Correlation Analysis and Realization of Gordon-Mills-Welch Sequences in Advanced Design System

Lei Tong, Fangfang Chen, Jingyu Hua, Limin Meng and Shouli Zhou
Zhejiang Provincial Key Laboratory of Optimumm Communication Technology, Zhejiang University of Technology, Hangzhou, 310023, China
State Key Laboratory Inf. Eng. in Survey, Mapping and Remote Sensing, Wuhan University, Wuhan, China

Abstract: In modern Spread Spectrum (SS) communications, how to generate spread spectrum sequence quickly is important in system modeling and design, and therefore has received wide attentions. Moreover, since ADS (Advanced Design System) software had been a widely used simulation tool in industrial areas and there was only the m-sequence (low linear complexity) in the SS sequence library, this paper investigates the generation of Gordon-Mills-Welch (GMW) sequence (high linear complexity) and designs GMW sequence in ADS software, which will enrich the sequence library of ADS and provide more security in information encryption when engineers design SS systems by ADS. In addition, after analyzing the correlation property, we also study a low-correlation GMW generator based on sequence pair choice. The results show that though original GMW sequences have poor cross-correlation, the latter presents good correlation performance and therefore is beneficial for spread spectrum communications.

Key words: Trace function, sequence generation, pseudo-noise sequence, spread spectrum

INTRODUCTION

Pseudo-Noise (PN) sequences (or spread spectrum sequences) have a very wide use in control and communications fields, such as Spread Spectrum (SS) communications, navigation, ranging, multi-target recognition, telemetry and security coding system (Britto et al., 2006; Tachikawa et al., 2007; Todorovic and Orlic, 2005; Mingxin et al., 2008; Golomb and Gong, 2005; Yang and Yang, 2008). Thus, studies on spread spectrum sequences have become important topics in spread spectrum systems (Tanimoto et al., 2008; Zhang and Hao, 2008; Tachikawa, 2007; Kavat et al., 2007).

Conventionally, many PN sequences had been studied, such as M-sequence, Gold sequence, M-sequence, GMW sequence (Golomb and Gong, 2005), geometric sequences (Sengupta and Porikli, 2009) and BENT sequence (Buadaghiyan et al., 2006; Pin-Hui et al., 2007; Izbenko et al., 2009; Chem et al., 2010). Among these sequences, GMW sequences and m sequences are known due to their ideal two-level auto-correlations (Golomb and Gong, 2005; Helleseth and Gong, 2002). However, m sequences with low linear complexity cannot meet the requirements of many applications, such as SS sequences. With the same period as m sequences, the GMW sequence (Hertel, 2005; Klapper and Cartel, 2004; Golomb and Gong, 2005) has more sequence choices and presents larger linear complexity as well as its good pseudo-randomness and balance characteristics, thus is a kind of good spread spectrum sequence.

Trace transform methods are most popular methods to generate SS sequence (Pin-Hui et al., 2007; Wen-Feng, 2006). Therefore, we design the GMW sequence generator according to the trace representation and realize it in ADS software, which will enrich the sequence library of ADS. Moreover, since ADS had been a popular tool in communication system design, our study will be beneficial for communication engineers. With the designed GMW sequences, we analyze their cross-correlations and in order to overcome the poor cross-correlations, we present a sequence pair based generation method, which XORs two GMW sequences with different primitive polynomials to produce better GMW sequences with triple-valued autocorrelations and small cross-correlations, which are confirmed by simulation verifications.

BENT SEQUENCE GENERATION

Definition of GMW sequence: In Galois Field (GF), the trace function $t^{(M)}_{m}(a)$ (with M divisible by 1) maps...
\( \alpha \) elements in \( \text{GF}(2^n) \) into elements of a subfield \( \text{GF}(2^e) \),
according to the relation:

\[
u^e_\alpha(a) = \sum_{i=0}^{M-1} \alpha^i \]

(1)

Then the trace function \( \nu^e_\alpha(a) \) maps \( x \in \text{GF}(2^n) \) into
\( \text{GF}(2) \) (Golomb and Gong, 2005). Accordingly, the GMW
sequence is defined as:

\[
u_r = \nu^e_\alpha \left( \left[ \nu^e_\alpha(\alpha^r) \right]^T \right)
\]

(2)

where, \( n = m \times e \) and \( e \) is any positive integer. In (2), \( \alpha \)
represents a primitive element of \( \text{GF}(2^n) \), with \( 1 \leq k \leq 2^n-1 \)
and \( \gcd(k, 2^n-1) = 1 \).

