2. Periodic Barker sequences

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

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

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

PDF erstellt am: **23.09.2024**

Definition. Let G be a finite abelian group and D a difference set on G. The integer m is a *multiplier* for D if m is prime to $v = |G|$, and if the isomorphism $m: G \to G$ induced by multiplication by m, permutes the translates $a + D$ $(a \in G)$ of D.

Thus, m is a multiplier if $(m, v) = 1$, and if $m \cdot D = a + D$ for some $a \in G$.

We will also need the following result:

PROPOSITION. *Let m be a multiplier of a difference set D in an abelian group G. Then some translate $D' = a + D$ $(a \in G)$ of D, is fixed under multiplication by m, i.e. $m \cdot D' = D'$.*

This follows at once from a more general result, stating that an automorphism of a symmetric block design fixes as many points as blocks. (See [L], Theorem 3.1, page 78.) In our context, the multiplication by m in G fixes 0, hence it must fix at least one translate of D.

As a consequence, if an abelian difference set D admits a multiplier m, we may very well suppose that D is fixed under multiplication by m, and thus, that D is a *union of orbits under multiplication by m.*

The multiplier theorem below tells us how to find multipliers of abelian difference sets.

MULTIPLIER THEOREM. *Let D be a (v, k, λ) difference set in an abelian group G. Let n_1 be a divisor of $n = k - \lambda$ such that $n_1 > \lambda$. Suppose m is an integer satisfying*

(1) $\gcd(m, v) = 1$;

(2) *for every prime divisor p of n_1, m is a power of p modulo the exponent e of G.*

Then, m is a multiplier of the difference set D.

In Section 4, we will use this theorem to exclude the existence of periodic Barker sequences of various lengths.

2. PERIODIC BARKER SEQUENCES

This section deals with periodic Barker sequences, i.e. binary sequences whose periodic correlations γ_j are constant and equal to $\gamma \in \{0, 1, -1\}$.

Case $\gamma = 0$. In this case, the parameters (v, k, λ) and $n = k - \lambda$ of the associated cyclic difference set (see Section 1) satisfy:

$$n = N^2, \quad v = 4N^2, \quad k = 2N^2 - N, \quad \lambda = N^2 - N.$$

These follow respectively from Schützenberger's theorem for v even, the relations $v - 4n = \gamma$, $k(k-1) = \lambda(v-1)$, and our assumption $k \leqslant v/2$.

We will now prove a theorem of R. Turyn [T1], stating that N must necessarily be odd. (See also [Bau].)

THEOREM 1. *Let D be a cyclic difference set with parameters $v = 4N^2, k = 2N^2 - N$ and $\lambda = N^2 - N$. Then N is odd.*

For the proof, we will need the following two lemmas.

LEMMA 1. *Let $\eta = \eta_r$ be a primitive 2^r-th root of unity $(r > 0)$. Let $\theta \in \mathbf{Z}[\eta]$ satisfy*

$$\theta\bar{\theta} \equiv 0 \mod (2)^{2s}, \qquad (s > 0)$$

where $^-$ denotes complex conjugation. Then

$$\theta \equiv 0 \mod (2)^s .$$

Proof. In $\mathbf{Z}[\eta]$, the ideal (2) is a power of the prime ideal $P = (1 - \eta)$, and clearly $P = \bar{P}$. We have $(2) = P^k$, say.

Suppose $\theta \in P^m$ where m is maximal. Then $\theta\bar{\theta} \in P^{2m}$, and $2m$ is also maximal. But $\theta\bar{\theta} \in (2)^{2s} = P^{2sk}$, which implies $2m \geqslant 2sk$, i.e. $m \geqslant sk$, and hence $\theta \in (2)^s$, as claimed. □

On the level of group rings, there is a similar result, albeit necessarily weaker. For $i > 0$, we will use the following notation:

(1) η_i is a primitive 2^i-th root of unity;

(2) Γ_i is the multiplicative cyclic group of order 2^i with generator x_i;

(3) $\rho: \mathbf{Z}\Gamma_i \to \mathbf{Z}[\eta_i]$ is the map induced by $\rho(x_i) = \eta_i$;

(4) $\nu_j: \mathbf{Z}\Gamma_i \to \mathbf{Z}\Gamma_{i-j}$ is the map induced by $\nu_j(x_i) = x_{i-j}$ $(j < i)$.

