http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 10 (4): 908-913, 2011
ISSN 1812-5638 / DOI: 10.3923/itj.2011.908.913

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

[1]Lei Tong, [1]Fangfang Chen, [1]Jingyu Hua, [1]Limin Meng and [1,2]Shouli Zhou
[1]Zhejiang Provincial Key Laboratery of Optimam Communication Technology,
Zhejiang University of Technology, Hangzhou, 310023, China
[2]State Key Laboratery 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 spetrum 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, 2009; 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; Kavut *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 (Budaghyan *et al*., 2006; Pin-Hui *et al*., 2007; Izbenko *et al*., 2009; Chen *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 can not 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-corrrelations, 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-corrrelations, which are confirmed by simulation verifications.

BENT SEQUENCE GENERATION

Definition of GMW sequence: In Galois Field (GF), the trace function $tr_J^M(\alpha)$ (with M divisible by J) maps

Corresponding Author: Lei Tong, Zhejiang Provincial Key Laboratery of Optimam Communication Technology, Zhejiang University of Technology, Hangzhou, 310023, China

αelements in GF(2^M) into elements of a subfield GF(2^J), according to the relation:

$$tr_J^M(\alpha) = \sum_{k=0}^{(M/J)-1} \alpha^{2^{Jk}} \quad (1)$$

Then the trace function tr_1^n (x) maps x∈GF(2^n) into GF(2) (Golomb and Gong, 2005). Accordingly, the GMW sequence is defined as:

$$b_t = tr_1^m\left\{\left[tr_m^n(\alpha^t)\right]^k\right\} \quad (2)$$

where, n = m×e and e is any positive integer. In (2), α represents a primitive element of GF(2^n), with $1 \le k \le 2^m$-1 and gcd(k, 2^m-1)=1.

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

- Select a nth-order primitive polynomial f(z) in the GF (2)
- The minimum polynomial of in GF(2^m) as follows:

$$g(z)=(z-)(z^{-q})\ldots(z^{-Q}) \quad (3)$$

where, q = 2^m and Q = q^{e-1}, then $tr_m^n(\alpha^t)$ can be constructed by the minimum polynomial g(z).

- The basis in GF (2^m) is m-dimensional vector space in GF(2), thus the element γ must obey:

$$r = \sum_{i=0}^{m-1} r_i \alpha^{(1+q+\cdots+q^{e-1})i}, \gamma_i \in GF(2) \quad (4)$$

- According to f(α)=0, calculate the elements in GF(2^m): 0,α,(1+q+···+q^{e-1})j, where, j=0,1…, (2^m -2)
- According to Eq. 1 and 4, $tr_1^m(r^k)$ 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:

$$b_t = tr_1^3\left\{\left[tr_3^6(\alpha^t)\right]^3\right\}$$

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(z)=z^6+z^5+z^2+z+1

Step 2: The minimum polynomial of α in GF (2^3) is (z-α)(z-α^8)=z^2+^{54}z+^{9}

Step 3: The elements of GF(2^3) are 0,α^9,α^{18},α^{27},α^{36},α^{45},α^{54} and the basis of GF(8) is {1,α^9,α^{18}}, then the element γ can be expressed as: γ =γ_0+$\gamma_1\alpha^9$+$\gamma_2\alpha^{18}$ with γ_0, γ_1, γ_2∈GF(2)

Step 4: Since α is a root of f(α)=0 and α^6=α^5+α^2+α+1, we have:

$$\begin{aligned}
\alpha^9 &= \alpha^3+\alpha^2+1,\\
\alpha^{18} &= \alpha^6+\alpha^4+1=\alpha^5+\alpha^4+\alpha^2+\alpha,\\
\alpha^{27} &= \alpha^{18}\alpha^9=\alpha^9+1,\\
\alpha^{36} &= \alpha^{18}\alpha^{18}=\alpha^{18}+^9,\\
\alpha^{45} &= \alpha^{27}\alpha^{18}=\alpha^{18}+\alpha^9+1,\\
\alpha^{54} &= \alpha^{45}\alpha^9=\alpha^6+\alpha^4=\alpha^{18}+1
\end{aligned} \quad (5)$$

Therefore, coefficients of minimal polynomial z^2+α^{54}z+α^9 can be written as:

$$\begin{aligned}
\alpha^{54}\gamma &= \gamma_0\alpha^{54}+\gamma_1\alpha^{63}+\gamma_2\alpha^{72}\\
&= (\gamma_0+\gamma_1)+\gamma_2\alpha^9+\gamma_0\alpha^{18},\\
\alpha^9\gamma &= \gamma_0\alpha^9+\gamma_1\alpha^{18}+\gamma_2\alpha^{27}\\
&= \gamma_2+(\gamma_0+\gamma_2)\alpha^9+\gamma_1\alpha^{18}
\end{aligned} \quad (6)$$

Now $tr_3^6(\alpha^t)$ can be constructed by the coefficients of (6).

