THREE-PHASE BARKER ARRAYS

JASON P. BELL, JONATHAN JEDWAB,
MAHDAD KHATIRINEJAD, AND KAI-UWE SCHMIDT

Abstract. A 3-phase Barker array is a matrix of third roots of unity for which all out-of-phase aperiodic autocorrelations have magnitude 0 or 1. The only known truly two-dimensional 3-phase Barker arrays have size 2×2 or 3×3. We use a mixture of combinatorial arguments and algebraic number theory to establish severe restrictions on the size of a 3-phase Barker array when at least one of its dimensions is divisible by 3. In particular, there exists a double-exponentially growing arithmetic function T such that no 3-phase Barker array of size $s \times t$ with $3 \mid t$ exists for all $t < T(s)$. For example, $T(5) = 4860$, $T(10) > 10^{11}$, and $T(20) > 10^{214}$. When both dimensions are divisible by 3, the existence problem is settled completely: if a 3-phase Barker array of size $3r \times 3q$ exists, then $r = q = 1$.

1. Introduction

We define an *array of size* $s \times t$ to be an infinite matrix $A = (a_{ij})$ of complex-valued elements satisfying

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

We call A an *H-phase array* if a_{ij} is an H-th root of unity for each i, j satisfying $0 \le i < s$ and $0 \le j < t$. For integers u and v, the *aperiodic autocorrelation* of $A = (a_{ij})$ at shift (u, v) is defined to be

$$C_A(u, v) = \sum_{i,j} a_{ij} \overline{a_{i+u,j+v}}.$$

Notice that $C_A(u, v) = 0$ for $|u| \ge s$ or $|v| \ge t$. Arrays with small aperiodic autocorrelation at all nonzero shifts have a wide range of applications in digital communications, including synchronisation [Bar53] and radar [AS89].

Date: 1 June 2013 (revised 17 September 2013).

J. Bell is with Department of Pure Mathematics, University of Waterloo, Waterloo, ON, N2L 3G1, Canada. Email: jpbell@uwaterloo.ca.

J. Jedwab is with Department of Mathematics, Simon Fraser University, 8888 University Drive, Burnaby, BC, V5A 1S6, Canada. Email: jed@sfu.ca.

M. Khatirinejad email: mahdadk@gmail.com.

K.-U. Schmidt is with Faculty of Mathematics, Otto-von-Guericke University, Universitätsplatz 2, 39106 Magdeburg, Germany. Email: kaiuwe.schmidt@ovgu.de.

J. Bell and J. Jedwab are supported by NSERC. K.-U. Schmidt was supported by German Research Foundation.

We would like to find 2-phase arrays A of size $s \times t$ satisfying

$$|C_A(u,v)| \le 1 \quad \text{for all } (u,v) \ne (0,0), \tag{1}$$

in which case A is called a *Barker array* [AS89]. However, the only $s \times t$ Barker arrays with $s,t > 1$ have size 2×2, as conjectured by Alquaddoomi and Scholtz [AS89] and proved by Davis, Jedwab, and Smith [DJS07]. See Leung and B. Schmidt [LS12] for recent nonexistence results for Barker sequences (namely $1 \times t$ Barker arrays).

A possible alternative to Barker arrays is to consider H-phase arrays A satisfying (1), in which case we call A an *H-phase Barker array.* In order to allow efficient implementation, it is desirable to limit H to a small number, and we will be interested in the case $H = 3$. Alquaddoomi and Scholtz [AS89] exhibited the 3-phase Barker array

$$\begin{bmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{bmatrix},$$

where throughout this paper ω denotes a primitive third root of unity (note that the Barker property of a 3-phase array does not depend on the particular choice of ω). Another example is

$$\begin{bmatrix} 1 & 1 \\ 1 & \omega \end{bmatrix}.$$

There also exist 3-phase Barker sequences of length t for $t \in \{2,3,4,5,7,9\}$ [GS65], but it has been conjectured since at least 1968 [Tur68, p. 211] that no further such sequences exist.

We adapt some of the ideas in [DJS07], used to establish the nonexistence result for 2-phase Barker arrays, and combine them with new combinatorial and algebraic number theoretic arguments to prove severe restrictions on the size of 3-phase Barker arrays of size $s \times t$ when st is divisible by 3. In particular, there exists a double-exponentially growing arithmetic function T such that no 3-phase Barker array of size $s \times t$ with $3 \mid t$ exists for all $t < T(s)$. For example,

$$T(5) = 4860,\ T(10) > 10^{11}, \text{ and } T(20) > 10^{214}.$$

When both dimensions are divisible by 3, the existence problem is settled completely: if a 3-phase Barker array of size $3r \times 3q$ exists, then $r = q = 1$.

2. Semiperiodic autocorrelation of a 3-phase Barker array

Given an array $A = (a_{ij})$ of size $s \times t$ and integers u and v, we follow Alquaddoomi and Scholtz [AS89, Sec. V] and define the *semiperiodic autocorrelation* of A at displacement (u,v) to be

$$P_A(u,v) = C_A(u,v) + C_A(u,v-t) \quad \text{for } 0 \le v < t. \tag{2}$$

By convention, any expression involving $P_A(u,v)$ implicitly refers only to values of (u,v) for which $P_A(u,v)$ is defined. In terms of the elements of A, we can write

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

In the following lemma, we establish restrictions on $P_A(u,v)$ when A is a 3-phase array. We then apply this lemma to 3-phase Barker arrays of size $s \times t$ with $3 \mid t$. This generalises Turyn's analysis [Tur68], [Tur74] of the one-dimensional case.

