# New Nonbinary Sequences With Ideal Two-Level Autocorrelation

Tor Helleseth, *Fellow, IEEE,* and Guang Gong, *Member, IEEE*

***Abstract*—We find new families of nonbinary sequences of period $p^n - 1$ with symbols from a finite field $F_p$ for any prime $p \geq 3$. The sequences have two-level ideal autocorrelation and are generalizations of recently found ternary sequences with ideal autocorrelation. Difference sets with parameters**

$$\left(\frac{p^n-1}{p-1}, \frac{p^{n-1}-1}{p-1}, \frac{p^{n-2}-1}{p-1}\right)$$

**can also be derived from these sequences in a natural way.**

***Index Terms*—Autocorrelation, difference sets, nonbinary sequences.**

## I. Introduction

GIVEN a sequence $\{s(t)\}$ of period $\varepsilon$ and with elements from a finite field $F_p$, the autocorrelation of the sequence at shift $\tau$ is defined by

$$a(\tau) = \sum_{t=0}^{\varepsilon-1} \omega^{s(t+\tau)-s(t)}$$

where $\omega$ is a complex $p$th root of unity.

An important problem in sequence design is to find sequences with two-level ideal autocorrelation, i.e., where $a(\tau) = -1$ for any $\tau \neq 0$. Recently, much progress has been obtained for binary sequences of period $\varepsilon = 2^n - 1$. These are of considerable interest also because of their close connections to difference sets. For recent work on binary sequences with two-level ideal autocorrelation the reader is referred to [5], [9], [12], [13], [4] and [3]. Recently, there has also been some progress leading to ternary sequences with two-level ideal autocorrelation: Helleseth, Kumar, and Martinsen [7] and Arasu and Player [1].

In this paper, we will construct new nonbinary sequences of period $\varepsilon = p^n - 1$ with ideal two-level autocorrelation. The sequences are generalizations of the ternary sequences in [7] and the proofs use the same basic ideas with some modifications.

In Section II, we will give some preliminaries and in Section III, we will present the new sequences with ideal autocorrelation.

## II. Preliminaries

In this section, we will give some basic results needed in order to prove our main result. The main idea comes from the recent paper by Helleseth, Kumar, and Martinsen [7] and is based on constructing sequences which leads to quadratic forms with odd ranks. Some of the basic lemmas are essentially given in [7], so we only indicate the proofs. Further, Trachtenberg [14] and Helleseth [6] used similar ideas during their studies of the cross correlation of nonbinary $m$-sequences.

In the following, we let $p$ be an odd prime and let

$$\mathrm{Tr}_k^n(x) = \sum_{i=0}^{n/k-1} x^{p^{ik}}$$

denote the trace from the field $F_{p^n}$ to the subfield $F_{p^k}$. For simplicity, we let $\mathrm{Tr}_n(x)$ (resp., $\mathrm{Tr}_k(x)$) denote the trace from $F_{p^n}$ to $F_p$ (resp., from $F_{p^k}$ to $F_p$). Sometimes we will also use the notation $q = p^k$ and, therefore, $q^{n/k} = p^n$ when convenient.

Throughout this paper, we let $f(x)$ be a polynomial with coefficients in $F_{p^n}$ such that

$$f(\lambda x) = \lambda f(x), \qquad \text{for any } \lambda \in F_{p^k}.$$

We define a nonbinary sequence $\{s(t)\}$ via

$$s(t) = \mathrm{Tr}_n\left(f\left(\alpha^t\right)\right)$$

where $\alpha$ is a primitive element in $F_{p^n}$ (i.e., an element of order $p^n - 1$). We will give sufficient conditions for the nonbinary sequence $\{s(t)\}$ to have an ideal autocorrelation and we will provide new functions $f(x)$ with this property.

*Lemma 1:* Let $n/k$ be odd and $d$ a positive integer such that $gcd(d, p^n-1) = 2$ and $d \equiv 2(\mathrm{mod} p^k - 1)$. Then the sequence $\{s(t)\}$ has autocorrelation

$$a(\tau) = -1 + S(\tau)$$

where

$$2S(\tau) = \sum_{x\in F_{p^n}} \omega^{\mathrm{Tr}_k(Q(x))} + \sum_{x\in F_{p^n}} \omega^{\mathrm{Tr}_k(rQ(x))}$$

and

$$Q(x) = \mathrm{Tr}_k^n(f(\alpha^\tau x^d) - f(x^d))$$

is a quadratic form over $F_{p^k}$ and $r$ a nonsquare in $F_{p^k}$.

