Design of Long Code Sequences from Addition of M-Sequences with Pairwise-Prime Periods

Jian Ren and Tongtong Li
Department of Electrical and Computer Engineering
Michigan State University, 2120 Engineering Building
East Lansing, MI 48824-1226, USA.
Email: {renjian,tongli}@egr.msu.edu

Abstract—Pseudo-random sequences with good correlation properties and large linear complexity are widely used in code-division multiple-access (CDMA) communication systems and cryptography for reliable and secure information transmission. In this paper, sequences with long period, large complexity, balance statistics and low correlation properties are constructed from addition of \( m \)-sequences with pairwise-prime periods (AMPP). Using \( m \)-sequences as building blocks, the proposed method proved to be an efficient and flexible approach to construct long period pseudo-random sequences with desirable properties from short period sequences. Applying the proposed method to two Gold sequences, a signal set \( ((2^n - 1)(2^n - 1), (2^n + 1)(2^n + 1), (2^{(n+1)/2} + 1)(2^{(m+1)/2} + 1)) \) is constructed.

Index Terms—Pseudo-random sequences, linear complexity, complexity, cross/auto-correlation, balance.

I. INTRODUCTION

Pseudo-random sequences with good correlation properties, large linear complexity and balance statistics are widely used in modern communication and cryptography. In CDMA systems, low cross-correlation between the desired and interfering users is important to suppress multiuser interference. Good autocorrelation properties are important for reliable initial synchronization and separation of the multipath components. Moreover, the number of available sequences should be sufficiently large so that it can accommodate enough users. From communication security point of view, sequences with low cross-correlation can be employed as key stream generators in stream ciphers to resist correlation attacks. Large linear complexity (also known as linear span, stands for the length of the shortest linear recursion over \( \mathbb{F}_2 \) satisfied by the sequence) of the sequence is required to prevent it from being reconstructed from a portion of sequence, for example, using the Berlekamp-Massey algorithm [1]. In literature, extensive research has been performed on how to generate sequences with these desired properties, some representative examples can be found in [2]–[10] and references therein.

Binary recursive sequences over the Galois field \( \mathbb{F}_2 \) are easy to generate. Binary \( m \)-sequences (also known as maximum sequences) [11] with period \( 2^n - 1 \) can easily be generated by linear recursions over \( \mathbb{F}_2 \) of degree \( n \). However, they suffer from one drawback: their linear complexity is short relative to their period, only relatively few terms of an \( m \)-sequence are needed to solve for its generating recursion. Such easy predictability makes binary \( m \)-sequences unsuitable for some applications requiring pseudo-random bits, especially in communication security.

In this paper, we propose to construct sequences from addition of multiple \( m \)-sequences with pairwise-prime periods, which are called AMPP sequences for short. It will be shown that if the \( m \)-sequences have pairwise-prime periods, then the sequences constructed from the modulo two addition of them have perfect balance statistics, low cross-correlation property, large periods, and large linear complexity. As a result, the proposed approach provides an efficient and flexible method to design long period pseudo-random sequences with desirable properties from short period sequences.

This paper is organized as follows: in Section II, some terminology and preliminary concepts are briefly introduced. In Section III, AMPP sequence is defined and its correlation properties, balance statistics are presented along with proofs. Meanwhile, shift equivalence and enumeration of shift distinct classes of AMPP are also presented. In Section IV, instead of using conventional linear complexity to characterize sequence complexity, a general concept of complexity of a sequence is proposed and is used to characterize the minimum number of stages required to generate the AMPP sequences. The generation of linear sequences are further discussed in Section V and we conclude in section VI.

II. TERMINOLOGY AND PRELIMINARY

In this section, some notations and preliminary results to be used throughout this paper are presented. For the theory of finite fields and a survey of linear recurring sequences, the readers are referred to [11]–[13]. Through this paper, we will focus ourselves to \( \mathbb{F}_2 \).

