number of "1"s; such codeword candidates are located in $\mathcal{T}\|\mathcal{A}$ at addresses that are 256 apart. Furthermore, both codeword candidates label edges that terminate in the same state and, therefore, replacement of a codeword with its alternate can be done locally within a generated sequence of codewords without affecting preceding or following codewords. This simple encoding mechanism follows from the fact that codewords generated from any given state are located in a *contiguous* segment of $\mathcal{T}\|\mathcal{A}$. This applies also to $\mathcal{E}_{(3,\,10)}$ if we regard only entries that are located at addresses of the form $3 + 4t$.

In order to obtain DC control, we need to be able to generate more than 64 codewords from certain states in $\mathcal{E}_{(3,\,10)}$, and more than 256 codewords in $\mathcal{E}_{(2,\,10)}$. Consider, for example, the codewords that can be generated from states $u \geq d_1$. While in Section III-B we have restricted the generated codeword to be taken only from $\mathcal{A}$, here we allow the codeword to be also $\mathcal{T}(j)$ as long as $k_i - \ell(j) \geq u$. Also, observe that in all instances where a codeword $\varphi_i(\mathcal{T}(j))$ can be generated we necessarily have $\ell(\mathcal{T}(j)) = \Delta_i + 1$ and, so, $\varphi_i(\mathcal{T}(j)) = \mathcal{A}(j)$.

Yet, on the other hand, we require that two codeword candidates for the same input tag have different parity, label edges that terminate in the same state, and be located in $\mathcal{T}\|\mathcal{A}$ at addresses 256 apart. Due to those conditions, only 53 entries in $\mathcal{A}$ are accessible by $\mathcal{E}_{(3,\,10)}$, compared to 64 entries in Section III-B.

A block decoder $\boldsymbol{w} \mapsto \mathcal{D}_{(2,\,10)}(\boldsymbol{w})$ of $\mathcal{E}_{(2,\,10)}$ is obtained by deleting the two most significant bits of the 10-bit address of the entry in $\mathcal{T}\|\mathcal{A}$ that contains the codeword $\boldsymbol{w}$. When restricted to the domain $\Sigma(\mathcal{E}_{(3,\,10)})$, this is also a block decoder of $\mathcal{E}_{(3,\,10)}$, with the range consisting of bytes having least significant bits "11."

The encoder $\mathcal{E}_{(3,\,10)}$ is weakly observable from $\mathcal{E}_{(2,\,10)}$. Nesting and full observability can be attained if we do not exclude the 28-bit pattern "$00010001\cdots0001$" from appearing in the bit stream; we then need to slightly modify $\mathcal{T}\|\mathcal{A}$ and unmerge state $[2,\,5]$ in $\mathcal{E}_{(2,\,10)}$ into states 2 and $[3,\,5]$.

The power spectral densities of the two encoders are shown in Fig. 2. We have used the same scaling of the axes as in [9] and applied the same local optimization (through encoding look-ahead) when selecting the generated codeword between two codeword candidates. The power spectral density of $\mathcal{E}_{(2,\,10)}$ is virtually the same as that of the $(2,\,10)$-RLL encoder in [9].

REFERENCES

[1] R. L. Adler, D. Coppersmith, and M. Hassner, "Algorithms for sliding block codes—An application of symbolic dynamics to information theory," *IEEE Trans. Inform. Theory*, vol. IT-29, pp. 5–22, Jan. 1983.

[2] G. F. M. Beenker and K. A. S. Immink, "A generalized method for encoding and decoding runlength-limited binary sequences," *IEEE Trans. Inform. Theory*, vol. IT-29, pp. 751–754, Sept. 1983.

[3] P. A. Franaszek, "Sequence-state methods for runlength-limited coding," *IBM J. Res. Develop.*, vol. 14, pp. 376–383, 1970.

[4] J. Gu and T. E. Fuja, "A new approach to constructing optimal block codes for runlength-limited channels," *IEEE Trans. Inform. Theory*, vol. 40, pp. 774–785, May 1994.

[5] J. Hogan, R. M. Roth, and G. Ruckenstein, "Nested input-constrained codes," *IEEE Trans. Inform. Theory*, vol. 46, pp. 1302–1316, July 2000.

[6] K. A. S. Immink, *Codes for Mass Data Storage Systems*. Eindhoven, The Netherlands: Shannon Foundation, 1999.

[7] ——, "FM Plus: The coding format of the multimedia compact disc," *IEEE Trans. Consum. Electron.*, vol. 41, pp. 491–497, 1995.

[8] H. Marcus, R. M. Roth, and P. H. Siegel, "Constrained systems and coding for recording channels," in *Handbook of Coding Theory*, V. S. Pless and W. C. Huffman, Eds. Amsterdam, The Netherlands, 1998, pp. 1635–1764.

[9] R. M. Roth, "On runlength-limited coding with DC control," *IEEE Trans. Commun.*, vol. 48, pp. 351–358, 2000.

[10] C. E. Shannon, "The mathematical theory of communication," *Bell Syst. Tech. J.*, vol. 27, pp. 379–423, 1948.

New Construction for Binary Sequences of Period $p^m - 1$ with Optimal Autocorrelation Using $(z+1)^d + az^d + b$

Jong-Seon No, *Member, IEEE*, Habong Chung, *Member, IEEE*, Hong-Yeop Song, *Member, IEEE*, Kyeongcheol Yang, *Member, IEEE*, Jung-Do Lee, and Tor Helleseth, *Fellow, IEEE*

***Abstract*—In this correspondence, we present a construction for binary sequences $\{s(t)\}$ of period $N = p^m - 1$ for an odd prime p based on the polynomial $(z+1)^d + az^d + b$, and discuss them in some cases of parameters p, m, d, a, and b. We show that new sequences from our construction are *balanced* or *almost balanced* and have *optimal three-level autocorrelation* for the case when the polynomial $(z+1)^d + z^d + a$ can be transformed into the form $z^2 - c$. We also derive the distribution of autocorrelation values they take on. The sequences satisfy *constant-on-the-coset* property, and we will show that there are more than one characteristic phases with constant-on-the-coset property. Some other interesting properties of these sequences will be presented. For the cases when the polynomial $(z+1)^d + z^d + a$ cannot be transformed into the form $z^2 - c$, we performed extensive computer search, and results are summarized. Based on these results, some open problems are formulated.**

***Index Terms*—Cyclotomic numbers, optimal autocorrelation, pseudorandom sequences, randomness properties.**

I. INTRODUCTION

Pseudorandom binary sequences $\{s(t)\}$, where $s(t) \in \{0,\,1\}$, of period N are widely used in many areas of engineering and sciences due to their randomness but simplicity in their generation. Some well-known applications include code-division multiple-access (CDMA) mobile communications and stream-cipher systems. Recently, there has been a lot of progress in constructing balanced binary sequences of period $2^m - 1$ with ideal autocorrelation [2], [3], [10], [11]. The idea of the (new) construction is to use a special polynomial over finite fields.