Lemma 1. *Let $A = (a_{ij})$ be a 3-phase array of size $s \times t$ and write*

$$P_A(u,v) = Q_A(u,v) + \omega\, R_A(u,v),$$

where $Q_A(u,v)$ and $R_A(u,v)$ are integer-valued. Then

$$Q_A(u,v) \equiv Q_A(u,v') \pmod 3 \tag{3}$$

and

$$R_A(u,v) \equiv R_A(u,v') \pmod 3 \tag{4}$$

for all (u,v,v').

Proof. Since $P_A(u,v)$ is a sum of $(s-|u|)t$ terms, each of which is a third root of unity, we can write

$$P_A(u,v) = B_0 + B_1\omega + B_2\omega^2$$

for nonnegative integers B_0, B_1, and B_2 satisfying

$$B_0 + B_1 + B_2 = (s-|u|)t. \tag{5}$$

Using the identity $\omega^2 = -1-\omega$, we find that

$$P_A(u,v) = (B_0 - B_2) + (B_1 - B_2)\omega.$$

We therefore have

$$Q_A(u,v) + R_A(u,v) = B_0 + B_1 - 2B_2,$$

which together with (5) gives

$$Q_A(u,v) + R_A(u,v) \equiv (s-|u|)t \pmod 3. \tag{6}$$

Now consider the product

$$\prod_i \prod_{j=0}^{t-1} a_{ij}\overline{a_{i+u,(j+v) \bmod t}} = 1^{B_0}\omega^{B_1}(\omega^2)^{B_2} = \omega^{B_1-B_2} = \omega^{R_A(u,v)},$$

which is independent of v. This proves assertion (4) and assertion (3) then follows from (6). □

Lemma 2. *Suppose that A is a 3-phase Barker array of size $s \times t$ with $3 \mid t$. Then*

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

Proof. Note that in $\mathbb{Q}(\omega)$ we have the factorisation

$$a + b\omega + c\omega^2 = \big((a-d) + (d-c)\omega\big)(1-\omega),$$

where $d = (a+b+c)/3$. Hence every sum of $3m$ third roots of unity is divisible by $1-\omega$ over $\mathbb{Z}[\omega]$. Furthermore, 0 is the only element of $\mathbb{Z}[\omega]$ that has magnitude at most 1 and is divisible by $1-\omega$.

Since $C_A(u,0)$ is a sum of $(s-|u|)t$ third roots of unity for $|u| < s$, and by assumption $3 \mid t$, the Barker property (1) then forces $C_A(u,0) = 0$ for all $u \neq 0$. Hence $P_A(u,0) = C_A(u,0) + C_A(u,-t) = 0$ for all $u \neq 0$. Also, since $P_A(0,0) = st$, we conclude that $P_A(u,0)$ is an integer divisible by 3 for all u. Then, for arbitrary u and v, Lemma 1 implies that $P_A(u,v) = 3n + 3n'\omega$ for some integers n and n' (depending on u and v). On the other hand, by the definition (2) of $P_A(u,v)$ and the Barker property, we have $|P_A(u,v)| \le 2$ for $(u,v) \neq (0,0)$. Hence $P_A(u,v) = 0$ for all $(u,v) \neq (0,0)$. □

Lemma 2 is now used to prove the following result, which will be our main tool for the remainder of this paper.

Proposition 3. *Suppose that $A = (a_{ij})$ is a 3-phase Barker array of size $s \times t$ with $3 \mid t$, and write $f_i(x) = \sum_j a_{ij}x^j$. Let ζ be a t-th root of unity. Then there exists some $I = I(\zeta)$ satisfying $0 \le I < s$ such that*

$$\big|f_i(\zeta)\big|^2 = \begin{cases} 0 & \text{for } i \neq I \\ st & \text{for } i = I. \end{cases}$$

Proof. Define the polynomial

$$g(y) = \sum_i f_i(\zeta)\, y^i = \sum_{i,j} a_{ij}\, y^i \zeta^j.$$

Straightforward manipulations give

$$g(y)\overline{g(y^{-1})} = \sum_{u,v} P_A(u,v) y^{-u}\zeta^{-v},$$

so that by Lemma 2, $g(y)\overline{g(y^{-1})} = st$. This forces $g(y)$ to be a monomial, for if $c_k y^k$ and $c_\ell y^\ell$ are the highest-degree and lowest-degree monomials in $g(y)$, respectively, and $k > \ell$, then $g(y)\overline{g(y^{-1})}$ contains $c_k\overline{c_\ell}y^{k-\ell}$. Therefore, $g(y) = cy^I$ for some $c \in \mathbb{Q}(\omega,\zeta)$ of magnitude $\sqrt{st}$ and some $I = I(\zeta)$ satisfying $0 \le I < s$, which completes the proof. □

If a 3-phase Barker array of size $s \times t$ with $3 \mid t$ exists, then Proposition 3 determines a partition of the t-th roots of unity into s sets. Moreover, if ζ belongs to one of these sets, then all roots of the minimal polynomial of ζ over $\mathbb{Q}(\omega)$ must belong to the same set.

For later reference, we note that, if ζ is a primitive m-th root of unity, then the degree of the minimal polynomial of ζ over $\mathbb{Q}(\omega)$ is $\phi(m)/2$ if $3 \mid m$ and is $\phi(m)$ otherwise (and so in this case the minimal polynomial is the m-th cyclotomic polynomial).