*Proof:* The autocorrelation of $\{s(t)\}$ at shift $\tau$ is given by

$$\begin{aligned} a(\tau) &= \sum_{t=0}^{p^n-2} \omega^{s(t+\tau)-s(t)} \\ &= \sum_{t=0}^{p^n-2} \omega^{\mathrm{Tr}_n(f(\alpha^{t+\tau})-f(\alpha^t))} \\ &= -1 + \sum_{x\in F_{p^n}} \omega^{\mathrm{Tr}_n(f(\alpha^\tau x)-f(x))}. \end{aligned}$$

Manuscript received May 21, 2001; revised June 12, 2002. This work was supported by the Norwegian Research Council.

T. Helleseth is with the Department of Informatics, University of Bergen, N-5020 Bergen, Norway (e-mail: Tor.Helleseth@ii.uib.no).

G. Gong is with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON N2L 3G1, Canada (e-mail: ggong@ece.uwaterloo.ca).

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

Digital Object Identifier 10.1109/TIT.2002.804052.

When $x$ runs through $F_{p^n}$, then $x^d$ runs twice through the nonzero squares in $F_{p^n}$ and takes on the value 0 once. Similarly, for a nonsquare $r$ in $F_{p^n}$, $rx^d$ runs twice through all the nonsquares in $F_{p^n}$ and takes on the value 0 once. Since $n/k$ is odd, we can select $r$ as a nonsquare in $F_{p^k}$. This will also be a nonsquare in $F_{p^n}$. Hence, since $f(rx) = rf(x)$, we get

$$\begin{aligned} 2S(\tau) = &\sum_{x\in F_{p^n}} \omega^{\mathrm{Tr}_k(\mathrm{Tr}_k^n(f(\alpha^\tau x^d)-f(x^d)))} \\ &+ \sum_{x\in F_{p^n}} \omega^{\mathrm{Tr}_k(\mathrm{Tr}_k^n(f(\alpha^\tau rx^d)-f(rx^d)))} \\ = &\sum_{x\in F_{p^n}} \omega^{\mathrm{Tr}_k(Q(x))} + \sum_{x\in F_{p^n}} \omega^{\mathrm{Tr}_k(rQ(x))}. \end{aligned}$$

Further, $Q(x)$ is a quadratic form over $F_{p^k}$, since for all $\lambda \in F_{p^k}$, we have

$$Q(\lambda x) = \mathrm{Tr}_k^n\left(f\left(c\lambda^d x^d\right) - f\left(\lambda^d x^d\right)\right) = \lambda^d Q(x) = \lambda^2 Q(x)$$

where $c = \alpha^\tau$. □

We present two examples $f_1(x)$ and $f_2(x)$ and the corresponding quadratic forms $Q_1(x)$ and $Q_2(x)$ over $F_{p^k}$. The main result in this paper is to show that under certain conditions for their coefficients, $s_1(t) = \mathrm{Tr}_n(f_1(\alpha^t))$ and $s_2(t) = \mathrm{Tr}_n(f_2(\alpha^t))$ lead to sequences with ideal two-level autocorrelation.

*Example 1:* Let $n/k = 2m+1$ and define

$$f_1(x) = \sum_{i=0}^{m} u_i x^{(q^{2^i}+1)/2}, \qquad u_i \in F_q.$$

Clearly, $f_1(\lambda x) = \lambda f_1(x)$ for any $\lambda \in F_q$. Let $c = \alpha^\tau$. Then, for $d = 2$, we obtain the quadratic form

$$\begin{aligned} Q_1(x) &= \mathrm{Tr}_k^n\left(f_1\left(\alpha^\tau x^d\right) - f_1\left(x^d\right)\right) \\ &= \mathrm{Tr}_k^n\left(\sum_{i=0}^{m} u_i\left(c^{(q^{2i}+1)/2} - 1\right) x^{q^{2i}+1}\right). \end{aligned}$$

