The Cross-Correlation of Binary Sequences With Optimal Autocorrelation

Cunsheng Ding, *Senior Member, IEEE*, and Xiaohu Tang, *Member, IEEE*

***Abstract*—Binary sequences with low correlation have applications in communication systems and cryptography. Though binary sequences with optimal autocorrelation were constructed in the literature, no pair of binary sequences with optimal autocorrelation are known to have also best possible cross correlation. In this paper, new bounds on the cross correlation of binary sequences with optimal autocorrelation are derived, and pairs of binary sequences having optimal autocorrelation and meeting some of these bounds are presented. These new bounds are better than the Sarwate bounds on the cross correlation of binary sequences with optimal autocorrelation.**

***Index Terms*—Almost difference sets, autocorrelation, cross correlation, difference sets, sequences.**

I. Introduction

THE periodic cross-correlation value of two binary sequences $(u(t))$ and $(v(t))$ of period N at shift τ is

$$\mathrm{R}_{u,v}(\tau)=\sum_{t=0}^{N-1}(-1)^{u(t+\tau)+v(t)} \tag{1}$$

where $u(t)\in\{0,1\}$ and $v(t)\in\{0,1\}$. When the two sequences u and v are identical, the periodic cross-correlation function is called the periodic autocorrelation function, and is denoted by R_u. Furthermore, these $\mathrm{R}_u(\tau),\tau\in\{1,2,\ldots,N-1\}$, are called the out-of-phase autocorrelation values of the sequence $(u(t))$.

Let $(u(t))$ be a binary sequence of period N. The set

$$C_u=\{0\le t\le N-1: u(t)=1\}$$

is called the *support* of $(u(t))$; and $(u(t))$ is referred to as the *characteristic sequence* of $C_u\subseteq\mathbf{Z}_N=\{0,1,2,\ldots,N-1\}$. If N is even and the cardinality $|C_u|=N/2$, we say that the binary sequence $(u(t))$ is balanced. If N is even and $|C_u|=N/2\pm1$, we say that $(u(t))$ is almost balanced. If N is odd and $|C_u|=(N\pm1)/2$, we say that $(u(t))$ is balanced.

Manuscript received June 15, 2009; revised December 21, 2009. Current version published March 17, 2010. This work of X. H. Tang was supported by the National Science Foundation of China (NSFC) by Grant 60772086.

C. Ding is with the Department of Computer Science and Engineering, The Hong Kong University of Science and Technology, Clearwater Bay, Kowloon, Hong Kong (e-mail: cding@ust.hk).

X. H. Tang is with the Provincial Key Lab of Information Coding and Transmission, Institute of Mobile Communications, Southwest Jiaotong University, Chengdu, Sichuan 610031, China (e-mail: xhutang@ieee.org).

Communicated by N. Yu, Associate Editor for Sequences.

Digital Object Identifier 10.1109/TIT.2010.2040883

The mapping $u\mapsto C_u$ is a one-to-one correspondence from the set of all binary sequences of period N to the set of all subsets of $\mathbf{Z}_N$. Hence, studying binary sequences of period N is equivalent to that of subsets of $\mathbf{Z}_N$.

For any subset A of $\mathbf{Z}_N$, the *difference function* of A is defined as

$$d_A(\tau)=|(\tau+A)\cap A|,\tau\in\mathbf{Z}_N.$$

Let $(u(t))$ be the characteristic sequence of $C_u\subseteq\mathbf{Z}_N$. It is easy to show that

$$\mathrm{R}_u(\tau)=N-4(k-d_{C_u}(\tau)) \tag{2}$$

where $k=|C_u|$. Thus the study of the autocorrelation property of the sequence $(u(t))$ further becomes that of the difference function d_A of the support C_u of the sequence $(u(t))$.

Let $k=|C_u|$, the size of the support of a binary sequence $(u(t))$ of period N. It is well known that

$$\sum_{\tau=1}^{N-1}\mathrm{R}_u(\tau)=-N+(N-2k)^2. \tag{3}$$

For applications in direct-sequence code-division multiple access, coding theory and cryptography, we wish to have binary sequences $(u(t))$ of period N with minimal value $\max_{1\le\tau\le N-1}|\mathrm{R}_u(\tau)|$.

The following results follow from (2).

1) Let $N\equiv3\pmod4$. Then $\max_{1\le\tau\le N-1}|\mathrm{R}_u(\tau)|\ge1$. On the other hand,
$$\max_{1\le\tau\le N-1}|\mathrm{R}_u(\tau)|=1$$
if and only if $\mathrm{R}_u(\tau)=-1$ for all $\tau\not\equiv0\pmod N$. In this case, the sequence $(u(t))$ is said to have *ideal autocorrelation* and *optimal autocorrelation*.
2) Let $N\equiv1\pmod4$. There is some evidence [1] that there is no binary sequence $(u(t))$ of period $N>13$ with
$$\max_{1\le\tau\le N-1}|\mathrm{R}_u(\tau)|=1.$$
It follows from (3) there is no balanced binary sequence $(u(t))$ of period $N\equiv1\pmod4$ with $\max_{1\le\tau\le N-1}|\mathrm{R}_u(\tau)|=1$. Then by (2), $\{1,-3\}$ is indeed the only optimal set of autocorrelation values for balanced binary sequences $(u(t))$ of period $N\equiv1\pmod4$.
3) Let $N\equiv2\pmod4$. Then $\max_{1\le\tau\le N-1}|\mathrm{R}_u(\tau)|\ge2$. On the other hand,
$$\max_{1\le\tau\le N-1}|\mathrm{R}_u(\tau)|=2$$

0018-9448/$26.00 © 2010 IEEE

if and only if $\mathrm{R}_u(\tau) \in \{2, -2\}$ for all $\tau \not\equiv 0 \pmod N$. In this case, the sequence $(u(t))$ is said to have *optimal autocorrelation*.