Based on the construction of trace function, the steps of designing a GMW sequence are follows:

- Select a \( m \)-th order primitive polynomial \( f(x) \) in the
  \( \text{GF}(2) \)
- The minimum polynomial of \( \alpha^r \) in \( \text{GF}(2^n) \) as follows:
  \( g(x) = (x^q-\gamma)(x^q-\gamma^2) \ldots (x^q-\gamma^{2^n}) \)

where, \( q = 2^m \) and \( \gamma = \alpha^{-1} \); then \( \nu^e_\alpha(\alpha^r) \) can be constructed
by the minimum polynomial \( g(x) \).

- The basis in \( \text{GF}(2^n) \) is \( m \)-dimensional vector space in \( \text{GF}(2) \), thus the element \( \gamma \) must obey:
  \[
r = \left\lfloor \frac{q-1}{\alpha} \right\rfloor \quad \gamma \in \text{GF}(2)
\]

(4)

- According to \( f(\alpha)=0 \), calculate the elements in \( \text{GF}(2^n): \alpha^0, (1+\alpha^j \tilde{\alpha}^j) \), where, \( j=0, \ldots, (2^n-2) \)
- According to Eq. 1 and 4, \( \nu^e(a) \) can be constructed

**GMW generator in ADS software:** Without loss of
generality, we design a GMW sequence with period of 63
with trace function as:

\[
u_r = \nu^e_\alpha \left( \left[ \nu^e_\alpha(\alpha^r) \right]^T \right)
\]

Then, we have \( n=6 \), \( m=3 \), \( e=2 \), \( q=8 \), \( Q=8 \) according to
Eq. 1 to 4 and

Step 1: Select primitive polynomial \( f(x)=x^2+x^2+z^2+z+1 \)
Step 2: The minimum polynomial of \( \alpha \) in \( \text{GF}(2^3) \)
is \( (z-a)(z-a^3) = z^8+z^2+z^2 \)
Step 3: The elements of \( \text{GF}(2^3) \) are \( 0, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6 \) and the basis of \( \text{GF}(8) \) is \( \{1, \alpha, \alpha^2\} \), then the

\[\begin{array}{cccc}
\gamma & \gamma_0 & \gamma_1 & \gamma_2 \\
0 & 0 & 0 & 0 \\
1 & 1 & 0 & 1 \\
\alpha & 0 & 1 & 0 \\
\alpha^2 & 0 & 0 & 1 \\
\alpha^3 & 1 & 1 & 0 \\
\alpha^4 & 0 & 1 & 1 \\
\alpha^5 & 1 & 1 & 1 \\
\alpha^6 & 1 & 0 & 0 \\
\alpha^7 & 1 & 1 & 0 \\
\end{array}\]

Therefore, the elements of minimal polynomial \( x^3+\alpha x^2+x \) can be written as:

\[\begin{array}{c}
\alpha^4 \gamma = \gamma_0 \alpha^4 + \gamma_1 \alpha^3 + \gamma_2 \\
\gamma_0 \gamma_1 \gamma_2 \end{array}\]

(6)

Now \( \nu^e_\alpha(\alpha^r) \) can be constructed by the coefficients
of (6).

Step 5: According to, \( \nu^e_\alpha(\alpha^r) \) and \( \nu^e_\alpha(\alpha^T) \) the
elements of \( \text{GF}(8) \) can be computed and presented in Table 1

**Table 1: The elements of \( \text{GF}(8) \) and \( \nu^e_\alpha(\alpha^r) \)**

\(\begin{array}{cccc}
\gamma & \gamma_0 & \gamma_1 & \gamma_2 \\
0 & 0 & 0 & 0 \\
1 & 1 & 0 & 1 \\
\alpha & 0 & 1 & 0 \\
\alpha^2 & 0 & 0 & 1 \\
\alpha^3 & 1 & 1 & 0 \\
\alpha^4 & 0 & 1 & 1 \\
\alpha^5 & 1 & 1 & 1 \\
\alpha^6 & 1 & 0 & 0 \\
\end{array}\)

According to the construction of \( \nu^e(\alpha^r) \) and \( \nu^e(\alpha^T) \) the
GMW sequence generator in ADS2005A is shown in
Fig. 1, where we exploits two kinds of kernel devices, i.e.,
delay device (one bit delay device with a parameter of
Initial value) and Logic device (logic function XOR or
AND). In Fig. 1, both \( \nu^e(\alpha^r) \) and \( \nu^e(\alpha^T) \) are constructed
according to Step 1-step 5), while the former consists six
delay devices and several XOR logic devices, and the
latter exploits two XOR logic devices and one AND logic
device.