Step 5: According to, $tr_1^3(r^3) = r^3 + r^6 + r^{12}$, $tr_1^3(r^3)$ and the elements of GF (8) can be computed and presented in Table 1

According to the construction of $tr_3^6(\alpha^t)$ and, $tr_1^3(r^3)$ 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 $tr_3^6(\alpha^t)$ and $tr_1^3(r^3)$ 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(z) will result in different GMW sequence with same periods. Moreover, since the auto-correlations of GMW sequences are

Table 1: The elements of GF(8) and $tr_1^3(r^3)$

γ	γ_0	γ_1	γ_2	$tr_1^3(r^3)$
0	0	0	0	0
1	1	0	0	1
α^9	0	1	0	1
α^{18}	0	0	1	1
α^{27}	1	1	0	0
α^{36}	0	1	1	1
α^{45}	1	1	1	0
α^{54}	1	0	1	0

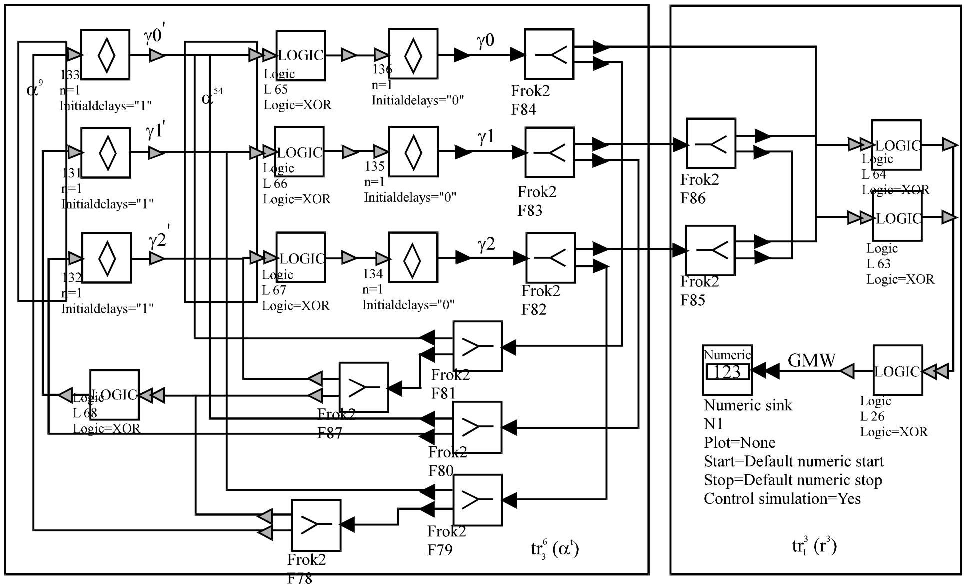

Fig. 1: The schematic diagram of GMW sequence

two-valued as m-sequence, we only simulated the cross-correlations.

The cross-correlation of six-order GMW sequence: According to the above discussion, we construct four six-order GMW sequences, in which GMW6-1 (trace function)

$$tr_1^3\left\{\left[tr_3^6\left(\alpha^t\right)\right]^2\right\}$$

and GMW6-2

$$tr_1^3\left\{\left[tr_3^6\left(\alpha^t\right)\right]^3\right\}$$

are constructed by primitive polynomial $f(z)=z^6+z^5+z^2+z+1$, while GMW6-3

$$\left(tr_1^3\left\{\left[tr_3^6\left(\alpha^t\right)\right]^2\right\}\right)$$

and GMW6-4

$$\left(tr_1^3\left\{\left[tr_3^6\left(\alpha^t\right)\right]^3\right\}\right)$$

are constructed by primitive polynomial $f(z) = z^6+z+1$. 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 conlcude 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 conlcusion, 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 GMW9-1 (with the trace function) and $tr_1^3\left\{\left[tr_3^9\left(\alpha^t\right)\right]^2\right\}$ GMW9-2