For convenience, let F_{p^m} denote the field of p^m elements and $F_{p^m}^* = F_{p^m}\backslash\{0\}$. For $p = 2$, No, Chung, and Yun [10] studied characteristic sequences of period $2^m - 1$ of the nonzero images under the mapping $(z+1)^d + z^d$ on F_{2^m} for an integer d. They conjectured that the characteristic sequence is balanced and has ideal autocorrelation in the case where $m = 3k \pm 1$ and $d = 2^{2k} - 2^k + 1$, which is inequivalent to m-sequences. They also proved that m-sequences can be described in this sense. Dillon [2] proved that the conjecture is true for all odd m.

Manuscript received September 15, 1999; revised November 4, 2000. This work was supported by the Basic Research Program of the Korea Science and Engineering Foundation under Grant 97-0100-0501-3. The material in this correspondence was presented in part at IEEE International Symposium on Information Theory, Sorrento, Italy, June 2000.

J.-S. No is with the School of Electrical Engineering, Seoul National University, Seoul 151-742, Korea (e-mail: jsno@snu.ac.kr).

H. Chung is with the School of Electronic and Electrical Engineering, Hong-Ik University, Seoul 121-791, Korea (e-mail: habchung@wow.hongik.ac.kr).

H.-Y. Song is with the Department of Electrical and Electronic Engineering, Yonsei University, Seoul 120-749, Korea (e-mail: hysong@yonsei.ac.kr).

K. Yang is with the Department of Electronic and Electrical Engineering, Pohang University of Science and Technology (POSTECH), Pohang, Kyungbuk 790-784, Korea (e-mail: kcyang@postech.ac.kr).

J.-D. Lee is with Hyundai Electronics Industries Co., Ltd., San 136-1, Ami-ri, Bubal-eub, Ichon-si, Kyoungki-do, 467-701, Korea (e-mail: jungdo@hei.co.kr).

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

Communicated by S. W. Golomb, Associate Editor for Sequences.

Publisher Item Identifier S 0018-9448(01)02998-4.

Dobbertin [3] studied the Kasami power functions x^d where $d = 2^{2k} - 2^k + 1$ with $k < m$ and $(k, m) = 1$, and slightly modified the setup in [10] by choosing the mapping $(z+1)^d + z^d + 1$ on F_{2^m} instead of $(z+1)^d + z^d$. He showed that the characteristic sequence of the nonzero images under $(z+1)^d + z^d + 1$ on F_{2^m} can be characterized by a trace function and also derived the linear span of these binary sequences. Finally, he gave a general conjecture that the characteristic sequence is balanced and has ideal autocorrelation. His conjecture covers some conjectures in [11].

Polynomials introduced in [3] and [10] can be generalized to generate *binary* sequences of period $p^m - 1$ with optimal autocorrelation for any prime p and an integer m. For brevity, in this correspondence, we will use F to denote the field of p^m elements. For $a, b \in F$ and a positive integer d, consider the subset of F^* given by

$$I(a, b) \triangleq \left\{x \mid x = (z+1)^d + az^d + b,\ z \in F\right\} \backslash \{0\}.$$

The characteristic sequence $\{s(t)\}$ of the set $I(a, b)$ in F^* is defined by $s(t) = 1$ if $\alpha^t \in I(a, b)$ and $s(t) = 0$ otherwise, where α is a primitive element of F. Clearly, $\{s(t)\}$ is a binary sequence of period $p^m - 1$. For a proper choice of a, b, and d it turns out to be (almost) balanced and have optimal autocorrelation as well as constant-on-the-coset property.

For $p > 2$, Lempel, Cohn, and Eastman [6] had studied balanced binary sequences of period $p^m - 1$ (which is even) with optimal autocorrelation. They considered the subset $S = \{\alpha^{2i+1} - 1\}$ of F^*, where α is a primitive element of F, and showed that the characteristic sequence of S is balanced, has optimal autocorrelation, and has constant-on-the-coset property. They mentioned a method of using the polynomial $z(1-z)$ to construct binary sequences and showed binary m-sequences can be constructed by this method [6], [14], [17].

In this correspondence, we present a construction for binary sequences $\{s(t)\}$ of period $N = p^m - 1$ for an odd prime p based on the polynomial $(z+1)^d + az^d + b$, and discuss them in some cases of parameters p, m, d, a, and b. We show that new sequences from our construction are *balanced* or *almost balanced* and have *optimal three-level autocorrelation*, for the case when the polynomial $(z+1)^d + z^d + a$ can be transformed into the form $z^2 - c$. We also derive the distribution of autocorrelation values they take on. The sequences satisfy *constant-on-the-coset* property, and we will show that there are more than one characteristic phases with constant-on-the-coset property. Some other interesting properties of these sequences will be presented. For the cases when the polynomial $(z+1)^d + z^d + a$ cannot be transformed into the form $z^2 - c$, we performed extensive computer search, and results are summarized. Based on these results, some open problems are formulated.

In Section II, we will review the equivalence relation and randomness properties of binary sequences. A formal setting of the new construction is given in terms of the polynomial $(z+1)^d + az^d + b$ over F. The case $d = 2$ is analyzed in detail and some cases of $d = 3$ and $d = 4$ are shown to be equivalent to the case $d = 2$. Section III provides our main results. Randomness properties and other interesting properties of new sequences are presented and some examples are given for illustration. A remark is given to discuss the relation with the results already covered by [6]. Section IV summarizes the result of our extensive computer search with an interesting open problem and conjecture.

