p-ary Unified Sequences: p-ary Extended d-Form Sequences With the Ideal Autocorrelation Property

Jong-Seon No, *Member, IEEE*

***Abstract*—In this paper, for a prime number p, a construction method to generate p-ary d-form sequences with the ideal autocorrelation property is proposed and using the ternary sequences found by Helleseth, Kumar, and Martinsen, ternary d-form sequences with the ideal autocorrelation property are constructed. By combining the methods for generating p-ary extended sequences (a special case of geometric sequences) and p-ary d-form sequences, a construction method of p-ary unified (extended d-form) sequences which also have the ideal autocorrelation property is proposed. This is a very general class of p-ary sequences including the binary and nonbinary extended sequences and the d-form sequences. From the ternary sequences by Helleseth, Kumar, and Martinsen, ternary unified sequences with the ideal autocorrelation property are also generated.**

***Index Terms*—d-form sequences, extended sequences, geometric sequences, p-ary sequences, pseudonoise (PN) sequences, ternary sequences, unified sequences.**

I. Introduction

PSEUDONOISE (PN) sequences have many applications in spread-spectrum communication systems [16] such as a code-division multiple-access (CDMA) system, which has been adopted as a standard for multiple-access methods in mobile radio communication systems. Signal design for CDMA systems has become an interesting research topic in application areas. One of the most important research areas for signal design for CDMA systems is the design of PN sequences with good correlation properties [1], [3]. Research has mostly been done on binary sequences with the ideal autocorrelation property and families of binary sequences with the optimal cross-correlation property [9], [11]–[15].

Chan and Games introduced geometric sequences [2] and work has been done on geometric sequences by Goresky, Chan, and Klapper [5]. No, Yang, Chung, and Song [14] also worked on the closed-form expression for some geometric sequences with the ideal autocorrelation, so-called extended sequences. Geometric sequences provide us with a method of constructing PN sequences by applying a nonlinear feedforward function to q-ary m-sequences. Geometric sequences include m-sequences, Gordon–Mills–Welch (GMW) sequences [15], cascaded (generalized) GMW sequences [9], [12], and extended sequences [14]. Klapper introduced d-form sequences [8] by using homogeneous functions (d-form if the degree is d). d-form sequences with $d = 2$ include No sequences [11], [13] as a special case. He also introduced trace-norm (TN) sequences, which are a family of sequences with good correlation properties. A TN sequence can be considered as a special case of generalized No sequences [12]. Although he introduced d-form sequences as a new method for generating a single sequence, most of his work was done on families of sequences with good cross-correlation properties. To my knowledge, there is no binary or nonbinary d-form sequences with the ideal autocorrelation property except for GMW sequences and cascaded (generalized) GMW sequences [9], [12]. It is not easy to find d-form functions which can be used to construct d-form sequences with the ideal autocorrelation property.

Recently, nonbinary sequences with good correlation properties such as Z_4 sequences and p-ary sequences have been investigated. Helleseth, Kumar, and Martinsen [7] found ternary sequences with the ideal autocorrelation property. These are the first nonbinary sequences with the ideal autocorrelation property, except for p-ary m-sequences and p-ary cascaded GMW sequences. A large class of p-ary sequences with the ideal autocorrelation property was also introduced by Helleseth and Gong [6], which can be used to construct p-ary d-form sequences and p-ary unified sequences.

In this paper, a method of constructing p-ary d-form sequences with the ideal autocorrelation property is proposed. Using the ternary sequences found by Helleseth, Kumar, and Martinsen [7], ternary d-form sequences with the ideal autocorrelation property are constructed. By combining the methods for generating p-ary extended sequences and p-ary d-form sequences, a method for constructing p-ary extended d-form sequences (called *unified sequences*) with the ideal autocorrelation property is proposed. The set of unified sequences is a very general class of sequences including d-form sequences and extended sequences. Finally, examples of ternary unified sequences are given from the ternary sequences introduced by Helleseth, Kumar, and Martinsen [7].

II. Preliminaries

Let $s(t)$ be a sequence over the alphabet F_p of period N as follows:

$$s(t) \in F_p, \qquad t = 0, 1, 2, \ldots, N-1$$

where F_p is the finite field with p elements and p is a prime number. A p-ary sequence $s(t)$ is *balanced* if the element "0" occurs in a period of $s(t)$ one times less than each nonzero element in F_p. A sequence $s(t)$ is said to be *difference-balanced* if

Manuscript received September 22, 2000; revised April 10, 2002. This work was supported in part by BK21 and ITRC program of the Korean Ministry of Information and Communications.

The author is with the School of Electrical Engineering and Computer Science, Seoul National University, Seoul 151-744, Korea (e-mail: jsno@snu.ac.kr).

Communicated by A. M. Klapper, Associate Editor for Sequences.

Publisher Item Identifier 10.1109/TIT.2002.801406.

the sequence $r(t) = s(t) - s(t+\tau) \bmod p$ is balanced for any nonzero τ, $1 \le \tau \le N-1$. Here indexes are computed modulo N. Let ω be a primitive pth root of unity. Then the periodic autocorrelation $R(\tau)$ of $s(t)$ is defined as

$$R(\tau) = \sum_{t=0}^{N-1} \omega^{s(t)-s(t+\tau)}.$$

A sequence $s(t)$ is said to have the *ideal autocorrelation property* if its periodic autocorrelation function $R(\tau)$ is given as

$$R(\tau) = \begin{cases} N, & \text{for } \tau \equiv 0 \bmod N \\ -1, & \text{for } \tau \not\equiv 0 \bmod N. \end{cases}$$

We can show that a sequence over the alphabet F_p has the ideal autocorrelation property if it is difference-balanced for all nonzero time shifts.

