New Family of p-ary Sequences with Optimal Correlation Property and Large Linear Span

Ji-Woong Jang[1], Young-Sik Kim
School of EECS
Seoul Nat'l University, Seoul, Korea
e-mail:
{stasera, kingsi}@ccl.snu.ac.kr

Jong-Seon No
School of EECS
Seoul Nat'l University, Seoul, Korea
e-mail: jsno@snu.ac.kr

Tor Helleseth
Department of Informatics
University of Bergen, Bergen, Norway
e-mail: Tor.Helleseth@ii.uib.no

Abstract — **For an odd prime p and an integer $n = (2m+1)k$, a new family of p-ary sequences with optimal correlation property is constructed using Helleseth-Gong sequences. Period of the sequences is $p^n - 1$ and the size of family is p^n. It is also derived that the linear span of the sequences in the family is $(m+2) \cdot n$ except the m-sequence in the family. The maximum nontrivial correlation value R_{max} does not exceed $1 + \sqrt{p^n}$, which means the optimal correlation property in terms of Welch's lower bound.**

I. Introduction

Let $\mathbf{S}$ be the family of M p-ary sequences of period $N = p^n - 1$ for an odd prime p given by

$$\mathbf{S} = \{s_i(t) \mid 0 \le i \le M-1, 0 \le t \le N-1\}.$$

The correlation function of the sequences $s_i(t)$ and $s_j(t)$ in $\mathbf{S}$ is written as

$$R_{i,j}(\tau) = \sum_{t=0}^{N-1} \omega^{s_i(t+\tau) - s_j(t)}$$

where ω is a p-th root of unity, $0 \le i, j \le M-1$, and $0 \le \tau \le N-1$. Let R_{max} be the maximum magnitude of the correlation values except for inphase autocorrelation value. A family of p-ary sequences of period $p^n - 1$ is said to have optimal correlation property if R_{max} doesn't exceed $p^{\frac{n}{2}} + 1$.

II. New family of p-ary sequences

Let p be an odd prime and $tr_k^n(x) = \sum_{i=0}^{n/k-1} x^{p^{ik}}$ denote the trace from the finite field F_{p^n} to the subfield F_{p^k}. Let $q = p^k$.

Helleseth and Gong introduced new p-ary sequences with ideal autocorrelation, which are referred to as Helleseth-Gong(HG) sequences [1] as in the following theorem:

Theorem 1 [Helleseth and Gong [1]]: Let n, m and k be positive integers such that $n = (2m+1)k$. Let $s, 1 \le s \le 2m$ be a positive integer such that $gcd(2m+1, s) = 1$. Let p be an odd prime and α be a primitive element in F_{p^n}. Let $b_0 = 1$ and $b_{ls} = (-1)^l$. Let $q = p^k$ and $u_0 = \frac{b_0}{2}$ and $u_l = b_{2l} = b_{2m+1-2l}$ for $l = 0, 1, 2, \cdots, m$. Then the Helleseth-Gong sequences of period $p^n - 1$ given by

$$s(t) = \mathrm{tr}_1^n\left(\sum_{l=0}^{m} u_l \cdot \alpha^{\frac{q^{2l}+1}{2}t}\right) \quad (1)$$

have the ideal autocorrelation property.

[1]This work was supported in part by the Korean Ministry of Information and Communications and the Norwegian Research Council.

Let $F_{p^n}^* = F_{p^n} \backslash \{0\}$ and $x = \alpha^t$. Then the Helleseth-Gong sequences in (1) can also be written as

$$s(x) = \mathrm{tr}_1^n\left(\sum_{l=0}^{m} u_l \cdot x^{\frac{q^{2l}+1}{2}}\right), \quad x \in F_{p^n}^*.$$

Let $h(x)$ be the Helleseth-Gong polynomial defined by

$$h(x) = \sum_{l=0}^{m} u_l \cdot x^{\frac{q^{2l}+1}{2}}, \quad x \in F_{p^n}.$$

Then the Helleseth-Gong sequences in (1) can be rewritten as

$$s(x) = \mathrm{tr}_1^n(h(x)), \quad x \in F_{p^n}^*.$$

We can modify the Helleseth-Gong sequences as follows

$$s_b(x) = \mathrm{tr}_1^n(x + h(b \cdot x^2)) = \mathrm{tr}_1^n\left(x + \sum_{l=0}^{m} u_l \cdot b^{\frac{q^{2l}+1}{2}} \cdot x^{q^{2l}+1}\right) \quad (2)$$

where $b \in F_{p^n}$. It is clear that the sequences in (2) have period of $p^n - 1$.

The crosscorrelation function of $s_{b_i}(x)$ and $s_{b_j}(x)$ for $b_i, b_j \in F_{p^n}$ is defined as

$$R_{ij}(c) = \sum_{x \in F_{p^n}^*} w^{s_{b_i}(cx) - s_{b_j}(x)} \quad (3)$$

where $c = \alpha^\tau \in F_{p^n}^*$ corresponds to time shift of the sequence. Using the modified Helleseth-Gong sequences defined in (2), a family of p-ary sequences with family size p^n and optimal correlation property can be constructed as follows:

Theorem 2 : Let $s_b(x)$ be the p-ary sequence defined in (2). Then the family of p-ary sequences given by

$$S = \{s_b(x) \mid b \in F_{p^n},\ x \in F_{p^n}^*\}$$

has optimal correlation property with maximum magnitude $\sqrt{p^n} + 1$. And sequences in the family are unbalanced except m-sequence.

Theorem 3 : The linear span of the sequence $s_b(t)$ for $b \in F_{p^n}^*$ defined in Theorem 2 is $(m+2) \cdot n$.

References

[1] T. Helleseth and G. Gong, "New nonbinary sequences with ideal two-level autocorrelation function," *IEEE Trans. on Inform. Theory*, Vol. 48, pp. 2868 -2872, Nov. 2002.