Notations:

- \( \mathbf{a} = (a_0, a_1, a_2, \ldots) \), a sequence over \( \mathbb{F}_2 \), i.e., \( a_i \in \mathbb{F}_2 \), is called a binary sequence. If \( \mathbf{a} \) is a periodic sequence with period \( v \), then we also denote \( \mathbf{a} = (a_0, a_1, \ldots, a_{v-1}) \), an element in \( \mathbb{F}_2^v \).
- Let \( \mathbf{a} = (a_0, a_1, \ldots) \) be a sequence over \( \mathbb{F}_2 \). The left operator \( L \) on \( \mathbf{a} \) is defined as
  \[ L(\mathbf{a}) = (a_1, a_2, \ldots) \].
For any \( i \), \( L^i(\mathbf{a}) = (a_i, a_{i+1}, \cdots) \). \( L^i(\mathbf{a}) \) is said to be a phase shift of \( \mathbf{a} \). For convenience, define \( L^0(\mathbf{a}) = \mathbf{a} \).

Let
\[
f(x) = \sum_{i=0}^{k} c_i x^i
\]
be a polynomial over \( \mathbb{F}_2 \), then
\[
f(L)(\mathbf{a}) = \sum_{i=0}^{k} c_i L^i(\mathbf{a}).
\]

If \( f(L)(\mathbf{a}) = 0 \) (0 represents zero or a zero sequence depending on the context), then \( f(x) \) is called a characteristic polynomial of \( \mathbf{a} \), and \( \mathbf{a} \) is said to be generated by \( f(x) \). The polynomial of the lowest degree in the set of characteristic polynomials of \( \mathbf{a} \) over \( \mathbb{F}_2 \) is called the minimal polynomial of characteristic polynomials of \( \mathbf{a} \) over \( \mathbb{F}_2 \).

- \( G(f) \) is defined as the set of all sequences over \( \mathbb{F}_2 \) generated by \( f(x) \).

### A. Shift Equivalent Relation

Two periodic sequences, \( \mathbf{a} = \{a_i\} \) and \( \mathbf{b} = \{b_i\} \) are called (cyclically) shift equivalent if there exists an integer \( k \) such that
\[
a_i = b_{i+k}, \quad \forall i \geq 0
\]
and in such a case we write \( \mathbf{a} = L^k(\mathbf{b}) \), or simply \( \mathbf{a} \sim \mathbf{b} \). Otherwise, \( \mathbf{a} \) and \( \mathbf{b} \) are called (cyclically) shift distinct.

### B. Correlation

Let \( \mathbf{a} = (a_0, a_1, \cdots, a_{v-1}) \) and \( \mathbf{b} = (b_0, b_1, \cdots, b_{v-1}) \) be two binary sequences with period \( v \), their (periodic) cross-correlation function \( C_{\mathbf{a}, \mathbf{b}}(\tau) \) is defined as
\[
C_{\mathbf{a}, \mathbf{b}}(\tau) = \sum_{i=0}^{v-1} (-1)^{a_i+b_{i+\tau}}, \quad \tau = 0, 1, \cdots
\]
where \( \{b_{i+\tau}\} \) is a phase shift of the sequence \( \{b_i\} \) and the indices are computed by modulo \( v \). If \( \mathbf{b} = \mathbf{a} \), then \( C_{\mathbf{a}, \mathbf{a}}(\tau) \) is called an auto-correlation function of \( \mathbf{a} \), denoted as \( C_{\mathbf{a}}(\tau) \) or simply \( C(\tau) \).

\[
C(\tau) = \begin{cases} v, & \text{if } \tau \equiv 0 \mod v \\ -1, & \text{otherwise} \end{cases}
\]
then we say that the sequence \( \mathbf{a} \) has an (ideal) two-level auto-correlation function. All \( m \)-sequences have ideal two-level auto-correlation functions.

### C. Balance Property

Let \( \mathbf{a} \) be a binary sequence with period \( v \). \( \mathbf{a} \) is called balanced if in every period the number of zeros and ones in \( \mathbb{F}_2 \) are nearly equal. More precisely, the disparity is not to exceed 1. In particular, when \( v = 2^n - 1 \), then \( \mathbf{a} \) is balanced if one occurs \( 2^{n-1} \) times and zero occurs \( 2^{n-1} - 1 \) times.

