

Zeitschrift: L'Enseignement Mathématique
Herausgeber: Commission Internationale de l'Enseignement Mathématique
Band: 38 (1992)
Heft: 3-4: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: BARKER SEQUENCES AND DIFFERENCE SETS
Autor: Eliahou, Shalom / Kervaire, Michel
Kapitel: 1. DIFFERENCE SETS
DOI: <https://doi.org/10.5169/seals-59496>

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. [Mehr erfahren](#)

Conditions d'utilisation

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. [En savoir plus](#)

Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. [Find out more](#)

Download PDF: 05.12.2025

ETH-Bibliothek Zürich, E-Periodica, <https://www.e-periodica.ch>

This follows from the obvious congruence $c_j \equiv l - j \pmod{2}$, and the fact that $c_j \in \{-1, 0, +1\}$, for all $j = 1, \dots, l - 1$.

Now, applying the relation $ab \equiv a + b - 1 \pmod{4}$ for any $a, b = \pm 1$, we have

$$(2) \quad c_j = \sum_{i=1}^{l-j} a_i a_{i+j} \equiv \sum_{i=1}^{l-j} (a_i + a_{i+j}) - (l-j) \pmod{4}$$

for $j = 1, \dots, l - 1$.

Comparing the above congruences for two successive values of j , we obtain

$$(3) \quad c_j - c_{j+1} \equiv a_{l-j} + a_{j+1} - 1 \pmod{4},$$

for $j = 1, \dots, l - 2$.

Changing j to $l - j - 1$ leaves the right-hand-side unchanged. Therefore, we have

$$(4) \quad c_j - c_{j+1} \equiv c_{l-j-1} - c_{l-j} \pmod{4},$$

for $j = 1, \dots, l - 2$. Since $|c_j - c_{j+1}| \leq 1$ for all j by (1), we have in fact an equality:

$$c_j - c_{j+1} = c_{l-j-1} - c_{l-j}$$

for $j = 1, \dots, l - 2$. Using Lemma 1, it follows that

$$\gamma_j = \gamma_{j+1}$$

for all $j = 1, \dots, l - 2$, and thus γ_j is independent of j , as claimed.

Now $|\gamma_j| = |c_j + c_{l-j}| \leq 2$, and equality can occur only if $c_j = c_{l-j} = \pm 1$, which by (1) implies in particular that j must be odd. But this is impossible, because γ_j is independent of j . Therefore $|\gamma_j| \leq 1$, as claimed. \square

1. DIFFERENCE SETS

In this section, we show that the notion of a binary sequence with constant periodic correlations is equivalent to that of a difference set on a cyclic group. We then recall basic results concerning these difference sets.

Definition. A difference set D on a group G is a subset $D \subset G$ such that the cardinality of the intersection

$$D \cap g \cdot D$$

is independent of g for $g \in G \setminus \{e\}$. Here, $gD = \{gx \mid x \in D\}$ is the translate of D by the element $g \in G$, and e is the neutral element of G .

It is traditional to denote by v the cardinality of G , by k the cardinality of D and by λ the cardinality of the intersection $D \cap gD$:

$$v = |G|, \quad k = |D|, \quad \lambda = |D \cap gD|.$$

The difference set D in G is then said to have *parameters* (v, k, λ) . It is also traditional to denote by n the difference $k - \lambda$.

Observe that if $D \subset G$ is a difference set, then so is $D' = G \setminus D$. Thus we can and will always assume that $k = |D| \leq \frac{1}{2}v$.

Note that if $D \subset G$ is a difference set, the collection of *right translates* of D , including D itself, viz.

$$\mathcal{B} = \{Dg \mid g \in G\}$$

constitutes a *symmetric block design* on G . This means that each element of G is contained in exactly k blocks (recall $k = |D|$), and every pair of (distinct) elements of G belongs to precisely λ blocks.

Indeed, if $g \in G$, let $g_x = x^{-1}g$; then

$$g \in Dg_x \quad \text{if and only if} \quad x \in D$$

and therefore the correspondence $x \mapsto Dg_x$ provides a bijection between D and the set of blocks containing g .