$$\left(tr_1^3\left\{\left[tr_3^9\left(\alpha^t\right)\right]^3\right\}\right)$$

are constructed by primitive polynomial $f(z)=z^9+z^4+1$, while GMW9-3

$$\left(tr_1^3\left\{\left[tr_3^9\left(\alpha^t\right)\right]^2\right\}\right)$$

and GMW9-4

$$\left(tr_1^3\left\{\left[tr_3^9\left(\alpha^t\right)\right]^3\right\}\right)$$

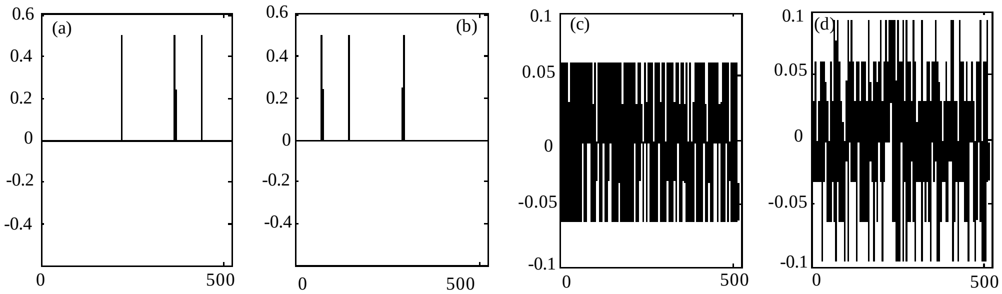

Fig. 2: (a)Tthe cross-correlation of GMW 6-1 and GMW 6-2, (b) the cross-correlation of GMW 6-3 and GMW 6-4, (c) The cross-correlation of GMW 6-1 and GMW 6-3, (d) the cross-correlation of GMW 6-2 and GMW 6-4

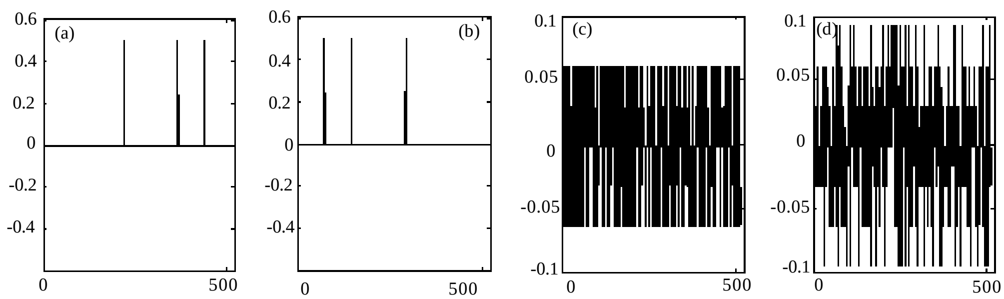

Fig. 3: (a) The cross-correlation of GMW 9-1 and GMW 9-2, (b) the cross-correlation of GMW 9-3 and GMW 9-4, (c) The cross-correlation of GMW 9-1 and GMW 9-3, (d) the cross-correlation of GMW 9-2 and GMW 9-4

are constructed by primitive polynomial $f(z)=z^9+z^6+z^4+z^3+1$.

From Fig. 3, we can clearly conclude that different primitive polynomials lead to large cross-correlation degration. 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$-1/(2^n-1)$、$-(2^{(n+2)/2}+1)/(2^n-1)$ or $(2^{(n+2)/2}-1)/(2^n-1)$ and when n is odd, the value of cross-correlation is$-1/(2^n-1)$、$-(2^{(n+1)/2}+1)/(2^n-1)$ or $(2^{(n+1)/2}-1)/(2^n-1)$.

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 $z^6+z^5+z^2+z+1$ and z^6+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^9+z^4+1 and $z^9+z^6+z^4+z^3+1$. In f act, all pairs of primitive polynomials lead to GMW equences (with trace function) $tr_1^m\left\{\left[tr_m^n(\alpha^t)\right]^r\right\}$ with triple-valued cross-correlations (Golomb 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-velued 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