4) Let $N \equiv 0 \pmod 4$. We have clearly that

$$\max_{1 \le \tau \le N-1} |\mathrm{R}_u(\tau)| \ge 0.$$

If $\max_{1 \le \tau \le N-1} |\mathrm{R}_u(\tau)| = 0$, the sequence $(u(t))$ is called *perfect*. The only known perfect binary sequence up to equivalence is the (0, 0, 0, 1). It is conjectured that there is no perfect binary sequence of period $N \equiv 0 \pmod 4$ greater than 4 [2]. This conjecture is true for all $N < 108900$ [2]. Hence, by (2) it is natural to construct binary sequences of period $N \equiv 0 \pmod 4$ with $\max_{1 \le \tau \le N-1} |\mathrm{R}_u(\tau)| = 4$. Anyway, it follows from (3) there is no balanced binary sequence $(u(t))$ of period N with $\mathrm{R}_u(\tau) = 0$ for all $1 \le \tau \le N-1$ or $\mathrm{R}_u(\tau) = -4$ for all $1 \le \tau \le N-1$ or $\mathrm{R}_u(\tau) = 4$ for all $1 \le \tau \le N-1$. Hence, $\{0, \pm 4\}$, $\{0, 4\}$, $\{0, -4\}$, and $\{4, -4\}$ are indeed the only possible optimum sets of autocorrelation values for balanced binary sequences of period $N \equiv 0 \pmod 4$.

A pair of binary sequences of period N is called an *optimal pair* if both sequences have optimal autocorrelation and their cross correlation is also the best possible.

A number of constructions of binary sequences with optimal autocorrelation are developed (see [3]–[6] for a survey on this topic). The cross correlation of periodic binary sequences with optimal autocorrelation has been studied by Antweiler [7], Calderbank and McGuire [8], Calderbank, McGuire, Poonen, and Rubinstein [9], Chan, Goresky, and Klapper [10], Helleseth [11], Hertel [12], Sarwate [13], Sarwate and Pursley [14]. In spite of the intensive study of the autocorrelation and cross correlation of binary periodic sequences, to the best of our knowledge, it is still open whether there is an optimal pair of binary sequences.

The first goal of this paper is to develop bounds on the cross-correlation values of binary sequences with optimal autocorrelation. The second one is to present optimal pairs of binary sequences for the first time in the literature.

II. Combinatorial Characterizations

To characterize binary sequences with optimal autocorrelation, we need to introduce difference sets and almost difference sets.

Let $(G, +)$ be an abelian group of order N. Let A be a k-subset of G. The set A is an (N, k, λ) difference set (DS) in G if the difference function $d_A(\tau) = \lambda$ for every nonzero element τ of G. The *complement* $\overline{A} := G \setminus A$ of an (N, k, λ) difference set A in G is an $(N, N-k, N-2k+\lambda)$ difference set. The reader is referred to [15] and [16] for detailed information of difference sets.

In addition, a k-subset A of G is an (N, k, λ, t) *almost difference set (ADS)* in G if $d_A(\tau)$ takes on λ altogether t times and $\lambda + 1$ altogether $N - 1 - t$ times when τ ranges over all the nonzero elements of G [3]. For example, $C = \{1, 3, 4, 9, 10, 12\}$, the set of quadratic residues modulo 13, is a (13, 6, 2, 6) ADS in $(\mathbf{Z}_{13}, +)$,

A necessary condition for the existence of an (N, k, λ, t) ADS is that $k(k-1) = t\lambda + (n-1-t)(\lambda+1)$. Difference sets are just special almost difference sets, i.e., $(n, k, \lambda, n-1)$ almost difference sets!

Two subsets D and E of a cyclic abelian group of order N are said to be *equivalent* if there are an integer ℓ relatively prime to N and an element $g \in G$ such that $E = \ell D + g$. In particular, we have the equivalence definition for two almost difference sets and two difference sets in any cyclic group.

It is well known that binary sequences with ideal autocorrelation are characterized by cyclic difference sets. Similarly, other binary sequences of period N with optimal autocorrelation are characterized by almost difference sets. Specifically, we have the following [3].

Theorem 1 ([3]): Let $(u(t))$ be a binary sequence of period N, and let C_u be its support.

1) Let $N \equiv 3 \pmod 4$. Then $\mathrm{R}_u(\tau) = -1$ for all $\tau \not\equiv 0 \pmod N$ if and only if C_u is an $(N, (N+1)/2, (N+1)/4)$ or $(N, (N-1)/2, (N-3)/4)$ DS in $\mathbf{Z}_N$.
2) Let $N \equiv 1 \pmod 4$. Then $\mathrm{R}_u(\tau) \in \{1, -3\}$ for all $\tau \not\equiv 0 \pmod N$ if and only if C_u is an $(N, k, k-(N+3)/4, Nk - k^2 - (N-1)^2/4)$ ADS in $\mathbf{Z}_N$.
3) Let $N \equiv 2 \pmod 4$. Then $\mathrm{R}_u(\tau) \in \{2, -2\}$ for all $\tau \not\equiv 0 \pmod N$ if and only if C_u is an $(N, k, k-(N+2)/4, Nk - k^2 - (N-1)(N-2)/4)$ ADS in $\mathbf{Z}_N$.
4) Let $N \equiv 0 \pmod 4$. Then $\mathrm{R}_u(\tau) \in \{0, -4\}$ for all $\tau \not\equiv 0 \pmod N$ if and only if C_u is an $(N, k, k-(N+4)/4, Nk - k^2 - (N-1)N/4)$ ADS in $\mathbf{Z}_N$.

Two binary sequences $(u_1(t))$ and $(u_2(t))$ of period N are said to be *equivalent* if there are an integer ℓ relatively prime to N and an integer j such that $u_2(t) = u_1(\ell t + j)$ for every $t \ge 0$. It is easily shown that two binary sequences are equivalent if and only if their supports are equivalent.

III. Bounds on the Cross Correlation of Binary Periodic Sequences

In 1979, Sarwate derived a lower bound on the maximum cross-correlation magnitude and the maximum out-of-phase autocorrelation magnitude [13].

