3. Barker sequences

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **38 (1992)**

Heft 3-4: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **26.05.2024**

In the fourth column of Table II, we have indicated the known existing cyclic difference sets or the relevant prime power exhibiting non-existence by the semi-primitivity theorem of Section 1. The values of the parameter n left out by these two classes are $n = 7, 25, 28, 37, 43, 44, 49, 52, 61, 67, 72, 75, 76, 86, 97, 99$ and 100. We have reached a non-existence conclusion in these cases by using the multiplier theorem of Section 1. The required calculations being quite lengthy, it is impossible to expose them all. Instead, Section 4 contains some typical examples of application of this theorem.

3. Barker sequences

Recall that a Barker sequence is a binary sequence $A = (a_1, \ldots, a_l)$ such that the aperiodic correlations $c_j(A) = \sum_{i=1}^{l-j} a_i a_{i+j}$ belong to $\{-1, 0, 1\}$ for all $j = 1, \ldots, l-1$.

The set of Barker sequences of a given length is preserved by the following transformations:

$$A \mapsto \alpha A, \text{ where } (\alpha A)_i = -a_i$$
$$A \mapsto \beta A, \text{ where } (\beta A)_i = (-1)^i a_i$$
$$A \mapsto \gamma A, \text{ where } (\gamma A)_i = a_{l-i+1},$$

with $l = \text{length}(A)$.

The group of transformations of Barker sequences generated by α, β and γ is the elementary abelian 2-group $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ of rank 3 if l is odd, and is the non-abelian dihedral 2-group of order 8 with presentation

$$D_8 = <\alpha, \beta, \gamma : \alpha^2 = \beta^2 = \gamma^2 = 1, \ \alpha\beta = \beta\alpha, \alpha\gamma = \gamma\alpha, \gamma\beta\gamma = \alpha\beta>$$

for l even. Note that in this case, D_8 is also generated by $\rho = \beta\gamma$ and γ with presentation

$$D_8 = <\rho, \gamma : \rho^4 = \gamma^2 = 1, \gamma\rho\gamma = \rho^{-1}> .$$

Case of odd length. The complete list of Barker sequences of odd length was established by R. Turyn and J. Storer, [ST] and reads as follows (in lengths $\geqslant 3$):

$$(1, 1, -1)$$
$$(1, 1, 1, -1, 1)$$
$$(1, 1, 1, -1, -1, 1, -1)$$
$$(1, 1, 1, -1, -1, -1, 1, -1, -1, 1, -1)$$
$$(1, 1, 1, 1, 1, -1, -1, 1, 1, -1, 1, -1, 1) .$$

The list is complete up to the transformations α, β and γ given above. The orbit of each Barker sequence in the above Turyn-Storer list under this transformation group consists of 4 sequences.

Case of even length. The situation here is completely different. The only known examples are

$$(1, 1) \quad \text{and} \quad (1, 1, 1, -1),$$

again up to modifications by the above transformations α, β and γ. Note that the sequence $(1, 1, 1, -1)$ gives rise to 8 sequences under this transformation group.

It is widely believed that these are the only Barker sequences of even length. We will show that this is true up to length 1 898 884.

We know from Section 1 that a Barker sequence of even length ($\geqslant 4$) is also a periodic Barker sequence with correlation $\gamma = 0$, and we know from Section 2 that the length l must be of the form $l = 4N^2$ with N odd, if $l \geqslant 4$. We also know from Section 2 that if N is an odd integer with a prime factor p such that p is self-conjugate modulo N, then there is no (periodic) Barker sequence of length $4N^2$. In other words, N is excluded if, for p as above, there is some positive integer f such that $p^f \equiv -1 \bmod N'$, where N' is the largest divisor of N which is relatively prime to p. An immediate consequence is that N cannot be a prime or a prime power. R. Turyn used the above theorem to show that, if there exists a (periodic) Barker sequence of length $l = 4N^2$ with $N > 1$, then necessarily $N \geqslant 55$. With the following result of [EKS], this bound can be improved to $N \geqslant 689$, but only for true (i.e. aperiodic) Barker sequences.

THEOREM. *Let l be an even integer having a prime factor $p \equiv 3$ mod 4. Then there is no Barker sequence of length l.*

For the proof, we will need the following

LEMMA. *Let $f(z), g(z) \in \mathbf{F}_p[z, z^{-1}]$ be non-zero elements satisfying*

$$f(z)f(z^{-1}) + g(z)g(z^{-1}) = 0 .$$

Then either $p = 2$ or $p \equiv 1$ mod 4.

Proof. Since $\mathbf{F}_p[z, z^{-1}]$ is a unique factorization domain, we may suppose that $f(z)$, $g(z)$ are coprime, by clearing any common factor. But then, the equation implies that $f(z)$ divides $g(z^{-1})$. We may thus write

$$g(z^{-1}) = h(z)f(z) , \quad g(z) = h(z^{-1})f(z^{-1})$$

for some $h(z) \in \mathbf{F}_p[z, z^{-1}]$. Substituting these expressions for $g(z)$ and $g(z^{-1})$ and clearing the common factor $f(z)f(z^{-1})$ in the resulting equation, we obtain

$$1 + h(z)h(z^{-1}) = 0 .$$

Letting $z = 1$, this gives $-1 = h(1)^2$ in $\mathbf{F}_p$, and therefore p is not congruent to 3 mod 4. □

Proof of the Theorem. Let $A = (a_1, \ldots, a_l)$ be a Barker sequence of even length l, and consider the two polynomials

$$F(z) = \sum_{i=1}^{l} a_i z^{i-1} \quad \text{and} \quad G(z) = F(-z) = \sum_{i=1}^{l} (-1)^{i-1} a_i z^{i-1} .$$