II. Preliminaries

A. Equivalence Relations and Randomness Properties

Let $\{s_1(t)\}$ and $\{s_2(t)\}$ be binary sequences of period N. If there is a constant τ such that $s_1(t) = s_2(t+\tau)$ for all t, then $\{s_1(t)\}$ is said to be a *cyclic shift* of $\{s_2(t)\}$. If there exists r with $(r, N) = 1$ such that $s_1(t) = s_2(rt)$ for all t, then $\{s_1(t)\}$ is called the r-decimation of $\{s_2(t)\}$. If $s_1(t) = s_2(t) + 1 \pmod 2$ for all t, then $\{s_1(t)\}$ is called the *complement* of $\{s_2(t)\}$. If $\{s_1(t)\}$ is a cyclic shift of any of decimations or complement of $\{s_2(t)\}$ or their combination, then they are said to be *equivalent*. Otherwise, they are said to be *inequivalent*.

Given a binary sequence $\{s(t)\}$ of period N, let D be the difference between the number of 1's and that of 0's in its period. We will call D the discrepancy of $\{s(t)\}$. The sequence is said to be *balanced* if D is zero when N is even, and if D is one when N is odd. We will define it to be *almost balanced* if D is 2. The absolute value of D is the same for equivalent sequences.

The periodic autocorrelation function $\theta(\tau)$ of $\{s(t)\}$ is defined as

$$\theta(\tau) \triangleq \sum_{i=0}^{N-1} (-1)^{s(t)+s(t+\tau)} \tag{1}$$

where the sum $t+\tau$ is computed $\bmod N$. It is well known that $\theta(\tau) \equiv N \pmod 4$ and $\sum_{\tau=0}^{N-1} \theta(\tau) = D^2$, where D is the discrepancy of $\{s(t)\}$. It is also well known that

$$\theta(\tau) = N - 4\left[|I| - |I \cap (I+\tau)|\right] \tag{2}$$

where

$$I = \{t \mid s(t) = 1,\ 0 \le t \le N-1\}$$

and

$$I + \tau = \{t + \tau \pmod N \mid t \in I\}.$$

Two equivalent sequences share the same set of autocorrelation values and their distribution.

The optimality of a binary sequence of period N in the sense of autocorrelation means that $\max_{\tau \not\equiv 0 \pmod N} |\theta(\tau)|$ is the least possible over all the binary sequences of period N. When $N \equiv 0 \pmod 4$, therefore, the best one can think of is $\theta(\tau) = 0$ for all $\tau \not\equiv 0 \pmod N$, which corresponds to *circulant* Hadamard matrices. This cannot be achieved for (almost) balanced sequences of period $N > 4$, and, therefore, the optimal autocorrelation in this case will be referred to satisfy $\theta(\tau) = 0$ or -4 for all $\tau \not\equiv 0 \pmod N$. When $N \equiv 2 \pmod 4$, the best is $|\theta(\tau)| = 2$ for all $\tau \not\equiv 0 \pmod N$, and will be referred to be optimal.

For any t in the integers $\bmod N = p^m - 1$, we define the cyclotomic coset $\bmod N$ containing t as $\{t, tp, tp^2, tp^3, \ldots\}$. A binary sequence $\{s(t)\}$ of period N is said to have the constant-on-the-coset property if, for some τ, $s(t_1+\tau) = s(t_2+\tau)$ whenever both t_1 and t_2 belong to the same cyclotomic coset. A cyclic shift of $\{s(t)\}$ with this property is called its characteristic phase. Constant-on-the-coset property is preserved by the equivalence relation.

B. Construction of Binary Sequences Using Polynomial

Let F denote the field of p^m elements and $F^* = F \backslash \{0\}$. For $a, b \in F$ and a positive integer d, let

$$f(z) \triangleq (z+1)^d + az^d + b \tag{3}$$

and define an index set $I(a, b)$ in F^* to be

$$I(a, b) \triangleq \{f(z) \mid z \in F\} \backslash \{0\}. \tag{4}$$

The binary sequence that we discuss in this correspondence is the characteristic sequence $\{s_{a,b}(t)\}$ of the index set $I(a, b)$ in F^*, that is,

$$s_{a,b}(t) \triangleq \begin{cases} 1, & \text{if } \alpha^t \in I(a, b) \\ 0, & \text{otherwise} \end{cases} \tag{5}$$

where α is a primitive element of F. The sequence $\{s_{a,b}(t)\}$ will also be called the characteristic sequence of $f(z)$. We will restrict our discussion exclusively to the case $p > 2$ in the remaining of this correspondence.

When $d = 2$, a simplification occurs as follows. Observe that

$$f(z) = (z+1)^2 + az^2 + b = (a+1)z^2 + 2z + b + 1.$$

If $a+1=0$ then we have $I(a,\,b)=F^*$ for any b. This implies that $\{s_{a,\,b}(t)\}$ as in (5) is a constant sequence. If $a+1\neq 0$, then, by completing the square, we have

$$f(z)=(a+1)\left[\left(z+\frac{1}{a+1}\right)^2\right]-\frac{1}{a+1}+(b+1).$$

Hence, the characteristic sequence of $f(z)$ is a cyclic shift of that of z^2-c for some $c\in F$. This proves the following.

Proposition 1: Let $p\geq 3$, $d=2$, and $a,\,b\in F$ with $a+1\neq 0$. Then, $\{s_{a,\,b}(t)\}$ is a cyclic shift of the characteristic sequence of the polynomial z^2-c, where $c\in F$ depends on a and b.

By virtue of the above proposition, we may define, for short notation

$$I_c\triangleq\left\{z^2-c\mid z\in F\right\}\backslash\{0\} \tag{6}$$

$\{s_c(t)\}$ to be its characteristic sequence in F^* of period $N=p^m-1$, and $\theta_c(\tau)$ its periodic autocorrelation function.

There are two more cases in which $\{s_{a,\,b}(t)\}$ becomes a cyclic shift of $\{s_c(t)\}$ for some $c\in F$.

