New nonbinary sequences with ideal two-level autocorrelation function

Tor Helleseth

Department of Informatics, University of Bergen
Høyteknologisenteret, N-5020 Bergen, Norway

Guang Gong

Department of Electrical and Computer Engineering, University of Waterloo,
Waterloo Ontario N2L 3G1, Canada

Abstract. We find new families of nonbinary sequences of period $p^n - 1$ with symbols from a finite field F_p for any $p \geq 3$. The sequences have two-level ideal autocorrelation functions and are generalizations of recently found ternary sequences with ideal autocorrelation. Difference sets with parameters $(\frac{p^n-1}{p-1}, \frac{p^{n-1}-1}{p-1}, \frac{p^{n-2}-1}{p-1})$ can also be derived from these sequences in a natural way.

1 Introduction

Given a sequence $\{s(t)\}$ of period ε and with elements from a finite field F_p. The autocorrelation of the sequence at shift τ is defined by

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

where ω is a complex pth 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 function the reader is referred to [5], [8], [12], [13], [4] and [3]. Recently, there has also been some progress leading to ternary sequences with a two-level ideal autocorrelation function, Helleseth, Kumar and Martinsen [7], Ludkovski and Gong [9], 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 generalization of the ternary sequences in [7] and the proofs use the same basic ideas with some modifications.

In Section 2 we will give some preliminaries and in Section 3 we will present the new sequences with ideal autocorrelation.

2 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] use similar ideas during their studies of the crosscorrelation of nonbinary m-sequences.

In the following we let p be an odd prime and let $Tr_k^n(x) = \sum_{i=0}^{n/k-1} x^{p^{ik}}$ denote the trace from the field F_{p^n} to the subfield F_{p^k}. For simplicity we let $Tr_n(x)$ (resp. $Tr_k(x)$) 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 $f(\lambda x) = \lambda f(x)$ for any $\lambda \in F_{p^k}$. Define a nonbinary sequence

$$s(t) = Tr_n(f(\alpha^t))$$

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

Lemma 1 *Let $gcd(d, p^n - 1) = 2$, n/k odd and $d \equiv 2 \pmod{p^k - 1}$. Let $f(x)$ be as above, then the sequence $\{s(t)\}$ has autocorrelation*

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

where

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

and $Q(x) = Tr_k^n(f(\alpha^\tau x^d) - f(x^d))$ is a quadratic form over F_{p^k} and r a nonsquare in F_{p^k}.

Proof. The autocorrelation function of $\{s(t)\}$ at shift τ is given by

$$a(\tau) = \sum_{t=0}^{p^n-2} \omega^{s(t+\tau)-s(t)}$$

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

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}, then 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

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

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

$$
Q(\lambda x) = Tr_k^n(f(c\lambda^d x^d) - f(\lambda^d x^d)) = \lambda^d Q(x) = \lambda^2 Q(x)
$$

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 then $s_1(t) = Tr_n(f_1(\alpha^t))$ and $s_2(t) = Tr_n(f_2(\alpha^t))$ lead to sequences with ideal two-level autocorrelation.

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

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

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

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

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

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

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

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

Let $x = \sum_{i=1}^{n/k} x_i \alpha_i$ where $x_i \in F_{p^k}$, and α_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 transferred to a canonical form with 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 lemma below.

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

$$a_1 x_1^2 + a_2 x_2^2 + \cdots + a_{2t+1} x_{2t+1}^2 = a$$

where each $a_i \neq 0$, $a_i \in F_q$ and $a \in F_q$, is given by

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

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

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*

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

Proof. Since the rank of the quadratic form $Q(x)$ is odd, say $2t + 1$, we can transform $Q(x)$ to 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 $1 \leq i \leq 2t+1$ and δ' refers to $Q'(x)$),

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

since $\chi(\delta') = \chi(r^{2t+1}\delta) = -\chi(\delta)$ and $n/k - 2t - 1$ 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 $gcd(d, p^n - 1) = 2$, n/k odd, $d \equiv 2 \pmod{p^k - 1}$ and select $f(x)$ such that $f(\lambda x) = \lambda f(x)$ for any $\lambda \in F_{p^k}$ and such that the quadratic form $Q(x) = Tr_k^n(f(cx^d) - f(x^d))$ has odd rank for all $c = \alpha^\tau \neq 1$.

The rank ρ of the quadratic form $Q(x)$ can be determined by,

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

since $Q(x)$ is independent of $n/k - \rho$ 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., odd. This will always be the case for the new sequences we construct in this paper.

Theorem 1 *Let α be a primitive element of F_{p^n}. Let $n = (2m+1)k$ and let s, $1 \leq s \leq 2m$ be an integer such that* $\gcd(s, 2m+1) = 1$. *Define*

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

and let $b_0 = 2u_0$, $u_i = b_{2i} = b_{2m+1-2i}$ for $i = 1, 2, ..., m$. Suppose $b_0 = \pm 1$ and $b_{is} = (-1)^i$ for $i = 1, 2, ..., m$, then the sequence over F_p defined by

$$s(t) = Tr_n(f(\alpha^t))$$

has an ideal two-level autocorrelation, where indices of b_{is} are taken mod $2m+1$.