*Example 2:* Let $n/k = 2m+1$ and define

$$f_2(x) = \sum_{i=0}^{m} u_{m-i}\, x^{(q^{2i+1}+1)/(q+1)}, \qquad u_i \in F_q.$$

Note that $f_2(\lambda x) = \lambda f_2(x)$ for any $\lambda \in F_q$. Let $c = \alpha^\tau$. Then for $d = q+1$ we obtain the quadratic form

$$\begin{aligned} Q_2(x) &= \mathrm{Tr}_k^n\left(f_2\left(\alpha^\tau x^d\right) - f_2\left(x^d\right)\right) \\ &= \mathrm{Tr}_k^n\left(\sum_{i=0}^{m} u_{m-i}\left(c^{(q^{2i+1}+1)/(q+1)} - 1\right) x^{q^{2i+1}+1}\right). \end{aligned}$$

Let $x = \sum_{i=1}^{n/k} x_i \alpha_i$ where $x_i \in F_{p^k}$, and $\alpha_i$ is a basis for $F_{p^n}$ over $F_{p^k}$. Then any quadratic form $Q(x)$ over $F_{p^k}$ can be written as

$$Q(x) = \sum_{i=1}^{n/k}\sum_{j=1}^{n/k} b_{ij} x_i x_j$$

where $b_{ij} \in F_{p^k}$.

Any quadratic form can be transformed into a canonical form by nonsingular transformations. The rank of a quadratic form is the (minimum) number of variables the form depends on. We next give a result concerning quadratic forms of odd rank from Dickson [2]. Any quadratic form of odd rank can be transformed into the form given in the following lemma.

*Lemma 2:* Let $q = p^k$, where $p$ is an odd prime. Let $N(a)$ be the number of solutions of the quadratic equation

$$a_1x_1^2 + a_2x_2^2 + \cdots + a_{2t+1}x_{2t+1}^2 = a$$

where each $a_i \neq 0$, $a_i \in F_q$, and $a \in F_q$. Then

$$N(a) = q^{2t} + \chi(\delta)q^t$$

where $\delta = (-1)^t a a_1 a_2 \cdots a_{2t+1}$ and $\chi$ is the quadratic character on $F_q$.

*Lemma 3:* Let $Q(x)$ be a quadratic form over $F_{p^k}$ of odd rank, and $r$ a nonsquare in $F_{p^k}$. Then

$$S = \sum_{x\in F_{p^n}} \omega^{\mathrm{Tr}_k(Q(x))} + \sum_{x\in F_{p^n}} \omega^{\mathrm{Tr}_k(rQ(x))} = 0.$$

*Proof:* Since the rank of the quadratic form $Q(x)$ is odd, say $2t+1$, we can transform $Q(x)$ into the form in Lemma 2 and calculate the number of solutions of $Q(x) = a$ and $rQ(x) = a$ for all $a \in F_{p^k}$. Then the combined number of solutions $T(a)$ of $Q(x) = a$ and $rQ(x) = a(=Q'(x))$ is (where $Q'(x)$ has $a_i' = ra_i$ for $1 \le i \le 2t+1$ and $\delta'$ refers to $Q'(x)$)

$$\begin{aligned} T(a) &= \left\{\left(q^{2t} + \chi(\delta)q^t\right) + \left(q^{2t} + \chi(\delta')q^t\right)\right\} q^{\frac{n}{k}-2t-1} \\ &= 2q^{\frac{n}{k}-1} \end{aligned}$$

since $\chi(\delta') = \chi(r^{2t+1}\delta) = -\chi(\delta)$ and $\frac{n}{k} - 2t - 1$ is the number of variables $Q(x)$ is independent of. It follows that $T(a)$ is independent of $a$ and, therefore, that $S = 0$. □

Hence, in order to find new sequences with ideal two-level autocorrelation, we let $n/k$ be odd and $d$ a positive integer such that $gcd(d, p^n - 1) = 2$ and $d \equiv 2 (\bmod\, p^k - 1)$. Thereafter, we select $f(x)$ such that $f(\lambda x) = \lambda f(x)$ for any $\lambda \in F_{p^k}$ and such that the quadratic form $Q(x) = \mathrm{Tr}_k^n(f(cx^d) - f(x^d))$ has odd rank for all $c = \alpha^\tau \neq 1$.