LEMMA 2. *Let $\theta \in \mathbf{Z}[\eta_r]$ $(r > 0)$ satisfy*

$$\theta\bar{\theta} \equiv 0 \mod (2)^{2s}, \qquad (0 < s \leqslant r)$$

and let $\alpha \in \mathbf{Z}\Gamma_r$ be any element such that $\rho(\alpha) = \theta$. Then

$$\nu_s(\alpha) \equiv 0 \mod (2)^s$$

in $\mathbf{Z}\Gamma_{r-s}$.

Proof. By induction on s.

(1) Case $s = 1$. Let us write α as

$$\alpha = \sum_{i=0}^{2^r - 1} \alpha_i x_r^i .$$

Then

$$\theta = \rho(\alpha) = \sum_{i=0}^{2^{r-1}-1} (\alpha_i - \alpha_{i+2^{r-1}})\eta_r^i ,$$

since $\eta_r^{2^{r-1}} = -1$. Furthermore, the powers η_r^k with $0 \leqslant k \leqslant 2^{r-1} - 1$ form a $\mathbf{Z}$-basis of $\mathbf{Z}[\eta_r]$. By Lemma 1, we have $\theta \equiv 0 \bmod (2)$, and therefore

(*) $$\alpha_i \equiv \alpha_{i+2^{r-1}} \mod (2)$$

for all $i = 0, \ldots, 2^{r-1} - 1$.

On the other hand,

$$\nu_1(\alpha) = \sum_{i=0}^{2^{r-1}-1} (\alpha_i + \alpha_{i+2^{r-1}})x_{r-1}^i ,$$

and (*) implies that $\nu_1(\alpha) \equiv 0 \bmod (2)$ in $\mathbf{Z}\Gamma_{r-1}$, as claimed.

(2) Case $s > 1$. By (1) above, we have $\nu_1(\alpha) \equiv 0 \bmod (2)$ in $\mathbf{Z}\Gamma_{r-1}$. Thus we have $\nu_1(\alpha) = 2\beta$ in $\mathbf{Z}\Gamma_{r-1}$. Now $\rho(\beta) = \frac{1}{2}\rho(\alpha)$, so that

$$\rho(\beta)\overline{\rho(\beta)} \equiv 0 \mod (2)^{2(s-1)}$$

in $\mathbf{Z}[\eta_{r-1}]$. By the induction hypothesis, we have $\nu_{s-1}(\beta) \equiv 0 \bmod (2)^{s-1}$ in $\mathbf{Z}\Gamma_{r-s}$, and therefore $\nu_s(\alpha) \equiv 0 \bmod (2)^s$ in $\mathbf{Z}\Gamma_{r-s}$. □

Proof of the Theorem. Let $D \subset \mathbf{Z}/v\mathbf{Z} = C_v$ denote a difference set with parameters $(v, k, \lambda) = (4N^2, 2N^2 - N, N^2 - N)$. Identifying $\mathbf{Z}C_v$ with $\mathbf{Z}[x]/(x^v - 1)$, we will denote by $\theta(x)$ the element $\theta(x) = \sum_{d \in D} x^d \in \mathbf{Z}C_v$. We have by hypothesis,

(1) $$\theta(x)\theta(x^{-1}) = N^2 + \lambda(1 + x + \cdots + x^{v-1}) .$$

Given any element z in some ring A, we will denote by $\theta(z)$ the image of $\theta(x)$ under the map $\phi: \mathbf{Z}C_v \to A$ induced by $x \mapsto z$.

Let us write $N = 2^t N_1$ with N_1 odd. Thus, $w = 2^{2t+2}$ is the highest power of 2 dividing $v = 4N^2$. Let Γ_i denote, as above, the cyclic group of order 2^i with generator x_i.

If η is a primitive 2^{2t+2}-th root of unity, we have $\theta(\eta) \cdot \overline{\theta(\eta)} = N^2 \equiv 0 \bmod (2)^{2t}$. Hence, Lemma 2 implies $\theta(x_{t+2}) \equiv 0 \bmod (2)^t$ in $\mathbf{Z}\Gamma_{t+2}$. Denoting x_{t+2} by y, we thus have

$$\theta(y) = 2^t\theta_1(y) ,$$

for some $\theta_1(y) \in \mathbf{Z}\Gamma_{t+2}$.