### D. Linear Complexity

The linear complexity of a sequence \( \mathbf{a} \) is defined to be the length of the shortest linear feedback shift register (LFSR) that generates \( \mathbf{a} \). Precisely, let
\[
f(x) = x^n + c_{n-1} x^{n-1} + \cdots + c_1 x + c_0 \in \mathbb{F}_2[x],
\]
and then \( \mathbf{a} = \{a_i\}_{i=0}^\infty \) satisfy the following recursive relation:
\[
a_{k+n} = c_{n-1} a_{k+n-1} + c_{n-2} a_{k+n-2} + \cdots + c_0 a_k, \quad k = 0, 1, \ldots
\]

### III. AMPP Sequence and Its Properties

In this section, first, the proposed AMPP sequence is defined. It is constructed from addition of multiple \( m \)-sequences with pairwise-prime periods. Secondly, the correlation property, balance statistics and shift equivalence of AMPP sequence are presented along with proofs.

The following theorem from [12] (Theorem 8.55) gives a good explanation of this statement.

**Proposition 1**: Let \( f(x) = f_1(x)^{m_1} f_2(x)^{m_2} \cdots f_s(x)^{m_s} \), where \( f_i(x) \) are distinct irreducible polynomials over \( \mathbb{F}_2 \) with \( s > 0 \), then \( G(f) \) can be decomposed as a direct sum of subspaces \( G(f_i(x)) \), i.e.,
\[
G(f(x)) = G(f_1(x)^{m_1}) \oplus G(f_2(x)^{m_2}) \oplus \cdots \oplus G(f_s(x)^{m_s})
\]

The following theorem from [12] (Theorem 8.59) plays a critical role in this paper, please refer to [12] for the proof.

**Proposition 2**: For each \( i = 1, 2, \cdots, s \), let \( \mathbf{a}_i \) be a linear recurrence sequence in \( \mathbb{F}_2 \) with minimal polynomial \( f_i(x) \in \mathbb{F}_2[x] \) and least period \( v_i \). If the polynomial \( f_1(x), f_2(x), \cdots, f_s(x) \) are pairwise relative prime, then the lease period of the sum \( \mathbf{a}_1 + \mathbf{a}_2 + \cdots + \mathbf{a}_s \) is equal to the least common multiple of \( v_1, v_2, \cdots, v_s \).

In fact, the sequence thus constructed has many desired properties. As an effort to construct sequences with long period, good correlation properties and large linear complexity, we hereby start with the following definition:

**Definition 1**: Let \( \mathbf{a}_i \) be an \( m \)-sequence over \( \mathbb{F}_2 \) with minimal polynomial \( f_i(x) \in \mathbb{F}_2[x] \) of degree \( n_i, i = 1, 2, \cdots, s \). If \( n_1, n_2, \cdots, n_s \) are pairwise relative prime, then the sequence \( \mathbf{a} = \mathbf{a}_1 + \mathbf{a}_2 + \cdots + \mathbf{a}_s \) is called the addition of \( m \)-sequences \( \mathbf{a}_1, \mathbf{a}_2, \cdots, \mathbf{a}_s \) with pairwise-prime periods, or AMPP sequence for short (See Fig. 1).

**Corollary 1**: For each \( i = 1, 2, \cdots, s \), let \( \mathbf{a}_i \) be an \( m \)-sequence over \( \mathbb{F}_2 \) with minimal polynomial \( f_i(x) \in \mathbb{F}_2[x] \) of degree \( n_i \). If \( n_1, n_2, \cdots, n_s \) are pairwise relative prime, then the period of the AMPP sequence of \( \mathbf{a}_1, \mathbf{a}_2, \cdots, \mathbf{a}_s \) is equal to \( (2^{n_1} - 1)(2^{n_2} - 2) \cdots (2^{n_s} - 1) \).
Example 1: Let \( \mathbf{a} = (010011010111100\cdots) \) be an \( m \)-sequence of period 15 with minimal polynomial \( f(x) = x^4 + x + 1 \) and \( \mathbf{b} = (1011100\cdots) \) be another \( m \)-sequence of period 15 with minimal polynomial \( g(x) = x^3 + x + 1 \). Let 
\[ \mathbf{c} = \mathbf{a} + \mathbf{b} \mod 2, \]
then 
\[ \mathbf{c} = (111101000000101011111101101010011011000000\cdots) \]
is an AMPP sequence of period \( 7 \times 15 = 105 \) and minimal polynomial \( f(x)g(x) = (x^7 + x + 1)(x^3 + x + 1) \).