For any prime power q, let F_q be the finite field with q elements. Let $n = em > 1$ for some positive integers e and m. Then the trace function $\mathrm{tr}_m^n(\cdot)$ is the mapping from F_{p^n} to its subfield F_{p^m} defined by [10]

$$\mathrm{tr}_m^n(x) = \sum_{i=0}^{e-1} x^{p^{mi}}$$

where x is an element in F_{p^n}.

The trace function satisfies the following:

i) $\mathrm{tr}_m^n(ax+by) = a\,\mathrm{tr}_m^n(x) + b\,\mathrm{tr}_m^n(y)$, for all $a, b \in F_{p^m}$, $x, y \in F_{p^n}$.

ii) $\mathrm{tr}_m^n(x^{p^m}) = \mathrm{tr}_m^n(x)$, for all $x \in F_{p^n}$.

iii) $\mathrm{tr}_1^n(x) = \mathrm{tr}_1^m(\mathrm{tr}_m^n(x))$, for all $x \in F_{p^n}$.

See [10], [16] for detailed properties of the trace function.

For the remainder of the paper, we use the following notation:

- p: prime number;
- m, n: positive integers such that $m|n$;
- $N = p^n - 1$, $M = p^m - 1$, and $T = \frac{N}{M} = \frac{p^n-1}{p^m-1}$;
- F_q: finite field with q elements;
- α, β: primitive elements of F_{p^n}, F_{p^m}, respectively, where $\beta = \alpha^T$.

Using the trace function, a p-ary m-sequence $m(t)$ of period N can be expressed as

$$m(t) = \mathrm{tr}_1^n(A\alpha^t) \tag{1}$$

where $A \in F_{p^n}^*$. It can easily be proved that the m-sequence defined in (1) is balanced and difference-balanced.

Definition 1: A p-ary sequence $s(t)$ is called a *characteristic sequence* or a *characteristic phase sequence* if

$$s(t) = s(pt), \qquad \text{for all } t. \tag{2}$$

□

It is shown that a p-ary m-sequence has a multicharacteristic phase property in the following corollary.

Corollary 2: The m-sequence $m(t)$ as defined in (1) has $p-1$ different characteristic phases. That is, for i, $0 \le i \le p-2$

$$m(t - iT) = m(p(t - iT)), \qquad \text{for all } t,\ 0 \le t \le N-1$$

where $T = \frac{p^n-1}{p-1}$.

Proof: The sequence $m(t-iT)$ for i, $0 \le i \le p-2$ can be expressed as

$$m(t-iT) = \mathrm{tr}_1^n(\alpha^{-i\cdot T} \cdot \alpha^t) = \alpha^{-i\cdot T}\mathrm{tr}_1^n(\alpha^t)$$

where α^T is a primitive element of F_p, since α^{-iT} is a nonzero element in F_p. Also,

$$\begin{aligned} m(p(t-iT)) &= \mathrm{tr}_1^n\left(\alpha^{-ip\cdot T} \cdot \alpha^{pt}\right) \\ &= \alpha^{-ipT} \cdot \left[\mathrm{tr}_1^n(\alpha^t)\right]^p \\ &= \alpha^{-iT} \cdot \mathrm{tr}_1^n(\alpha^t). \end{aligned}$$

Therefore, there are $p-1$ different phases for the m-sequences in (1) which satisfy (2). □

Klapper introduced the d-form function $H(x)$. 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 $y \in F_{p^m}$, a function that satisfies

$$H(yx) = y^d H(x). \tag{3}$$

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

Definition 3 (Klapper [8]): For an integer r, $1 \le r \le M-1$, relatively prime to M, a d-form sequence of period N is defined as

$$c_d(t) = \mathrm{tr}_1^m([H(\alpha^t)]^r) \tag{4}$$

where $H(\alpha^t)$ is a d-form function, as defined in (3). □

As a special case of geometric sequences, No, Yang, Chung, and Song [14] introduced closed-form expressions for sequences with the ideal autocorrelation property, so-called the extended sequences. They give a method for constructing binary sequences for longer periods with the ideal autocorrelation property in a trace representation if a given binary sequence with the ideal autocorrelation property is described using the trace functions. By extending the alphabet from binary to p-ary, the construction of binary extended sequences can be modified to that of p-ary extended sequences.

Theorem 4: Assume that for an index set I, the p-ary sequence $b(t_1)$ of period M given by

$$b(t_1) = \sum_{a \in I} b_a \cdot \mathrm{tr}_1^m(\beta^{at_1}), \qquad b_a \in F_p^*$$

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

$$c(t) = \sum_{a \in I} b_a \cdot \mathrm{tr}_1^m\left\{[\mathrm{tr}_m^n(\alpha^t)]^{ar}\right\}$$

also has the ideal autocorrelation property. □

The proof for Theorem 4 is almost the same as that of binary extended sequences [14] and so the proof has been omitted

here. A construction of d-form sequences by d-form functions is a new method to construct sequences with the ideal autocorrelation property, which is described in the following section.

III. p-ARY d-FORM SEQUENCES

In order to construct p-ary d-form sequences, we have to find the corresponding d-form functions. But it is not easy to find d-form functions which can be used to construct d-form sequences with the ideal autocorrelation property, except for the cases such as GMW sequences and cascaded GMW sequences. Most work on d-form sequences has been done for families of d-form sequences with good crosscorrelation properties such as TN sequences [8]. TN sequences with $\gamma = 0$ become cascaded GMW sequences with the ideal autocorrelation property. Klapper derived the cross correlations of a family of the d-form sequences by using the d-form functions. To construct d-form sequences of period N with the ideal autocorrelation property, we have to find the condition which the corresponding d-form function satisfies. It is already been given by Klapper [8] and we can modify it as follows.