Propostition 2: Let $p\geq 5$, $d=3$, and $a=-1$. For any positive integer m and any $b\in F$, $\{s_{a,\,b}(t)\}$ is a cyclic shift of $\{s_c(t)\}$, where $c\in F$ depends on b.

Proof: $a+1=0$ and $d=3$, the polynomial reduces as

$$f(z)=(z+1)^3-z^3+b=3z^2+3z+b+1.$$

By completing the square, the result follows easily. □

Proposition 3: Let $p=3$, $d=4$, $a=1$, and m be odd so that $N=3^m-1\equiv 2\,(\mathrm{mod}\,4)$. For any $b\in F$, $\{s_{a,\,b}(t)\}$ is a cyclic shift of $\{s_c(t)\}$, where $c\in F$ depends on b.

Proof: The polynomial reduces as

$$\begin{aligned}f(z)&=(z+1)^4+z^4+b\\&=2(z-1)^4+b-1\\&=2((z-1)^2)^2+b-1.\end{aligned}$$

Since m is odd so that $N=3^m-1\equiv 2\,(\mathrm{mod}\,4)$, the square of $(z-1)^2$ again takes all the even powers of a primitive elements of F. □

Proposition 4: Let $p\geq 3$, $d=p^m-p^{m-1}-1$, $a=-1$, and $b=0$. Then $\{s_{a,\,b}(t)\}$ is equivalent to $\{s_c(t)\}$ for some $c\in F$.

Proof: Since $z^d=z^{-p^{m-1}}$, the polynomial reduces as

$$f(z)=-\{y(y+1)\}^{-1}$$

where we let $y=z^{p^{m-1}}$. Since $z\to y$ is a permutation, we are done. □

If $c=0$, then the characteristic sequence of z^2 becomes $010101\ldots$, and its autocorrelation is never optimal for $N\geq 4$.

We now characterize how the index set changes as one sequence is transformed into its equivalent sequence in the following lemma without proof.

Lemma 5: Let α be a primitive element of F, the finite field of size p^m. Let $\{s(t)\}$ and $\{s'(t)\}$ be the characteristic sequences of index set I and I' in F^*, respectively, both of period $N=p^m-1$, then i) $s'(t)=s(t-\tau)$ for all t if and only if $I'=\alpha^\tau I$ for a constant τ, where $aI\triangleq\{ax\mid x\in I\}$; ii) $s'(t)=s(rt)$ for all t, where $(r,\,N)=1$, if and only if $I'=I^e$, where $er\equiv 1\,(\mathrm{mod}\,N)$ and $I^e\triangleq\{x^e\mid x\in I\}$; and iii) $s'(t)=s(t)+1\,(\mathrm{mod}\,2)$ for all t if and only if $I'\cup I=F^*$ and $I'\cap I=\phi$, that is, F^* is partitioned into I' and I.

III. Randomness Properties of New Sequences from z^2-c

We recall the definition of I_c in (6) and its characteristic sequence $s_c(t)$ in F^* of period $N=p^m-1$. In this section, we will prove that $s_c(t)$ is balanced (almost balanced, resp.) when c is a nonsquare (square, resp.), and has optimal autocorrelation. We will also prove some other interesting properties of these sequences.

Let C_i, where $i=0$ or 1, be the cyclotomic class in F given by

$$C_i=\left\{\alpha^{2s+i}\mid s=0,\,1,\,\ldots,\,N/2-1\right\}.$$

In other words, C_0 (C_1, resp.) is the set of squares (nonsquares, resp.) in F^*. For fixed i and j, the cyclotomic number $(i,\,j)$ is defined to be the number of solutions of the equation

$$1+z_i=z_j$$

where $z_i\in C_i$, $z_j\in C_j$. From the theory of cyclotomic numbers (cf. [19]), it is easy to determine $(i,\,j)$ as in the following lemma.

Lemma 6 [19, Lemma 6]: The cyclotomic numbers are given as follows:

b) if $N\equiv 0\,(\mathrm{mod}\,4)$, then
$$(0,\,0)=(p^m-5)/4$$
$$(0,\,1)=(1,\,0)=(1,\,1)=(p^m-1)/4;$$
c) if $N\equiv 2\,(\mathrm{mod}\,4)$, then
$$(0,\,0)=(1,\,0)=(1,\,1)=(p^m-3)/4$$
$$(0,\,1)=(p^m+1)/4.$$

Before we show the (almost) balance property and optimal autocorrelation of $\{s_c(t)\}$, let us consider

$$I_c^*\triangleq\left\{z^2-c\mid z\in F^*\right\}\backslash\{0\} \tag{7}$$

slightly modified from I_c by excluding $z=0$ in (6). Define $\{s_c^*(t)\}$ to be its characteristic sequence in F^* of period $N=p^m-1$, and $\theta_c^*(\tau)$ its periodic autocorrelation function. Note that if $c\neq 0$, then $I_c^*=I_c\backslash\{-c\}$ and hence $|I_c^*|=|I_c|-1$.

Theorem 7: Let $\{s_c(t)\}$ and $\{s_c^*(t)\}$ be the characteristic sequences of I_c and I_c^*, respectively, of period $N=p^m-1$, and α be a primitive element of F. Then, both $\{s_\alpha^*(t)\}$ and $\{s_1(t)\}$ are balanced, and both $\{s_\alpha(t)\}$ and $\{s_1^*(t)\}$ are almost balanced. Furthermore, we have i) $s_\alpha^*(t)=s_1(t-1)+1$ for all t; ii) $s_\alpha(t)=s_1^*(t-1)+1$ for all t; iii) $s_\alpha(N/2+1)=s_1(N/2)=1$ and $s_1(t)=s_\alpha(t+1)+1$ for all $t\neq N/2$; and iv) $s_\alpha^*(N/2+1)=s_1^*(N/2)=0$ and $s_1^*(t)=s_\alpha^*(t+1)+1$ for all $t\neq N/2$.

Proof: Balance or almost balance property of the sequence comes from the following:

$$I_1^*=(C_0-1)\backslash\{0\}\quad\text{of size } N/2-1$$

$$I_1=\{-1\}\cup I_1^*\qquad\text{of size } N/2$$

$$I_\alpha^*=C_0-\alpha\qquad\text{of size } N/2$$

and

$$I_\alpha=\{-\alpha\}\cup I_\alpha^*\qquad\text{of size } N/2+1$$

where $C_0-c\triangleq\{x-c\mid x\in C_0\}$.