**Theorem 1:** Let \( \mathbf{a} \) be an \( m \)-sequence with period \( v \), where \( i = 1, 2, \ldots, s \). Suppose \( v_i \)'s are pairwise relative prime. Let 
\[ \mathbf{a} = \sum_{i=1}^{s} a_i \mod 2, \]
then \( \mathbf{a} \) is a non-zero sequence. Then

1. The least period \( v \) of \( \mathbf{a} \) is equal to \( v_1 v_2 \cdots v_s \).
2. The auto-correlation function \( C_{\mathbf{a}}(\tau) \) is \( 2^s \)-valued. Explicitly
   a. \( C_{\mathbf{a}}(\tau) = (−1)^{s−l}v_i v_{i+1} \cdots v_{l+1} \), if \( \tau = 0 \mod v_i v_{i+1} \cdots v_{l+1} \), where \( \{v_1, \ldots, v_s\} \subseteq \{v_i, \ldots, v_s\} \).
   b. \( C_{\mathbf{a}}(\tau) = (−1)^s \), if \( \tau \neq 0 \mod v_i, i = 1, 2, \cdots, s \).
3. The distribution of auto-correlation is
   a. \( (−1)^s \) appears \( \prod_{i=1}^{s} (v_i − 1) \) times.
   b. \( (−1)^{s−l} \prod_{j=1}^{l} v_{j−1} \) \( l \leq s \) appears \( (−1)^{s−l} \prod_{j=1}^{l} (v_j − 1) \) times.

**Theorem 2:** Let \( \mathbf{a} = (a_0, a_1, \ldots, a_{v−1}) \) be an AMPP sequence associated with sequences \( \mathbf{a}_1, \ldots, \mathbf{a}_n \). Then in every period of sequence \( \mathbf{a} \), the disparity of the number of ones and the number of zeros is not to exceed 1. Thus \( \sum_{i=0}^{v−1} (−1)^{a_i} \leq 1 \).

**Proof:** Denote \( \mathbf{a}_j = (a_{j,0}, a_{j,1}, \ldots, a_{j,v−1}), j = 1, 2, \ldots, s \), then
\[ \sum_{i=0}^{v−1} (−1)^{a_i} = \sum_{i=0}^{v−1} (−1)^{\sum_{j=1}^{s} a_{j,i}} \]
\[ = \sum_{i=0}^{v−1} (−1)^{a_{1,i}}(−1)^{a_{2,i}} \cdots (−1)^{a_{s,i}} \]
\[ = \sum_{i=0}^{v−1} (−1)^{a_{1,i}} \sum_{i=0}^{v−2} (−1)^{a_{2,i}} \cdots \sum_{i=0}^{v−1} (−1)^{a_{s,i}}. \]
Since \( \sum_{i=0}^{v−1} (−1)^{a_{j,i}} \leq 1, \) for \( j = 1, 2, \ldots, s \), hence
\[ \left| \sum_{i=0}^{v−1} (−1)^{a_{j,i}} \right| \leq 1. \]

**Lemma 1:** Let \( m_1, m_2, \ldots, m_s \) be distinct positive integers larger than or equal to 2, then we have the following inequality
\[ (2^{m_1} − 1)(2^{m_2} − 1) \cdots (2^{m_s} − 1) > 2^{m_1 + m_2 + \cdots + m_s − 1}. \]

**Proof:** Define
\[ f_s(m_1, \cdots, m_s) = (2^{m_1} − 1) \cdots (2^{m_s} − 1) \]
\[ = 2^{m_1 + \cdots + m_s − 1} \]
where \( g_s = (2^{m_1} − 1) \cdots (2^{m_s} − 1), h_s = 2^{m_1 + \cdots + m_s − 1} \).