The rank $\rho$ of the quadratic form $Q(x)$ can be determined by

$$q^{\frac{n}{k}-\rho} = |\{z \in F_{q^{n/k}} | Q(x+z) = Q(x) \text{ for all } x \in F_{q^{n/k}}\}|$$

since $Q(x)$ is independent of $\frac{n}{k} - \rho$ coordinates.

It is useful to observe that if $z = 0$ is the only element in $F_{p^n}$ such that $Q(x+z) = Q(x)$ for all $x \in F_{p^n}$, then the rank of $Q(x)$ equals $n/k = 2m+1$ i.e., is odd. This will always be the case for the new sequences we construct in this paper.

## III. New Nonbinary Sequences With Ideal Autocorrelation

The main result is to construct new nonbinary sequences with ideal two-level autocorrelation.

*Theorem 1:* Let $\alpha$ be a primitive element of $F_{p^n}$. Let $n = (2m+1)k$ and let $s$, $1 \le s \le 2m$ be an integer such that $gcd(s, 2m+1) = 1$. Define $b_0 = 1$, $b_{is} = (-1)^i$, and $b_i =$

$b_{2m+1-i}$ for $i = 1, 2, \ldots, m$. Let $u_0 = b_0/2 = (p+1)/2$ and $u_i = b_{2i}$ for $i = 1, 2, \ldots, m$. Define

$$f(x) = \sum_{i=0}^{m} u_i x^{(q^{2i}+1)/2}.$$

Then the sequence over $F_p$ defined by

$$s(t) = \mathrm{Tr}_n\left(f\left(\alpha^t\right)\right)$$

has an ideal two-level autocorrelation, where all indexes of the $b_i$'s are taken $\bmod 2m+1$.

*Proof:* From the definition, it follows that $f(\lambda x) = \lambda f(x)$ for $\lambda \in F_{p^k}$ and, therefore, that $Q(x) = \mathrm{Tr}_k^n(f(cx^2) - f(x^2))$ is the quadratic form

$$Q(x) = \mathrm{Tr}_k^n\left(\sum_{i=0}^{m} u_i\left(c^{(q^{2i}+1)/2} - 1\right)x^{q^{2i}+1}\right).$$

To determine the rank $\rho$, we observe that $q^{2m+1-\rho}$ is the number of solutions $z \in F_{p^n}(=F_{q^{2m+1}})$, such that $Q(x+z) = Q(x)$ for all $x \in F_{p^n}$. Let $a_i = u_i(c^{(q^{2i}+1)/2} - 1)$. Then we have $Q(x+z) = Q(x)$ if and only if

$$\mathrm{Tr}_k^n\left(\sum_{i=0}^{m} a_i(x+z)^{q^{2i}+1}\right) = \mathrm{Tr}_k^n\left(\sum_{i=0}^{m} a_i x^{q^{2i}+1}\right)$$

which is equivalent to

$$\mathrm{Tr}_k^n\left(\sum_{i=0}^{m} a_i\left(x^{q^{2i}}z + xz^{q^{2i}}\right) + \sum_{i=0}^{m} a_i z^{q^{2i}+1}\right) = 0.$$

Raising the first term to the $q^{2m+1-i}$ power, we obtain

$$\mathrm{Tr}_k^n\left(x\left(\sum_{i=0}^{m}\left(a_i^{q^{2m+1-2i}}z^{q^{2m+1-2i}} + a_i z^{q^{2i}}\right)\right) + \sum_{i=0}^{m} a_i z^{q^{2i}+1}\right) = 0.$$

If this holds for all $x \in F_{q^{2m+1}}$, we must have

$$\sum_{i=0}^{m} a_i^{q^{2m+1-2i}} z^{q^{2m+1-2i}} + \sum_{i=0}^{m} a_i z^{q^{2i}} = 0$$

and

$$\mathrm{Tr}_k^n\left(\sum_{i=0}^{m} a_i z^{q^{2i}+1}\right) = 0.$$

From the definition of $a_i$ it follows that the first of these two equations becomes

$$\sum_{i=0}^{m} u_i\left(\left(\left(c^{(q^{-2i}+1)/2} - 1\right)z^{q^{-2i}}\right)^{q^{2m+1}} + \left(c^{(q^{2i}+1)/2} - 1\right)z^{q^{2i}}\right) = 0.$$

We will in the following represent each element $c \in F_{q^{2m+1}}$ in the form $c = r\gamma^2$ where $r = 1$ or $r$ is a nonsquare in the field $F_q$.