3. Consequences of Proposition 3

In this section, we use Proposition 3 to prove severe restrictions on the size of a 3-phase Barker array. Throughout this section, we use the following notation. For a positive integer n, we let ζ_n denote the primitive n-th root of unity $e^{2\pi i/n}$. Given a prime p and a nonzero integer n, we let $\nu_p(n)$ denote the p-adic valuation of n; that is, $\nu_p(n)$ is the unique nonnegative integer with the property that $p^{\nu_p(n)}$ divides n but $p^{\nu_p(n)+1}$ does not.

We begin with an elementary result that restricts the prime divisors of the number of nonzero elements in a 3-phase Barker array.

Theorem 4. *Suppose that there exists a* 3*-phase Barker array of size* $s \times t$ *with* $3 \mid t$*. Then* $\nu_p(st)$ *is even for every prime* $p \equiv 2 \pmod 3$*.*

Proof. Taking $\zeta = 1$ in Proposition 3, we see that $st = v\overline{v}$ for some $v \in \mathbb{Z}[\omega]$. In $\mathbb{Z}[\omega]$, the prime 3 ramifies and primes $p \equiv 1 \pmod 3$ split, whereas primes $p \equiv 2 \pmod 3$ remain inert. The theorem follows. □

For example, there are no 3-phase Barker arrays of size 2×3, 5×9, and 10×15.

If there exists a 3-phase Barker array of size $s \times t$ with $3 \mid t$, then Proposition 3 determines a partition of the t-th roots of unity into s sets. We now show that all of these sets must have equal size t/s, which forces s to divide t.

Theorem 5. *Suppose that there exists a* 3*-phase Barker array* (a_{ij}) *of size* $s \times t$ *with* $3 \mid t$*, and write* $f_i(x) = \sum_j a_{ij} x^j$*. Then, for each* i *satisfying* $0 \le i < s$*,*

$$\left|\{k \in \mathbb{Z}/t\mathbb{Z} : f_i(\zeta_t^k) \neq 0\}\right| = t/s.$$

In particular, s *divides* t*.*

Proof. If (a_{ij}) is an arbitrary array of size $s \times t$, then, for each i,

$$\frac{1}{st}\sum_{k=0}^{t-1} |f_i(\zeta_t^k)|^2 = \frac{1}{st}\sum_{k=0}^{t-1}\left|\sum_{j=0}^{t-1} a_{ij}\zeta_t^{kj}\right|^2 = \frac{1}{s}\sum_{j=0}^{t-1} |a_{ij}|^2$$

by Parseval's identity. If (a_{ij}) is a 3-phase Barker array, the right-hand side equals t/s for each i satisfying $0 \le i < s$ and, by Proposition 3, the left-hand side counts the number of $k \in \mathbb{Z}/t\mathbb{Z}$ such that $f_i(\zeta_t^k) \neq 0$. □

Theorem 5 can be used to prove the following nonexistence result.

Theorem 6. *Suppose that there exists a* 3*-phase Barker array of size* $s \times t$ *with* $3 \mid s$ *and* $3 \mid t$*. Then* $s = t = 3$*.*

Proof. Write the 3-phase Barker array as $A = (a_{ij})$. By application of Theorem 5 to A and A^T (which is also a 3-phase Barker array), we conclude that $s \mid t$ and $t \mid s$, hence $s = t$. By Proposition 3, there exists some I satisfying $0 \le I < s$ for which

$$\left|\sum_{j=0}^{t-1} a_{Ij}\zeta_t^j\right| = t.$$

Hence, $\arg(a_{Ij}\zeta_t^j)$ is constant for all j satisfying $0 \le j < t$, forcing $s = t = 3$ since $a_{Ij} \in \{1, \omega, \omega^2\}$. □

Combining Theorems 5 and 6 shows for example that, if there exists a 3-phase Barker array of size $s \times 3^n$ with $n \ge 2$, then $s = 1$; it then follows from [Tur68, pp. 205 and 211] that $n = 2$.

Recall that, if a 3-phase Barker array of size $s \times t$ with $3 \mid t$ exists, then Proposition 3 partitions the t-th roots of unity into s sets, according to the associated value of I, and by Theorem 5 each of these sets has size t/s. In Theorems 10 and 11 below, we derive constraints on the possible values of s and t. Our strategy in the proof of Theorem 10 will be to write $t = 3^n q$, where $3 \nmid q$, and determine an upper and lower bound on the number of distinct values of I associated with the following 3^n-th roots of unity:

$$1,\, \zeta_3,\, \zeta_3^2,\, \zeta_9,\, \zeta_9^2, \dots, \zeta_{3^n},\, \zeta_{3^n}^2.$$

Our strategy in the proof of Theorem 11 will be to write $t = t_0 r$, where $3 \mid t_0$ and $3 \nmid r$ and r is square-free, and determine a lower bound on the size of the set associated with a specific primitive t_0-th root of unity. In preparation for these theorems, we prove the following result.

Proposition 7. *Let n and $t > 0$ be integers, and let p be a prime divisor of t. Suppose that a polynomial $f \in \mathbb{Z}[\omega][x]$ has the property that for each t-th root of unity ζ, $|f(\zeta)|^2$ is integral and $\nu_p(|f(\zeta)|^2) = n$ whenever $f(\zeta) \ne 0$. Suppose also that η is a t-th root of unity whose order is not divisible by p and that $f(\eta) \ne 0$. Then:*

(i) In the case $p \ne 3$,

$$\left\{j \in \{1, 2, \dots, \nu_p(t)\} : f(\eta \cdot \zeta_{p^j}) \ne 0\right\}$$

has cardinality at least $\nu_p(t) - n/2$ and, for each k coprime to p, $f(\eta \cdot \zeta_{p^j}) = 0$ if and only if $f(\eta \cdot \zeta_{p^j}^k) = 0$.