\( k_s = 2^{m_1 + \cdots + m_s} \), Without loss of generality, we only need to prove that \( f_s > 0 \) if \( m_i \geq i + 1 \) for all \( 2 \leq i \leq s \).

First, for \( s = 2, f_2(m_1, m_2) = (2^{m_1} − 1)(2^{m_2} − 1) − 2^{m_1 + m_2} − 2m_1 \cdot 2m_2 \). It is easy to prove the \( f_2(m_1, m_2) \) is a convex function that attains the minimum 1 when \( m_1 = 2, m_2 = 3 \).

Secondly, suppose \( f_s > 0 \). Then we have
\[ f_{s+1}(m_1, m_2, \ldots, m_{s+1}) \]
\[ = (2^{m_{s+1}} − 1)g_s − 2^{m_{s+1}}h_s − 2^{m_{s+1}} \]
\[ > 2^{m_{s+1}}g_s - g_s - 2^{m_{s+1}}h_s \]
\[ > 2^{m_{s+1}}h_s - g_s \]
\[ > 0. \]

This proves that \( f_s > 0 \) for all \( s \geq 2 \). Thus
\[ (2^{m_1} − 1) \cdots (2^{m_s} − 1) − 2^{m_1 + \cdots + m_s − 1} = g_s - h_s > f_s > 0. \]

Hence
\[ (2^{m_1} − 1) \cdots (2^{m_s} − 1) > 2^{m_1 + \cdots + m_s − 1}. \]

**Theorem 3:** Let \( \mathbf{a}_i \) and \( \mathbf{b}_i \) be two \( m \)-sequences with the same minimal polynomial, \( i = 1, 2, \ldots, s \). Suppose \( \mathbf{a} \) is an AMPP sequence of sequences \( \mathbf{a}_i \), and \( \mathbf{b} \) is an AMPP sequence of sequences \( \mathbf{b}_i, i = 1, 2, \ldots, s \), then \( \mathbf{a} \) and \( \mathbf{b} \) are shift equivalent.

**Proof:** Let the minimal polynomial for \( \mathbf{a}_i \) and \( \mathbf{b}_i \) be \( f_i(x), i = 1, 2, \ldots, s \), then the generating polynomial for \( \mathbf{a} \) and \( \mathbf{b} \) is \( f_1(x)f_2(x) \cdots f_s(x) \). From Theorem 1, the period of \( \mathbf{a} \) and \( \mathbf{b} \) is equal to \( \prod_{i=1}^{s} (2^{m_i} − 1) \), where \( m_i \) is the degree of \( f_i(x), i = 1, 2, \ldots, s \). Corresponding to this period, there are \( \prod_{i=1}^{s} (2^{m_i} − 1) \) different initial states.

According to Lemma 1, in this particular case, for the same generating polynomial, there is only one shift equivalent class. In fact, if \( \mathbf{a} \) and \( \mathbf{b} \) are shift distinct, since the different initial states for \( \mathbf{a} \) and \( \mathbf{b} \) are both equal to \( \prod_{i=1}^{s} (2^{m_i} − 1) \), the total number of different initial states is at least equal to \( 2 \prod_{i=1}^{s} (2^{m_i} − 1) > 2 \times 2^{m_1 + m_2 + \cdots + m_s} = 2^{2^{(f_1(x)\cdots f_s(x))}}. \) This is a contradiction. Hence, we have proved that sequence \( \mathbf{a} \) and sequence \( \mathbf{b} \) are shift equivalent.

Actually, based on Corollary 1 and Theorem 3, we have the following stronger theorem:

**Theorem 4:** Let \( \mathbf{a} \) be an AMPP sequence of sequences \( \mathbf{a}_1, \mathbf{a}_2, \cdots, \mathbf{a}_r \), and \( \mathbf{b} \) be an AMPP sequence of sequences \( \mathbf{b}_1, \mathbf{b}_2, \cdots, \mathbf{b}_s \). Then \( \mathbf{a} \sim \mathbf{b} \).
if and only if $r = s$ and $\mathbf{a}$’s if the $\mathbf{b}$’s are and the $\mathbf{b}$’s are both arranged in increasing order in terms of period.