Theorem 5: Let $H(\alpha^t)$ be a d-form function on F_{p^n} over F_{p^m} and d, $1 \le d \le M-1$, be an integer relatively prime to M. For an integer r, $1 \le r \le M-1$, relatively prime to M, the d-form sequence of period N given by

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

has the ideal autocorrelation property if and only if for any nonzero shift τ, the set

$$\{t | H(\alpha^t) = H(\alpha^{t+\tau}),\ 0 \le t \le T-1\}$$

has size $\frac{p^{n-m}-1}{p^m-1}$.

Proof: Let t_1 and t_2 be the digits occurring in the base-T expansion of t, i.e., $t = t_1 \cdot T + t_2$, $0 \le t_1 \le M-1$, $0 \le t_2 \le T-1$. Then, the difference of the p-ary d-form sequence $c_d(t)$ can be written in the two-dimensional representation as follows:

$$\begin{aligned}
&c_d(t) - c_d(t+\tau)\\
&\quad = \mathrm{tr}_1^m\left\{\left[H(\alpha^t)\right]^r\right\} - \mathrm{tr}_1^m\left\{\left[H(\alpha^{t+\tau})\right]^r\right\}\\
&\quad = \mathrm{tr}_1^m\left\{\left[H(\alpha^{t_1 T + t_2})\right]^r\right\} - \mathrm{tr}_1^m\left\{\left[H(\alpha^{t_1 T + t_2 + \tau})\right]^r\right\}\\
&\quad = \mathrm{tr}_1^m\left\{\alpha^{Tdrt_1}\left[H(\alpha^{t_2})\right]^r\right\} - \mathrm{tr}_1^m\left\{\alpha^{Tdrt_1}\left[H(\alpha^{t_2+\tau})\right]^r\right\}\\
&\quad = \mathrm{tr}_1^m\left\{\beta^{drt_1}\left[H(\alpha^{t_2})\right]^r\right\} - \mathrm{tr}_1^m\left\{\beta^{drt_1}\left[H(\alpha^{t_2+\tau})\right]^r\right\}\\
&\quad = \mathrm{tr}_1^m\left\{\beta^{drt_1}\left\{\left[H(\alpha^{t_2})\right]^r - \left[H(\alpha^{t_2+\tau})\right]^r\right\}\right\}
\end{aligned}$$

where dr is relatively prime to M, and the subsequence for t_1 is either the all zero sequence if $H(\alpha^{t_2}) = H(\alpha^{t_2+\tau})$ or a cyclic shift of the p-ary m-sequence $\mathrm{tr}_1^m(\beta^{drt_1})$ if $H(\alpha^{t_2}) \ne H(\alpha^{t_2+\tau})$, which is balanced. From the fact that m-sequences are balanced, we have

$$\sum_{t=0}^{M-1} \omega^{\mathrm{tr}_1^m(\beta^t)} = -1$$

where ω is a pth root of unity. As t_2 varies from 0 to $T-1$, for any nonzero τ, $H(\alpha^{t_2}) = H(\alpha^{t_2+\tau})$ occurs $A = \frac{p^{n-m}-1}{p^m-1}$ times. Therefore, the autocorrelation of the sequence $c_d(t)$ for any nonzero τ, is calculated as

$$\begin{aligned}
R(\tau) &= \sum_{t=0}^{N-1} \omega^{c_d(t) - c_d(t+\tau)}\\
&= A \cdot (p^m - 1) + (T - A) \cdot (-1)\\
&= \frac{p^{n-m}-1}{p^m-1} \cdot (p^m - 1) + \left(\frac{p^n - 1}{p^m - 1} - \frac{p^{n-m}-1}{p^m-1}\right) \cdot (-1)\\
&= -1
\end{aligned}$$

which means that the sequence $c_d(t)$ has the ideal autocorrelation property. □

To construct p-ary d-form sequences with the ideal autocorrelation property, we have to find a d-form function $H(\alpha^t)$ satisfying the condition derived in Theorem 5. We propose a d-form function in the following theorem, which can be used to construct d-form sequences.

Theorem 6: Let $s \equiv d \bmod M$, for all s in index set I, where d is relatively prime to M. Then the function from F_{p^n} onto F_{p^m}

$$H(\alpha^t) = \sum_{s \in I} b_s \cdot \mathrm{tr}_m^n(\alpha^{st}), \qquad b_s \in F_p^* \tag{5}$$

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

Proof: Let β be an element in F_{p^m}. Then

$$\begin{aligned}
H(\beta\alpha^t) &= \sum_{s \in I} b_s \cdot \mathrm{tr}_m^n((\beta\alpha^t)^s)\\
&= \sum_{s \in I} \beta^s \cdot b_s \cdot \mathrm{tr}_m^n((\alpha^t)^s)\\
&= \sum_{s \in I} \beta^d \cdot b_s \cdot \mathrm{tr}_m^n(\alpha^{st})\\
&= \beta^d \cdot H(\alpha^t)
\end{aligned}$$

where $\beta^s = \beta^d$ because $s \equiv d \bmod M$, for all s in index set I. □

This does not guarantee the ideal autocorrelation property of the d-form sequences constructed by the d-form function in (5), but the d-form function has to satisfy the condition derived in Theorem 5 in order for the corresponding d-form sequences to have the ideal autocorrelation property.

Using Theorems 5 and 6, we can construct a p-ary d-form sequence with the ideal autocorrelation property as in the following theorem.

Theorem 7: 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 given by

$$c(t) = \sum_{s \in I} b_s \cdot \mathrm{tr}_1^n(\alpha^{st}), \qquad b_s \in F_p^* \tag{6}$$

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

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

also has the ideal autocorrelation property.