(ii) In the case $p = 3$,

$$\left\{(j, k) \in \{1, 2, \dots, \nu_3(t)\} \times \{1, 2\} : f(\eta \cdot \zeta_{3^j}^k) \ne 0\right\} \tag{7}$$

has cardinality at least $2\nu_3(t) - n$, and, for each k and ℓ satisfying $0 \not\equiv k \equiv \ell \pmod 3$, $f(\eta \cdot \zeta_{3^j}^k) = 0$ if and only if $f(\eta \cdot \zeta_{3^j}^\ell) = 0$.

(iii) In the case $p = 3$, suppose further that $f(1) \ne 0$ and $0 < \nu_3(|f(1)|^2) < 2\nu_3(t)$ and

$$f(x) - (1 + x + \cdots + x^{t-1}) \in (1 - \omega)\mathbb{Z}[\omega][x].$$

Then the set (7) has cardinality at least $2\nu_3(t) - n + 1$.

Before we prove Proposition 7, we introduce some standard notation and prove an auxiliary result. Let $\Phi_n(x)$ be the n-th cyclotomic polynomial. The following result can be easily proved by induction (see [Lan94, p. 74], for example) or by Möbius inversion of $n = \prod_{d|n, d>1} \Phi_d(1)$.

Lemma 8. *Let $n > 1$ be an integer. If n is a power of a prime p, then $\Phi_n(1) = p$; otherwise, $\Phi_n(1) = 1$.*

Given a finite extension K of $\mathbb{Q}$ and $\alpha \in K$, we let $N^K(\alpha)$ denote the norm of α; that is, $N^K(\alpha)$ is the product of $\sigma(\alpha)$, where σ ranges over the $[K : \mathbb{Q}]$ complex embeddings of K into $\mathbb{C}$.

Lemma 9. *Let n be a positive integer, let d and p be divisors of n with p prime, and write $K = \mathbb{Q}(\zeta_n)$. Let ζ be a primitive d-th root of unity. Then*

$$\nu_p\big(N^K(1-\zeta)\big) = \begin{cases} \phi(n)/\phi(d) & \text{if } d \text{ is a power of } p; \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Since K is a Galois extension of $\mathbb{Q}$, we have

$$N^K(1-\zeta) = \prod_{\sigma \in \mathrm{Gal}(K)} (1 - \sigma(\zeta)),$$

where $\mathrm{Gal}(K)$ denotes the group of field automorphisms of K. Let $F = \mathbb{Q}(\zeta)$, so that F is a Galois extension of $\mathbb{Q}$ of degree $\phi(d)$ and K is a Galois extension of F of degree $\phi(n)/\phi(d)$. Each automorphism of F lifts to $\phi(n)/\phi(d)$ automorphisms of K, and therefore,

$$N^K(1-\zeta) = \prod_{\tau \in \mathrm{Gal}(F)} (1 - \tau(\zeta))^{\phi(n)/\phi(d)}.$$

Since

$$\prod_{\tau \in \mathrm{Gal}(F)} (1 - \tau(\zeta)) = \prod_{\substack{j=1 \\ (j,d)=1}}^{d} (1 - \zeta_d^j) = \Phi_d(1),$$

we find that

$$\nu_p\big(N^K(1-\zeta)\big) = \nu_p\big(\Phi_d(1)\big)\, \phi(n)/\phi(d).$$

The result now follows from Lemma 8. □

We are now ready to prove Proposition 7.

Proof of Proposition 7. We first prove (i). Since the order of η is not divisible by p and $p \neq 3$, we have

$$[\mathbb{Q}(\omega, \eta, \zeta_{p^j}) : \mathbb{Q}(\omega, \eta)] = [\mathbb{Q}(\zeta_{p^j}) : \mathbb{Q}]$$

for each natural number j. In particular, the identity automorphism of $\mathbb{Q}(\omega, \eta)$ lifts to exactly $\phi(p^j)$ distinct automorphisms of $\mathbb{Q}(\omega, \eta, \zeta_{p^j})$. If σ is one of these $\phi(p^j)$ liftings, then σ extends naturally to polynomials in $\mathbb{Q}(\omega, \eta, \zeta_{p^j})[x]$. Then, since $\sigma(f) = f$, we have $f(\eta \cdot \zeta_{p^j}) = 0$ if and only if $f(\eta \cdot \sigma(\zeta_{p^j})) = 0$. But as σ ranges over the $\phi(p^j)$ liftings of the identity automorphism of $\mathbb{Q}(\omega,\eta)$, the image $\sigma(\zeta_{p^j})$ ranges over all primitive p^j-th roots of unity, proving the second part of (i).