Now, a direct computation yields

$$\theta_1(y)\overline{\theta_1(y)} = N_1^2 + N_1^3(N-1)(1 + y + \cdots + y^{2^{t+2}-1}) ,$$

so that the constant term (i.e., the coefficient of $1 = y^0$) of $\theta_1(y)\overline{\theta_1(y)}$ is equal to $N_1^2 + N_1^3(N-1)$. On the other hand, write $\theta_1(y)$ as

$$\theta_1(y) = \sum_{i=0}^{2^{t+2}-1} d_i y^i$$

in $\mathbf{Z}\Gamma_{t+2}$. In this notation, the constant term of $\theta_1(y)\overline{\theta_1(y)}$ is equal to $\sum d_i^2$, so that

$$N_1^2 + N_1^3(N-1) = \sum d_i^2 .$$

Now, $\sum d_i^2 \equiv (\sum d_i)^2 \bmod 2$, and

$$(\sum d_i)^2 = \theta_1(1)^2 = N_1^2 + N_1^3(N-1)2^{t+2} .$$

Thus,

$$N_1^2 + N_1^3(N-1) \equiv N_1^2 + N_1^3(N-1)2^{t+2} \mod 2 ,$$

which implies $N \equiv 1 \bmod 2$, as claimed. □

Another very strong restriction on the parameter N is provided by the following easy consequence of Turyn's Inequality, Section 1.

THEOREM 2. *Let N be an odd integer. If N has a prime factor p which is self-conjugate modulo N, then there is no periodic Barker sequence of length $l = 4N^2$.*

Recall that, by definition, p is self-conjugate modulo N if and only if there is a 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.

Proof. In the notation of Turyn's Inequality, take $v = 4N^2$ of course, $m = p$, and $w = v/2 = 2N^2$. Thus $v/w = 2$ and r, the number of distinct prime factors of $\gcd(m, w) = p$ is equal to 1 here.

Let now N' denote the largest divisor of N which is relatively prime to p. By hypothesis, there is a positive integer f such that $p^f \equiv -1 \bmod N'$. Since N' and p are odd, we also have $p^{N'f} \equiv -1 \bmod 2N'^2$. Therefore p is self-conjugate modulo $2N^2 = w$, because $2N'^2$ is the largest divisor of $2N^2$ which is relatively prime to p. If a periodic Barker sequence of length $4N^2$ existed, Turyn's Inequality would then imply

$$p = m \leqslant 2^{r-1}v/w = 2 ,$$

contrary to the fact that p divides N. □

An immediate corollary is that N cannot be a prime or a prime power. R. Turyn used his inequality to show that there exists no periodic Barker sequence of length $l = 4N^2$ with $1 < N < 55$. (The case $N = 39$ required a special argument.) See [T2].

As an example, suppose that $N = p^\lambda \cdot q^\mu$, where both p, q are prime and $\equiv 3 \bmod 4$. The hypothesis of Theorem 2 is then satisfied, i.e. either p or q is self-conjugate modulo N.

This follows from quadratic reciprocity, which implies that either $p^{\frac{q-1}{2}} \equiv -1 \bmod q$, or $q^{\frac{p-1}{2}} \equiv -1 \bmod p$.

More generally, suppose that $N = p^\lambda \cdot q^\mu \cdot N_1$, where p, q are as above, and where N_1 is coprime to p, q, and satisfies furthermore $N_1^2 < \min(p, q)$. Then there are no periodic Barker sequences of length $4N^2$. This follows from Turyn's Inequality, by choosing $w = 4p^{2\lambda}q^{2\mu}$, and $m = p$ or q, according as to wether p is self-conjugate modulo q, or q is self-conjugate modulo p.

(As observed by J. Jedwab, it even suffices to have $N_1^2 < \min(p^\lambda, q^\mu)$, taking $m = p^\lambda$ or q^μ, as the case may be.)