The statement i) comes from $\alpha I_1\cap I_\alpha^*=\phi$ and $\alpha I_1\cup I_\alpha^*=F^*$ by Lemma 5. The statement ii) comes from $I_\alpha\cap\alpha I_1^*=\phi$ and $|I_\alpha|=|I_1^*|+2=N/2+1$. Since $\alpha I_1\cup I_\alpha=F^*$, and $\alpha I_1\cap I_\alpha=\{-\alpha\}$, and $\alpha^{N/2+1}=-\alpha$, the statement iii) follows easily. Similarly for iv). □

When c is a nonsquare, $\{s_c(t)\}$ is a cyclic shift of $\{s_\alpha(t)\}$, and $\{s_c^*(t)\}$ is a cyclic shift of $\{s_\alpha^*(t)\}$ by Lemma 5. When c is a square, similarly, $\{s_c(t)\}$ is a cyclic shift of $\{s_1(t)\}$ and $\{s_c^*(t)\}$ is a cyclic shift of $\{s_1^*(t)\}$. Therefore, it is enough to consider $\{s_1^*(t)\}$ and $\{s_\alpha^*(t)\}$ in order to discuss the optimal autocorrelation property of $\{s_c(t)\}$ by Theorem 7.

Lemma 8: For any $\tau\not\equiv 0\,(\mathrm{mod}\,N)$ such that $1-\alpha^\tau\in C_i$ and $\alpha^\tau\in C_j$, we have

$$|I_\alpha^*\cap\alpha^\tau I_\alpha^*|=(i+j+1,\,i+1).$$

TABLE I
BINARY SEQUENCES OF PERIOD $N = 12$

name	sequence	D	$\#(\theta_c(\tau) = 0)$	$\#(\theta_c(\tau) = -4)$	Relation
$\{s_1^*(t)\}$	010110<u>0</u>11000	2	9	2	$s_1^*(t) = s_2^*(t+1) + 1 \ \forall t \neq N/2$
$\{s_2(t)\}$	110100<u>1</u>0011	2	9	2	$s_2(t) = s_1^*(t-1) + 1 \ \forall t$
$\{s_1(t)\}$	010110<u>1</u>11000	0	8	3	$s_1(t) = s_2(t+1) + 1 \ \forall t \neq N/2$
$\{s_2^*(t)\}$	110100<u>1</u>0011	0	8	3	$s_2^*(t) = s_1(t-1) + 1 \ \forall t$

TABLE II
BINARY SEQUENCES OF PERIOD $N = 26$

name	sequence	D	$\#(\theta_c(\tau) = -2)$	$\#(\theta_c(\tau) = 2)$
$\{s_1(t)\}$	00100110100001<u>0</u>1011110011 1	0	19	6
$\{s_\alpha(t)\}$	01101100101111<u>1</u>10100001100	2	18	7

Proof: For $x \in I_\alpha^* \cap \alpha^\tau I_\alpha^*$, we can write down $x = y - \alpha$ for $y \in C_0$ and $x = \alpha^\tau(z - \alpha)$ for $z \in C_0$. Thus, we have

$$1 + \frac{\alpha^\tau z}{\alpha(1-\alpha^\tau)} = \frac{y}{\alpha(1-\alpha^\tau)}.$$

The lemma follows from the relation

$$\frac{\alpha^\tau z}{\alpha(1-\alpha^\tau)} \in C_{i+j+1} \quad \text{and} \quad \frac{y}{\alpha(1-\alpha^\tau)} \in C_{i+1}$$

for $1 - \alpha^\tau \in C_i$ and $\alpha^\tau \in C_j$. □

Theorem 9: The sequences $\{s_\alpha^*(t)\}$ and $\{s_1(t)\}$ of period N are balanced and have optimal autocorrelation. Specifically, for $\tau \not\equiv 0 \pmod N$

$$\theta_\alpha^*(\tau) = \begin{cases} -4\epsilon, & \text{if } N \equiv 0 \pmod 4 \\ 2 - 4\epsilon, & \text{if } N \equiv 2 \pmod 4 \end{cases}$$

where $\epsilon \in \{0, 1\}$.

Proof: It follows from (2), Theorem 7, and Lemmas 6 and 8. □

Remark 10: In [6], Lempel, Cohn, and Eastman considered the characteristic sequence $\{s(t)\}$ of the set

$$S = \{\alpha^{2i+1} - 1 \mid i = 0, 1, \ldots N/2 - 1\}.$$

Clearly, $S = \alpha^{-1}(C_0 - \alpha)$ and $s(t) = s_\alpha^*(t+1)$. Therefore, their sequence is a cyclic shift of $\{s_\alpha^*(t)\}$, and our approach using cyclotomic numbers gives another simple proof of the construction in [6].

Lemma 11: For any $\tau \not\equiv 0 \pmod N$ such that $1 - \alpha^\tau \in C_i$ and $\alpha^\tau \in C_j$, we have

$$|I_1^* \cap \alpha^\tau I_1^*| = (i + j, i) - 1.$$

Proof: For $x \in I_1^* \cap \alpha^\tau I_1^*$, we can write down $x = y - 1$ for $y \in C_0 \backslash \{1\}$ and $x = \alpha^\tau(z - 1)$ for $z \in C_0 \backslash \{1\}$. Thus, we have

$$1 + \frac{\alpha^\tau z}{1-\alpha^\tau} = \frac{y}{1-\alpha^\tau}.$$

Note that the solution $(y, z) = (1, 1)$ is not allowed. Therefore, the lemma comes from the relation

$$\frac{\alpha^\tau z}{1-\alpha^\tau} \in C_{i+j} \quad \text{and} \quad \frac{y}{1-\alpha^\tau} \in C_i$$

for $1 - \alpha^\tau \in C_i$ and $\alpha^\tau \in C_j$. □

Theorem 12: The sequences $\{s_1^*(t)\}$ and $\{s_\alpha(t)\}$ of period N are almost balanced and have optimal autocorrelation. Specifically, for $\tau \not\equiv 0 \pmod N$

$$\theta_1^*(\tau) = \begin{cases} -4\epsilon, & \text{if } N \equiv 0 \pmod 4 \\ 2 - 4\epsilon, & \text{if } N \equiv 2 \pmod 4 \end{cases}$$

where $\epsilon \in \{0, 1\}$.