Now write $S=\{j\in\{1,2,\dots,\nu_p(t)\}\;:\;f(\eta\cdot\zeta_{p^j})=0\}$ and $K=\mathbb{Q}(\zeta_t)$. We must show that $|S|\le n/2$. If $j\in S$, then we have $f(\eta\cdot\zeta_{p^j}^k)=0$ for all k coprime to p^j. Thus

$$g(x)=\prod_{j\in S}\prod_{\substack{k=1\\(k,p)=1}}^{p^j}(x-\eta\cdot\zeta_{p^j}^k)$$

divides $f(x)$ in $\mathbb{Z}[\zeta_t][x]$. It follows that $N^K(g(\eta))$ divides $N^K(f(\eta))$ and hence

$$\nu_p\left(N^K(g(\eta))\right)\le\nu_p\left(N^K(f(\eta))\right)=\phi(t)\,n/2, \tag{8}$$

using $\nu_p(|f(\eta)|^2)=n$. From Lemma 9 with $n=t$ and $d=p^j$ and $\zeta=\zeta_{p^j}^k$, we find that

$$\begin{aligned}\nu_p\big(N^K(g(\eta))\big)&=\sum_{j\in S}\sum_{\substack{k=1\\(k,p)=1}}^{p^j}\nu_p\big(N^K(\eta-\eta\cdot\zeta_{p^j}^k)\big)\\&=\sum_{j\in S}\sum_{\substack{k=1\\(k,p)=1}}^{p^j}\nu_p\big(N^K(1-\zeta_{p^j}^k)\big)\\&=\sum_{j\in S}\sum_{\substack{k=1\\(k,p)=1}}^{p^j}\frac{\phi(t)}{\phi(p^j)}\\&=\sum_{j\in S}\phi(t)\\&=\phi(t)|S|.\end{aligned}$$

Thus, after combination with (8), we get $|S|\le n/2$, as required.

The proof of (ii) is similar to (i), except that we now have

$$[\mathbb{Q}(\omega,\eta,\zeta_{3^j}):\mathbb{Q}(\omega,\eta)]=\tfrac{1}{2}\cdot[\mathbb{Q}(\zeta_{3^j}):\mathbb{Q}]$$

and, if $\zeta_{3^j}^k$ and $\zeta_{3^j}^\ell$ are two primitive 3^j-th roots of unity, then, among the $\phi(3^j)/2$ liftings of the identity automorphism of $\mathbb{Q}(\omega,\eta)$ to $\mathbb{Q}(\omega,\eta,\zeta_{3^j})$, there is one that sends $\zeta_{3^j}^k$ to $\zeta_{3^j}^\ell$ if and only if $k\equiv\ell \pmod 3$. The remainder of the argument is identical to that employed in establishing (i), taking

$$S=\big\{(j,k)\in\{1,2,\dots,\nu_3(t)\}\times\{1,2\}:f(\eta\cdot\zeta_{3^j}^k)=0\big\}$$

and

$$g(x)=\prod_{(j,k)\in S}\prod_{\substack{\ell=1\\k\equiv\ell\pmod 3}}^{3^j}(x-\eta\cdot\zeta_{3^j}^\ell)$$

to show that $|S| \le n$.

We shall now prove (iii) by applying (ii), with n replaced by $n-1$, to

$$f_0(x) = (1-\omega)^{-1} \cdot \big(f(x) - (1 + x + \cdots + x^{t-1})\big).$$

By assumption, $f_0 \in \mathbb{Z}[\omega][x]$. From the assumptions, we also have $f(1) \neq 0$ and so $\nu_3(|f(1)|^2) = n$ and so $0 < n < 2\nu_3(t)$. Let ζ be a t-th root of unity. We need to show that $|f_0(\zeta)|^2$ is integral and that $\nu_3(|f_0(\zeta)|^2) = n-1$ whenever $f_0(\zeta) \neq 0$. In the case that $\zeta \neq 1$, this follows from $|f_0(\zeta)|^2 = |f(\zeta)|^2/3$ and the assumption that $\nu_3(|f(\zeta)|^2) = n > 0$ whenever $f(\zeta) \neq 0$. In the case that $\zeta = 1$, we have $|f_0(1)|^2 = |f(1) - t|^2/3$. Since $n < 2\nu_3(t)$, by extending the 3-adic valuation ν_3 from $\mathbb{Z}$ to $\mathbb{Z}[\omega]$ via $\nu_3(1-\omega) = 1/2$ we find that $\nu_3(f(1)) < \nu_3(t)$ and so $\nu_3(|f_0(1)|^2) = n-1$, as required. These calculations also show that $f_0(\eta) \neq 0$. We may therefore apply (ii), with n replaced by $n-1$, to $f_0(x)$. Since the order of η is not divisible by 3, we have $f_0(\eta \cdot \zeta_{3^j}^k) = (1-\omega)^{-1} f(\eta \cdot \zeta_{3^j}^k)$ for all $(j,k) \in \{1, 2, \dots, \nu_3(t)\} \times \{1, 2\}$ and we therefore obtain (iii). $\square$

We next prove two consequences of Propositions 3 and 7.

Theorem 10. *Suppose that there exists a 3-phase Barker array of size $s \times t$ with $3 \mid t$ and $3 \nmid s$. Then $s \le \nu_3(t)$.*

Proof. Let (a_{ij}) be the 3-phase Barker array and write $f_i(x) = \sum_j a_{ij} x^j$. Let $n = \nu_3(t)$, so that $t = 3^n q$ for some q not divisible by 3.

We write $V = \{1, 2, \dots, n\} \times \{1, 2\}$ and consider the cardinality of the set

$$R = \big\{ I(\zeta_{3^j}^k) : (j,k) \in V \big\},$$

with the function I as given in Proposition 3.