To show that the rank $\rho$ of $Q(x)$ is $2m+1$ (i.e., odd), it is, therefore, sufficient to show that the equation

$$L(z) = \sum_{i=0}^{2m} b_i\left(r\gamma^{q^i+1} - 1\right)z^{q^i} = 0$$

has $z = 0$ as its only solution for any $c = r\gamma^2 \neq 1$. Since this is a linearized polynomial, we can raise this to the $q^{is}$th power for $i = 0, 1, \ldots, 2m$ and obtain a linear equation system with $2m+1$ equations in the $2m+1$ unknowns $z^{q^{js}}$ for $j = 0, 1, \ldots, 2m$. The coefficient matrix $M = (m_{i,j})$ of this system is given by

$$m_{i,j} = b_{(j-i)s}\left(r\gamma^{q^{is}+q^{js}} - 1\right)$$

where the indexes are taken modulo $2m+1$ and where $m_{i,j}$ is the coefficient of $z^{q^{js}}$ in $(L(z))^{q^{is}}$. Note also that the coefficient matrix is symmetric since $b_i = b_{2m+1-i}$ for $i = 1, 2, \ldots, m$.

Introduce the variables $x_i = \gamma^{q^{is}}$ for $i = 0, 1, \ldots, 2m$ and $y$ for $r$. Then the coefficient matrix for the equation system is given by

$$m_{i,j} = b_{(j-i)s}(yx_ix_j - 1).$$

From the definition of the $b_i$'s it is straightforward to see that the determinant is

$$\Delta = (-1)^m 2^{2m}\prod_{i=0}^{2m}(yx_ix_{i+m} - 1)$$

i.e.,

$$\Delta = (-1)^m 2^{2m}\prod_{i=0}^{2m}\left(r\gamma^{q^{is}+q^{(i+m)s}} - 1\right)$$

where $c = r\gamma^2$.

Since $\gamma^{q^{is}+q^{(i+m)s}}$ is a square, it follows that $\Delta$ is nonzero when $r$ is a nonsquare. In the case, $r = 1$, in order for the determinant to be zero, we must have $\gamma^{gcd\,(q^{ms}+1,\, q^{2m+1}-1)} = 1$. Since $gcd\,(q^{ms}+1, q^{2m+1}-1)$ divides

$$gcd\,(q^{2ms}-1, q^{2m+1}-1) = q-1$$

and

$$q^{ms}+1 \equiv 2 \bmod q-1$$

we obtain $c = \gamma^2 = 1$. Hence, the equation system has $z = 0$ as its only solution except when $c = 1$ and we conclude that $\{s(t)\}$ has ideal two-level autocorrelation. □

*Theorem 2:* Let $\alpha$ be a primitive element of $F_{p^n}$. Let $n = (2m+1)k$ and let $1 \leq s \leq 2m$ be an integer such that $gcd\,(s, 2m+1) = 1$. Define $b_0 = 1$, $b_{is} = (-1)^i$, and $b_i = b_{2m+1-i}$ for $i = 1, 2, \ldots, m$. Let $u_0 = b_0/2 = (p+1)/2$ and $u_i = b_{2i}$ for $i = 1, 2, \ldots, m$. Define

$$f(x) = \sum_{i=0}^{m} u_{m-i}x^{(q^{2i+1}+1)/(q+1)}.$$

Then the sequence over $F_p$ defined by

$$s(t) = \mathrm{Tr}_n\left(f\left(\alpha^t\right)\right)$$

has an ideal two-level autocorrelation, where all indexes of the $b_i$'s are taken modulo $2m+1$.

