) that

$$s \leq t, \text{ with equality} \Leftrightarrow \arg(a_{Ij}\zeta^j) \text{ is constant for all } j \text{ satisfying } 0 \leq j < t. \tag{2.4}$$

Since $s$ is even, by symmetry in $s$ and $t$ (or equivalently by applying the same procedure to $A^T$) we have $t \leq s$, forcing equality. Therefore $s = t$ and, since $t > 1$, by (2.4) we have $t = 2$.

*Case* 2. *$s$ even, $t > 1$ odd:* By Proposition 1.4, the $t \times s$ array $A^T$ satisfies

$$P_{A^T}(v, u) = 0 \ \text{ for } (u, v) \neq (0, 0).$$

The argument of Case 1 that led to (2.4), when applied to $A^T$, gives $t \leq s$. Furthermore the expression for $P_A$ in Proposition 1.4, together with Lemma 2.1, gives

$$\begin{aligned} C_X(u) &= \begin{cases} 0 & \text{for } u \text{ even and } u \neq 0 \\ k(u) \sum_{v=0}^{t-1} \zeta^{-v} & \text{for } u \text{ odd} \\ st & \text{for } u = 0 \end{cases} \\ &= \begin{cases} 0 & \text{for } u \neq 0 \\ st & \text{for } u = 0, \end{cases} \end{aligned}$$

since $\zeta^{-1}$ is a primitive $t^{\text{th}}$ root of unity and $t > 1$. By Lemma 2.2 we then obtain $s \leq t$, by the same argument as in Case 1. Since we already have $t \leq s$ this implies $s = t$, which contradicts the assumption that $s$ is even and $t$ is odd.

*Case* 3. $s,t>1$ *odd:* Proposition 1.4 and Lemma 2.1 together give

$$\begin{aligned} C_X(u) &= \begin{cases} k\sum_{v=0}^{t-1}\zeta^{-v} & \text{for } u \text{ even and } u\neq 0\\ 0 & \text{for } u \text{ odd}\\ st+k\sum_{v=1}^{t-1}\zeta^{-v} & \text{for } u=0\end{cases}\\ &= \begin{cases} 0 & \text{for } u\neq 0\\ st-k & \text{for } u=0,\end{cases}\end{aligned}$$

where $k=1$ or $-1$. Then by Lemma 2.2 there is some $I$ satisfying $0\le I<s$ for which

$$|x_I|^2 = st-k. \tag{2.5}$$

But, as in Case 1, $|x_I|^2\le t^2$ and so

$$st-k\le t^2.$$

By symmetry in $s$ and $t$ we then have

$$st-k\le \min\{s^2,t^2\}. \tag{2.6}$$

Suppose, for a contradiction, that $s\neq t$ and without loss of generality that $s\ge t+1$. Then $st-k\ge t(t+1)-k>t^2$, since $k=1$ or $-1$ and $t>1$. This contradicts (2.6), and so $s=t$.

Then (2.6) forces $k=1$, and from (2.1) and (2.5) we have

$$\left|\sum_{j=0}^{t-1} a_{Ij}\zeta^j\right|^2 = t^2-1. \tag{2.7}$$

Since $t$ is odd, one of the sets $\{j: a_{Ij}=1\}$ and $\{j: a_{Ij}=-1\}$ contains at most $(t-1)/2$ elements; without loss of generality, suppose it is the former. This implies that

$$\begin{aligned}\left|\sum_{j=0}^{t-1} a_{Ij}\zeta^j\right|^2 &= \left|\sum_{j=0}^{t-1} a_{Ij}\zeta^j + \sum_{j=0}^{t-1}\zeta^j\right|^2\\ &= \left|2\sum_{j:\, a_{Ij}=1}\zeta^j\right|^2\\ &\le 4\left(\sum_{j:\, a_{Ij}=1}|\zeta^j|\right)^2\\ &\le 4\left(\frac{t-1}{2}\right)^2\\ &< t^2-1,\end{aligned}$$

since $t>1$. This contradicts (2.7).