Proof: The proof follows from (2), Theorem 7, and Lemmas 6 and 11. □

Example 13: Let $p = 13$ and $m = 1$ so that $N = 12 \equiv 0 \pmod 4$. It is easy to check that 2 is a primitive root $\bmod 13$. Then, we obtain two inequivalent sequences as shown in Table I. Observe all four relations given in Theorem 7.

Example 14: Let $p = 3$ and $m = 3$ so that $N = 26 \equiv 2 \pmod 4$. Let $\alpha \in F$ be primitive with $\alpha^3 + 2\alpha + 1 = 0$. Then, we obtain two inequivalent sequences as shown in Table II.

Example 15: Let $p = 5$ and $m = 2$ so that $N = 24 \equiv 0 \pmod 4$. Let $\alpha \in F$ be primitive with $\alpha^2 + \alpha + 2 = 0$. Then, we obtain two inequivalent sequences as shown in Table III.

Theorem 16: For u and v shown in Table IV, $\{s_c(t)\}$ has the following distribution:

$$\theta_c(\tau) = \begin{cases} 0 \quad (+2, \text{ resp.}), & \text{for } u \text{ values of } \tau \\ -4 \quad (-2, \text{ resp.}), & \text{for } v \text{ values of } \tau \end{cases}$$

when $N \equiv 0 \pmod 4$ ($N \equiv 2 \pmod 4$, resp.).

Proof: It can be shown easily by solving two simultaneous equations. When $N \equiv 0 \pmod 4$ and $s_c(t)$ is balanced, we have

$$N + 0u + (-4)v = 0$$

$$u + v + 1 = N$$

which gives $u = (3N-4)/4$ and $v = N/4$. The other cases are proved similarly. □

Theorem 17: The sequences $\{s_1(t)\}$ and $\{s_\alpha(t+1)\}$ are in characteristic phase. Furthermore, the cyclic shifts of $\{s_1(t)\}$ and $\{s_\alpha(t+1)\}$ by every integer multiple of T are in characteristic phase, where $T \triangleq (p^m - 1)/(p - 1)$.

Proof: The period $N = p^m - 1$ and observe that $Tp \equiv T \pmod N$. Let k be an integer. Then

$$s_1(t - kT) = 1 \Leftrightarrow \alpha^{t-kT} = z^2 - 1 \in I_1 \quad \text{some } z$$
$$\Leftrightarrow \alpha^{tp-kTp} = \alpha^{tp-kT} = z^{2p} - 1 \in I_1.$$

TABLE III
BINARY SEQUENCES OF PERIOD $N = 24$

name	sequence	D	$\#(\theta_c(\tau) = 0)$	$\#(\theta_c(\tau) = -4)$
$\{s_1(t)\}$	100100101000$\underline{1}$0111110001	0	17	6
$\{s_\alpha(t)\}$	001101101011$\underline{1}$0100000111	2	18	5

TABLE IV
DISTRIBUTION OF AUTOCORRELATION VALUES OF $\{s_c(t)\}$

	balanced ($D = 0$)	almost balanced ($D = 2$)
$N \equiv 0 \pmod 4$	$u = (3N-4)/4$ $v = N/4$	$u = 3N/4$ $v = (N-4)/4$
$N \equiv 2 \pmod 4$	$u = (3N-2)/4$ $v = (N-2)/4$	$u = (3N-6)/4$ $v = (N+2)/4$

For the sequence $\{s_\alpha(t+1)\}$, we have the following:

$$\begin{aligned} s_\alpha(t-kT+1) = 1 &\Leftrightarrow \alpha^{t-kT+1} = z^2 - \alpha \in I_\alpha \quad \text{some } z \\ &\Leftrightarrow \alpha^{tp-kTp+p} = z^{2p} - \alpha^p \\ &\Leftrightarrow \alpha^{tp-kT+1} = \alpha^{-(p-1)}(z^{2p} - \alpha^p) \in I_\alpha. \quad \square \end{aligned}$$

IV. RESULT OF COMPUTER SEARCH AND CONCLUDING REMARKS

In this section, we summarize the result of an extensive computer search and discuss some miscellaneous cases. The computer search was restricted to the case of balanced or almost balanced binary sequences $\{s_{a,b}(t)\}$ with optimal autocorrelation generated by $(z+1)^d + az^d + b$ as in Section II. For $m = 1$, we were able to search completely for odd primes up to 97. For odd primes p up to 19 and appropriate m (manageable by Pentium PC), we have tried every possible d from 2 to $N-1$ and all $a \in F^*$ and $b \in F$. Observe that it is enough to consider coset representatives for d since

$$(z+1)^{dp} + a^p z^{dp} + b^p = (z^p+1)^d + a'(z^p)^d + b'$$

and $z \mapsto z^p$ is a permutation of F.

We present the result of our computer search in three tables. Tables V and VI show the values of d for which there exists some $(a \neq 0, b)$ such that a balanced (or an almost balanced or both) binary sequence with optimal autocorrelation exists. No other values of d in this range produce (almost) balanced binary sequences with optimal autocorrelation. We have omitted the result of the computer search with the value $a = 0$ included due to the limited space simply because too many values of d have popped up. It turned out that inequivalent binary sequences with the same discrepancy D exists (including $a = 0$) for some short lengths. Table VII shows all the inequivalent classes of period $N = p - 1$ for $5 \leq p \leq 97$. For $p = 19$, we have found three inequivalent classes with $D = 2$ (almost balanced). We conjecture that no further multiple inequivalence classes exist for $p > 97$, but we shall remain this as a future research topic.