Proof: We previously defined t_1 and t_2 as the digits occurring in the base-T expansion of t, i.e., $t = t_1 \cdot T + t_2$, $0 \le t_1 \le M-1$, $0 \le t_2 \le T-1$. Then, the p-ary sequence $c(t)$ in (6) can be expressed in terms of t_1 and t_2 as follows:

$$\begin{aligned} c(t) &= \sum_{s\in I} b_s \cdot \mathrm{tr}_1^m \left\{\mathrm{tr}_m^n(\alpha^{st})\right\} \\ &= \sum_{s\in I} b_s \cdot \mathrm{tr}_1^m \left\{\mathrm{tr}_m^n(\alpha^{st_1T+st_2})\right\} \\ &= \sum_{s\in I} b_s \cdot \mathrm{tr}_1^m \left\{\alpha^{Tst_1} \cdot \mathrm{tr}_m^n(\alpha^{st_2})\right\} \\ &= \sum_{s\in I} b_s \cdot \mathrm{tr}_1^m \left\{\beta^{dt_1} \cdot \mathrm{tr}_m^n(\alpha^{st_2})\right\} \\ &= \mathrm{tr}_1^m \left\{\beta^{dt_1} \cdot \sum_{s\in I} b_s \cdot \mathrm{tr}_m^n(\alpha^{st_2})\right\} \end{aligned}$$

where $\beta^s = \beta^d$ because $s \equiv d \bmod M$, for all s in index set I. Let $g(t_2)$ be the function defined by

$$\beta^{d\cdot g(t_2)} = \sum_{s\in I} b_s \cdot \mathrm{tr}_m^n(\alpha^{st_2}). \tag{7}$$

Then the sequence $c(t)$ can be rewritten as

$$c(t) = \mathrm{tr}_1^m \left\{\beta^{d(t_1+g(t_2))}\right\}$$

where the subsequence of $c(t)$ for a fixed value of t_2, $0 \le t_2 \le T-1$, is either the all-zero sequence of period M if $g(t_2) = -\infty$ (i.e., $\beta^{d\cdot g(t_2)} = 0$) or a cyclic shift of the p-ary decimated m-sequence $\mathrm{tr}_1^m\{\beta^{t_1}\}$ of period M otherwise. We assumed that the sequence $c(t)$ has the ideal autocorrelation property. The difference of the sequence $c(t)$ can be expressed as

$$\begin{aligned} &c(t) - c(t+\tau) \\ &\quad= \sum_{s\in I} b_s \cdot \mathrm{tr}_1^m \left\{\mathrm{tr}_m^n(\alpha^{st})\right\} - \sum_{s\in I} b_s \cdot \mathrm{tr}_1^m \left\{\mathrm{tr}_m^n\left(\alpha^{s(t+\tau)}\right)\right\} \\ &\quad= \mathrm{tr}_1^m \left\{\beta^{d(t_1+g(t_2))}\right\} - \mathrm{tr}_1^m \left\{\beta^{d(t_1+g(t_2+\tau))}\right\} \\ &\quad= \mathrm{tr}_1^m \left\{\beta^{d(t_1+g(t_2))} - \beta^{d(t_1+g(t_2+\tau))}\right\}. \end{aligned}$$

Then the autocorrelation $R(\tau)$ of the sequence $c(t)$ is rewritten as

$$\begin{aligned} R(\tau) &= \sum_{t=0}^{N-1} \omega^{c(t)-c(t+\tau)} \\ &= \sum_{t_2=0}^{T-1} \sum_{t_1=0}^{M-1} \omega^{c(t_1T+t_2)-c(t_1T+t_2+\tau)} \\ &= \sum_{t_2=0}^{T-1} \sum_{t_1=0}^{M-1} \omega^{\mathrm{tr}_1^m\{\beta^{d(t_1+g(t_2))}-\beta^{d(t_1+g(t_2+\tau))}\}}. \end{aligned}$$

Suppose the subsequence for a fixed t_2, $0 \le t_2 \le T-1$ is not identically zero. Let $R_{\mathrm{sub}}(\tau, t_2)$ be the autocorrelation function of this subsequence

$$R_{\mathrm{sub}}(\tau, t_2) = \sum_{t_1=0}^{M-1} \omega^{\mathrm{tr}_1^m\{\beta^{d(t_1+g(t_2))}-\beta^{d(t_1+g(t_2+\tau))}\}}.$$

As the subsequence is a p-ary m-sequence, the autocorrelation function of the subsequence takes the values as follows:

$$R_{\mathrm{sub}}(\tau, t_2) = \begin{cases} p^m - 1, & \text{if } g(t_2) = g(t_2+\tau) \\ -1, & \text{if } g(t_2) \ne g(t_2+\tau). \end{cases}$$

Then the autocorrelation function of the sequence $c(t)$ can be represented as a summation of $R_{\mathrm{sub}}(\tau, t_2)$ over t_2, $0 \le t_2 \le T-1$, that is,

$$R(\tau) = \sum_{t_2=0}^{T-1} R_{\mathrm{sub}}(\tau, t_2).$$

Assume that for any nonzero τ, as t_2 varies from 0 to $T-1$, $g(t_2) = g(t_2+\tau)$ occurs A times and $g(t_2) \ne g(t_2+\tau)$ occurs $T-A$ times. Using the assumption of the ideal autocorrelation property of the sequence $c(t)$ and its (not all-zero) subsequences, we have the following equation for any nonzero τ:

$$\begin{aligned} R(\tau) &= \sum_{t_2=0}^{T-1} R_{\mathrm{sub}}(\tau, t_2) \\ &= A \cdot (p^m - 1) + (T-A) \cdot (-1) \\ &= -1. \end{aligned}$$