Case $\gamma = 1$. In this case, the parameters (v, k, λ) and $n = k - \lambda$ satisfy

$$v = 2t(t+1) + 1$$
$$k = t^2$$
$$\lambda = \frac{1}{2}t(t-1)$$

and $$n = \frac{1}{2}t(t+1) ,$$

for some positive integer t. Indeed, $v = 4n + 1$ (since $v - \gamma = 4n$ for a periodic Barker sequence with correlation γ), and the symmetric block design relation $k(k-1) = \lambda(v-1)$ yields $k = (k - 2\lambda)^2$. Setting $t = k - 2\lambda$, we find the parametrization above. Since the parameter values are the same for $-t$ and $t-1$, we may assume $t \geqslant 1$. (Recall also our convention $k \leqslant \frac{1}{2}v$.) Observe that the Chowla-Ryser condition is here always satisfied: the triple $X = 1, Y = 1$ and $Z = t$ is a nontrivial integral solution to the equation $nX^2 + (-1)^{\frac{1}{2}(v-1)}\lambda Y^2 = Z^2$. The case $t = 1$ is trivial: $\lambda = 0$. It does however correspond to the Barker sequence $1, 1, 1, -1, 1$. For $t = 2$, we have the parameter values $(13, 4, 1)$ and the essentially unique cyclic difference set

$$D = \{0, 1, 3, 9\} .$$

More geometrically, we can describe this difference set using the projective plane $\mathbf{P}^2(\mathbf{F}_3)$ over the field $\mathbf{F}_3$ with 3 elements which possesses an automorphism, the Singer automorphism of order 13. Viewing $E = \mathbf{P}^2(\mathbf{F}_3)$ as a G-set with G cyclic of order 13, the difference set $D \subset E$ is then given by any line $\mathbf{P}^1(\mathbf{F}_3) \subset \mathbf{P}^2(\mathbf{F}_3)$. The Singer automorphism is best described by taking the orbits of the $\mathbf{F}_3^*$-action on $\mathbf{F}_{27}$. The map $S: \mathbf{P}^2(\mathbf{F}_3) \to \mathbf{P}^2(\mathbf{F}_3)$ then corresponds to the multiplication by a generator α of the cyclic group $\mathbf{F}_{27}^*$. (See [L], page 125.)

We will prove that there is no other cyclic difference set with parameters $\left(2t(t+1), t^2, \frac{1}{2}t(t-1)\right)$ for $t \leqslant 100$, except perhaps for $t = 50$, where the existence of a cyclic difference set with parameters $(5101, 2500, 1225)$ still remains unsettled. We only know that 191 is a multiplier if such a difference set exists.

These non-existence claims are obtained by using the semi-primitivity and multiplier theorems of Section 1. Table I at the end of the paper indicates in each case which of these two results was used. When relevant, the semi-primitivity theorem is very easy to use. In our case, where the parameters are of the form $(v, k, \lambda) = \left(2t(t+1) + 1, t^2, \frac{1}{2}t(t-1)\right)$, there is one further simplification; the semi-primitivity theorem implies the non-existence of a cyclic difference set with n even, in the following two instances:

(1) $v = 2t(t+1) + 1$ is a prime power

(2) $n = k - \lambda = \frac{1}{2}t(t-1)$ is square-free.

(Unfortunately, this simplified criterion does not apply for n odd.) Indeed, since $v = 4n + 1$, we have

$$4n \equiv -1 \mod v ,$$

so that one of the primes dividing $4n$ must be of even order in the group of units $(\mathbf{Z}/v\mathbf{Z})^*$.

If n is even, then $4n$ and n are divisible by the same primes and one of the primes dividing n must be of even order modulo v. Let p, say, be a prime divisor of n and let $2f$ be its order in $(\mathbf{Z}/v\mathbf{Z})^*$.

If v is a prime power, the group $(\mathbf{Z}/v\mathbf{Z})^*$ is cyclic (yes, v is odd) and $p^f \equiv -1 \mod v$. The semi-primitivity theorem applies. If v is not a prime power, there is a prime power divisor w of v such that p is of even order, $2f'$ say, in $(\mathbf{Z}/w\mathbf{Z})^*$. Again, $(\mathbf{Z}/w\mathbf{Z})^*$ being cyclic, this implies $p^{f'} \equiv -1 \mod w$, and the semi-primitivity theorem applies. In the range $3 \leqslant t \leqslant 100$, the semi-primitivity theorem takes care of all the cases, except the values $t = 9, 49, 50$ and 82. (See Table I.)

