p-ary d-Form Sequences with Ideal Autocorrelation Property

Jong-Seon No[1]
Seoul National University
School of Electrical Engineering
Seoul, 151-742 Korea
e-mail: jsno@snu.ac.kr

Abstract — **In this paper, for a prime number p, a construction method to generate p-ary d-form sequences with ideal autocorrelation property is proposed.**

I. Introduction

Recently, Helleseth, Kumar and Martinsen [1] found ternary sequences with ideal autocorrelation, which are the only nonbinary sequences with ideal autocorrelation, so far, except for p-ary m-sequences and cascaded GMW sequences. Klapper introduced d-form sequences [2]. In this paper, a construction method to generate p-ary d-form sequences with ideal autocorrelation property is proposed.

II. New Construction of The Sequences

Klapper introduced a d-form function $H(x)$ [2], which can be used to construct d-form sequences. In his paper, a d-form function on F_{p^n} over F_{p^m} means a homogeneous function of degree d, that is, for any $x \in F_{p^n}$ and $y \in F_{p^m}$, it satisfies

$$H(yx) = y^d H(x). \tag{1}$$

Using the d-form function $H(x)$, he introduced d-form sequences as follows:

Definition 1 [Klapper [2]]: Let m and n be positive integers such that $m \mid n$. Let α be a primitive element of F_{p^n} and set $\beta = \alpha^T$, where $T = (p^n-1)/(p^m-1)$. For an integer r, $1 \le r \le p^m - 2$, relatively prime to $p^m - 1$, a d-form sequence of period $p^n - 1$ is defined as

$$c_d(t) = \mathrm{tr}_1^m([H(\alpha^t)]^r), \tag{2}$$

where $H(\alpha^t)$ is a d-form function defined in (1).

In order to construct d-form sequences, we have to find the corresponding d-form function.

Theorem 2 : Let m and n be positive integers such that $m \mid n$. Let α be a primitive element of F_{p^n}. Let $s \equiv d \bmod (p^m-1)$, for all s in an index set I, where d is relatively prime to $p^m - 1$. Then a function from F_{p^n} onto F_{p^m}

$$H(\alpha^t) = \sum_{s \in I} \mathrm{tr}_m^n(\alpha^{st}) \tag{3}$$

is a d-form on F_{p^n} over F_{p^m}.

Using (2) and Theorem 2, we can construct a p-ary d-form sequence with ideal autocorrelation property as in the following theorem.

[1]This work was supported by ITRC program.

Theorem 3 : Let m and n be positive integers such that $m \mid n$. Let p be a prime number and $M = p^m - 1$. Let α be a primitive element of F_{p^n} and set $\beta = \alpha^T$, where $T = (p^n-1)/(p^m-1)$. Let $s \equiv d \bmod M$ for all s in some index set I, where d is relatively prime to M. Assume that the p-ary sequence $c(t)$ of period $N = p^n - 1$ given by

$$c(t) = \sum_{s \in I} \mathrm{tr}_1^n(\alpha^{st}) \tag{4}$$

has ideal autocorrelation property. For an integer r, $1 \le r \le M-1$, relatively prime to M, a p-ary d-form sequence $c_d(t)$ of period N defined by

$$c_d(t) = \mathrm{tr}_1^m\{[\sum_{s \in I} \mathrm{tr}_m^n(\alpha^{st})]^r\} \tag{5}$$

also has the ideal autocorrelation property.

Helleseth, Kumar and Martinsen introduced the new ternary sequence ($p = 3$) with ideal autocorrelation as in the following theorem.

Theorem 4 [Helleseth, Kumar and Martinsen [1]]: Let $s = 3^{2m} - 3^m + 1$ and $n = 3m$. Let α be a primitive element of $F_{3^{3m}}$. Then, a ternary sequence of period $3^{3m} - 1$ given by

$$c(t) = \mathrm{tr}_1^n(\alpha^t) + \mathrm{tr}_1^n(\alpha^{st}) \tag{6}$$

has ideal autocorrelation property.

A ternary d-form sequence with ideal autocorrelation property can be given as follows.

Theorem 5 : Let $s = 3^{2ek} - 3^{ek} + 1$ and $n = 3ek$, where e and k are positive integers. Let α be a primitive element of $F_{3^{3ek}}$. Let r, $1 \le r \le 3^k - 2$, be relatively prime to $3^k - 1$. Then a ternary d-form sequence of period $3^{3ek} - 1$ given by

$$c_d(t) = \mathrm{tr}_1^k\{[\mathrm{tr}_k^{3ek}(\alpha^t) + \mathrm{tr}_k^{3ek}(\alpha^{st})]^r\}$$

has ideal autocorrelation property.

As an example, a ternary d-form sequence of period $3^9 - 1$ with ideal autocorrelation property is given as:

Example 6 : Let $m = ek = 3$. Then, $s = 3^6 - 3^3 + 1 = 703$ and $n = 9$. Let r, $1 \le r \le 3^3 - 2$, be relatively prime to $3^3 - 1$. Then a ternary d-form sequence of period $3^9 - 1 = 19682$ with ideal autocorrelation property is given by

$$c_d(t) = \mathrm{tr}_1^3\{[\mathrm{tr}_3^9(\alpha^t) + \mathrm{tr}_3^9(\alpha^{703t})]^r\}.$$

References

[1] T. Helleseth, P.V. Kumar, and H.M. Martinsen, "A new family of ternary sequences with ideal two-level autcorrelation," *Proceedings of International Symposium on Information Theory*, pp. 3289, Jun. 2000.

[2] A. Klapper, " d-form sequences: Families of sequences with low correlation values and large linear spans," *IEEE Trans. Inform. Theory*, vol. 41, no.2, pp. 423-431, Mar. 1995.

0-7803-7123-2/01/$10.00 ©2001 IEEE