From the above relationship, the value A can be calculated as $\frac{p^{n-m}-1}{p^m-1}$. That is, as t_2 varies from 0 to $T-1$, $g(t_2) = g(t_2+\tau)$ occurs $\frac{p^{n-m}-1}{p^m-1}$ times, for any nonzero τ. From Theorem 6, $c_d(t)$ is a d-form sequence, since

$$H(\alpha^t) = \sum_{s\in I} b_s \cdot \mathrm{tr}_m^n(\alpha^t)$$

is d-form. Now we have to prove the ideal autocorrelation property of the d-form sequence $c_d(t)$. As before, the difference of the d-form sequence $c_d(t)$ can be represented in the two-dimensional expression as

$$\begin{aligned} &c_d(t) - c_d(t+\tau) \\ &\quad= \mathrm{tr}_1^m \left\{\left[\sum_{s\in I} b_s \cdot \mathrm{tr}_m^n(\alpha^{st})\right]^r\right\} \\ &\qquad - \mathrm{tr}_1^m \left\{\left[\sum_{s\in I} b_s \cdot \mathrm{tr}_m^n\left(\alpha^{s(t+\tau)}\right)\right]^r\right\} \\ &\quad= \mathrm{tr}_1^m \left\{\alpha^{Tdrt_1}\left[\sum_{s\in I} b_s \cdot \mathrm{tr}_m^n(\alpha^{st_2})\right]^r\right\} \\ &\qquad - \mathrm{tr}_1^m \left\{\alpha^{Tdrt_1}\left[\sum_{s\in I} b_s \cdot \mathrm{tr}_m^n\left(\alpha^{s(t_2+\tau)}\right)\right]^r\right\} \\ &\quad= \mathrm{tr}_1^m \left\{\beta^{drt_1} \cdot \left[\sum_{s\in I} b_s \cdot \mathrm{tr}_m^n\left(\alpha^{st_2}\right)\right]^r - \beta^{drt_1} \right. \\ &\qquad \left. \cdot \left[\sum_{s\in I} b_s \cdot \mathrm{tr}_m^n\left(\alpha^{s(t_2+\tau)}\right)\right]^r\right\}. \end{aligned}$$

Using the function $g(t_2)$ defined in (7), the difference of the d-form sequence $c_d(t)$ can be rewritten as

$$\begin{aligned} c_d(t) - c_d(t+\tau) &= \mathrm{tr}_1^m\left\{\alpha^{Tdrt_1}\left[\beta^{d\cdot g(t_2)}\right]^r\right\} - \mathrm{tr}_1^m\left\{\alpha^{Tdrt_1}\left[\beta^{d\cdot g(t_2+\tau)}\right]^r\right\} \\ &= \mathrm{tr}_1^m\left\{\beta^{dr(t_1+g(t_2))}\right\} - \mathrm{tr}_1^m\left\{\beta^{dr(t_1+g(t_2+\tau))}\right\} \end{aligned}$$

where dr is relatively prime to M and the subsequence is either the all-zero sequence or a cyclic shift of the p-ary m-sequence $\mathrm{tr}_1^m(\beta^{drt_1})$, because $\gcd(dr, p^m-1)=1$. From the previous result, as t_2 varies from 0 to $T-1$, $g(t_2)=g(t_2+\tau)$ occurs $A=\frac{p^{n-m}-1}{p^m-1}$ times for any nonzero τ. That is, the set of t_2 such that

$$H(\alpha^{t_2})^r = H(\alpha^{t_2})^r, \qquad 0 \le t_2 \le T-1$$

has the same cardinality as the case for $r=1$ because $\gcd(r, M)=1$. Similarly to the derivation of autocorrelation values of the sequence $c(t)$, the autocorrelation of the sequence $c_d(t)$ for any nonzero τ is calculated as follows:

$$\begin{aligned} R_d(\tau) &= A\cdot(p^m-1) + (T-A)\cdot(-1) \\ &= \frac{p^{n-m}-1}{p^m-1}\cdot(p^m-1) \\ &\quad + \left(\frac{p^n-1}{p^m-1} - \frac{p^{n-m}-1}{p^m-1}\right)\cdot(-1) \\ &= -1 \end{aligned}$$

which means that the sequence $c_d(t)$ also has the ideal autocorrelation property. □

Helleseth, Kumar, and Martinsen introduced a new ternary sequence ($p=3$) with the ideal autocorrelation, which was the first nonbinary sequence with the ideal autocorrelation property except for the p-ary m-sequences and the p-ary cascaded GMW sequences.

Theorem 8 (Helleseth, Kumar, and Martinsen [7]): Let $s = 3^{2m}-3^m+1$ and $n=3m$. Let α be a primitive element of $F_{3^{3m}}$. Then, the ternary sequence of period $3^{3m}-1$ given by

$$c(t) = \mathrm{tr}_1^n(\alpha^t) + \mathrm{tr}_1^n(\alpha^{st}) \tag{8}$$

has the ideal autocorrelation property. □

Let e and k be integers and $m = e\cdot k$. Then the index set I in the ternary sequence in (8) is

$$I = \{1, 3^{2ek} - 3^{ek} + 1\}$$

where $3^{2ek}-3^{ek}+1 \equiv 1 \bmod 3^k-1$. That is, all elements in index set I are congruent to $1 \bmod 3^k-1$ and the sequence has the ideal autocorrelation property. The sequence in (8) satisfies the condition for index set I in the sequence (6) assumed in Theorem 7. Therefore, without proof, ternary d-form sequences with the ideal autocorrelation property can be given as follows.

Theorem 9: 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 the ternary d-form sequence of period $3^{3ek}-1$ given by

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

has the ideal autocorrelation property. □

Up to now, the ternary d-form sequences defined in Theorem 9 were the only d-form sequences with the ideal autocorrelation property including binary and nonbinary sequences. As far as the binary case is concerned, no d-form function satisfying the property derived in Theorem 5 has been found yet.