**Theorem 5:** There are $\lambda_2(n_1)\lambda_2(n_2)\cdots\lambda_2(n_s)$ shift distinct classes of AMPP sequences with period $(2^{n_1} - 1)(2^{n_2} - 2)\cdots(2^{n_s} - 1)$, where $\lambda_2(n) = \frac{\phi(2^n - 1)}{n}$ as defined in [11] (page 40) and $\phi(n)$ is the Euler Totient function defined as the number of positive integers not exceeding $n$ and relatively prime to $n$. Therefore, $\phi(v) = (v_1 - 1)(v_2 - 1)\cdots(v_s - 1)$.

**Proof:** Since the number of polynomials mod 2 of degree $r$ which generate maximum sequence is given by

$$\lambda_2(n) = \frac{\phi(2^n - 1)}{n},$$

The result then follows from Theorem 3.

IV. COMPLEXITY OF AMPP

In this section, the general concept of complexity of a periodic sequence is first introduced and illustrated with examples. The complexity properties of general linear and AMPP sequence are studied.

**Definition 2:** Let $\mathbf{a}$ be a periodic sequence with least period $v$. The minimal number of states of the finite state machine that generates this sequence is defined as the complexity of $\mathbf{a}$, denoted as $\mathcal{C}(\mathbf{a})$.

**Corollary 2:** The linear complexity of a sequence is always larger than or equal to the complexity of the sequence.

**Remark 1:** The complexity of a periodic sequence defines the minimal number of states of a finite state machine (FSM) that generates the sequence. The corresponding generator could be linear feedback shift register (LFSR) or nonlinear feedback shift register (NLFSR). The feedback of the NLFSR sequence generators can be determined from the truth table.

The following example shows that the complexity of a periodic sequence can be strictly smaller than its linear complexity.

**Example 2:** Suppose we have sequence

$$101001101001\cdots$$

The linear complexity of this sequence is 6 since it is the shortest LFSR that can generate this sequence is a 6-stage linear recursion $s_{n+6} = s_n$ with initial state 101001. However, this sequence can also be generated through a 3-stage nonlinear recursion $s_{n+3} = s_{n+2} + s_{n+2}s_{n+1} + s_n$ with initial state 101.

For a sequence whose linear complexity is equal to its complexity, the periodicity gives the minimal number of stages required to regenerate the sequence. In other word, the sequence cannot be generated from a feedback function with fewer stages.

**Lemma 2:** Let $\mathbf{a}$ be a sequence with least period $v$, then the feedback shift register (FSR) that generates $\mathbf{a}$ has at least $\lceil \log_2 v \rceil$ stages in $\mathbb{F}_2$, where $\lceil x \rceil$ denotes the smallest integer greater than or equal to $x$.

**Proof:** For a given feedback shift register (FSR), the next state of the FSR is completely determined by the current state. Hence, for a sequence with period $v$, the total number of possible states is $v$ which requires at least $\lceil \log_2 v \rceil$ stages in $\mathbb{F}_2$.

From this Lemma, it follows immediately that:

**Corollary 3:** The complexity of an m-sequence is equal to its linear complexity. In other words, m-sequence has the maximal nonlinearity.

The following theorem presents a method to characterize and also to compute the complexity of a periodic sequence.

**Theorem 6:** Let $\mathbf{a} = (a_0, a_1, \cdots, a_{v-1})$ be a periodic sequence with least period $v$. The complexity of $\mathbf{a}$ is equal to the minimal number $k$ such that the $k$-tuples $(a_i, a_{i+1}, \cdots, a_{i+k-1})$ are all different, where $i = 0, 1, \cdots, v-1$.

