On the Cross-Correlation Distribution of p-ary m-Sequences [1]

*Eun-Young Seo O, *Young-Sik Kim, *Jong-Seon No, and **Dong-Joon Shin
*School of Electrical Engineering and Computer Science and INMC, Seoul National University
**Division of Electronics and Computer Engineering, Hanyang University
Email: jsno@snu.ac.kr

Abstract

For an odd prime p, an even integer n, and $d = p^k + 1$ with $\gcd(n, k) = 1$, there are $p + 1$ distinct decimated sequences $s(dt + l)$, $0 \le l < p + 1$, for a p-ary m-sequence $s(t)$ of period $p^n - 1$ since $\gcd(d, p^n - 1) = p + 1$. In this paper, the cross-correlation distribution between a p-ary m-sequence $s(t)$ and its $p+1$ distinct decimated sequences $s(dt + l)$ is derived. The maximum magnitude $C_{\max}$ of their cross-correlation values is $1+p\sqrt{p^n}$ when $l = 0 \mod p+1$ for $n = 0 \mod 4$ or when $l = (p + 1)/2 \mod p+1$ for $n = 2 \mod 4$. For the remaining cases, $C_{\max}$ is $1+\sqrt{p^n}$. Also by using $s(t)$ and $s(dt+l)$, a new family of p-ary sequences of period $p^n - 1$ is constructed, whose family size is p^n and $C_{\max}$ is $1 + p\sqrt{p^n}$.

1. Introduction

To construct a family of p-ary sequences of period p^n-1 with good correlation property, the cross-correlation distribution between a p-ary m-sequence $s(t)$ of period p^n-1 and its decimated sequence $s(dt)$ with $\gcd(d, p^n-1) = 1$ has been studied for many years [1]-[3].

There are some research results dealing with a decimation factor d which is not relatively prime to the period $p^n - 1$ [4]-[6]. Kumar and Moreno [5] derived the cross-correlation values of $s(t)$ and $s(dt)$ with $d = p^k + 1$, where $n/\gcd(n, k) =$ odd. In this case, $\gcd(d, p^n - 1)$ is 2 and the maximum magnitude $C_{\max}$ of the cross-correlation values of the sequence family is $1 + \sqrt{p^n}$, which is optimal with respect to the Welch bound. Furthermore, in Theorem 4 of [6], Müller found the upper bound on the cross-correlation values of the sequences $s(t)$ and only one decimated sequence $s(dt)$ when n is even, $n/\gcd(n, k)$ is not divisible by 4, and d is $p^k + 1$.

For an odd prime p, an even integer n, and $d = p^k+1$ with $\gcd(n, k) = 1$, there are $p + 1$ distinct decimated sequences $s(dt+l)$, $0 \le l < p+1$, of a p-ary m-sequence $s(t)$ of period $p^n - 1$ since $\gcd(d, p^n - 1) = p + 1$. In this paper, the cross-correlation distribution between a p-ary m-sequence $s(t)$ and its decimated sequences $s(dt + l)$, $0 \le l < p + 1$, is derived. It is also shown that $C_{\max}$ is $1 + p\sqrt{p^n}$ when $l = 0 \mod p + 1$ for $n = 0 \mod 4$ or when $l = (p + 1)/2 \mod p + 1$ for $n = 2 \mod 4$, and for the remaining cases, $C_{\max}$ is $1 + \sqrt{p^n}$. By using $s(t)$ and $s(dt + l)$, a new family of p-ary sequences of period $p^n - 1$ is constructed, whose family size is p^n and $C_{\max}$ is $1 + p\sqrt{p^n}$.

[1]This research was supported by the MIC, Korea, under the ITRC support program and by the MOE, the MOCIE, and the MOLAB, Korea, through the fostering project of the Laboratory of Excellency.

2. Preliminaries

Let p be an odd prime, F_{p^n} the finite field with p^n elements, and $F_{p^n}^* = F_{p^n} \setminus \{0\}$. Then the trace function from F_{p^n} to F_{p^m} is defined as $\mathrm{tr}_m^n(x) = \sum_{i=0}^{n/m-1} x^{p^{mi}}$ where $x \in F_{p^n}$ and $m|n$.

Let α be a primitive element of F_{p^n}. Then a p-ary m-sequence $s(t)$ of period $p^n - 1$ can be written in terms of the trace function as $s(t) = \mathrm{tr}_1^n(\alpha^t)$.

Let n be an even integer and $d = p^k + 1$ with $\gcd(n, k) = 1$. Since $\gcd(p^n - 1, d) = p + 1$, we have $p + 1$ distinct decimated sequences $s_l(dt)$ of period $(p^n - 1)/(p + 1)$ using shift value l, $0 \le l < p + 1$, which are defined as

$$s_l(dt) = \mathrm{tr}_1^n(\alpha^{dt+l}). \tag{1}$$

Then the cross-correlation function of m-sequence $s(t)$ and its decimated sequence $s_l(dt)$ at shift τ is defined as

$$C_l(\tau) = \sum_{t=0}^{p^n-2} \omega^{s_l(dt)-s(t+\tau)} = \sum_{x \in F_{p^n}^*} \omega^{\mathrm{tr}_1^n(ax^d-bx)} \tag{2}$$

where ω is a primitive complex p-th root of unity, $a = \alpha^l$, and $b = \alpha^\tau$. From now on, we will use the notations $C_l(\tau)$ and $C_l(b)$ interchangeably.

Let ψ denote the canonical additive character of the additive group F_{p^n}, which is defined as $\psi(c) = e^{j2\pi \mathrm{tr}_1^n(c)/p}$, for all $c \in F_{p^n}$. All additive characters of F_{p^n} can be expressed in terms of ψ.