In order to verify our design, we further run
simulations and test sequences’ correlations. Note that
From (1), changing the trace function parameters \( k \) or
selecting different primitive polynomial \( f(x) \) will result in
different GMW sequence with same periods. Moreover,
since the auto-correlations of GMW sequences are
The cross-correlation of six-order GMW sequence: According to the above discussion, we construct four six-order GMW sequences, in which GMW-6-1 (trace function)

\[ t_1^f \left[ \left[ t_2^f (\alpha') \right]^2 \right] \]

and GMW-6-2

\[ t_4^f \left[ \left[ t_2^f (\alpha') \right]^2 \right] \]

are constructed by primitive polynomial \( f(z) = z^4 + z^3 + z^2 + z + 1 \), while GMW-6-3

\[ t_4^f \left[ \left[ t_2^f (\alpha') \right]^2 \right] \]

and GMW-6-4

\[ t_4^f \left[ \left[ t_2^f (\alpha') \right]^2 \right] \]

are constructed by primitive polynomial \( f(z) = z^4 + z^3 + 1 \).

Their cross-correlations are shown in Fig. 2. In Fig. 2, X-coordinate denotes shift between two sequences and Y-coordinate represents the values of correlation.

From Fig. 2, we explicitly see that (a) and (b) only have triple-valued, but the maximum value approaches 0.5, which is much larger than those observed in Fig. 2c or d. Therefore, we conclude that the cross-correlation of GMW sequences with same primitive polynomials and different trace function parameters \( k \) is much less than that of GMW sequences with different primitive polynomials and same trace function parameters \( k \). In order to confirm this conclusion, we further observe the nine-order GMW sequences next.

The cross-correlation of nine-order GMW sequence: We constructing four nine-order GMW sequences, in which GMW-9-1 (with the trace function ) and \( t_1^f \left[ \left[ t_2^f (\alpha') \right]^2 \right] \)

GMW-9-2

\[ t_4^f \left[ \left[ t_2^f (\alpha') \right]^2 \right] \]

GMW-9-3

\[ t_4^f \left[ \left[ t_2^f (\alpha') \right]^2 \right] \]

are constructed by primitive polynomial \( f(z) = z^4 + z^3 + z + 1 \), while GMW-9-4

\[ t_4^f \left[ \left[ t_2^f (\alpha') \right]^2 \right] \]

and GMW-9-4

\[ t_4^f \left[ \left[ t_2^f (\alpha') \right]^2 \right] \]
Fig. 2: (a) The cross-correlation of GMW 6-1 and GMW 6-2, (b) the cross-correlation of GMW 6-3 and GMW 6-4, (c) The cross-correlation of GMW 6-1 and GMW 6-3, (d) the cross-correlation of GMW 6-2 and GMW 6-4

Fig. 3: (a) The cross-correlation of GMW 9-1 and GMW 9-2, (b) the cross-correlation of GMW 9-3 and GMW 9-4, (c) The cross-correlation of GMW 9-1 and GMW 9-3, (d) the cross-correlation of GMW 9-2 and GMW 9-4

are constructed by primitive polynomial \( f(z) = z^4 + z^3 + z^2 + z + 1 \).

From Fig. 3, we can clearly conclude that different primitive polynomials lead to large cross-correlation degradation. However, the number of primitive polynomial is limited and if we want to generate many GMW sequences with the same period, we have to modify the trace function parameters \( k \), which means that we cannot ensure small cross-correlations for a large number of GMW sequences.

SEQUENCE PAIR BASED GENERATOR

In order to address the contract between the sequence number and the cross-correlation, this section will provide a new GMW sequence generator, which comes from the sequence pair choice like GOLD sequence. It is well known that the pairs of \( n \)-order \( m \) sequences have 3-values cross-correlations. When, \( n \) is even and not as a multiple of four, the value of cross-correlation is \(-1/(2^n-1)\). \((-2^m+1)/(2^n-1)\) or \((-2^m+1)/(2^n-1)\) and when \( n \) is odd, the value of cross-correlation is \(-1/(2^n-1)\), \(-2^m+1)/(2^n-1)\) or \((-2^m+1)/(2^n-1)\).

In Fig. 2c, the cross-correlation of GMW6-1 and GMW6-3 are triple-valued at -1/63, -17/63 or 15/63, which is the same as the cross-correlation of six-order \( m \) sequence pairs with primitive polynomials \( z^4 + z^3 + z^2 + z + 1 \) and \( z^4 + z + 1 \). From Fig. 3c, the cross-correlation of GMW9-1 and GMW9-3 are triple-value d at -1/511, -33/511 or 31/511, which is also the same as the cross-correlation of nine-order \( m \) sequence pairs with primitive polynomials \( z^4 + z^3 + z^2 + z + 1 \). In fact, all pairs of primitive polynomials lead to GMW sequences (with trace function) \( \psi \left[ \left( \psi (z_1) \right)^3 \right] \) with triple-valued cross-correlations (Gold and Gong, 2005).