We know from Proposition 3 that $\big|f_{I(1)}(\zeta)\big|^2$ is either 0 or st for each t-th root of unity ζ, and by definition $f_{I(1)}(1) \neq 0$. Since $3 \nmid s$, we have $\nu_3(st) = \nu_3(t) = n$. Then, taking $\eta = 1$ and $f = f_{I(1)}$ in Proposition 7 (iii), we find that $\big\{(j,k) \in V : f_{I(1)}(\zeta_{3^j}^k) \neq 0\big\}$ has cardinality at least $n+1$. Therefore, by Proposition 3, the number of values $(j,k) \in V$ for which $I(\zeta_{3^j}^k) = I(1)$ is at least $n+1$, hence $|R| \le n$.

On the other hand, fix a value $i \in \{0, 1, \dots, s-1\} \setminus \{I(1)\}$ and let τ be a primitive 3^n-th root of unity. Then

$$\begin{aligned} \frac{1}{3^n} \sum_{\ell=0}^{3^n-1} \big|f_i(\tau^\ell)\big|^2 &= \frac{1}{3^n} \sum_{\ell=0}^{3^n-1} \left| \sum_{j=0}^{3^n-1} \tau^{j\ell} \sum_{k=0}^{q-1} a_{i,k\cdot 3^n+j} \right|^2 \\ &= \sum_{j=0}^{3^n-1} \left| \sum_{k=0}^{q-1} a_{i,k\cdot 3^n+j} \right|^2, \end{aligned}$$

by Parseval's identity. Since $3 \nmid q$, the right-hand side is nonzero and so $f_i(\tau^\ell)$ is nonzero for some integer ℓ. Now the polynomial $x^{3^n} - 1$ splits into

$2n+1$ irreducible factors over $\mathbb{Q}(\omega)$, and the minimal polynomials over $\mathbb{Q}(\omega)$ of

$$1,\, \zeta_3,\, \zeta_3^2,\, \zeta_9,\, \zeta_9^2, \dots, \zeta_{3^n},\, \zeta_{3^n}^2$$

are all distinct. Since the value of I in Proposition 3 is the same for all roots of a given minimal polynomial, it follows that $f_i(\zeta_{3^j}^k)$ is nonzero for some $(j,k) \in V$. Therefore, for each $i \in \{0,1,\dots,s-1\} \setminus \{I(1)\}$, there is at least one value of $(j,k) \in V$ for which $I(\zeta_{3^j}^k) = i$, hence $|R| \geq s$.

Combining results, we find that $s \leq n$. □

Theorem 11. *Suppose that there exists a 3-phase Barker array of size $s \times t$ with $3 \mid t$. Write $t = t_0 r$, where r is the product of all primes $p \neq 3$ dividing t such that $\nu_p(st) = 1$. Then*

$$\prod_{p \mid t_0} (1 - 1/p) \leq 2/s,$$

where the product is taken over all prime divisors of t_0.

Proof. Since $s \mid t$ by Theorem 5, $\nu_p(st) = 1$ implies $\nu_p(t) = 1$ for every prime p. Let (a_{ij}) be the 3-phase Barker array and write $f_i(x) = \sum_j a_{ij} x^j$. Let η be a primitive t_0-th root of unity. By Proposition 3, there exists I such that $|f_I(\eta)|^2 = st$, and $|f_I(\zeta)|^2$ is either 0 or st for each t-th root of unity ζ. Let d be a divisor of r, noting that d is square-free and not divisible by 3. We claim that

$$f_I(\eta \cdot \zeta_d^k) \neq 0 \quad \text{for all } k \text{ coprime to } d, \tag{9}$$

which we prove by induction on the number of prime divisors of d. In the case that d is prime, (9) is an immediate consequence of Proposition 7 (i). Now, suppose that (9) is true for all d having at most $\ell - 1$ prime divisors. If d has ℓ prime divisors, write $d = d'p$ for some prime divisor p of d and let k be coprime to d. Then $\zeta_d^{p+d'} = \zeta_{d'} \cdot \zeta_p$ and so

$$f_I(\eta \cdot \zeta_d^{(p+d')k}) = f_I(\eta \cdot \zeta_{d'}^k \cdot \zeta_p^k) \neq 0$$

by the inductive hypothesis and by Proposition 7 (i) with $n = 1$ and $f = f_I$ and η replaced by $\eta \cdot \zeta_{d'}^k$. Since $(p + d', d) = 1$ (because d is square-free), this implies that (9) is true when d has ℓ prime divisors and so completes the induction.

Now, since $3 \mid t_0$ and $(t_0, d) = 1$, the minimal polynomial of $\eta \cdot \zeta_d$ over $\mathbb{Q}(\omega)$ has degree $\phi(t_0 d)/2 = \phi(t_0)\phi(d)/2$. Since $f_I(\eta \cdot \zeta_d) \neq 0$ for all $d \mid r$ by (9), we conclude that

$$\big|\{k \in \mathbb{Z}/t\mathbb{Z} : f_I(\zeta_t^k) \neq 0\}\big| \geq \sum_{d \mid r} \phi(t_0)\phi(d)/2 = \phi(t_0)\, r/2.$$

Thus, by Theorem 5, $t/s \geq \phi(t_0) r/2$, and so $\phi(t_0)/t_0 \leq 2/s$, from which the theorem follows. □

TABLE 1. Restrictions on t for a 3-phase Barker array of size $s \times t$ with $3 \mid t$.

s	$t \geq$
2	18
4	324
5	4 860
7	61 236
8	64 297 800
10	591 671 570 490
11	466 344 774 195 300
13	548 127 023 739 189 674 570 891 100

4. Explicit bounds on s and t

In this section, we consider the existence of a 3-phase Barker array of size $s \times t$ with $3 \mid t$. We combine Theorems 5, 6, 10, and 11 to show that no such array exists for $t < T(s)$, where $T(s)$ is a double-exponentially growing function.