Theorem 2 (The Sarwate Bound [13]): For any set X of M complex roots-of-unity sequences of period N

$$\frac{\theta_c^2}{N} + \frac{N-1}{N(M-1)} \frac{\theta_a^2}{N} \ge 1$$

where the maximum cross-correlation magnitude θ_c, and the maximum out-of-phase autocorrelation magnitude θ_a, are defined by

$$\theta_c = \max\{|\mathrm{R}_{x,y}(\tau)| : x, y \in X \quad x \ne y,\ 0 \le \tau < N\}$$
$$\theta_a = \max\{|\mathrm{R}_x(\tau)| : x \in X, 0 < \tau < N\}.$$

Sarwate commented in [13, Column 2, p. 721] that the bound in Theorem 2 was the best known bound and is likely the best possible for the case $M \le N$. In this section, we demonstrate that the Sarwate bound in Theorem 2 can be improved when $M = 2$ and the sequences are binary ones with optimal autocorrelation.

Throughout this section N denotes a positive integer. Let u and v be a pair of binary sequences with period N, and let θ_c denote the maximum cross-correlation magnitude between u and v. To develop lower bounds on θ_c, we will need the following equation (see [17, eqn. (2.21)]) :

$$\sum_{\tau=0}^{N-1}(\mathrm{R}_{u,v}(\tau))^2 = \sum_{\tau=0}^{N-1}\mathrm{R}_u(\tau)\mathrm{R}_v(\tau). \tag{4}$$

In addition, we need the following lemma.

Lemma 3: For any τ with $0 \le \tau < N$, we have $R_{u,v}(\tau) \equiv N \pmod 2$.

Proof: According to (1)

$$\begin{aligned}\mathrm{R}_{u,v}(\tau) &= |\{u(t+\tau) = v(t) : 0 \le t < N\}| \\ &\quad - |\{u(t+\tau) \ne v(t) : 0 \le t < N\}| \\ &= N - 2|\{u(t+\tau) \ne v(t) : 0 \le t < N\}|.\end{aligned}$$

Then, the conclusion directly follows. ∎

A. Bounds for the Case $N \equiv 3 \pmod 4$

The following follows from Theorem 2, and is a special case of the Sarwate bound.

Corollary 4 ([13]): Let $N \equiv 3 \pmod 4$. Let u and v be a pair of binary sequences with period N and optimal autocorrelation. Then

$$\theta_c \ge \lceil\sqrt{N}\rceil \tag{5}$$

where $\lceil x\rceil$ is the ceiling function.

The bounds in the following theorem are in general better than the Sarwate bound in Corollary 4.

Theorem 5: Let $N \equiv 3 \pmod 4$. Let u and v be a pair of binary sequences with period N and optimal autocorrelation. Then

$$\theta_c \ge \begin{cases} \lceil\sqrt{N+2}\rceil, & \text{if } \lceil\sqrt{N+2}\rceil \text{ odd} \\ \lceil\sqrt{N+2}\rceil + 1, & \text{if } \lceil\sqrt{N+2}\rceil \text{ even.}\end{cases} \tag{6}$$

Proof: Since u and v are optimal, they have only the out-of-phase autocorrelation value -1. By (4), we have then

$$\sum_{\tau=0}^{N-1}(\mathrm{R}_{u,v}(\tau))^2 = N^2 + N - 1.$$

It then follows that

$$N\theta_c^2 \ge N^2 + N - 1$$

which gives

$$\theta_c^2 \ge N + 1 - \frac{1}{N}.$$

Note that θ_c^2 is an integer. We have $\theta_c^2 \ge N+1$. By Lemma 3, θ_c^2 is odd. Note that $N+1$ is even. We know that $\theta_c^2 \ne N+1$. Whence

$$\theta_c^2 \ge N + 2.$$

We have then

$$\theta_c \ge \lceil\sqrt{N+2}\rceil.$$

The conclusions of this theorem then follows since θ_c is an odd number. ∎

Remark 1: The bound of this theorem improves the Sarwate bound by 1. However, it is open whether the new bound can be further improved.

B. Bounds for the Case $N \equiv 2 \pmod 4$

The following follows from Theorem 2, and is a special case of the Sarwate bound.

Corollary 6 ([13]): Let $N \equiv 2 \pmod 4$ and $N > 2$. Let u and v be a pair of binary sequences with period N and optimal autocorrelation. Then

$$\theta_c \ge \lceil\sqrt{N-3}\rceil. \tag{7}$$

The bounds in the following theorem are in general better than the Sarwate bound in Corollary 6.

Theorem 7: Let $N \equiv 2 \pmod 4$ and $N > 2$. Let u and v be a pair of binary sequences with period N and optimal autocorrelation. Then

$$\theta_c \ge \begin{cases} \lceil\sqrt{N-2}\rceil & \text{if } \lceil\sqrt{N-2}\rceil \text{ even} \\ \lceil\sqrt{N-2}\rceil + 1 & \text{if } \lceil\sqrt{N-2}\rceil \text{ odd.}\end{cases} \tag{8}$$

Proof: It follows from Theorem 2 that

$$\theta_c^2 \ge N - 4 + \frac{4}{N}.$$

Since θ_c^2 is a nonnegative integer, $\theta_c^2 \ge N-3$. Note that $\theta_c^2 \equiv 0 \pmod 4$ and $N-3 \equiv 3 \pmod 4$. We have that $\theta_c^2 \ne N-3$. Whence $\theta_c^2 \ge N-2$. The bounds then follows from Lemma 3. ∎

For balanced binary sequences of period $N \equiv 2 \pmod 4$, the bound of (8) can be further improved as follows.