*Proof:* Observe that $(\bmod q^{2m+1}-1)$, we have

$$\frac{q^{2m}+1}{2}\cdot\frac{q^{2(m-i)+1}+1}{q+1}\equiv\frac{q^{2i}+1}{2}\,q^{2(m-i)}.$$

This follows since their difference $D$ equals

$$\begin{aligned}D&=\frac{q^{2(m-i)+2m+1}+1-q^{2m+1}-q^{2(m-i)}}{2(q+1)}\\&=\left(q^{2m+1}-1\right)\frac{q^{2(m-i)}-1}{2(q+1)}\\&\equiv 0\qquad(\bmod q^{2m+1}-1).\end{aligned}$$

Let $v=\frac{q^{2m}+1}{2}$. Then $gcd(v,\,q^{2m+1}-1)=1$ and

$$\mathrm{Tr}_n(f_1(x))=\mathrm{Tr}_n(f(x^v)),\qquad \text{for all } x\in F_{q^{2m+1}}$$

where $f_1(x)$ represents a polynomial in Theorem 1. Thus, the sequences obtained from Theorem 2 are just proper decimations of the sequences in Theorem 1. □

*Remark:* The recently found ternary sequences in Helleseth, Kumar, and Martinsen [7] are (within equivalence) obtained from Theorem 2 by letting $p=3$, $m=1$, and, therefore, $f(x)=x+x^{\frac{q^3+1}{q+1}}$.

The following corollary generalizes and solves Conjecture A in Ludkowski and Gong [8].

*Corollary 1:* Let $u_0=\frac{p+1}{2}$ and $u_i=(-1)^i$ for $i=1,2,\ldots,m$. Let $f(x)$ be as in one of the two previous theorems. Then the sequence over $F_p$ defined by

$$s(t)=\mathrm{Tr}_n(f(\alpha^t))$$

has an ideal two-level autocorrelation.

*Proof:* The theorems above with $s=2$ gives

$$u_i=b_{2i}=(-1)^i(=b_{2m+1-2i}),\qquad \text{for } i=1,\,2,\,\ldots,\,m.$$

Further, $u_0=b_0/2=(p+1)/2$ and the result follows directly. □

Table I gives some parameters of sequences with ideal two-level autocorrelation obtained in this paper. Note that $s$ and $2m+1-s$ give the same sequences.

A problem for further investigation is to find more functions $f(x)$ that lead to sequences such that each of the corresponding quadratic forms (one for each shift $\tau$) has an odd rank for all nonzero shifts.

Finally, we note that it is straightforward (for example, using methods in No [10]) to see that the sequences lead to

$$\left(\frac{p^n-1}{p-1},\,\frac{p^{n-1}-1}{p-1},\,\frac{p^{n-2}-1}{p-1}\right)$$

difference sets in a natural way, i.e.,

$$D=\left\{t|s_t=0,\;0\le t<\frac{p^n-1}{p-1}\right\}.$$

Using ideas in No [10], [11], the sequences in this paper are excellent building blocks for constructing other sequences with ideal autocorrelation as well as many other families of difference sets.

TABLE I
SOME SEQUENCES WITH IDEAL AUTOCORRELATION

| $p$ | $n$ | $m$ | $u_0u_1\cdots u_m$ | $s$ |
|---|---|---|---|---|
| 3 | 5 | 2 | 2 1 2 | 1 |
| 3 | 5 | 2 | 2 2 1 | 2 |
| 3 | 7 | 3 | 2 1 2 2 | 1 |
| 3 | 7 | 3 | 2 2 1 2 | 2 |
| 3 | 7 | 3 | 2 2 2 1 | 3 |
| 3 | 9 | 4 | 2 1 1 2 2 | 1 |
| 3 | 9 | 4 | 2 2 1 2 1 | 2 |
| 3 | 9 | 4 | 2 1 2 2 1 | 4 |
| 3 | 11 | 5 | 2 1 1 2 2 2 | 1 |
| 3 | 11 | 5 | 2 2 1 2 1 2 | 2 |
| 3 | 11 | 5 | 2 2 2 1 2 1 | 3 |
| 3 | 11 | 5 | 2 2 2 1 1 2 | 4 |
| 3 | 11 | 5 | 2 1 2 2 2 1 | 5 |
| 5 | 5 | 2 | 3 1 4 | 1 |
| 5 | 5 | 2 | 3 4 1 | 2 |
| 5 | 7 | 3 | 3 1 4 4 | 1 |
| 5 | 7 | 3 | 3 4 1 4 | 2 |
| 5 | 7 | 3 | 3 4 4 1 | 3 |
| 7 | 5 | 2 | 4 1 6 | 1 |
| 7 | 5 | 2 | 4 6 1 | 2 |