From Theorem 6, if $s > 3$ then $3 \nmid s$. From Theorem 5, we find that $s \mid t$ and from Theorem 10, we find that $3^s \mid t$. Theorem 11 gives a lower bound for the number of prime divisors p of t such that $\nu_p(st) \geq 2$. For example, for $s = 7$, we find that t has at least three prime divisors p such that $\nu_p(st) \geq 2$, and therefore $t \geq 2^2 \cdot 3^7 \cdot 7 = 61\,236$. As another example, for $s = 8$, we find that t has at least four prime divisors such that $\nu_p(st) \geq 2$, and thus $t \geq 2^3 \cdot 3^8 \cdot 5^2 \cdot 7^2 = 64\,297\,800$. For $s = 20$, we find that $t > 10^{214}$. More results are given in Table 1. (Application of Theorem 4 cannot improve these results.)

We next derive an explicit lower bound for t that holds for all $s \geq 60$. To do so, we shall need the following two technical lemmas. Henceforth, a sum or product over p is taken over the primes.

Lemma 12. *For all $x > 1.04 \times 10^7$, we have*

$$\prod_{p \leq x} p > \exp(0.999x).$$

Proof. We define

$$\theta(x) = \sum_{p \leq x} \log p.$$

Then a result due to Schoenfeld [Sch76, p. 360] gives

$$|\theta(x) - x| < 0.0077629 \frac{x}{\log x} \quad \text{for } x > 1.04 \times 10^7.$$

Thus,

$$\theta(x) > x\left(1 - \frac{0.0077629}{\log x}\right) > 0.999x \quad \text{for } x > 1.04 \times 10^7.$$

Exponentiating both sides gives the desired result. □

Lemma 13. *Let $c \in (0, 1/30]$ and let S be a set of primes such that*

$$\prod_{p\in S}(1-1/p) \le c.$$

Then

$$\prod_{p\in S} p > 2.71^{1.72^{1/c}}.$$

Proof. Let $p_1 < \cdots < p_n$ denote the first n primes, where n is the smallest natural number such that

$$\prod_{i=1}^{n}(1-1/p_i) \le c.$$

Since $\prod_{p\in S}(1-1/p) \le c$, we have $|S| \ge n$ and so

$$\prod_{p\in S} p \ge p_1\cdots p_n.$$

Hence, it is sufficient to choose x such that

$$\prod_{p\le x}(1-1/p) \le c \tag{10}$$

and then show

$$\prod_{p\le x} p > 2.71^{1.72^{1/c}}. \tag{11}$$

Taking logarithms on both sides of (10), we find that

$$-\sum_{p\le x}\sum_{k\ge 1}\frac{1}{kp^k} \le \log c, \tag{12}$$

using $\log(1-y) = -\sum_{k\ge 1} y^k/k$ for $|y| < 1$. For all real $z \ge 2$, we have

$$\sum_{k\ge 2}\frac{1}{kz^k} \le \frac{1}{2z^2} + \frac{1}{3z^3} + \frac{1}{4z^4}\sum_{k\ge 0}\frac{1}{z^k} \le \frac{1}{2z^2} + \frac{1}{3z^3} + \frac{1}{2z^4}.$$

Hence

$$\sum_{p\le x}\sum_{k\ge 2}\frac{1}{kp^k} \le \frac{1}{2}\sum_{p}\frac{1}{p^2} + \frac{1}{3}\sum_{p}\frac{1}{p^3} + \frac{1}{2}\sum_{p}\frac{1}{p^4} \le 0.33$$

using bounds on the prime zeta function $\sum_p p^{-s}$ (see [Slo, A085548, A085541, A085964], for example). Thus, from (12),

$$-\log c \le \sum_{p\le x}\frac{1}{p} + 0.33.$$

It follows from

$$\sum_{p\le x}\frac{1}{p} \le \log\log x + 0.27 + \frac{1}{(\log x)^2}$$

(see [BS96, Thm. 8.8.5], for example) that

$$-\log c \le \log\log x + 0.6 + \frac{1}{(\log x)^2}. \tag{13}$$

Now from (10) and $c \le 1/30$ we find that $x > 1.04 \cdot 10^7$, which implies that $1/(\log x)^2 < 0.004$. Then from (13) we obtain

$$-\log c < \log\log x + 0.604$$

and therefore $x > N(c)$, where

$$N(c) = \exp(c^{-1}e^{-0.604}).$$

Since $N(c) > 1.04 \cdot 10^7$, we have by Lemma 12,

$$\prod_{p\le x} p \ge \prod_{p\le N(c)} p > \exp\big(0.999\exp(0.546c^{-1})\big) > 2.71^{1.72^{1/c}},$$

proving (11) as required. □

We now state the main result of this section.