Theorem 8: Let $N \equiv 2 \pmod 4$ and $N > 2$. Let u and v be a pair of balanced binary sequences with period N and optimal autocorrelation. Then

$$\theta_c \ge \begin{cases} \lceil\sqrt{N+2}\rceil, & \text{if } \lceil\sqrt{N+2}\rceil \text{ even} \\ \lceil\sqrt{N+2}\rceil + 1, & \text{if } \lceil\sqrt{N+2}\rceil \text{ odd.}\end{cases} \tag{9}$$

Proof: Since u and v are optimal, they have only the out-of-phase autocorrelation values -2 and 2. Note that both u and v are balanced. It then follows from (2) and Theorem 1 that $\mathrm{R}_u(\tau)$ (respectively, $\mathrm{R}_v(\tau)$) takes on -2 altogether $(3N-2)/4$ times and 2 altogether $(N-2)/4$ times when τ ranges over all the elements in $\{1, 2, \ldots, N-1\}$. Hence

$$\sum_{\tau=1}^{N-1}\mathrm{R}_u(\tau)\mathrm{R}_v(\tau) \ge 4 \times \frac{N}{2} - 4 \times \frac{N-2}{2} = 4.$$

Hence the right-hand side (RHS) of (4) is lower bounded by $N^2 + 4$.

It then follows that

$$\theta_c^2 \ge N + \frac{4}{N}.$$

Note that θ_c^2 is an integer. We have $\theta_c^2 \geq N+1$. By Lemma 3, θ_c^2 is even. Notice that $N+1$ is odd. We have that $\theta_c^2 \neq N+1$. Whence

$$\theta_c^2 \geq N+2.$$

We have then

$$\theta_c \geq \lceil \sqrt{N+2} \rceil.$$

The conclusion of this theorem then follows since θ_c is an even number. ∎

Remark 2: The bound of Theorem 8 improves the Sarwate bound by 1. It is open if it is tight.

C. Bounds for the Case $N \equiv 0 \pmod 4$

The following follows from Theorem 2, and is a special case of the Sarwate bound.

Corollary 9 ([13]): Let $N \equiv 0 \pmod 4$. Let u and v be a pair of binary sequences with period N and optimal autocorrelation values 0 and -4. Then

$$\theta_c \geq \lceil \sqrt{N-15} \rceil.$$

The bounds in the following theorem are in general better than the Sarwate bound in Corollary 9.

Theorem 10: Let $N \equiv 0 \pmod 4$. Let u and v be a pair of balanced binary sequences with period N and optimal autocorrelation values 0 and -4. Then

$$\theta_c \geq \begin{cases} \lceil \sqrt{N} \rceil, & \text{if } \lceil \sqrt{N} \rceil \text{ even} \\ \lceil \sqrt{N} \rceil + 1, & \text{if } \lceil \sqrt{N} \rceil \text{ odd.} \end{cases} \tag{10}$$

Proof: Note that both u and v are balanced. It then follows from (2) and Theorem 1 that $\mathrm{R}_u(\tau)$ (respectively, $\mathrm{R}_v(\tau)$) takes on -4 and 0 altogether $N/4$ times and $(3N-4)/4$ times, respectively, when τ ranges over all the elements of $\{1, 2, \ldots, N-1\}$. So we have

$$\sum_{\tau=1}^{N-1} \mathrm{R}_u(\tau)\mathrm{R}_v(\tau) \geq 0.$$

Hence the left-hand side (LHS) of (4) is lower bounded by N^2.

It then follows that

$$\theta_c^2 \geq N.$$

The conclusion of this theorem then follows from Lemma 3. ∎

Remark 3: The bound of Theorem 10 improves the Sarwate bound by 2. It is open if it can be improved.

D. Bounds for the Case $N \equiv 1 \pmod 4$

The following follows from Theorem 2, and is a special case of the Sarwate bound.

Corollary 11 ([13]): Let $N \equiv 1 \pmod 4$. Let u and v be a pair of binary sequences with period N and optimal autocorrelation. Then

$$\theta_c \geq \lceil \sqrt{N-8} \rceil. \tag{11}$$

The bounds in the following theorem are in general better than the Sarwate bound in Corollary 11.

Theorem 12: Let $N \equiv 1 \pmod 4$ and $N > 9$. Let u and v be a pair of balanced binary sequences with period N and optimal autocorrelation. Then

$$\theta_c \geq \begin{cases} \lceil \sqrt{N} \rceil, & \text{if } \lceil \sqrt{N} \rceil \text{ odd} \\ \lceil \sqrt{N} \rceil + 1, & \text{if } \lceil \sqrt{N} \rceil \text{ even.} \end{cases} \tag{12}$$

Proof: Note that both u and v are balanced. It then follows from (2) and Theorem 1 that $\mathrm{R}_u(\tau)$ (respectively, $\mathrm{R}_v(\tau)$) takes on each of -3 and 1 altogether $(N-1)/2$ times and τ ranges over all the elements of $\{1, 2, \ldots, N-1\}$. So we have

$$\sum_{\tau=1}^{N-1} \mathrm{R}_u(\tau)\mathrm{R}_v(\tau) \geq -3(N-1).$$

Hence the LHS of (4) is lower bounded by $N^2 - 3(N-1)$.

It then gives

$$\theta_c^2 \geq N - 3 + \frac{3}{N}.$$

Note that θ_c^2 is an integer. We have $\theta_c^2 \geq N-2$. Since $\theta_c^2 \equiv 1 \pmod 4$ and $N-2 \equiv 3 \pmod 4$, $\theta_c^2 \neq N-2$ and $\theta_c^2 \neq N-1$. Whence

$$\theta_c^2 \geq N.$$

We have then

$$\theta_c \geq \lceil \sqrt{N} \rceil.$$

The conclusion of this theorem then follows from the fact that θ_c is an odd number (see Lemma 3). ∎

Remark 4: The bound of Theorem 12 improves the Sarwate bound by 2. It cannot be improved, as it can be reached by some pairs of sequences presented in the next section.

IV. Pairs of Binary Sequences With Optimal Autocorrelation and Cross Correlation

Throughout this section, let N be a positive integer with $N \equiv 1 \pmod 4$. Only three constructions of binary sequences with period N and optimal autocorrelation are known, which are listed here.