□

## Acknowledgement

We are grateful to Denis Dmitriev for supplying the above argument that (2.7) cannot hold for odd $t>1$, which is much neater than our original reasoning.

## References


1. S. Alquaddoomi and R.A. Scholtz, *On the nonexistence of Barker arrays and related matters*, IEEE Trans. Information Theory **35** (1989), 1048–1057.
2. R.H. Barker, *Group synchronizing of binary digital systems*, Communication Theory (W. Jackson, ed.), Academic Press, New York, 1953, pp. 273–287.
3. T. Beth, D. Jungnickel, and H. Lenz, *Design theory*, 2nd ed., Cambridge University Press, Cambridge, 1999, Volumes I and II.
4. Y.K. Chan, M.K. Siu, and P. Tong, *Two-dimensional binary arrays with good autocorrelation*, Information and Control **42** (1979), 125–130.
5. J. Jedwab, *Nonexistence results for Barker arrays*, The Institute of Mathematics and its Applications Conference Series (New Series) No. 33: Cryptography and Coding II (C. Mitchell, ed.), Clarendon Press, Oxford, 1992, pp. 121–126.
6. ______, *Barker arrays I: Even number of elements*, SIAM J. Discrete Math. **6** (1993), 294–308.
7. J. Jedwab, *A survey of the merit factor problem for binary sequences*, Sequences and Their Applications — Proceedings of SETA 2004 (T. Helleseth et al., eds.), Lecture Notes in Computer Science, vol. 3486, Springer-Verlag, Berlin Heidelberg, 2005, pp. 30–55.
8. J. Jedwab, S. Lloyd, and M. Mowbray, *Barker arrays II: Odd number of elements*, SIAM J. Discrete Math. **6** (1993), 309–328.
9. J. Jedwab and K. Yoshida, *The peak sidelobe level of families of binary sequences*, IEEE Trans. Inform. Theory (2006), to appear.
10. K.H. Leung, S.L. Ma, and B. Schmidt, *Nonexistence of abelian difference sets: Lander's conjecture for prime power orders*, Trans. Amer. Math. Soc. **356** (2004), 4343–4358.
11. K.H. Leung and B. Schmidt, *The field descent method*, Designs, Codes and Cryptography **36** (2005), 171–188.
12. A. Pott, *Finite geometry and character theory*, Lecture Notes in Mathematics 1601, Springer-Verlag, Berlin, 1995.
13. G.S. Ramakrishna and W.H. Mow, *A new search for optimal binary arrays with minimum peak sidelobe levels*, Sequences and Their Applications — Proceedings of SETA 2004 (T. Helleseth et al., eds.), Lecture Notes in Computer Science, vol. 3486, Springer-Verlag, Berlin Heidelberg, 2005, pp. 355–360.
14. H.D. Schotten and H.D. Lüke, *On the search for low correlated binary sequences*, AEU — Int. J. of Electronics and Communications **59** (2005), 67–78.
15. R. Turyn and J. Storer, *On binary sequences*, Proc. Amer. Math. Soc. **12** (1961), 394–399.
16. R.J. Turyn, *Sequences with small correlation*, Error Correcting Codes (H.B. Mann, ed.), Wiley, New York, 1968, pp. 195–228.
17. P. Wild, *Infinite families of perfect binary arrays*, Electron. Lett. **24** (1988), 845–847.



Department of Mathematics and Computer Science, University of Richmond, VA 23173, USA

*E-mail address*: jdavis@richmond.edu

Department of Mathematics, Simon Fraser University, 8888 University Drive, Burnaby, BC, Canada, V5A 1S6

*E-mail address*: jed@sfu.ca

Department of Mathematics, Central Michigan University, Mount Pleasant, MI 48859, USA

*E-mail address*: Ken.W.Smith@cmich.edu