If $g_1, g_2 \in G$ is a pair of distinct elements of G , set $g_x = x^{-1}g_1$. Then,

$$g_1, g_2 \in Dg_x \quad \text{if and only if} \quad x \in D \cap g_1 g_2^{-1} D$$

and the assignment $x \mapsto Dg_x$ establishes a bijection between $D \cap g_1 g_2^{-1} D$ of cardinality λ and the set of blocks Dg containing the pair g_1, g_2 .

PROPOSITION. *There is a bijection between the set of binary sequences $A = (a_1, \dots, a_v)$ with constant periodic correlation γ , i.e.*

$$\gamma = \sum_{i \bmod v} a_i \cdot a_{i+j}$$

for $j = 1, \dots, v-1$, and difference sets D on the cyclic group $G = \mathbf{Z}/v\mathbf{Z}$ of order v with parameters (v, k, λ) , where $\lambda = k - (v - \gamma)/4$. The set D associated to the sequence A is given by $D = \{i \mid a_i = -1\}$.

Remark. In particular, if there is a binary sequence of length v with constant periodic correlation γ , then one must have $v \equiv \gamma \pmod{4}$, and γ is given by

$$\gamma = v - 4n,$$

where, as above, $n = k - \lambda$.

We call $\gamma = v - 4n$ the *correlation* of the cyclic difference set D with parameters (v, k, λ) .

In the proposition we must momentarily relax our convention $|D| \leq |G|/2$.

Proof. Let $G = \mathbf{Z}/v\mathbf{Z}$. We will represent the elements of G by $\{1, 2, \dots, v\}$. Suppose $A = (a_1, \dots, a_v)$ is a binary sequence and $\gamma = \sum_{i=1}^v a_i a_{i+j}$ is independent of j for $j = 1, \dots, v-1$. To A we associate the subset

$$D = \{i \mid a_i = -1\} \subset G.$$

Set $k = |D|$. We claim that

$$\lambda = |D \cap (j + D)| = k - (v - \gamma)/4$$

for all $j \neq 0$. Indeed, we have

$$\begin{aligned} \gamma = \sum_{i=1}^v a_i a_{i+j} &= |D' \cap (j + D')| + |D \cap (j + D)| - |D \cap (j + D')| \\ &\quad - |D' \cap (j + D)|, \end{aligned}$$

where $D' = G \setminus D$.

Now, we have

- (1) $|D \cap (j + D)| + |D \cap (j + D')| = k$
- (2) $|D \cap (j + D)| + |D' \cap (j + D)| = k$
- (3) $|D' \cap (j + D')| + |D \cap (j + D')| = v - k$
- (4) $|D' \cap (j + D')| + |D' \cap (j + D)| = v - k$

from which we conclude (by comparing (1) and (2)):

$$|D \cap (j + D')| = |D' \cap (j + D)| = k - \lambda$$

and (by subtracting (3) from (1)):

$$|D \cap (j + D)| - |D' \cap (j + D')| = 2k - v.$$

Comparing this with

$$\gamma = |D \cap (j + D)| + |D' \cap (j + D')| - 2(k - \lambda),$$

we get the desired relation

$$2\lambda = 2k - v + \gamma + 2(k - \lambda).$$

Conversely, if $D \subset \mathbf{Z}/v\mathbf{Z}$ is a cyclic difference set, then viewing D as a subset of $\{1, \dots, v\}$, define $a_i = +1$ if $i \notin D$ and $a_i = -1$ if $i \in D$. The periodic correlations $\gamma = \sum_{i \bmod v} a_i a_{i+j}$ ($j = 1, \dots, v-1$) are independent of j and have the common value $\gamma = v - 4n$.