1) (1798) Lengendre sequence of period $N \equiv 1 \pmod 4$, where N is a prime.
2) (1998) The two-prime sequence of period $N = p(p+4)$ in [18], where both p and $p+4$ are primes.
3) (1999) The cyclotomic sequence of period $N = x^2 + 4$ in [19], where N is a prime.

In this section, we prove that some pairs of these sequences have also optimal cross correlation.

TABLE I
THE RELATIONS OF THE CYCLOTOMIC NUMBERS OF ORDER 4, f ODD

(i,j)	0	1	2	3
0	A	B	C	D
1	E	E	D	B
2	A	E	A	E
3	E	D	B	E

A. The Known Constructions

In 1798, Adrien-Marie Legendre introduced the Legendre symbol and hence the Legendre sequence of period N, where N is a prime [20]. It is defined by

$$u(t)=\begin{cases}1, & \text{if } t \bmod N \text{ is a quadratic residue}\\ 0, & \text{otherwise.}\end{cases}$$

If $N \equiv 1 \pmod 4$, the Legendre sequence has only out-of-phase autocorrelation values -3 and 1.

In 1962, Whiteman discovered the so-called twin-prime difference sets [21] and thus the twin-prime sequences with optimal autocorrelation value -1. In 1991, the two-prime sequences, which are a generalization of the twin-prime sequences, were described in [18]. It is defined by

$$v(j)=\begin{cases}0, & j\in\{0,q,2q,\ldots,(p-1)q\}\\ 1, & j\in\{p,2p,\ldots,(q-1)p\}\\ \left(1-\left(\frac{j}{p}\right)\left(\frac{j}{q}\right)\right)/2, & \text{otherwise}\end{cases}$$

where $(\frac{a}{p})$ and $(\frac{b}{q})$ denote the Legendre symbol, and p and q are two distinct prime numbers. Seven years later in 1998, it was discovered that the two-prime sequence has optimal autocorrelation when the two primes satisfy $q=p+4$ [22], [23]. So it took two hundred years to discover the second class of binary sequences with period $N \equiv 1 \pmod 4$ and optimal autocorrelation after the Legendre sequences.

In 1999, the third class of binary sequences with period $N \equiv 1 \pmod 4$ and optimal autocorrelation was described in [19]. We now introduce this class of sequences.

Let $N=4f+1$ be an odd prime, where f is a positive integer. Let α be the primitive element of $\mathbf{Z}_N$ [19]. Denote by D_0 the multiplicative subgroup generated by α^4, i.e., $D_0=\{\alpha^{4k}: k=0,\ldots,f-1\}$, then

$$\mathbf{Z}_N^*=\cup_{i=0}^{3}D_i$$

where $D_i=\alpha^i D_0=\{\alpha^{4k+i}, k=0,\ldots,f-1\}$ for $0\le i<4$. The cosets D_i are called the cyclotomic classes of order 4. Note that D_0 and D_2 do not depend on the choice of the primitive element α. However, different choice of α may result in a swapping between D_1 and D_3.

The cyclotomic number (i,j) is defined as the cardinality of the intersection of the two sets D_i+1 and D_j, i.e.

$$(i,j)=|(D_i+1)\cap D_j|.$$

Let $N=4f+1$ be an odd prime, where f is an odd integer. It is known that N has the quadratic partition $N=x^2+4y^2$, where $x\equiv 1 \pmod 4$ and the sign of y is ambiguous and depends on the choice of α. When f is odd, the relations between the 16 cyclotomic numbers are given in Table I [24].

Thus there are five possible different cyclotomic numbers in the case f being odd [24], i.e.

$$A=\frac{N-7+2x}{16}$$
$$B=\frac{N+1+2x-8y}{16}$$
$$C=\frac{N+1-6x}{16}$$
$$D=\frac{N+1+2x+8y}{16}$$
$$E=\frac{N-3-2x}{16}.$$

The following was proven in [25].

Lemma 13: Let $N=4f+1$ be an odd prime, where f is an odd integer. Then

$$\sum_{m=0}^{3}(m+n,m)=\begin{cases}f-1, & \text{if } n=0\\ f, & \text{if } 1\le n\le 3.\end{cases}$$

The third class of binary sequences with optimal autocorrelation and period $N\equiv 1 \pmod 4$ is defined in the following theorem.

Theorem 14: [19, Theorems 4 and 5] Let $N=4f+1=x^2+4y^2$ with $x\equiv 1 \pmod 4$. Then $D_0\cup D_1$, $D_0\cup D_3$, $D_1\cup D_2$, and $D_2\cup D_3$ are $(N,(N-1)/2,(N-5)/4,(N-1)/2)$ ADSs if and only if f is odd and $y=\pm 1$. Hence, the corresponding sequence with support set $D_0\cup D_1$, or $D_0\cup D_3$ or $D_1\cup D_2$, or $D_2\cup D_3$, has optimal autocorrelation if and only if f is odd and $y=\pm 1$.

B. The Optimal Pairs

In what follows, we use u, v, and w, respectively, to denote the sequence with support $D_0\cup D_1$, $D_0\cup D_2$, and $D_0\cup D_3$. Hence, sequence v is the Legendre sequence. As mentioned before, different choice of the primitive element α will lead to a possible swapping of the two sequences u and w. We now prove that the pair (u,w) has optimal cross correlation.

Theorem 15: Let u and w be the binary sequences defined before. Then the cross-correlation function satisfies

$$\max_{0\le\tau<N}|\mathrm{R}_{u,w}(\tau)|=|x|+2=\lceil\sqrt{N}\rceil+1.$$

More precisely, when τ ranges over $\{1,2,\ldots,N\}$, the distribution of the cross-correlation values is the following:

$$\mathrm{R}_{u,w}(\tau)=\begin{cases}1, & 1 \text{ time}\\ x, & \frac{N-1}{2} \text{ times}\\ -x+2, & \frac{N-1}{4} \text{ times}\\ -x-2, & \frac{N-1}{4} \text{ times}\end{cases}$$

where x is defined by the quadratic partition $N=x^2+4y^2$ with $x\equiv 1 \pmod 4$ as before. In addition, the pair u and w have optimal cross correlation with respect to the bound of (12).

