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: 0. Preliminaries
DOI: https://doi.org/10.5169/seals-59496

Finally, in Section 4 and 5, we give several examples of the use of the Multiplier Theorem.

0. PRELIMINARIES

In this section, we establish the simple relationship between periodic and aperiodic correlation coefficients, and show that every Barker sequence of length greater than 2 is also a *periodic* Barker sequence.

LEMMA. *Let* $A = (a_1, \ldots, a_l)$ *be a binary sequence. Then*

$$\gamma_j(A) = c_j(A) + c_{l-j}(A)$$

for all $j = 1, \ldots, l-1$.

Proof. We have

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

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

as claimed. □

For the next result, we will use, as other papers on binary sequences do, the simple observation that

$$ab \equiv a + b - 1 \bmod 4$$

for all $a, b \in \{+1, -1\}$.

PROPOSITION 2. *Let* $A = (a_1, \ldots, a_l)$ *be a Barker sequence, with* $l \geqslant 3$. *Then* A *is also a periodic Barker sequence.*

Proof. We have to prove that $\gamma_j = \gamma_j(A)$ is independent of $j = 1, \ldots, l-1$, and equal to 0 or ± 1. First of all, we have (with $c_j = c_j(A)$)

$$c_j = \begin{cases} 0 & \text{if} \quad l-j \text{ is even} \\ \pm 1 & \text{if} \quad l-j \text{ is odd} \end{cases} \tag{1}$$

for all $j = 1, \ldots, l-1$.

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

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

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

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

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

$$c_j - c_{j+1} \equiv a_{l-j} + a_{j+1} - 1 \quad \bmod 4\ , \tag{3}$$

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

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

$$c_j - c_{j+1} \equiv c_{l-j-1} - c_{l-j} \quad \bmod 4\ , \tag{4}$$

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

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

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

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

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

Now $|\gamma_j| = |c_j + c_{l-j}| \leqslant 2$, 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 $|\gamma_j| \leqslant 1$, as claimed. □

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 $g \in G \backslash \{e\}$. 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.