CLAIM: *Then, (F, G) is a Golay pair, i.e.*

$$F(z)F(z^{-1}) + G(z)G(z^{-1}) = 2l \quad \textit{in } \mathbf{Z}[z, z^{-1}] .$$

Indeed, the constant term of $F(z)F(z^{-1}) + G(z)G(z^{-1})$ is equal to $2\sum a_i^2 = 2l$. On the other hand, for $j > 0$, the coefficient of $z^j + z^{-j}$ in $F(z)F(z^{-1}) + G(z)G(z^{-1})$ is equal to

$$\sum_{i=1}^{l-j} (a_i a_{i+j} + (-1)^j a_i a_{i+j}) ,$$

which is zero if j is odd, and is equal to $2c_j(A)$ if j is even. But $c_j(A) = 0$ if j is even and positive, since $c_j(A)$ belongs to $\{-1, 0, 1\}$ by hypothesis, and $c_j \equiv j \bmod 2$. Therefore, $F(z)F(z^{-1}) + G(z)G(z^{-1}) = 2l$ in $\mathbf{Z}[z, z^{-1}]$, as claimed.

Reducing the above equation modulo p, we obtain two non-zero elements $f(z), g(z)$ in $\mathbf{F}_p[z, z^{-1}]$ satisfying

$$f(z)f(z^{-1}) + g(z)g(z^{-1}) = 0 .$$

By the lemma above, we conclude that p cannot be congruent to 3 mod 4. □

APPLICATION. *There is no Barker sequence of length $l = 4N^2$, if $1 < N < 689$. In particular, there is no Barker sequence of even length greater than 4 and less than 1 898 884.*

Of course, it suffices to consider only those $N < 689$ which are odd, are not a prime or a prime power, and have no factor congruent to 3 mod 4. Since the square root of 689 is smaller than 26, every such N must have a prime factor equal to 5, 13 or 17.

The remaining candidates are listed below, together with an indication in parenthesis showing that each one (except 505) is excluded by Theorem 2 in Section 2: if N has a prime factor p such that $p^f \equiv -1 \bmod N'$, where N' is the largest divisor of N relatively prime to p, then there is no (periodic) Barker sequence of length $4N^2$.

REMAINING CANDIDATES (excluded by Theorem 2, except $N = 505$.)

N		N	
$65 = 5 \cdot 13$	$(5^2 \equiv -1 \bmod 13)$	$425 = 5^2 \cdot 17$	$(5^8 \equiv -1 \bmod 17)$
$85 = 5 \cdot 17$	$(17^2 \equiv -1 \bmod 5)$	$445 = 5 \cdot 89$	$(89 \equiv -1 \bmod 5)$
$145 = 5 \cdot 29$	$(29 \equiv -1 \bmod 5)$	$481 = 13 \cdot 37$	$(37^6 \equiv -1 \bmod 13)$
$185 = 5 \cdot 37$	$(37^2 \equiv -1 \bmod 5)$	$485 = 5 \cdot 97$	$(97^2 \equiv -1 \bmod 5)$
$205 = 5 \cdot 41$	$(5^{10} \equiv -1 \bmod 41)$	$493 = 17 \cdot 29$	$(17^2 \equiv -1 \bmod 29)$
$221 = 13 \cdot 17$	$(13^2 \equiv -1 \bmod 17)$	$505 = 5 \cdot 101$	
$265 = 5 \cdot 53$	$(53^2 \equiv -1 \bmod 5)$	$533 = 13 \cdot 43$	$(43^3 \equiv -1 \bmod 13)$
$305 = 5 \cdot 61$	$(5^{15} \equiv -1 \bmod 61)$	$545 = 5 \cdot 109$	$(109 \equiv -1 \bmod 5)$
$325 = 5^2 \cdot 13$	$(5^2 \equiv -1 \bmod 13)$	$565 = 5 \cdot 113$	$(113^2 \equiv -1 \bmod 5)$
$365 = 5 \cdot 73$	$(73^2 \equiv -1 \bmod 5)$	$629 = 17 \cdot 37$	$(37^8 \equiv -1 \bmod 17)$
$377 = 13 \cdot 29$	$(13^7 \equiv -1 \bmod 29)$	$685 = 5 \cdot 137$	$(137^2 \equiv -1 \bmod 5)$

The case $N = 505 = 5 \cdot 101$ cannot be excluded by Theorem 2, because $101 \equiv 1 \bmod 5$ and $5^{25} \equiv 1 \bmod 101$. However, 505 can still be excluded by Turyn's Inequality, as observed in [JL]: choosing $p = 101$ and $w = 2 \cdot 101^2$, so that p is trivially semi-primitive modulo w, we would have

$$p \leqslant \frac{v}{w} = 2 \cdot 5^2 = 50 ,$$

a contradiction to the assumed existence of a Barker sequence of length $4 \cdot 505^2$.

The first open case is thus $N = 689 = 13 \cdot 53$. We have $53 \equiv 1 \bmod 13$ and $13^{13} \equiv 1 \bmod 53$, so that neither 53 is semi-primitive mod 13, nor 13 is semi-primitive mod 53. The next open case is $N = 793 = 13 \cdot 61$.

4. THE USE OF THE MULTIPLIER THEOREM

In this section we give the details of some (typical) non-existence proofs needed to establish the tables, using the multiplier theorem.

Recall that if D is a cyclic difference set with parameters (v, k, λ), and if $n = k - \lambda$ is greater than λ, then the group of multipliers of D contains the intersection M in $(\mathbf{Z}/v\mathbf{Z})^*$ of the subgroups generated by $l_1, \ldots, l_r$, where $l_1, \ldots, l_r$ are the prime factors of n.