Proof: Obviously, $\mathrm{R}_{u,w}(0)=1$. In what follows, we consider the case that $0<\tau<N$.

By definition, the cross-correlation function is given by

$$\begin{aligned}\mathrm{R}_{u,w}(\tau) &= (-1)^{u(0)+w(\tau)} + (-1)^{u(N-\tau)+w(0)} \\ &\quad + |\{t:\ t\in D_0, t+\tau\in D_0\}| \\ &\quad + |\{t:\ t\in D_0, t+\tau\in D_3\}| \\ &\quad + |\{t:\ t\in D_1, t+\tau\in D_0\}| \\ &\quad + |\{t:\ t\in D_1, t+\tau\in D_3\}| \\ &\quad + |\{t:\ t\in D_2, t+\tau\in D_1\}| \\ &\quad + |\{t:\ t\in D_2, t+\tau\in D_2\}| \\ &\quad + |\{t:\ t\in D_3, t+\tau\in D_1\}| \\ &\quad + |\{t:\ t\in D_3, t+\tau\in D_2\}| \\ &\quad - |\{t:\ t\in D_0, t+\tau\in D_1\}| \\ &\quad - |\{t:\ t\in D_0, t+\tau\in D_2\}| \\ &\quad - |\{t:\ t\in D_1, t+\tau\in D_1\}| \\ &\quad - |\{t:\ t\in D_1, t+\tau\in D_2\}| \\ &\quad - |\{t:\ t\in D_2, t+\tau\in D_0\}| \\ &\quad - |\{t:\ t\in D_2, t+\tau\in D_3\}| \\ &\quad - |\{t:\ t\in D_3, t+\tau\in D_0\}| \\ &\quad - |\{t:\ t\in D_3, t+\tau\in D_3\}| \\ &= (-1)^{w(\tau)} + (-1)^{u(N-\tau)} \\ &\quad + \sum_{m=0}^{3} |(D_{m+1}+\tau)\cap D_m| \\ &\quad - \sum_{m=0}^{3} |(D_{m+3}+\tau)\cap D_m| \\ &\quad + \sum_{m=0}^{3} (-1)^m |(D_m+\tau)\cap D_m| \\ &\quad - \sum_{m=0}^{3} (-1)^m |(D_{m+2}+\tau)\cap D_m|.\end{aligned}$$

Let $\tau=\alpha^k$. We need only to consider

$$\begin{aligned}\Gamma_{n,k} &= \sum_{m=0}^{3} |(D_{m+n}+\alpha^k)\cap D_m| \\ &\quad k=0,1,2,3 \text{ and } n=1,3\end{aligned}$$

and

$$\begin{aligned}\Delta_{n,k} &= \sum_{m=0}^{3} (-1)^m |(D_{m+n}+\alpha^k)\cap D_m| \\ &\quad k=0,1,2,3 \text{ and } n=0,2.\end{aligned}$$

We have that

$$\begin{aligned}\Gamma_{n,k} &= \sum_{m=0}^{3} |(\alpha^{-k}D_{m+n}+1)\cap \alpha^{-k}D_m| \\ &= \sum_{m=0}^{3} |(D_{m+n-k}+1)\cap D_{m-k}| \\ &= \sum_{m=0}^{3} (m+n-k, m-k) \\ &= \sum_{m=0}^{3} (m+n, m).\end{aligned}$$

Similarly, we can prove that

$$\Delta_{n,k} = \sum_{m=0}^{3} (-1)^{m+k}(m+n, m).$$

By Lemma 13, $\Gamma_{1,k}=\Gamma_{3,k}$. For simplicity, write $\Delta_n = \sum_{m=0}^{3}(-1)^m(m+n,m)$. Then, the cross-correlation function becomes

$$\mathrm{R}_{u,w}(\tau) = (-1)^{w(\tau)} + (-1)^{u(N-\tau)} + (-1)^k[\Delta_0 - \Delta_2].$$

Plugging the five cyclotomic numbers into the cross-correlation function, we have

$$\begin{aligned}&\mathrm{R}_{u,w}(\tau) - \left[(-1)^{w(\tau)} + (-1)^{u(N-\tau)}\right] \\ &\quad = (-1)^k[(A-E+A-E)-(C-B+A-D)] \\ &\quad = (-1)^k x.\end{aligned}$$

When $\tau=\alpha^k$, $\tau\in D_k$ and $N-\tau=\alpha^{k+2f}\in D_{k+2}$ where the subscripts are modulo 4, since $-1=\alpha^{2f}\in D_2$ if f is odd. Then, the relation among k, $w(\tau)$ and $u(N-\tau)$ is illustrated in the following table.

$k \bmod 4$	$k \bmod 2$	$w(\tau)$	$u(N-\tau)$
0	0	1	0
1	1	0	0
2	0	0	1
3	1	1	1

The distribution of the cross-correlation values and the maximum absolute cross-correlation value then follow.

Finally, we show the optimality of the cross correlation of the two sequences. Note that $|x|$ is odd. On the other hand, $\lceil\sqrt{N}\rceil = \lceil\sqrt{x^2+4}\rceil = |x|+1$, which is then even. The bound of (12) is met. ■

Example 1: Let $N=29=5^2+4$. Let the primitive root α of $\mathbf{Z}_N$ be 2. Then the two sequences u and w are given by

$$\begin{aligned}u &= (01110001000100101101110111000) \\ w &= (01000001101010011010100111110).\end{aligned}$$

Their cross correlation is

$$\begin{aligned}R_{u,w} = \{&1,5,-3,-3,5,5,5,5,-7,5,-7,-3,-7,5,-3, \\ &-7,5,-3,-7,-3,5,-3,5,5,5,5,-7,-7,5\}\end{aligned}$$

where $1, 5, -3$, and 7, respectively, occur 1, 14, 7, and 7 times, which are consistent with the results in Theorem 15. So, the maximum cross correlation value between u and w is 7. The lower bound of (12) is 7, while the Sarwate bound of (11) is 5.

