Almost $p$-Ary Perfect Sequences

Yeow Meng Chee$^1$, Yin Tan$^{1,*}$, and Yue Zhou$^2,**$

$^1$ Division of Mathematical Sciences, School of Physical & Mathematical Sciences, Nanyang Technological University, 21 Nanyang Link, 637371 Singapore
ymchee@ntu.edu.sg, itanyinmath@gmail.com

$^2$ Department of Mathematics, Otto-von-Guericke-University Magdeburg, 39106 Magdeburg, Germany
yue.zhou@st.ovgu.de

Abstract. A sequence $a = (a_0, a_1, a_2, \cdots, a_n)$ is said to be an almost $p$-ary sequence of period $n + 1$ if $a_0 = 0$ and $a_i = \zeta^b_i$ for $1 \leq i \leq n$, where $\zeta_p$ is a primitive $p$-th root of unity and $b_i \in \{0, 1, \cdots, p - 1\}$. Such a sequence $a$ is called perfect if all its out-of-phase autocorrelation coefficients are zero; and is called nearly perfect if its out-of-phase autocorrelation coefficients are all 1, or are all $-1$. In this paper, on the one hand, we construct almost $p$-ary perfect and nearly perfect sequences; on the other hand, we present results to show they do not exist with certain periods. It is shown that almost $p$-ary perfect sequences correspond to certain relative difference sets, and almost $p$-ary nearly perfect sequences correspond to certain direct product difference sets. Finally, two tables of the existence status of such sequences with period less than 100 are given.

Keywords: almost $p$-ary sequences, almost $p$-ary perfect sequences, almost $p$-ary nearly perfect sequences, relative difference set, direct product difference set.

1 Introduction

Let $a = (a_0, a_1, a_2, \cdots, a_n)$ be a complex sequence of period $n + 1$. We call $a$ an $m$-ary sequence if $a_i = \zeta_m^{b_i}$, where $\zeta_m$ is a primitive $m$-th root of unity and $b_i \in \{0, 1, \cdots, m - 1\}$ for $0 \leq i \leq n$. In particular, the sequence $a$ is called an almost $m$-ary sequence if $a_0 = 0$. For an (almost) $m$-ary sequence $a$ with period $n + 1$, the autocorrelation coefficients of $a$ are the elements in the set

$$\{C_t(a) = \sum_{i=0}^{n} a_ia_{i+t} : 0 \leq t \leq n\},$$

* Research of Yeow Meng Chee and Yin Tan is supported in part by the National Research Foundation of Singapore under Research Grant NRF-CRP2-2007-03 and by the Nanyang Technological University under Research Grant M58110040.

** Research of Yue Zhou is partially supported by China Scholarship Council.

© Springer-Verlag Berlin Heidelberg 2010
where $\overline{z}$ is the complex conjugate and all subscripts are computed modulo $n+1$. For all $t \not\equiv 0 \mod (n+1)$, the $C_t(a)'s$ are called out-of-phase autocorrelation coefficients, and in-phase autocorrelation coefficients otherwise.

Motivated by applications in engineering, sequences with small out-of-phase coefficients are of particular interests. Usually, the complex sequence $a$ is expected to have a two-level autocorrelation function, i.e. all out-of-phase autocorrelation coefficients are a constant $\gamma$. For an almost $m$-ary sequence $a$, we call a perfect if it has a two-level autocorrelation function and $\gamma = 0$. Moreover, we call a nearly perfect if out-of-phase autocorrelation coefficients $\gamma$ all satisfy $\gamma = 1$, or all they satisfy $\gamma = -1$. We refer to [7] for a well-rounded survey on perfect binary sequences, to [9] for results of perfect and nearly perfect $p$-ary sequence, where $p$ is an odd prime. In the following we briefly introduce the relationship between (almost) binary (with entries $\pm 1$) perfect sequences and (Conference) Hadamard matrices.

A matrix $H$ with entries $\pm 1$ and order $v$ is called a Hadamard matrix if $HH^T = vI$; and a matrix $C$ with entries 0, $\pm 1$ and order $v$ is called a Conference matrix if $CC^T = (v-1)I$, where $I$ is the identity matrix. It is well known that perfect binary (with entries $\pm 1$) sequences of period $v$ are equivalent to cyclic difference sets (see [7] Section 2). In particular, when $v \equiv 0 \mod 4$, the perfect binary sequences are equivalent to circulant Hadamard matrices, or cyclic Hadamard difference sets (see [12] Section 1.1). More precisely, let $a = (a_0, a_1, \ldots, a_{v-1})$ be a binary perfect sequence of period $v$. Let $H = (h_{i,j})_{i,j=0}^{v-1}$ be a circulant matrix ($H$ is called circulant if $h_{i+1,j+1} = h_{i,j}$ for all $i, j$) defined by $h_{0,j} = a_j$ for $j \in \mathbb{Z}_v$, then $H$ is a circulant Hadamard matrix of order $v$. Similarly, let $a = (a_0, a_1, \ldots, a_{v-1})$ be an almost binary perfect sequence, i.e. $a_0 = 0$ and $a_i = \pm 1$ for $1 \leq i \leq v-1$. Then the circulant matrix $C = (c_{i,j})_{i,j=0}^{v-1}$ defined by $h_{0,j} = a_j$ for $j \in \mathbb{Z}_v$ is a circulant Conference matrix. The famous circulant Hadamard matrices conjecture is that there do not exist circulant Hadamard matrices if $v > 4$. In contrast to this still open problem, an elegant and elementary proof in [13] shows that there do not exist circulant Conference matrices: It seems that the mathematical behavior of binary perfect sequences and almost binary perfect sequences are quite different, which is one motivation of our paper. In this paper, we study the properties of general almost $p$-ary perfect sequences, where $p$ is a prime. It turns out that almost $p$-ary perfect sequences of period $n+1$ are equivalent to $(n+1, p, n, (n-1)/p)$ relative difference sets in $\mathbb{Z}_{n+1} \times \mathbb{Z}_p$ relative to $\mathbb{Z}_p$ (Theorem 1).

The lack of examples of almost $p$-ary perfect sequences motivates our research in almost $p$-ary nearly perfect sequences. It is shown that periodic almost $p$-ary nearly perfect sequences correspond to certain direct product difference sets (Theorem 5).

This paper is organized as follows. In Section 2, we give necessary definitions and results. The discussions about almost $p$-ary perfect and nearly perfect sequences are given in Section 3 and 4 respectively. In Appendix, we give two tables of the existence status of almost $p$-ary perfect and nearly perfect sequences.