COMBINATORICA 6 (3) (1986) 275—278

ON THE NON-EXISTENCE OF BARKER SEQUENCES

M. ELIA

Received 1 August 1983

It is an old conjecture that there are no unknown Barker sequences. Here, a sufficient condition for the non-existence of Barker sequences of even length $4m^2$ is given, which allows us to show that there are no unknown sequences with m less than 105, except $m=63$, which remains still undecided.

A sequence $x_0, x_1, \ldots, x_{N-1}$, $x_i = \pm 1$, is called a Barker sequence if its aperiodic autocorrelation sequence $c_0, c_1, \ldots, c_{2N-2}$ defined as

$$c_k = c_{2N-2-k} = \sum_{i=0}^{k} x_i x_{i+N-k-1} \tag{1}$$

takes on absolute values not greater than 1 for $k \neq N-1$.

If we define respectively the generating polynomials $f(z)$ and $F(z)$ of a Barker sequence and of its autocorrelation sequence as

$$f(z) = \sum_{i=0}^{N-1} x_i z^i$$

$$F(z) = \sum_{k=0}^{2N-2} c_k z^k$$

then equation (1) yields

$$F(z) = z^{N-1} f(z) f(z^{-1}). \tag{2}$$

About these sequences, first considered by Barker [1], a number of results are known which can be summarized as follows:

i) No Barker sequence is known with $N > 13$;

ii) If $f(z)$ is the generating polynomial of a Barker sequence, also $-f(z)$, $f(-z)$, $-f(-z)$, $z^{N-1}f(z^{-1})$, $-z^{N-1}f(z^{-1})$, $(-z)^{N-1}f(-z^{-1})$ and $-(-z)^{N-1}f(-z^{-1})$ are generating polynomials of Barker sequences;

iii) Should any other Barker sequence exist its length must be an even square $N=4m^2$, with m an odd integer (see Th. 2.17, page 50 of [2]) greater than or equal to 55;

AMS subject classification (1980): 05 B 99

iv) The existence of a Barker sequence of even length $N \geqq 4$ entails the existence of a cyclic Hadamard matrix of order N (its first row is just a Barker sequence). This in turn is equivalent to the existence of cyclic difference sets with parameters [2]: $v=N$; $k=N/2-\sqrt{N}/2$; $\lambda=N/4-\sqrt{N}/2$.

In this paper we shall consider Barker sequences of even length $N=4m^2$, where m is an odd integer greater than one; the main result consists of a simple sufficient condition for the non-existence of Barker sequences: this condition lets us exclude all values of m less than 105, except 63, which remains still undecided.

Let us recall some facts about the cyclotomic extensions of the field $\mathbf{Q}$ of rational numbers for easy reference; proofs may be found, for example in [3].

Let ξ be a primitive n-th root of unity, let $\mathbf{Q}(\xi)$ denote the cyclotomic extension of $\mathbf{Q}$. Therefore $\mathbf{Q}(\xi)$ is a normal extension of degree $\varphi(n)$, $\varphi(\cdot)$ is the totient Euler function. The conjugates of ξ in $\mathbf{Q}(\xi)$ under the Galois group are the roots of the cyclotomic polynomial $\Phi_n(z)$ given by

$$\Phi_n(z) = \prod_{d|n} (z^d-1)^{\mu(n/d)}$$

where $\mu(\cdot)$ denotes the Möbius function.

The only elements of $\mathbf{Q}(\xi)$ of modulus 1 are $\pm\xi^i$, $i=0, 1, \ldots, n-1$; thus, if two sets of numbers $a(\xi^h), b(\xi^h) \in \mathbf{Q}(\xi)$ have the same moduli, i.e.

$$|a(\xi^h)| = |b(\xi^h)| \quad h = 0, 1, \ldots, n-1$$

then

$$a(\xi^h) = \pm \xi^{t(h)} b(\xi^h) \quad h = 0, 1, \ldots, n-1,$$

where $t(\cdot)$ is a function taking on integer values. Moreover, as h is forced to range into the set of integers prime to n, then $t(h)=sh$ for some integer s, i.e.

$$a(\xi^h) = \pm \xi^{sh} b(\xi^h) \quad h \text{ prime to } n.$$

This equation allows us to write

$$a(z) = z^s b(z) + \Phi_n(z) g(z) \tag{3}$$

for some polynomial $g(z)$.