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

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

To determine the rank ρ, 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

$$Tr_k^n(\sum_{i=0}^{m} a_i(x+z)^{q^{2i}+1}) = Tr_k^n(\sum_{i=0}^{m} a_i x^{q^{2i}+1})$$

which is equivalent to

$$Tr_k^n(\sum_{i=0}^{m} a_i(x^{q^{2i}} z + x z^{q^{2i}}) + \sum_{i=0}^{m} a_i z^{q^{2i}+1}) = 0$$

i.e.,

$$Tr_k^n(x(\sum_{i=0}^{m} a_i^{q^{-2i}} z^{q^{-2i}} + \sum_{i=0}^{m} a_i z^{q^{2i}}) + \sum_{i=0}^{m} a_i z^{q^{2i}+1}) = 0.$$

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

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

and

$$Tr_k^n(\sum_{i=0}^{m} a_i z^{q^{2i}+1}) = 0.$$

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

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

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

$$L(z) = \sum_{i=0}^{2m} b_i(c^{(q^i+1)/2} - 1) z^{q^i} = 0$$

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

$$m_{i,j} = b_{(j-i)s}(c^{(q^{is}+q^{js})/2} - 1)$$

where the indices 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 $i = 1, 2, ..., m$.

Any element $c \in F_{p^n}$ can be written in the form $c = r\gamma^2$ where $r = 1$ or r is a nonsquare in the field. Introduce the variables $x_i = \gamma^{q^{is}}$ for $i = 0, 1, ..., 2m$ and y for r. Then the coefficient matrix for the equation system is given by

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

Since, $b_{is} = (-1)^i$ it is straightforward to see that the determinant is

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

i.e.,

$$\Delta = \pm 2^{2m} \prod_{i=0}^{2m} (c^{(q^{is}+q^{(i+m)s})/2} - 1).$$

It follows that the determinant is nonzero except when $c^{(q^{is}+q^{(m+i)s})/2} = 1$, which implies that $c = 1$ since $d = \gcd((q^{ms}+1)/2, q^{2m+1}-1) = 1$. This last fact follows since we also have $q^{ms}+1 \equiv 2 \pmod{q-1}$ and that $\gcd((q^{ms}+1)/2, q^{2m+1}-1)$ divides $\gcd(q^{2ms}-1, q^{2m+1}-1) = q-1$ and not both $q^{ms}+1$ and $q-1$ are $\equiv 0 \pmod 4$. 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 α be a primitive element of F_{p^n}. Let $n = (2m+1)k$ and let $1 \le s \le 2m$ be an integer such that $\gcd(s, 2m+1) = 1$. Define*

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

and let $b_0 = 2u_0$, $u_i = b_{2i} = b_{2m+1-2i}$ for $i = 1, 2, ..., m$. Suppose $b_0 = \pm 1$ and $b_{is} = (-1)^i$ for $i = 1, 2, ..., m$, then the sequence over F_p defined by

$$s(t) = Tr_n(f(\alpha^t))$$

has an ideal two-level autocorrelation, where indices of b_{is} are taken modulo $2m+1$.

Proof. The proof goes similar to the previous theorem. In this case, using $d = q+1$ the rank of the corresponding quadratic form depends on the number of solution of a linearized polynomial $L(z)$ which in this case becomes

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

Using the same technique as in the previous theorem we show that $L(z)$ has $z = 0$ as its only solution for any $c \neq 1$. We again conclude that $\{s(t)\}$ has ideal two-level autocorrelation.

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

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 τ) have 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 $(\frac{p^n-1}{p-1}, \frac{p^{n-1}-1}{p-1}, \frac{p^{n-2}-1}{p-1})$ difference sets in a natural way i.e., $D = \{t \mid s_t = 0, \quad 0 \leq t < \frac{p^n-1}{p-1}\}$. Using ideas in No [10] and No [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.

3 Conclusions

If $n/k = 2m+1$ is odd, $q = p^k$, and α is a primitive element of F_{p^n}, then we have found functions of the form $f(x) = \sum_{i=0}^{m} u_i x^{(q^{2i}+1)/2}$, 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 $s(t) = Tr_n(f(\alpha^t))$ has a two-level ideal autocorrelation function. The sequences also give rise to difference sets with Singer parameters.

4 Acknowledgements

This research was supported by the Norwegian Research Council. We thank Khoongming Khoo and Matthew 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,” submitted for publication.

[2] L.E. Dickson, *Linear groups with an exposition of the Galois field theory*, Dover publications, New York (1983).

[3] J. Dillon, "Multiplicative difference sets via additive characters," *Designs, Codes and Cryptography*, Vol. 17, (1999) pp. 225-235.

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

[5] R. Evans, H. Hollmann, C. Krattenthaler and Q. Xiang, "Gauss sums, Jacobi sums, and p-ranks of cyclic difference sets," *Journal of Combinatorial Theory Series A*, Vol. 87, (1999) pp. 74-119.

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

[7] T. Helleseth, P.V. Kumar and H. Martinsen "A new family of ternary sequences with ideal two-level autocorrelation function," *Designs, Codes and Cryptography*, Vol. 14, (2001) pp. 157-166.

[8] A. Maschietti, "Difference sets and hyperovals," *Designs, Codes and Cryptography*, Vol. 14, (1998) pp. 89-98.

[9] Michael Ludkovski and Guang Gong, "New families of ideal 2-level autocorrelation ternary sequences from second order DHT", *the proceedings of the International Workshop on Coding and Cryptography*, January 8-12, 2001, Paris, pp. 345-354.

[10] J.S. No, "New Cyclic Differnce Sets with Singer Parameters Constructed from q-ary Sequences," submitted for publication.

[11] J.S. No, "p-ary Unified Sequences p-ary Extended d-form Sequences with Ideal Autocorrelation Property," submitted for publication.

[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, (1998) pp. 1278-1282.

[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, (1998) pp. 814-817.

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