## IV. CONCLUSION

If $n/k=2m+1$ is odd, $q=p^k$, and $\alpha$ is a primitive element of $F_{p^n}$, then we have found functions of the form

$$f(x)=\sum_{i=0}^{m}u_ix^{(q^{2i}+1)/2}$$

and

$$f(x)=\sum_{i=0}^{m}u_{m-i}x^{(q^{2i+1}+1)/(q+1)}$$

such that the nonbinary sequence $\{s(t)\}$ over $F_p$ given by $s(t)=\mathrm{Tr}_n(f(\alpha^t))$ has a two-level ideal autocorrelation. The sequences also give rise to difference sets with Singer parameters. Whether the sequences (or difference sets) are nonequivalent is a topic for further research.

## ACKNOWLEDGMENT

The authors wish to thank K. Khoo and M. Parker for computer assistance during this work.

## REFERENCES

[1] K. T. Arasu and K. J. Player, “A new family of cyclic difference sets with Singer parameters in characteristic three,” manuscript, submitted for publication.

[2] L. E. Dickson, *Linear Groups With an Exposition of the Galois Field Theory*. New York: Dover, 1983.

[3] J. Dillon, “Multiplicative difference sets via additive characters,” *Des., Codes Cryptogr.*, vol. 17, pp. 225–235, 1999.

[4] J. F. Dillon and H. Dobbertin, “New cyclic difference sets with Singer parameters,” manuscript, submitted for publication.

[5] R. Evans, H. Hollmann, C. Krattenthaler, and Q. Xiang, "Gauss sums, Jacobi sums, and p-ranks of cyclic difference sets," *J. Comb. Theory Ser. A*, vol. 87, pp. 74–119, 1999.

[6] T. Helleseth, "Some results about the cross-correlation function between two maximal linear sequences," *Discr. Math.*, vol. 16, pp. 209–232, 1976.

[7] T. Helleseth, P. V. Kumar, and H. Martinsen, "A new family of ternary sequences with ideal two-level autocorrelation function," *Des., Codes Cryptogr.*, vol. 23, pp. 157–166, 2001.

[8] M. Ludkovski and G. Gong, "New families of ideal 2-level autocorrelation ternary sequences from second order DHT," in *Proc. Int. Conf. Coding and Cryptography*, Paris, France, Jan. 8–12, 2001, pp. 345–354.

[9] A. Maschietti, "Difference sets and hyperovals," *Des., Codes Cryptogr.*, vol. 14, pp. 89–98, 1998.

[10] J. S. No, "New cyclic difference sets with Singer parameters constructed from $q$-ary sequences," manuscript, submitted for publication.

[11] ——, "$p$-ary unified sequences: $p$-ary extended $d$-form sequences with ideal autocorrelation property," *IEEE Trans. Inform. Theory*, vol. 48, pp. 2540–2546, Sept. 2002.

[12] J. S. No, H. Chung, and M. S. Yun, "Binary pseudorandom sequences of period $2^m - 1$ with ideal autocorrelation generated by the polynomial $z^d + (z+1)^d$," *IEEE Trans. Inform. Theory*, vol. 44, pp. 1278–1282, May 1998.

[13] J. S. No, S. W. Golomb, G. Gong, H. K. Lee, and P. Gaal, "Binary pseudorandom sequences of period $2^n - 1$ with ideal autocorrelation," *IEEE Trans. Inform. Theory*, vol. 44, pp. 814–817, Mar. 1998.

[14] H. M. Trachtenberg, "On the cross-correlation functions of maximal linear sequences," Ph.D. dissertation, University of Southern California, Los Angeles, 1970.