Besides all the parameter sets of (a, b, d, p) so far discussed, one more case of interest comes from the computer search. In this case, we were currently able to show only the (almost) balance property of the characteristic sequences:

Theorem 18: The characteristic sequence of period $N = p^m - 1$ of $I(a, b)$ for $d = (p^m+1)/2$, $a = (-1)^{d-1}$, and $b = \pm 1$ is balanced when $N \equiv 0 \pmod 4$ and is almost balanced when $N \equiv 2 \pmod 4$. For a given N, the sequence for $b = 1$ is a cyclic shift of that for $b = -1$.

Proof: Note that for $x \in F^*$ we have $x^{N/2} = 1$ when $x \in C_0$ and $x^{N/2} = -1$ when $x \in C_1$. Therefore, the polynomial $f(z)$ becomes

$$f(z) = \left\{(-z)^{N/2} + (z+1)^{N/2}\right\} z + b + (z+1)^{N/2}.$$

First, $f(0) = b+1$ and $f(-1) = b-1$. For all other values of $z \in F$, we have the following expression, where the ordered pair (i, j) for $i, j \in \{0, 1\}$ denotes the cyclotomic number given in Lemma 6:

$$f(z) = \begin{cases} \left(1 + (-1)^{N/2}\right) z + b + 1, & (0,0) \text{ values of } z \\ \left(-1 + (-1)^{N/2}\right) z + b - 1, & (0,1) \text{ values of } z \\ \left(1 - (-1)^{N/2}\right) z + b + 1, & (1,0) \text{ values of } z \\ \left(-1 - (-1)^{N/2}\right) z + b - 1, & (1,1) \text{ values of } z. \end{cases}$$

Therefore, we have the table of values of $f(z)/2$ for all z in F at the bottom of the following page. Consider the case $N \equiv 0 \pmod 4$ and

TABLE V
THE VALUES OF d FOR WHICH THERE EXISTS SOME $(a \neq 0, b)$ SUCH THAT AN (ALMOST) BALANCED SEQUENCE OF PERIOD $N = p - 1$ WITH OPTIMAL AUTOCORRELATION EXISTS

p	d
5	2, 3, 4
7	2, 3, 4, 5, 6
11	2, 3, 4, 5, 6, 7, 8, 9
13	2, 3, 4, 5, 6, 7, 8, 9, 10, 11
17	2, 3, 4, 6, 7, 9, 11, 12, 13, 14, 15
19	2, 3, 4, 5, 7, 8, 10, 11, 14, 15, 17
23	2, 3, 12, 15, 17, 21
29	2, 3, 15, 19, 27
31	2, 3, 16, 18, 29
37	2, 3, 19, 35
41	2, 3, 21, 27, 39
43	2, 3, 22, 41
47	2, 3, 24, 31, 45
53	2, 3, 27, 35, 51
59	2, 3, 30, 39, 57
61	2, 3, 31, 59
67	2, 3, 34, 65
71	2, 3, 36, 47, 69
73	2, 3, 37, 71
79	2, 3, 40, 77
83	2, 3, 42, 55, 81
89	2, 3, 45, 59, 87
97	2, 3, 49, 95

TABLE VI
THE VALUES OF d FOR WHICH THERE EXISTS SOME $(a \neq 0, b)$ SUCH THAT AN (ALMOST) BALANCED SEQUENCE OF PERIOD $N = p^m - 1$ $(m \geq 2)$ WITH OPTIMAL AUTOCORRELATION EXISTS

p	m	$N = p^m - 1$	d
3	2	8	2, 4, 5, 7
	3	26	2, 4, 10, 14, 16, 17, 22, 23, 25
	4	80	2, 14, 41, 43, 46, 49, 53, 58, 67, 71, 77, 79
	5	242	2, 4, 10, 14, 28, 82, 122, 124, 130, 136, 148, 161, 166, 202, 215, 233, 239, 241
5	2	24	2, 3, 6, 7, 11, 13, 17, 19, 23
	3	124	2, 3, 6, 26, 43, 63, 67, 83, 87, 91, 99, 119, 123
	4	624	2, 3, 63, 313, 317, 327, 337, 387, 437, 499, 599, 619, 623
7	2	48	2, 3, 25, 31, 41, 47
	3	342	2, 3, 8, 50, 172, 178, 220, 293, 335, 341
11	2	120	2, 3, 61, 71, 109, 119
13	2	168	2, 3, 85, 97, 155, 167
17	2	288	2, 3, 145, 161, 271, 287
19	2	360	2, 3, 181, 199, 341, 359

TABLE VII
THE INEQUIVALANCE CLASSES OF BINARY SEQUENCES OF LENGTH $p - 1$ FOR $5 \leq p \leq 97$ WITH OPTIMAL AUTOCORRELATION AND THE SAME DISCREPANCY D

D	p	d	(a, b)	inequivalent sequences
0	13	2	(0, 1)	111000010110
		9	(12, 0)	101011011000
2	7	5	(1, 1)	111100
		3	(0, 1)	101000
	11	3	(1, 1)	1110011010
		5	(1, 1)	1100010010
	13	4	(1, 3)	011100001001
		11	(2, 0)	110000011010
	19	2	(0, 1)	110100100110001111
		11	(2, 2)	111000101110010110
		13	(8, 3)	011110110000110101

$N \equiv 0 \pmod 4$		$N \equiv 2 \pmod 4$		# of times
$b = 1$	$b = -1$	$b = 1$	$b = -1$	
1	0	1	0	once at $z = 0$
0	-1	0	-1	once at $z = -1$
$z + 1$	z	1	0	$(0, 0)$ times
0	-1	$-z$	$-(z + 1)$	$(0, 1)$ times
1	0	$z + 1$	z	$(1, 0)$ times
$-z$	$-(z + 1)$	0	-1	$(1, 1)$ times

$b = 1$. The index set I must be of the form $I = A \cup B \cup C$ where

$$A = \{1\}$$
$$B = \{z + 1 \mid z \in C_0,\ z + 1 \in C_0\}$$

and

$$C = \{-z \mid z \in C_1,\ z + 1 \in C_1\}.$$

Observe that these three sets are pairwise-disjoint. Therefore,

$$|I| = 1 + |B| + |C| = 1 + (N/4 - 1) + N/4 = N/2.$$

The other cases can be treated similarly. □

ACKNOWLEDGMENT

The authors wish to thank the anonymous referee for careful review of the original manuscript and helpful comments. Double-check of the computer work by S.-E. Park and C.-Y. Yum at Yonsei University and independently by S.-H. Kim at Seoul National University are greatly appreciated.