As an example, a ternary d-form sequence of period 3^9-1 with the ideal autocorrelation property can be constructed as follows.

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 the ideal autocorrelation property is given as

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

IV. p-ary Unified Sequences

In this section, a method for constructing new sequences, so-called *unified sequences* (extended d-form sequences), is proposed by combining the methods used to generate the extended sequences and d-form sequences.

Theorem 10: Assume that for an index set I, the sequence $b_u(t_1)$ of period M given by

$$b_u(t_1) = \sum_{a\in I} b_a \cdot \mathrm{tr}_1^m(\beta^{at_1}), \qquad b_a \in F_p^* \tag{9}$$

has the ideal autocorrelation property. Let $s \equiv d \bmod M$ for all s in some index set J, where d is relatively prime to M. Assume that the p-ary sequence $c(t)$ of period N given by

$$c(t) = \sum_{s\in J} c_s \cdot \mathrm{tr}_1^n(\alpha^{st}), \qquad c_s \in F_p^*$$

has the ideal autocorrelation property. For an integer r, $1 \le r \le M-1$, relatively prime to M, the unified sequence $c_u(t)$ of period N defined by

$$c_u(t) = \sum_{a\in I} b_a \cdot \mathrm{tr}_1^m\left\{\left[\sum_{s\in J} c_s \cdot \mathrm{tr}_m^n(\alpha^{st})\right]^{ar}\right\} \tag{10}$$

also has the ideal autocorrelation property.

Proof: As in the proof of Theorem 7, let t_1 and t_2 be the digits occurring in the base-T expansion of t, i.e., $t = t_1\cdot T + t_2$, $0 \le t_1 \le M-1$, $0 \le t_2 \le T-1$. Then, the p-ary unified sequence $c_u(t)$ in (10) can be expressed in the two-dimensional representation as follows:

$$\begin{aligned} c_u(t) &= \sum_{a\in I} b_a \cdot \mathrm{tr}_1^m\left\{\left[\sum_{s\in J} c_s \cdot \mathrm{tr}_m^n\left(\alpha^{s(t_1T+t_2)}\right)\right]^{ar}\right\} \\ &= \sum_{a\in I} b_a \cdot \mathrm{tr}_1^m\left\{\left[\sum_{s\in J} c_s \cdot \alpha^{sTt_1}\mathrm{tr}_m^n(\alpha^{st_2})\right]^{ar}\right\} \end{aligned}$$

$$= \sum_{a\in I} b_a \cdot \mathrm{tr}_1^m \left\{ \beta^{adrt_1} \left[\sum_{s\in J} c_s \cdot \mathrm{tr}_m^n(\alpha^{st_2}) \right]^{ar} \right\}$$
$$= \sum_{a\in I} b_a \cdot \mathrm{tr}_1^m \left\{ \beta^{adrt_1} \left[\beta^{d\cdot g(t_2)} \right]^{ar} \right\}$$
$$= \sum_{a\in I} b_a \cdot \mathrm{tr}_1^m \left\{ \beta^{adr(t_1+g(t_2))} \right\}$$

where the function $g(t_2)$ is defined as

$$\beta^{d\cdot g(t_2)} = \sum_{s\in J} c_s \cdot \mathrm{tr}_m^n(\alpha^{st_2}).$$

The subsequence of $c_u(t)$ for a fixed value of $t_2, 0 \le t_2 \le T-1$, is either the all-zero sequence of period M if $g(t_2) = -\infty$ or a cyclic shift of the decimated (by dr) sequence of the p-ary sequence in (9). That is,

$$b_u(drt_1) = \sum_{a\in I} b_a \cdot \mathrm{tr}_1^m(\beta^{adrt_1})$$

which has period M, because $\gcd(M, dr) = 1$. By assumption, the subsequence $b_u(drt_1)$ also has the ideal autocorrelation property. That is, the autocorrelation function $R_{u,\,sub}(\tau, t_2)$ of the subsequence $b_u(drt_1)$ defined by

$$R_{u,\,sub}(\tau, t_2) = \sum_{t_1=0}^{M-1} \omega^{b_u(dr(t_1+g(t_2)))-b_u(dr(t_1+g(t_2+\tau)))}$$

takes the values of $p^m - 1$ or -1. That is,

$$R_{u,\,sub}(\tau, t_2) = \begin{cases} p^m - 1, & \text{if } g(t_2) = g(t_2+\tau) \\ -1, & \text{if } g(t_2) \ne g(t_2+\tau). \end{cases}$$

The difference of the unified sequence $c_u(t)$ can be expressed as

$$\begin{aligned} &c_u(t) - c_u(t+\tau) \\ &= \sum_{a\in I} b_a \cdot \mathrm{tr}_1^m \left\{ \beta^{adrt_1} \left[\sum_{s\in J} c_s \cdot \mathrm{tr}_m^n(\alpha^{st_2}) \right]^{ar} \right\} \\ &\quad - \sum_{a\in I} b_a \cdot \mathrm{tr}_1^m \left\{ \beta^{adrt_1} \left[\sum_{s\in J} c_s \cdot \mathrm{tr}_m^n\left(\alpha^{s(t_2+\tau)}\right) \right]^{ar} \right\} \\ &= \sum_{a\in I} b_a \cdot \mathrm{tr}_1^m \left\{ \beta^{adrt_1} \left[\beta^{d\cdot g(t_2)} \right]^{ar} \right\} - \sum_{a\in I} b_a \\ &\quad \cdot \mathrm{tr}_1^m \left\{ \beta^{adrt_1} \left[\beta^{d\cdot g(t_2+\tau)} \right]^{ar} \right\} \\ &= \sum_{a\in I} b_a \cdot \mathrm{tr}_1^m \left\{ \beta^{adr(t_1+g(t_2))} \right\} - \sum_{a\in I} b_a \\ &\quad \cdot \mathrm{tr}_1^m \left\{ \beta^{adr(t_1+g(t_2+\tau))} \right\}. \end{aligned}$$