In contrast, applying the multiplier theorem may require quite lengthy computations on the structure of multiplier orbits. The cases $t = 9$, $t = 82$ (easy) and $t = 49$ (harder) are treated in Section 4 using the multiplier theorem.

Case $\gamma = -1$. The symmetric block design equation $k(k-1) = \lambda(v-1)$ in this case yields the parameter values $(v, k, \lambda) = (4n-1, 2n-1, n-1)$, where $n = k - \lambda$ as usual. Recall that we are assuming $k \leqslant \frac{1}{2} v$, without loss of generality.

Again the Chowla-Ryser equation $nX^2 + (-1)^{\frac{1}{2}(v-1)} \lambda Y^2 = Z^2$ is non-trivially solvable in integers: $X = 1$, $Y = 1$, $Z = 1$.

However, here the situation is quite different from the one in case $\gamma = 1$. There are well known families of cyclic difference sets with parameters of the form $(4n-1, 2n-1, n-1)$.

(1) *Quadratic residues.*

Suppose $v = 4n - 1 = p$ is a prime. Let $D \subset \mathbf{Z}/p\mathbf{Z}$ be the set of non-zero quadratic residues mod p. Then,

$$k = |D| = \frac{1}{2} (p-1) = 2n - 1$$

and D is a difference set with $\lambda = (p-3)/4 = n - 1$. We shall denote this difference set by $QR(p)$.

(2) *Projective spaces.*

Let $E = \mathbf{P}^d(\mathbf{F}_2)$ be the projective d-space over the field with two elements $\mathbf{F}_2$. Of course, $|E| = 2^{d+1} - 1$. The hyperplanes in E form a symmetric block design with parameters

$$(2^{d+1} - 1, 2^d - 1, 2^{d-1} - 1) .$$

The Singer automorphism exhibits this design as a cyclic design on the cyclic group of order $v = 2^{d+1} - 1$. We use $\mathbf{P}^d(\mathbf{F}_2)$ as a notation for this cyclic difference set.

(3) *Gordon-Mills-Welch difference sets.*

Other difference sets with the same parameters as projective spaces have been discovered by B. Gordon, W. H. Mills and L. R. Welch. (See [GMW].) They appear in Table II under the label *GMW*. We give some details of their construction in Section 5.

(4) *Twin primes cyclic difference sets.*

If p and q are twin primes, $q = p + 2$, there is a difference set on $\mathbf{Z}/pq\mathbf{Z} = \mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/q\mathbf{Z}$ with parameters $\left(pq, \frac{1}{2}(pq - 1), \frac{1}{4}(pq - 3)\right)$ and which we shall denote by $TP(p, q)$.

The set $D \subset \mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/q\mathbf{Z}$ is defined by

$$D = (\mathbf{Z}/p\mathbf{Z} \times \{0\}) \cup (S_p \times S_q) \cup (N_p \times N_q) ,$$

where S_p and N_p denote the (non-zero) squares and non-squares mod p respectively, and similarly for S_q and N_q.

(5) *Marshall Hall cyclic difference sets.*

If v is a prime number of the form $v = 4x^2 + 27$ where x is an integer, there is a cyclic difference set with parameters $\left(v, \frac{v-1}{2}, \frac{v-3}{4}\right)$ [H], page 170. We will denote this difference set by $MH(v)$. In Table II, they occur for the values $n = 56$ and $n = 71$ of the parameter n.

In Table II, we settle the existence question for a cyclic difference set with parameters $(4n - 1, 2n - 1, n - 1)$ for $n = 2, \ldots, 100$.

It turns out that the cyclic difference sets with parameters (7, 3, 1) provided by $\mathbf{P}^2(\mathbf{F}_2)$ and $QR(7)$ are isomorphic. In the two other cases of Table II where $4n - 1$ is a prime p of the form $p = 2^d - 1$ (that is, $n = 8$ and 32), $\mathbf{P}^{d-1}(\mathbf{F}_2)$ and $QR(p)$ are non-isomorphic difference sets. (According to [BF], there actually are 6 distinct examples for $n = 32$.)

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 $\geqslant 3$):

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