**Proof:** First, it is clear that for a periodic sequence, such a $k$ always exists. Secondly, suppose $k$ is the smallest integer such that the $k$-tuples $(a_i, a_{i+1}, \cdots, a_{i+k-1})$ are all different for $i = 0, 1, \cdots, v-1$. Define the following feedback function $f$:

$$a_{i+k} = f(a_i, a_{i+1}, \cdots, a_{i+k-1}), \quad i = 0, 1, \cdots, v-1.$$

Clearly, $f$ is well defined since the $k$-tuples $(a_i, a_{i+1}, \cdots, a_{i+k-1})$ are all different. Since $k$ is the minimal number such that the $k$-tuples $(a_i, a_{i+1}, \cdots, a_{i+k-1})$ are all different, the $f$ thus defined gives the minimal feedback function that generates $\mathbf{a}$. Therefore, $k$ is equal to the complexity of the sequence $\mathbf{a}$.

It is very interesting that the complexity of the sequence derived through addition of $m$-sequences is equal to the addition of the complexity of all $m$-sequences. This is proved in the following theorem.

**Theorem 7:** Let $\mathbf{a}_i$ be $m$-sequences with $m_i$ stages, where $m_i$’s are pairwise relative prime for $i = 1, 2, \cdots, s$. Let $\mathbf{a} = \mathbf{a}_0 + \mathbf{a}_1 + \cdots + \mathbf{a}_s$ mod 2, then the complexity of sequence $\mathbf{a}$ is equal to the addition of the linear complexity of $\mathbf{a}_i$’s, $i = 0, 1, \cdots, s - 1$. That is

$$\mathcal{C}(\mathbf{a}) = \sum_{i=0}^{s-1} \mathcal{C}(\mathbf{a}_i).$$

**Proof:** According to Lemma 1, we have

$$(2^{m_1} - 1)(2^{m_2} - 1)\cdots(2^{m_s} - 1) > 2^{m_1 + m_2 + \cdots + m_s - 1}.$$ 

For feedback shift register sequences, the same initial state values will generate the same subsequent sequences. Therefore, the number of different initial state assignments is at least equal to the period $(2^{m_1} - 1)(2^{m_2} - 1)\cdots(2^{m_s} - 1)$. This gives the number of different stages to be $m_1 + m_2 + \cdots + m_s$. In other words, $\mathcal{C}(\mathbf{c}) \geq \sum_{i=0}^{s-1} \mathcal{C}(\mathbf{a}_i)$. On the other hand, it is straightforward from Proposition 1 to see that $\mathcal{C}(\mathbf{c}) \leq \sum_{i=0}^{s-1} \mathcal{C}(\mathbf{a}_i)$.

**Corollary 4:** Let $\mathbf{a} = \mathbf{a}_1 + \mathbf{a}_2 + \cdots + \mathbf{a}_s$ be an AMPP sequence of $\mathbf{a}_1, \mathbf{a}_2, \cdots, \mathbf{a}_s$. Denote the linear complexity of $\mathbf{a}_i$ as $\mathcal{C}(\mathbf{a}_i)$, $i = 1, \cdots, s$, then the linear complexity of $\mathbf{a}$ is equal to

$$\sum_{i=1}^{s} \mathcal{C}(\mathbf{a}_i).$$

In particularly, if the linear complexity of sequence $\mathbf{a}_i$ is $m_i$, $i = 1, 2, \cdots, s$, then the linear complexity of sequence $\mathbf{a}$ is equal to $m_1 + m_2 + \cdots + m_s$. 


V. FURTHER DISCUSSIONS ON SEQUENCE GENERATION AND DECOMPOSITION

Gold sequence [14] has been widely used in code division multiple access (CDMA) communication systems to mitigate multiuser interference from other users who share a common channel. Gold sequence is constructed by adding two specified m-sequences of the same period, while AMPP sequence is generated through addition of multiple m-sequences with pairwise-prime periods. In this section, we further discuss the generation methods and analyze structure of linear sequences.