The following two theorems can be similarly proven.

Theorem 16: Let u and v be the binary sequences defined before. Then the distribution of cross-correlation values is the following:

$$\mathrm{R}_{u,v}(\tau)=\begin{cases}1, & 1 \text{ time}\\ -x+2y, & \frac{N-1}{4} \text{ times}\\ x+2y+2, & \frac{N-1}{4} \text{ times}\\ x-2y-2, & \frac{N-1}{4} \text{ times}\\ -x-2y, & \frac{N-1}{4} \text{ times}\end{cases}$$

where x and $y=\pm 1$ are defined before.

Theorem 17: Let v and w be the binary sequences defined before. Then the distribution of the cross-correlation values is the following:

$$\mathrm{R}_{v,w}(\tau)=\begin{cases}1, & 1 \text{ time}\\ x+2y-2, & \frac{N-1}{4} \text{ times}\\ x-2y+2, & \frac{N-1}{4} \text{ times}\\ -x-2y, & \frac{N-1}{4} \text{ times}\\ -x+2y, & \frac{N-1}{4} \text{ times}\end{cases}$$

where x and $y=\pm 1$ are defined before.

Then, we have the following conclusion.

Theorem 18: One and only one of the two pairs (u,v) and (v,w) has optimal cross correlation with respect to the bound of (12). The exact optimal pair depends on the choice of the primitive element α employed in defining the cyclotomic classes of order four.

Proof: By the distributions of the cross-correlation values given in Theorem 16 and Theorem 17, one and only one of (u,v) and (v,w) is an optimal pair, depending on the sign of $y=\pm 1$. The sign of y is determined by the choice of the primitive element α. ∎

Example 2: Let $N=13=(-3)^2+4$. Let the primitive root α of $\mathbf{Z}_N$ be 2. Then the three sequences u, v and w are given by

$$u=(0111011001000)$$
$$v=(0101100001101)$$
$$w=(0101000111010).$$

Their cross correlation are as follows:

$$R_{u,v}=\{1,1,-3,1,-3,-3,-3,5,5,1,-3,5,-3\}$$
$$R_{v,w}=\{1,-7,1,-7,5,1,1,1,1,-7,5,1,5\}$$

which are coincident with the correlation distributions shown in Theorems 16 and 17 in place of $x=-3$ and $y=-1$. The maximum cross-correlation value between v and w is 7. The maximum cross-correlation value between u and v is 5. The lower bound of (12) is 5, while the Sarwate bound of (11) is 3. So only (u,v) is an optimal pair.

Let u', v' and w' be the sequences obtained by modifying only the first bit of the binary sequences u, v, and w, respectively, which are, respectively, the complement of the sequences with support $D_2\cup D_3$, $D_1\cup D_3$, and $D_1\cup D_2$. The following theorem can be similarly proven. We omit the proof here.

Theorem 19: The following pairs of binary sequences are optimal pairs with respect to the bound of (12):

$$(u',w'),\ (u',w),\ (u,w').$$

In addition, one and only one in each of the following set is an optimal pair with respect to the bound of (12):

$$\{(u',v'),\ (v',w')\},\ \{(u',v),(v,w')\},\ \{(u,v'),(v',w')\}$$
$$\{(u',v'),(v',w)\},\{(u,v),\ (v,w')\},\ \{(u',v),\ (v,w)\},$$
$$\{(u,v'),\ (v',w)\}.$$

The specific optimal pair in each set above depends on the choice of the primitive element employed to define the cyclotomic classes of order four.

In summary, twelve optimal pairs of binary sequences of period $N\equiv 1 \pmod 4$ are obtained for every prime N of the form $N=x^2+4$, where $x\equiv 1 \pmod 4$. These are the first group of optimal pairs discovered in the literature.

V. Open Problems

It is open if the bounds of (6), (9), and (10) can be improved. This is quite interesting as no optimal pairs of binary sequences are known for the three cases that $N\equiv 3 \pmod 4$, $N\equiv 0 \pmod 4$, and $N\equiv 2 \pmod 4$. It would be nice to find out new optimal pairs of binary sequences for the case that $N\equiv 1 \pmod 4$.

Acknowledgment

The authors would thank the anonymous reviewers and the Associate Editor N. Y. Yu for their comments that improved the presentation of this paper.

References

[1] D. Jungnickel and A. Pott, "Perfect and almost perfect sequences," *Discr. Appl. Math.*, vol. 95, pp. 331–359, 1999.

[2] D. Jungnickel and A. Pott, , A. Pott, P. V. Kumar, T. Helleseth, and D. Jungnickel, Eds., "Difference sets: An introduction," in *Difference Sets, Sequences, and Their Correlation Properties*. Amsterdam: Kluwer, 1999, pp. 259–296.

[3] K. T. Arasu, C. Ding, T. Helleseth, P. V. Kumar, and H. Martinsen, "Almost difference sets and their sequences with optimal autocorrelation," *IEEE Trans. Inf. Theory*, vol. 47, no. 7, pp. 2934–2943, Nov. 2001.

[4] Y. Cai and C. Ding, "Binary sequences with optimal autocorrelation," *Theoret. Comput. Sci.*, vol. 410, no. 24–25, pp. 2316–2322, May 2009.

[5] S. W. Golomb and G. Gong, *Signal Design for Good Correlation—For Wireless Communication, Cryptography and Radar*. Cambridge, U.K.: Cambridge Univ. Press, 2005.

[6] H. D. Lüke, H. D. Schotten, and H. Hadinejad-Mahram, "Binary and quadraphase sequences with optimal autocorrelation properties: A survey," *IEEE Trans. Inf. Theory*, vol. 49, no. 2, pp. 3271–3282, Dec. 2003.