Corollary 14. *Suppose that there exists a 3-phase Barker array of size $s \times t$ with $3 \mid t$ and $s \ge 60$. Then*

$$t > \frac{3^s}{9s} \cdot 7.344^{1.311^s}.$$

Proof. Recall from Theorems 5 and 6 that $s \mid t$ and $3 \nmid s$. Let $n = \nu_3(t)$ and let r be the product of all primes $p \ne 3$ such that $\nu_p(st) = 1$. Furthermore, let s_1 and t_1 be such that $s \mid s_1$ and $(s, t_1) = 1$ and $t = 3^n s_1 t_1 r$. Then, from Theorem 11 we have

$$\prod_{p\mid 3s_1t_1} (1 - 1/p) \le 2/s.$$

By assumption, $2/s \le 1/30$ and therefore, by Lemma 13,

$$\prod_{p\mid 3s_1t_1} p > 2.71^{1.72^{s/2}}. \tag{14}$$

If $p \mid t_1$, then $p^2 \mid t_1$ and hence

$$t \ge 3^n s_1 t_1 \ge \frac{3^n}{9s} \prod_{p\mid 3s_1t_1} p^2$$

since every prime factor of s_1 is also a prime factor of s. By Theorem 10, $n \ge s$ and therefore from (14),

$$t > \frac{3^s}{9s} \cdot 2.71^{2\cdot 1.72^{s/2}} > \frac{3^s}{9s} \cdot 7.344^{1.311^s},$$

as required. □

As an example of how quickly this function grows, we note that, if a 3-phase Barker array of size $s \times t$ exists with $3 \mid t$, then for $s = 61$ we get $t > 10^{12919604}$; for $s = 70$ we get $t > 10^{147799386}$; and for $s = 80$ we find that t must have more than 2.2 billion digits!

5. Final Remarks

Lemma 2 was established by Turyn [Tur68, p. 211] for $s = 1$, which implies that a 3-phase Barker array of size $1 \times 3q$ gives rise to a circulant complex Hadamard matrix whose elements are third roots of unity [Tur68, p. 211] and to a relative difference set [MN09]. Some nonexistence results for these objects have been derived in [Tur68] and [MN09] and references therein. These, of course, imply nonexistence results for 3-phase Barker arrays of size $1 \times 3q$. In particular, we can deduce the case $s = 1$ of Theorem 4 from [Tur68, p. 211]. Moreover, as reported in [Jed08], it has been verified by an exhaustive search that there is no 3-phase Barker array of size $1 \times t$ for $10 \le t \le 76$.

We have restricted our analysis of 3-phase Barker arrays of size $s \times t$ to the case $3 \mid st$. Indeed, the approach taken in this paper does not seem to be directly applicable to the case $3 \nmid st$. The reason is that the proof of Proposition 3 relies crucially on the property that $P_A(u, v)$ is independent of v for $(u, v) \neq (0, 0)$. This property does not hold for 3-phase Barker arrays in general. For example, take $A = [1, \omega, \omega, \omega^2, \omega, \omega, 1]$, which is a 3-phase Barker array of size 1×7 satisfying $(P_A(0, v) : 0 \le v < 7) = (7, 1, -2, 1, 1, -2, 1)$.

We have, however, verified the nonexistence of 3-phase Barker arrays of many small sizes by exhaustive search. Table 2 shows a summary of the search results combined with Theorem 4. Based on the data and the results of this paper, we conjecture that there is no 3-phase Barker array of size $s \times t$ with $s, t > 1$, except when $s = t = 2$ or $s = t = 3$.

Table 2. Restrictions on t for a 3-phase Barker array of size $s \times t$ with $(s, t) \neq (2, 2)$

s	$t \geq$
2	31
4	20
5	10
7	8

References

[AS89] S. Alquaddoomi and R. A. Scholtz. On the nonexistence of Barker arrays and related matters. *IEEE Trans. Inf. Theory*, 35(5):1048–1057, 1989.

[Bar53] R. H. Barker. Group synchronization of binary digital systems. In W. Jackson, editor, *Communication Theory*, pages 173–187. Academic Press, New York, 1953.

[BS96] E. Bach and J. Shallit. *Algorithmic Number Theory, Volume I: Efficient Algorithms*. Foundations of Computing. The MIT Press, Cambridge, MA, 1996.

[DJS07] J. A. Davis, J. Jedwab, and K. W. Smith. Proof of the Barker array conjecture. *Proc. Amer. Math. Soc.*, 135:2011–2018, 2007.

[GS65] S. W. Golomb and R. A. Scholtz. Generalized Barker sequences. *IEEE Trans. Inf. Theory*, IT-11(4):433–437, 1965.

[Jed08] J. Jedwab. What can be used instead of a Barker sequence? *Contemp. Math.*, 461:153–178, 2008.

[Lan94] S. Lang. *Algebraic number theory*, volume 110 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2nd edition, 1994.

[LS12] K. H. Leung and B. Schmidt. New restrictions on possible orders of circulant Hadamard matrices. *Des. Codes Cryptogr.*, 64:143–151, 2012.

[MN09] S. L. Ma and W. S. Ng. On the non-existence of perfect and nearly perfect sequences. *Int. J. Inf. Coding Theory*, 1(1):15–38, 2009.

[Sch76] L. Schoenfeld. Sharper bounds for the Chebyshev functions $\theta(x)$ and $\psi(x)$. II. *Math. Comp.*, 30(134):337–360, 1976.

[Slo] N. J. A. Sloane. The On-Line Encyclopedia of Integer Sequences. `http://oeis.org`.

[Tur68] R. J. Turyn. Sequences with small correlation. In Henry B. Mann, editor, *Error Correcting Codes*. Wiley, New York, 1968.

[Tur74] R. J. Turyn. Four-phase Barker codes. *IEEE Trans. Inf. Theory*, 20(3):366–371, 1974.