We can now state our main theorem.

Theorem. *Barker sequences of length $N=4m^2$, where $m=p^k q$, p^k an odd prime power relatively prime to q, do not exist whenever $p^k > 2q$; this is always the case if $q=1$.*

Proof. Consider the cyclic Hadamard matrix H obtained as follows

$$H = f(C)$$

where C is the cyclic permutation matrix defined as

$$C = \begin{pmatrix} 0 & 1 & 0 & \ldots & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \ldots & & 0 & 0 \\ \cdot & & & \cdot & \cdot & \cdot & \cdot \\ \cdot & & & \cdot & \cdot & \cdot & \cdot \\ \cdot & & & & \cdot & \cdot & \cdot \\ 0 & 0 & \ldots & & 0 & 0 & 1 \\ 1 & 0 & \ldots & & & 0 & 0 \end{pmatrix}.$$

If we let Q denote a matrix that diagonalizes C, then we have

$$QCQ^{-1} = \operatorname{diag}(1, \zeta, \zeta^2, \ldots, \zeta^{N-1}) \tag{4}$$

where ζ turns out to be an N-th primitive root of unity. Due to (4), Q also diagonalizes both H and its transpose H^T

$$\begin{aligned} QHQ^{-1} &= \operatorname{diag}(f(1),\ f(\zeta), \ldots, f(\zeta^{N-1})) \\ QH^TQ^{-1} &= \operatorname{diag}(f(1), f(\bar{\zeta}), \ldots, f(\bar{\zeta}^{M-1})) \end{aligned} \tag{5}$$

where an overbar denotes complex conjugation.

Since H is an Hadamard matrix, i.e. $HH^T = N \cdot I$ where I denotes the identity matrix, from equation (5) we obtain

$$f(\zeta^i) f(\bar{\zeta}^i) = N \quad i = 0, 1, \ldots, N-1$$

that is

$$|f(\zeta^i)| = 2m \quad i = 0, 1, \ldots, N-1. \tag{6}$$

Now restricting ourselves to consider only primitive $4p^k$-th roots of unity, p^k being the greatest prime power dividing m, due to equations (3) and (6) we may write

$$f(z) = 2mz^s + (z^{2p^{2k}} + 1) g(z) / (z^{2p^{2k-1}} + 1)$$

which will be more conveniently rewritten in the form

$$(z^{2p^{2k-1}} + 1) f(z) = 2mz^{s+2p^{2k-1}} + 2mz^s + (z^{2p^{2k}} + 1) \sum_{i=0}^{(4q^2-2)p^{2k}+2p^{2k-1}-1} g_i z^i.$$

From the right side polynomial of this equation we may extract the following chain of coefficients

$$2m + g_w,\ g_w + g_{w+2p^{2k}},\ g_{w+2p^{2k}} + g_{w+4p^{2k}},\ \ldots,\ g_{w+2rp^{2k}} \tag{7}$$

where $w = s + 2p^{2k-1}$, and r is the maximum integer such that

$$(4q^2-2)p^{2k} + 2p^{2k-1} - 1 > s + 2rp^{2k} + 2p^{2k-1}$$

thus r is upper bounded by $2q^2 - 2$.

On the other hand, the left side polynomial has coefficients of absolute value not greater than 2; hence chain (7) implies

$$2m - 2r \leqq |g_{s+2rp^{2k}+2p^{2k-1}}|,$$

thus a contradiction is obtained whenever $2 < m - r$, this is always the case if $p^k > 2q$, given that $r < 2q^2 - 2$. ∎

This theorem excludes Barker sequences of length $4m^2$, with m greater than 53 and less than 105, except 63, 77 and 99, but theorem 2.13 of [2] eliminates 77 and 99 so that only 63 remains still undecided.

References

[1] R. H. BARKER, Group synchronizing of binary digital systems, *in: Communication Theory*, (W. Jackson, ed.), Academic Press, New York, (1953), 273—287.
[2] L. D. BAUMERT, *Cyclic Difference Sets*, Springer Verlag, New York, (1971).
[3] T. W. HUNGERFORD, *Algebra*, Springer-Verlag, New York, (1980).
[4] R. TURYN and J. STORER, On binary sequences, *Proc. Am. Math. Soc.*, **12** (1961), 394—399.

Michele Elia

Instituto Matematico
Politecnico di Torino
Italy