REFERENCES

[1] L. D. Baumert, *Cyclic Difference Sets (Lecture Notes in Mathematics)*. Berlin, Germany: Springer-Verlag, 1971.
[2] J. F. Dillon, "Multiplicative difference sets via additive characters," report, preprint, 1998.
[3] H. Dobbertin, "Kasami power functions, permutation polynomials and cyclic difference sets," in *Proc. NATO Advanced Study Institute Workshop: Difference Sets, Sequences and their Correlation Properties*, Bad Windshiem, Germany, August 3–14, 1998.
[4] S. W. Golomb, *Shift-Register Sequences*. San Francisco, CA: Holden-Day, 1967. revised edition: Laguna Hills, CA: Aegean Park, 1982.
[5] J.-H. Kim and H.-Y. Song, "Existence of cyclic Hadamard difference sets and its relation to binary sequences with ideal autocorrelation," *J. Commun. and Networks*, vol. 1, no. 1, pp. 14–18, Mar. 1999.
[6] A. Lempel, M. Cohn, and W. L. Eastman, "A class of binary sequences with optimal autocorrelation properties," *IEEE Trans. Inform. Theory*, vol. IT-23, pp. 38–42, Jan. 1977.
[7] R. Lidl and H. Niederreiter, "Finite fields," in *Encyclopedia of Mathematics and Its Applications*. Reading, MA: Addison-Wesley, 1983, vol. 20.
[8] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North-Holland, 1977.
[9] J.-S. No, "Generalization of GMW sequences and No sequences," *IEEE Trans. Inform. Theory*, vol. 42, pp. 260–262, Jan. 1996.
[10] 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 1999.
[11] 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.
[12] J.-S. No, H.-K. Lee, H. Chung, H.-Y. Song, and K. Yang, "Trace representation of Legendre sequences of Mersenne prime period," *IEEE Trans. Inform. Theory*, vol. 42, pp. 2254–2255, Nov. 1996.
[13] J.-S. No, H.-Y. Song, H. Chung, and K. Yang, "Extension of binary sequences with ideal autocorrelation property," paper, preprint, 1999.
[14] D. V. Sarwate, "Comments on 'A class of balanced binary sequences with optimal autocorrelation properties'," *IEEE Trans. Inform. Theory*, vol. IT-24, Jan. 1978.
[15] D. V. Sarwate and M. B. Pursley, "Crosscorrelation properties of pseudorandom and related sequences," *Proc. IEEE*, vol. 68, pp. 593–619, May 1980.
[16] R. A. Scholtz and L. R. Welch, "GMW sequences," *IEEE Trans. Inform. Theory*, vol. IT-30, pp. 548–553, May 1984.
[17] V. M. Sidelnikov, "Some k-valued pseudo-random sequences and nearly equividistant codes," *Probl. Pered. Inform.*, vol. 5, no. 1, pp. 16–22, 1969. English translation in: *Probl. Inform. Transm.*.
[18] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt, *Spread Spectrum Communications*. Rockville, MD: Computer Science Press, 1985, vol. 1. Revised edition: New York: McGraw-Hill, 1994.
[19] T. Storer, *Cyclotomy and Difference Sets (Lecture Notes in Advanced Mathematics)*. Chicago, IL: Markham, 1967.
[20] *Mobile Station–Base Station Compatibility Standard for Dual-Mode Wideband Spread Spectrum Cellular System*, TIA-EIA-IS-95, Telecommun. Ind. Assoc. as a North American 1.5 MHz Cellular CDMA Air-Interface Std., July 1993.

A Class of Pseudonoise Sequences over GF (P) with Low Correlation Zone

Xiaohu H. Tang and Pingzhi Z. Fan, *Senior Member, IEEE*

***Abstract*—In this correspondence, a new class of pseudonoise sequences over GF (p), based on Gordon–Mills–Welch (GMW) sequences, is constructed. The sequences have the property that, in a specified zone, the out-of-phase autocorrelation and cross-correlation values are all equal to −1. Such sequences with low correlation zone (LCZ) are suitable for approximately synchronized code-division multiple-access (CDMA) system.**

***Index Terms*—ACF, CCF, Gordon–Mills–Welch (GMW) sequence, low correlation zone (LCZ), zero correlation zone (ZCZ).**

I. INTRODUCTION

The pseudonoise sequences with low out-of-phase autocorrelation and cross-correlation values are required for direct-sequence (DS) code-division multiple-access (CDMA) (DS-CDMA) system to reduce the multiple-access interference (MAI). M-sequences, Gold sequences, Kasami sequences, and Gordon–Mills–Welch (GMW) sequences are well known for their good periodic correlation [1]. A survey on the binary pseudonoise sequences was given in [2], and the related p-ary sequences were introduced by [3], [4].

Recently, an approximately synchronized (AS) CDMA (AS-CDMA) system was proposed by Suehiro [5], where the synchronization among users can be controlled within permissible time difference. AS-CDMA system without cochannel interference can be realized by using the sequences with zero correlation zone (ZCZ) [6], [7]. On the other hand, AS-CDMA system with low cochannel interference can be realized by using the sequences with low correlation zone (LCZ), as it is the case of [8]. The binary LCZ sequences introduced in [8] is based on GMW sequences. The correlation values of the sequences are almost all equal to -1 except for a few values. In this correspondence, we have extended the sequences from binary to p-ary with the same correlation property. It is shown that the binary sequence set in [8] is only a special case of our result.

In the following sections, we will first present the main result of this correspondence, then give a proof of the main result, and finally conclude by an illustrative construction example.

Manuscript received July 13, 1999; revised October 16, 2000. This work was supported by the National Science Foundation of China (NSFC) under Grants 69825102 and 69931050.

The authors are with the Institute of Mobile Communications, Southwest Jiaotong University, Chengdu, Sichuan 610031, China (e-mail: xhutang@sina.com; p.fan@ieee.org).

Communicated by S. W. Golomb, Associate Editor for Sequences.
Publisher Item Identifier S 0018-9448(01)03000-0.