[7] M. Antweiler, "Cross-correlation of p-ary GMW sequences," *IEEE Trans. Inf. Theory*, vol. 40, no. 4, pp. 1253–1261, Jul. 1994.

[8] A. R. Calderbank and G. McGuire, "On a conjecture of Sarwate and Pursley regarding pairs of binary m-sequence," *IEEE Trans. Inf. Theory*, vol. 41, no. 4, pp. 1153–1155, Jul. 1995.

[9] A. R. Calderbank, G. McGuire, B. Poonen, and M. Rubinstein, "On a conjecture of Helleseth regarding pairs of binary m-sequence," *IEEE Trans. Inf. Theory*, vol. 42, no. 3, pp. 988–990, May 1996.

[10] A. H. Chan, M. Goresky, and A. Klapper, "Correlation functions of geometric sequences," in *Advances in Cryptography-Eurocrypt' 90*. New York: Springer-Verlag, 1990, pp. 214–221.
[11] T. Helleseth, "Some results about the cross correlation function between two maximal linear sequences," *Discr. Math.*, vol. 16, pp. 209–232, 1976.
[12] D. Hertel, "Cross correlation between GMW and Dillion-Dobbertin sequences," *IEICE Trans. Fundament.*, vol. E89-A, no. 9, pp. 2264–2267, Sep. 2006.
[13] D. V. Sarwate, "Bounds on cross correlation and autocorrelation of sequences," *IEEE Trans. Inf. Theory*, vol. IT-25, pp. 720–724, Nov. 1979.
[14] D. V. Sarwate and M. B. Pursley, "Cross-correlation properties of pseudo-noise and related sequences," *Proc. IEEE*, vol. 68, pp. 593–619, May 1980.
[15] D. Jungnickel, , J. Dinitz and D. R. Stinson, Eds., "Difference sets," in *Contemporary Design Theory, A Collection of Surveys*, ser. Wiley-Intersci. Series in Discr. Math. Optimiz.. New York: Wiley, 1992, pp. 241–324.
[16] D. Jungnickel and B. Schmidt, , J. W. P. Hirschfeld, S. S. Magliveras, and M. J. de Resmini, Eds., "Difference sets: An update," in *Geometry, Combinatorial Designs and Related Structures*. Cambridge, U.K.: Cambridge Univ. Press, 1997, pp. 89–112.
[17] P. Z. Fan and M. Darnell, *Sequence Design for Communications Applications*. London, U.K.: Research Studies Press; Wiley, 1996.
[18] J. M. Jensen, H. E. Jensen, and T. Hoholdt, "The merit factor of binary sequences related to difference sets," *IEEE Trans. Inf. Theory*, vol. 37, no. 3, pp. 617–626, May 1991.
[19] C. Ding, T. Helleseth, and K. Y. Lam, "Several classes of binary sequences with three-level autocorrelation," *IEEE Trans. Inf. Theory*, vol. 45, no. 7, pp. 2606–2612, Nov. 1999.
[20] A. M. Legendre, in *Essai sur la Theorie des Nombres*, Paris, France, 1798, pp. 186–.
[21] A. L. Whiteman, "A family of difference sets," *Illinois J. Math.*, vol. 6, pp. 107–121, 1962.
[22] C. Ding, "Autocorrelation values of generalized cyclotomic sequences of order two," *IEEE Trans. Inf. Theory*, vol. 44, pp. 1698–1702, July 1998.
[23] S. Mertens and C. Bessenrodt, "On the ground states of the Bernasconi model," *J. Phys. A: Math. Gen.*, vol. 31, pp. 3731–3749, 1998.
[24] T. Storer, *Cyclotomy and Difference Sets*. Chicago, IL: Markham, 1967.
[25] C. Ding and J. Yin, "Sets of optimal frequency-hopping sequences," *IEEE Trans. Inf. Theory*, vol. 54, pp. 3741–3745, Aug. 2008.

Cunsheng Ding (M'98–SM'05) was born in Shaanxi, China, in 1962. He received the M.Sc. degree in 1988 from the Northwestern Telecommunications Engineering Institute, Xi'an, China; and the Ph.D. degree in 1997 from the University of Turku, Turku, Finland.

From 1988 to 1992, he was a Lecturer of Mathematics with Xidian University, China. Before joining the Hong Kong University of Science and Technology in 2000, where he is currently a Professor of Computer Science and Engineering, he was an Assistant Professor of Computer Science with the National University of Singapore. His research fields are cryptography and coding theory. He has coauthored four research monographs.

Dr. Ding was the corecipient of the State Natural Science Award of China in 1989. He was the Guest Editor/Co-Editor for four journal special issues on coding and cryptography for *Designs, Codes and Cryptography*, *Information and Computation*, *Theoretical Computer Science*, and *Journal of Complexity*; and an Editor for the *Journal of Communications and Networks*, the *Journal of Universal Computer Science*, *Applicable Algebra in Engineering*, *Communication and Computing, Cryptography and Communications*, and *Advances in Mathematics of Communications*.

Xiaohu Tang (M'04) received the B.S. degree in applied mathematics from the Northwest Polytechnic University, Xi'an, China, the M.S. degree in applied mathematics from the Sichuan University, Chengdu, China, and the Ph.D. degree in electronic engineering from the Southwest Jiaotong University, Chengdu, China, in 1992, 1995, and 2001, respectively.

From 2003 to 2004, he was a Postdoctoral member with the Department of Electrical and Electronic Engineering, Hong Kong University of Science and Technology. From 2007 to 2008, he was a Visiting Professor with the University of Ulm, Germany. Since 2001, he has been with the Institute of Mobile Communications, Southwest Jiaotong University, where he is currently a Professor. His research interests include sequence design, coding theory, and cryptography.

Dr. Tang was the recipient of the National Excellent Doctoral Dissertation award in 2003 (China) and the Humboldt Research Fellowship in 2007 (Germany).