Therefore, the autocorrelation of the unified sequence $c_u(t)$ is given as

$$\begin{aligned} R(\tau) &= \sum_{t=0}^{N-1} \omega^{c_u(t)-c_u(t+\tau)} \\ &= \sum_{t_2=0}^{T-1} \sum_{t_1=0}^{M-1} \omega^{c_u(t_1T+t_2)-c_u(t_1T+t_2+\tau)} \\ &= \sum_{t_2=0}^{T-1} \sum_{t_1=0}^{M-1} \omega^{\sum_{a\in I} b_a\cdot \mathrm{tr}_1^m\{\beta^{adr(t_1+g(t_2))}\} - \sum_{a\in I} b_a\cdot \mathrm{tr}_1^m\{\beta^{adr(t_1+g(t_2+\tau))}\}} \\ &= \sum_{t_2=0}^{T-1} \sum_{t_1=0}^{M-1} \omega^{b_u(dr(t_1+g(t_2)))-b_u(dr(t_1+g(t_2+\tau)))} \\ &= \sum_{t_2=0}^{T-1} R_{u,\,\mathrm{sub}}(\tau, t_2). \end{aligned}$$

Similar to the autocorrelation of the sequences in Theorem 7, for any nonzero τ, the autocorrelation of the unified sequence $c_u(t)$ is the summation of the autocorrelation functions over t_2, $0 \le t_2 \le T-1$ of the subsequences with the ideal autocorrelation property. In the proof of Theorem 7, it is already derived that for any nonzero τ, as t_2 varies from 0 to $T-1$, $g(t_2) = g(t_2+\tau)$ occurs $A = \frac{p^{n-m}-1}{p^m-1}$ times. Thus, we have the autocorrelation value of the sequence $c_u(t)$ for any nonzero τ as in

$$\begin{aligned} R(\tau) &= A \cdot M + (T - A) \cdot (-1) \\ &= -1. \end{aligned}$$

Therefore, the unified sequence $c_u(t)$ has the ideal autocorrelation property. □

If we replace the sequence (9) by the p-ary GMW sequence or the p-ary cascaded GMW sequence in Theorem 10, then a (cascaded) unified sequence can be constructed as

$$c_u(t) = \mathrm{tr}_1^k \left\{ \left[\mathrm{tr}_k^l \left\{ \left[\mathrm{tr}_l^m \left\{ \left[\sum_{s\in J} c_s \cdot \mathrm{tr}_m^n(\alpha^{st}) \right]^r \right\} \right]^v \right\} \right]^u \right\}$$

where $c_s \in F_p^*$ and $b_u(t_1)$ is replaced by the p-ary cascaded GMW sequence

$$\mathrm{tr}_1^k\{[\mathrm{tr}_k^l\{[\mathrm{tr}_l^m(\beta^{t_1})]^v\}]^u\}$$

and k, l are integers such that $k|l|m$ and $\gcd(p^k-1, u) = 1$, $1 \le u \le p^k - 2$ and $\gcd(p^l-1, v) = 1$, $1 \le v \le p^l - 2$, respectively. Modifying the proof of Theorem 10, it can be easily shown that this sequence also has the ideal autocorrelation property. But any p-ary GMW sequence or p-ary cascaded GMW sequence can be expressed as the summation of decimated m-sequences as in (9) by expansion and therefore Theorem 10 may include the cases of the p-ary GMW sequences or the p-ary cascaded GMW sequences.

The unified sequence is a class of sequences, which includes the d-form sequences and the extended sequences. That is, if $J = \{1\}$, the unified sequences defined in (10) becomes the extended sequences with the ideal autocorrelation given by

$$c_u(t) = \sum_{a\in I} b_a \cdot \mathrm{tr}_1^m \left\{ \left[\mathrm{tr}_m^n(\alpha^t) \right]^{ar} \right\}.$$

In Theorem 10, let $m = 3k$ and $n = 9ek$, where e and k are positive integers. Using Theorem 10 and the ternary sequences with the ideal autocorrelation property introduced by Helleseth,

Kumar, and Martinsen, we can construct a ternary unified sequence for positive integers $m = 3k$ and $n = 9ek$ in the following theorem, given without proof.

Theorem 11: Let e and k be positive integers. Let α be a primitive element of $F_{3^{9ek}}$ and set $\beta = \alpha^T$, where $T = (3^{9ek} - 1)/(3^{3k} - 1)$. The ternary sequence $b_u(t_1)$ of period $M = 3^{3k} - 1$ given by

$$b_u(t_1) = \sum_{a \in I} \mathrm{tr}_1^{3k}(\beta^{at_1})$$

has the ideal autocorrelation property, where the index set I is $\{1, 3^{2k} - 3^k + 1\}$. For the index set $J = \{1, 3^{6ek} - 3^{3ek} + 1\}$, where $s \equiv 1 \bmod (3^{3k} - 1)$ for all s in the index set J and $d = 1$ is relatively prime to $3^{3k} - 1$, the ternary sequence $c(t)$ of period $3^{9ek} - 1$ given by

$$c(t) = \sum_{s \in J} \mathrm{tr}_1^{9ek}(\alpha^{st})$$

has the ideal autocorrelation property. For an integer r, $1 \le r \le 3^{3k} - 2$, relatively prime to $3^{3k} - 1$, and $s = 3^{6ek} - 3^{3ek} + 1$ and $a = 3^{2k} - 3^k + 1$, the ternary unified sequence $c_u(t)$ of period $3^{9ek} - 1$ defined by