Equivalently, we may recast the proof as follows: write

$$D(z) = \sum_{d \in D} z^d \in \mathbf{Z}[z]/(z^v - 1)$$

if $D \subset \mathbf{Z}/v\mathbf{Z}$. We see that D is a difference set with parameters (v, k, λ) if and only if

$$(1) \quad D(z)D(z^{-1}) = n + \lambda T,$$

where $n = k - \lambda$ and $T = 1 + z + \cdots + z^{v-1}$. Now, $A(z) = \sum_{i=1}^v a_i z^{i-1}$ has constant periodic correlation γ if and only if

$$(2) \quad A(z)A(z^{-1}) = v + \gamma(T - 1) \quad \text{in} \quad \mathbf{Z}[z]/(z^v - 1)$$

If $D \subset \mathbf{Z}/v\mathbf{Z}$ is the set of exponents of the monomials z^i occurring with coefficient -1 in $A(z)$, then $A(z) = T - 2D(z)$, where $D(z) = \sum_{d \in D} z^d$ as above.

An easy calculation, using $T(z^{-1}) = T(z)$ and $z \cdot T(z) = T(z)$, shows that (2) is equivalent to

$$D(z)D(z^{-1}) = \frac{v - \gamma}{4} + \left(k - \frac{v - \gamma}{4} \right) T$$

and therefore (2) is equivalent to D being a cyclic difference set with parameters

$$(v, k, \lambda), \text{ where } \lambda = k - \frac{v - \gamma}{4}. \quad \square$$

Note that a difference set on a group G could equivalently be defined as a subset D of a G -set E such that

$$(1) \quad |E| = |G|,$$

(2) G acts transitively on E , i.e. E affords the regular representation of G , and

$$(3) \quad \lambda = |D \cap gD| \text{ is independent of } g \text{ for } g \in G \setminus \{1\}.$$

We shall sometimes use this presentation in the sequel.

Several necessary conditions must be satisfied by a given triple (v, k, λ) to be realized as the parameters of some difference set. These well known conditions are recalled below. We refer to [L] for more details.

First of all, the triple (v, k, λ) must satisfy the equation

$$k(k-1) = \lambda(v-1).$$

This follows easily from the definition of a symmetric block design. Next, we have:

- (1) if v is even, then $n = k - \lambda$ must be a square (Schützenberger);
- (2) if v is odd, the equation

$$nX^2 + (-1)^{\frac{1}{2}(v-1)} \lambda Y^2 = Z^2$$

must have a solution $(X, Y, Z) \neq (0, 0, 0)$ in integers (Chowla-Ryser).

A deeper condition on the parameters of a difference set in an *abelian group* is provided by the following result. First we need a

Definition. A prime number p is said to be *semi-primitive* modulo the positive integer w if there is some integer f for which the equation

$$p^f \equiv -1 \pmod{w}$$

holds. A number m is said to be *semi-primitive* modulo w if all its prime factors are. Finally, the number m is said to be *self-conjugate* modulo w , if m is semi-primitive modulo w' , where w' denotes the largest divisor of w which is prime to m .

SEMI-PRIMITIVITY THEOREM. Suppose that there exists a (v, k, λ) -difference set in an abelian group G . Let p be any prime divisor of $n = k - \lambda$. Then p is not semi-primitive modulo the exponent $e(G)$ of G .

Furthermore, if p divides the square-free part of n , then there is no divisor $w > 1$ of $v = |G|$ for which p is semi-primitive mod w .

(See [L], Theorem 4.5, page 134.)

Another very useful theorem of R. Turyn is:

TURYN'S INEQUALITY. Assume a non-trivial (v, k, λ) difference set in a cyclic group exists. Let $m > 1$ be an integer such that m^2 divides $n = k - \lambda$ and such that m is self-conjugate modulo w for some divisor $w > 1$ of v . If $\gcd(m, w) = 1$ then $m \leq v/w$. If $\gcd(m, w) > 1$ then

$$m \leq 2^{r-1} v/w,$$

where r is the number of distinct prime factors of $\gcd(m, w)$.

(See [T1]; in the special case $r = 1$, see also [Y] and [R].)

We now turn to one of the *multiplier theorems*, which sometimes describes a difference set as a union of orbits under multiplication by a certain integer. First a

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 $m: G \rightarrow G$ 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

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

(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:

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