As we known, the pairs of \( m \) sequences can generate Gold sequences by shift XOR. Analogous to Gold sequence, XOR of GMW6-1 and GMW6-3 get a new Sequence 1, while XOR of GMW9-1 and GMW9-3 get a new Sequence 2. It can be proved that such sequences have the similar properties of Gold sequence: Triple-valued auto-correlations and small cross-correlations. However, the process will be lengthy and tedious. Therefore we only show some results in Fig. 4 and Table 2.
Table 2: Autocorrelation and cross-correlation of some GMW sequence pairs

<table>
<thead>
<tr>
<th>Sequence Order</th>
<th>Trace function</th>
<th>Primitive polynomials</th>
<th>Autocorrelation</th>
<th>Cross-correlation</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>$t^2 \left[ [t^2 \left( \alpha' \right) ] \right]$</td>
<td>$f(z)=z^2+z^2+1$, $f(z)=z^4+z^4+1$</td>
<td>1, -1/63</td>
<td>-1/63, -17/63, 15/63</td>
</tr>
<tr>
<td>6</td>
<td>$t^3 \left[ [t^3 \left( \alpha' \right) ] \right]$</td>
<td>$f(z)=z^2+z^2+2z^2+1$, $f(z)=z^4+z^4+2z^4+1$</td>
<td>1, -1/63</td>
<td>-1/63, -17/63, 15/63</td>
</tr>
<tr>
<td>9</td>
<td>$t^2 \left[ [t^2 \left( \alpha' \right) ] \right]$</td>
<td>$f(z)=z^2+z^2+1$, $f(z)=z^4+z^4+2z^4+1$</td>
<td>1, -1/511</td>
<td>-1/511, -33/511, 31/511</td>
</tr>
<tr>
<td>9</td>
<td>$t^3 \left[ [t^3 \left( \alpha' \right) ] \right]$</td>
<td>$f(z)=z^2+z^2+2z^2+1$, $f(z)=z^4+z^4+2z^4+1$</td>
<td>1, -1/511</td>
<td>-1/511, -33/511, 31/511</td>
</tr>
<tr>
<td>9</td>
<td>$t^2 \left[ [t^2 \left( \alpha' \right) ] \right]$</td>
<td>$f(z)=z^2+z^2+2z^2+1$, $f(z)=z^4+z^4+2z^4+1$</td>
<td>1, -1/511</td>
<td>-1/511, -33/511, 31/511</td>
</tr>
<tr>
<td>9</td>
<td>$t^3 \left[ [t^3 \left( \alpha' \right) ] \right]$</td>
<td>$f(z)=z^2+z^2+2z^2+1$, $f(z)=z^4+z^4+2z^4+1$</td>
<td>1, -1/511</td>
<td>-1/511, -33/511, 31/511</td>
</tr>
</tbody>
</table>

Fig. 4: (a) The auto-correlation of sequence 1. (b) the auto-correlation of sequence 2

Figure 4 demonstrates that the new sequence has the triple-valued autocorrelation like the Gold sequence. Moreover, since GMW sequences have larger linear complexity than m sequence, then the new sequence also has larger linear complexity than Gold sequence. Most important, with the sequence pair method, we can use limited primitive polynomials to generate some good GMW sequence, then do XOR operation to these GMW sequence and generate many GOLD like sequences, finally we have a family of sequence with GMW-liked linear complexity, triple-valued autocorrelations and small cross-correlations. Moreover, Table 2 provides some examples of GMW Sequence pair, where we explicitly see that cross-correlations of these sequence pairs are triple valued analogous to the optimal chosen m-sequence pair, while Fig. 4 produced by the first and the third rows of Table 2.

CONCLUSIONS

Spread spectrum sequences require excellent correlation performance. Meeting this requirement, the GMW sequence, including its fast generation, has received much attention. Accordingly, this paper performs the GMW sequence generation in ADS software and analyzes their cross-correlation properties, the results show that the cross-correlation of GMW sequences with different trace function parameters is large, hence it can not meet the engineering requirements. Accordingly, after carefully choosing the the GMW sequence pairs with triple-valued cross-correlations, we can generate a series of new sequences from pairs of GMW sequences analogous to GOLD sequence generation, and the simulations confirm its good correlation properties.
ACKNOWLEDGEMENT

This paper is sponsored by science foundation for the excellent youth scholars of Chinese Zhejiang province (2010), Chinese Zhejiang provincial NSF under grant No.Y10906645 (2010-2011) and the open fund of Chinese state key laboratory of information engineering in survey, mapping and remote sensing, Wuhan university, Grant No.(08)03 (2009-2010).

REFERENCES