$$c_u(t) = \mathrm{tr}_1^{3k}\left\{\left[\mathrm{tr}_{3k}^{9ek}(\alpha^t) + \mathrm{tr}_{3k}^{9ek}(\alpha^{st})\right]^r\right\} + \mathrm{tr}_1^{3k}\left\{\left[\mathrm{tr}_{3k}^{9ek}(\alpha^t) + \mathrm{tr}_{3k}^{9ek}(\alpha^{st})\right]^{ar}\right\} \quad (11)$$

also has the ideal autocorrelation property. □

If we replace the index set J by $\{1\}$, the sequence given in (11) becomes the ternary extended sequence with the ideal autocorrelation property as follows:

$$c_u(t) = \mathrm{tr}_1^{3k}\left\{\left[\mathrm{tr}_{3k}^{9ek}(\alpha^t)\right]^r\right\} + \mathrm{tr}_1^{3k}\left\{\left[\mathrm{tr}_{3k}^{9ek}(\alpha^t)\right]^{(3^{2k} - 3^k + 1)r}\right\}$$

where r, $1 \le r \le 3^{3k} - 2$, is relatively prime to $3^{3k} - 1$.

As an example, a ternary unified sequence of period $3^{27} - 1$ with the ideal autocorrelation property is given in the following example.

Example 12: Let $k = 3$ and α be a primitive element of $F_{3^{27}}$. Then $m = 9$, $n = 27$, $a = 3^6 - 3^3 + 1$, and $s = 3^{18} - 3^9 + 1$. Let r, $1 \le r \le 3^9 - 2$, be relatively prime to $3^9 - 1$. Then a ternary unified sequence of period $3^{27} - 1$ with the ideal autocorrelation property is given as

$$c_u(t) = \mathrm{tr}_1^9\left\{\left[\mathrm{tr}_9^{27}(\alpha^t) + \mathrm{tr}_9^{27}(\alpha^{st})\right]^r\right\} + \mathrm{tr}_1^9\left\{\left[\mathrm{tr}_9^{27}(\alpha^t) + \mathrm{tr}_9^{27}(\alpha^{st})\right]^{ar}\right\}. \quad \square$$

Recently, Helleseth and Gong [6] introduced a large class of p-ary sequences with the ideal autocorrelation property. They can also be used to construct the p-ary d-form sequences and the p-ary unified sequences.

REFERENCES

[1] L. D. Baumert, *Cyclic Difference Sets (Lecture Notes in Mathematics)*. New York: Springer-Verlag, 1971, vol. 182.

[2] A. H. Chan and R. Games, "On the linear span of binary sequences from finite geometries, q odd," in *Proc. Crypto 1986*, Santa Barbara, CA, 1986, pp. 405–417.

[3] S. W. Golomb, *Shift-Register Sequences*. Laguna Hills, CA: Aegean Park, 1982.

[4] G. Gong, "Q-ary cascaded GMW sequences," *IEEE Trans. Inform. Theory*, vol. 42, pp. 263–267, Jan. 1996.

[5] M. Goresky, A. H. Chan, and A. Klapper, "Cross-correlation of linearly and quadratically related geometric sequences and GMW sequences," *Discr. Appl. Math.*, vol. 46, no. 1, pp. 1–20, 1993.

[6] T. Helleseth and G. Gong, "New nonbinary sequences with ideal two-level autcorrelation function," preprint, 2001.

[7] T. Helleseth, P. V. Kumar, and H. M. Martinsen, "A new family of ternary sequences with ideal two-level autcorrelation," in *Proc. IEEE Int. Symp. Information Theory*, Sorrento, Italy, Jun. 2000, p. 3289.

[8] A. Klapper, "d-form sequences: Families of sequences with low correlation values and large linear spans," *IEEE Trans. Inform. Theory*, vol. 41, pp. 423–431, Mar. 1995.

[9] A. Klapper, A. H. Chan, and M. Goresky, "Cascaded GMW sequences," *IEEE Trans. Inform. Theory*, vol. 39, pp. 177–183, Jan. 1993.

[10] R. Lidl and H. Niederreiter, "Finite fields," in *Encyclopedia of Mathematics and Its Applications*. Reading, MA: Addison-Wesley, 1983, vol. 20.

[11] J. S. No, "A new family of binary pseudorandom sequences having optimal periodic correlation properties and large linear span," Ph.D. dissertation, Univ. Southern Calif., Los Angeles, May 1988.

[12] ——, "Generalization of GMW sequences and No sequences," *IEEE Trans. Inform. Theory*, vol. 42, pp. 260–262, Jan. 1996.

[13] J. S. No and P. V. Kumar, "A new family of binary pseudorandom sequences having optimal periodic correlation properties and large linear span," *IEEE Trans. Inform. Theory*, vol. 35, pp. 371–379, Mar. 1989.

[14] J. S. No, K. Yang, H. Chung, and H. Y. Song, "On the construction of binary sequences with ideal autocorrelation property," in *Proc. 1996 IEEE Int. Symp. Information Theory and Its Applications (ISITA '96)*, Victoria, BC, Canada, Sept. 17–20, 1996, pp. 837–840.

[15] R. A. Sholtz and L. R. Welch, "GMW sequences," *IEEE Trans. Inform. Theory*, vol. IT-30, pp. 548–553, May 1984.

[16] M. K. Simon, J. K. Omura, R. A. Sholtz, and B. K. Levitt, *Spread Spectrum Communications*. Rockville, MD: Computer Sci., 1985, vol. 1.