

Introduction

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

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

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

PDF erstellt am: **26.05.2024**

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.

Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.

Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

BARKER SEQUENCES AND DIFFERENCE SETS

by Shalom ELIAHOU and Michel KERVAIRE

INTRODUCTION

This paper deals with binary sequences $A = (a_1, \dots, a_l)$, i.e. $a_i = \pm 1$ for $i = 1, \dots, l$, and classical coefficients associated with them, the aperiodic and periodic correlation coefficients. The *aperiodic correlation coefficients* of A are defined as

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

and the *periodic correlation coefficients* of A as

$$\gamma_j(A) = \sum_{i=1}^l a_i a_{i+j}, \quad \text{for } j = 1, \dots, l-1,$$

where the indices are read modulo l , i.e. $a_r = a_{r-l}$ if $r \geq l+1$.

It is well-known that $\gamma_j = c_j + c_{l-j}$ for $j = 1, \dots, l-1$.

There are many interesting and difficult problems concerned with the existence of binary sequences whose correlation coefficients (or *correlations*, for short) are subject to various conditions. We will examine here three classical situations.

(1) One may require the *periodic* correlations γ_j to be constant, i.e.

$$\gamma_1 = \gamma_2 = \dots = \gamma_{l-1} = \gamma.$$

We will see below that binary sequences satisfying this condition are equivalent to the classical notion of cyclic difference sets.

(2) In addition to the condition above, one may furthermore impose the constant γ to be small, i.e. $\gamma = 0$, or $\gamma = 1$, or $\gamma = -1$. We will call such

sequences *periodic Barker sequences*. Periodic Barker sequences with $\gamma = 0$ are equivalent to circulant Hadamard matrices. We will not follow the link with Hadamard matrices any further here.

(3) Without any condition on the periodic correlations, one may require the *aperiodic* correlations to be small, i.e.

$$c_j \in \{0, 1, -1\} \quad \text{for } j = 1, \dots, l-1.$$

Such sequences are known as *Barker sequences*. They were invented by Barker [Bar] in connection with radar theory. Note that we cannot impose the c_j to be constant, since $c_j \equiv l-j \pmod{2}$.

Barker sequences of *odd length* have been classified in 1961 by Storer and Turyn [ST]. Their lengths are bounded by 13. In the *even length* case, a longstanding conjecture states that the only such sequences are of length 2 or 4. It is known since Turyn [T2] that if the length of a Barker sequence is even and greater than 4, then it must be at least 12 100. We will show in Section 3 that this lower bound can be improved to 1 898 884, thanks to a recent result on Golay pairs and Barker sequences [EKS], and an observation in [JL].

Here is a summary of the content of this paper. In Section 0, we prove that Barker sequences of length greater than 2 are in fact *periodic* Barker sequences (i.e., (3) \Rightarrow (2)), an elementary and well known fact. It is sometimes asserted in the literature that the converse holds as well. This is not true, and clarifying the situation was one of our motivations to write this survey. Another motivation was our exploration of the existence question of periodic Barker sequences for an extensive range of possible lengths. This work is summarized in Tables I and II at the end of the paper.

In Section 1, we show that binary sequences with constant periodic correlations (condition (1)) are equivalent to cyclic difference sets. We then recall the main results concerning these difference sets.

Section 2 deals with condition (2), that is, *periodic* Barker sequences. We examine the cases $\gamma = 0, 1$ and -1 separately. In the case $\gamma = 0$, it is widely believed that the only possible length is $l = 4$. We recall a theorem of Turyn stating that l must be of the form $l = 4N^2$, where N is an odd integer. Further results of Turyn imply that N must necessarily be greater than or equal to 55. In the case $\gamma = 1$, there is only one known example. The case $\gamma = -1$, in contrast, provides many interesting classical examples. In that case we make explicit the complete classification of $(4n-1, 2n-1, n-1)$ cyclic difference sets up to $n = 100$. (See Sections 4 and 5, and Tables I and II.)

In Section 3, we show that there exists no aperiodic Barker sequence of length divisible by $2p$, when p is a prime number congruent to 3 mod 4.

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

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

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

Proof. We have

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

as claimed. \square

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

$$ab \equiv a + b - 1 \pmod{4}$$

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

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

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

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

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