Answering a Question of Pott on Almost Perfect Sequences

K. T. ARASU*
Department of Mathematics and Statistics, Wright State University, Dayton, OH 45435

N. J. VOSS
Department of Mathematics and Statistics, Wright State University, Dayton, OH 45435

Dedicated to the memory of E. F. Assmus

Accepted September 6, 1998

Abstract. Periodic binary (plus-minus) sequences all but one of whose out-of-phase autocorrelation coefficients are zero are studied by Wolfmann [6]. Using the equivalence of these almost perfect sequences to certain cyclic divisible difference sets (noted by Bradley and Pott [1]), we settle the existence status of a previously open case of an almost perfect sequence of length 852, thereby answering a question of Pott [5] negatively.

Keywords: autocorrelation, perfect sequence, difference sets, multipliers

1. Introduction

Let \( S = (s_i) \) be a sequence of period \( n \) with entries \( \pm 1 \), i.e. \( s_i = s_{i+n} \) and \( s_i = 1 \) or \(-1\) for \( i = 0, 1, 2, \ldots \). Its autocorrelation coefficients are defined by

\[
C_t(S) = \sum_{i=0}^{n-1} s_i s_{i+t}.
\]

The sequence \( S \) is said to be almost perfect if \( C_t(S) = 0 \) for all \( t \neq 0 \) (mod \( n \)) with exactly one exception. Almost perfect sequences were first introduced by Wolfmann [6]. For a recent survey on these, we refer the reader to Jungnickel and Pott [4].

A subset \( D \) of the additive group \( \mathbb{Z}_{mn} \) is said to be a (cyclic) \((m, n, k, \lambda_1, \lambda_2)\) divisible difference set if \(|D| = k\) and the list of differences

\[
\left( d - d' : d, d' \in D \right)
\]

contains each element \( im(i = 1, 2, \ldots, (n-1)) \) exactly \( \lambda_1 \) times and each element \( w \in \mathbb{Z}_{mn}, \ w \neq im (i = 0, 1, \ldots, (n-1)) \) exactly \( \lambda_2 \) times.


* Research partially supported by NSA Grant MDA 904-97-1-0012 and by AFOSR Grant F 49620-96-1-0328.
THEOREM 1.1 An n-periodic sequence $S = (s_i)$ with entries $\pm 1$ is almost perfect if and only if $D = \{i \mid 0 \leq i < n, s_i = +1\}$ is a cyclic divisible difference set where $\frac{n - 2\theta}{2}$ is the number of ‘+1’ entries in a generating cycle. (Note that $n$ must be $\equiv 0 \pmod{4}$.)

The case $\theta = 1$ corresponds to the so called affine difference sets. By the prime power conjecture on affine difference sets, it is believed that $\frac{n - 2\theta}{2}$ must be an odd prime power.

The following is due to Jungnickel, Pott, Reuschling [3]:

THEOREM 1.2 A cyclic relative $(m, 2, m - 1, \frac{m-2}{2})$ difference set (equivalently an almost perfect sequence of length $2m$ with $\theta = 1$) with $m \leq 424$ exists if and only if $m - 1$ is a prime power.

Theorem 1.2 was proved using "multipliers and orbits" techniques. Pott [5] says: "It is apparently rather difficult to decide whether a cyclic relative difference set with $m = 426$ exists or not". Problem 14, Page 155 of Pott [5] asks "decide the case $m = 426".

In this note we answer Pott’s question, by ruling out the existence of the aforementioned objects for $m = 426$. Our methods are similar to the ones used in Theorem 1.2, but we look at certain appropriate homomorphic images to get our result.

2. Preliminaries

We list some preliminary results required to prove our theorem.

The following multiplier theorem can be found in Pott [5] (Corollary 1.3.12).

THEOREM 2.1 Let $R$ be an abelian $(m, d, m - 1, \frac{m-2}{d})$ difference set. If $m - 1 = p^i q^j$ is the product of two prime powers, then $p^i$ and $q^j$ are both multipliers of $R$.

The next result follows from standard theorems (See Pott [5] for instance.)

PROPOSITION 2.2 Let $R$ be an abelian $(m, d, m - 1, \frac{m-2}{d})$ difference set and $t$ a multiplier of $R$. Then there is a translate of $R$ fixed by $t$.

Let $G$ be a group and $N$ a normal subgroup of $G$. Let $G/N = \{Ng_1, \ldots, Ng_m\}$.

For a subset $D$ of $G$, the numbers $|D \cap Ng_i|$, $i = 1, \ldots, m$, are called the intersection numbers of $D$ mod $N$.

PROPOSITION 2.3 Let $D$ be a $(m, 2, m - 1, \frac{m-2}{2})$ relative difference set in $G = \langle g \rangle$. Let $(a_i)_{x \in G/N}$ denote the intersection numbers of $D$ mod $N$, where $N$ is a normal subgroup of $G$. Then

$$\sum_{x \in G/N} a_x^2 = \begin{cases} m - 1 + \frac{m-2}{2} [\lceil N \rceil - 2] & \text{if } |N| \text{ is even} \\ m - 1 + \frac{m-2}{2} [\lceil N \rceil - 1] & \text{if } |N| \text{ is odd} \end{cases}$$