**Theorem 8:** Let \( \mathbf{a} \) and \( \mathbf{b} \) be two m-sequences with period \( v_2 = v_2 = 2^{n_2} - 1, \) \( i = 1, 2, \ldots, s. \) Assume that \( v_2, v_2, \ldots, v_2 \) are relative prime, then the cross-correlation between \( \mathbf{a} = \sum_{i=1}^{s} a_i \) and \( \mathbf{b} = \sum_{i=0}^{s} b_i \) is given by the following equation

\[
C_{\mathbf{a}, \mathbf{b}}(\tau) = C_{\mathbf{a}, \mathbf{b}}(\tau) \cdots C_{\mathbf{a}, \mathbf{b}}(\tau).
\]

**Proof:** Let \( v \) be the period of \( \mathbf{a} = a_1 + \cdots + a_a. \) According to Corollary 1, \( v = v_1 \cdots v_n. \) According to equation (3), we have

\[
C_{\mathbf{a}, \mathbf{b}}(\tau) = \sum_{i=0}^{v-1} (-1)^{a_i,\cdots+a_i} + (-1)^{b_i,\cdots+b_i}.
\]

This is because that if \( \gcd(r, v_2) = 1, \) then \( r \times (0, 1, \ldots, v_2 - 1) \) is simply a rearrangement of \((0, 1, \ldots, v_2 - 1). \]

**Corollary 5:** Let \( \mathbf{a} \) and \( \mathbf{b} \) be a Gold pair with period \( 2^n - 1, \) and \( \mathbf{r} \) and \( \mathbf{s} \) be another Gold pair with period \( 2^m - 1. \) Assume that these two Gold pairs have relative prime periods, then the cross-correlation between \( \mathbf{a} + \mathbf{r} \) and \( \mathbf{b} + \mathbf{s} \) is given by the following set:

\[
(1, -t(n), -t(m), t(n) - 2, t(m) - 2, t(n)t(m), -t(n)(t(m) - 2), -t(m)(t(n) - 2), (t(n) - 2)(t(m) - 2)),
\]

where \( t(n) \) is defined as

\[
1 + 2^{[(n+1)/2]}.
\]

That is

\[
C_{\mathbf{a}, \mathbf{b}}(\tau) \leq (2^{(n+1)/2}) + 1 + (2^{(n+1)/2}) + 1.
\]

Therefore, a signal set \( \left( (2^n - 1)(2^n - 1), (2^n + 1)(2^n + 1), (2^{(n+1)/2}) + 1 \right) \) can be constructed, where \( (2^n - 1)(2^n - 1) \) is the period of these sequences, \( (2^n + 1)(2^n + 1) \) is the number of these sequences, and \( (2^{(n+1)/2}) + 1 \) is the maximum cross-correlation of these sequences.

**Proof:** The result follows directly from Theorem 8 and the fact that the cross-correlation of a Gold pair is the set \(-t(n), -n, t(n) - 2\) [14].

**Example 3:** Let \( \mathbf{a} \) and \( \mathbf{b} \) be a Gold pair with minimal polynomials \( x^s + x + 1 \) and \( x^d + x^d + x^3 + x^3 + x^2 + 1 \) respectively. Let \( \mathbf{r} \) and \( \mathbf{s} \) be another Gold pair with minimal polynomials \( x^6 + x + 1 \) and \( x^6 + x^5 + x^2 + x + 1 \) respectively. Suppose

the initial states for sequences \( \mathbf{a}, \mathbf{b}, \mathbf{r} \) and \( \mathbf{s} \) are \([1, 0, 0, 0, 0], [1, 1, 1, 1, 1], [1, 0, 0, 0, 0, 0] \) and \([1, 1, 1, 1, 1, 1] \) respectively. Then

\[
t(5) = 9, \; t(7) = 17.
\]

Therefore,

\[
C_{\mathbf{a}+\mathbf{r}, \mathbf{b}+\mathbf{s}}(\tau) = (-135, -119, -15, -7, 1, 9, 17, 105, 153).
\]

The signal set is thus given by

\[
(3937, 4257, 153),
\]

which is a set of sequences with period 3937, the total number of sequences is 4257, and their maximum cross-correlation is only 153.

VI. CONCLUSIONS

In this paper, a method to generate long period sequences with large linear complexity and good correlation properties was presented. Actually, a new class of sequences, called AMPP sequences, were constructed from addition of multiple m-sequences with pairwise-prime periods. It was proved that AMPP sequences have excellent autocorrelation property, balance statistics and large complexity. The proposed design method provides an efficient and flexible approach to generate large sequences with desirable properties.

REFERENCES