Sequence Order	Trace function	Primitive polynomials	Autocorrelation	Cross-correlation
6	$tr_1^3\left\{\left[tr_3^6\left(\alpha^t\right)\right]^2\right\}$	$f(z)=z^6+z^5+z^2+z+1$, $f(z)=z^6+z+1$	1, -1/63	-1/63, -17/63, 15/63
6	$tr_1^3\left\{\left[tr_3^6\left(\alpha^t\right)\right]^2\right\}$	$f(z)=z^6+z^5+z^2+z+1$, $f(z)=z^6+z^5+z^3+z^2+1$	1, -1/63	-1/63, -17/63, 15/63
9	$tr_1^3\left\{\left[tr_3^9\left(\alpha^t\right)\right]^2\right\}$	$f(z)=z^9+z^4+1$, $f(z)=z^9+z^6+z^4+z^3+1$	1, -1/511	-1/511, -33/511, 31/511
9	$tr_1^3\left\{\left[tr_3^9\left(\alpha^t\right)\right]^2\right\}$	$f(z)=z^9+z^4+1$, $f(z)=z^9+z^7+z^6+z^4+z^3+1$	1, -1/511	-1/511, -33/511, 31/511
9	$tr_1^3\left\{\left[tr_3^9\left(\alpha^t\right)\right]^2\right\}$	$f(z)=z^9+z^5+z^3+z^2+1$, $f(z)=z^9+z^6+z^4+z^3+1$	1, -1/511	-1/511, -33/511, 31/511
9	$tr_1^3\left\{\left[tr_3^9\left(\alpha^t\right)\right]^2\right\}$	$f(z)=z^9+z^7+z^4+z^2+1$, $f(z)=z^9+z^6+z^4+z^3+1$	1, -1/511	-1/511, -33/511, 31/511

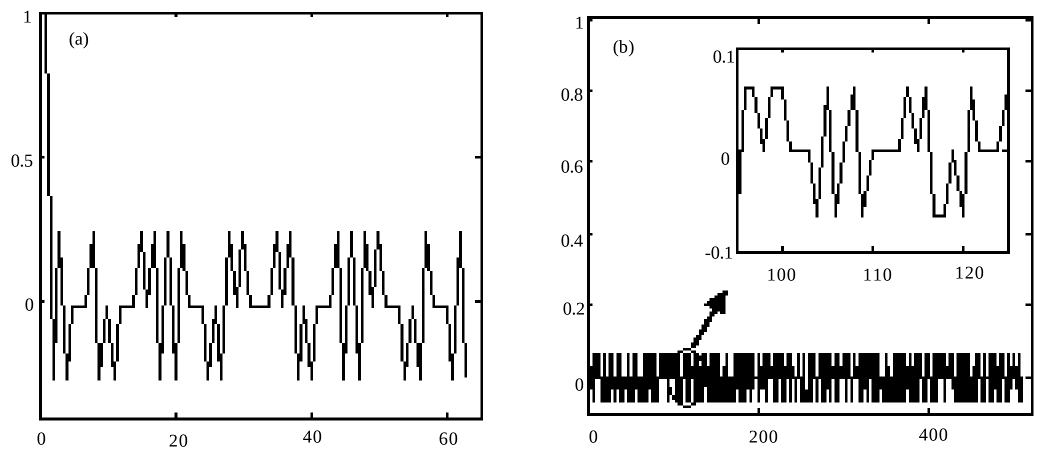

Fig. 4: (a) The auto-correlation of sequence 1, (b) the auto-correlation of sequence 2

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-corrrelations. 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.Y1090645 (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

Britto, K.S.S. and P.E. Sankaranarayanan, 2006. CDMA based optical lan. Inform. Technol. J., 5: 673-678.

Budaghyan, L., C. Carlet and A. Pott, 2006. New classes of almost bent and almost perfect nonlinear polynomials. IEEE Trans. Inform. Theory, 52: 1141-1152.

Chen, F., J. Hua, C. Zhao and S. Zhou, 2010. Fast generation of bent sequence family. Inform. Technol. J., 9: 1397-1402.

Golomb, S.W. and G. Gong, 2005. Signal Design for Good Correlation: For Wireless Communication, Cryptography and Radar. Cambridge University Press, Cambridge.

Helleseth, T. and G. Gong, 2002. New nonbinary sequences with ideal two-level autocorrelation function. IEEE Trans. Inform. Theory, 48: 2868-2872.

Hertel, D., 2005. Crosscorrelation properties of perfect binary sequences. Lecture Notes Comput. Sci., 3486: 208-219.

Izbenko, Y., V. Kovtun and A. Kuznetsov, 2009. The design of boolean functions by modified hill climbing method. Proceedings of the 6th International Conference on Information Technology: New Generations, April 27-29, Las Vegas, Nevada, USA., pp: 356-361.

Kavut, S., S. Maitra and M.D. Yucel, 2007. Search for boolean functions with excellent profiles in the rotation symmetric class. IEEE Trans. Inform. Theor., 53: 1743-1751.

Klapper, A. and C. Cartel, 2004. Spectral methods for cross correlations of geometric sequences. IEEE Trans. Inform. Theor., 50: 229-232.

Mingxin, Z., R. Wenhui, X. Feng, Z. Yatong, J. Shen and Z. Yaling, 2008. A novel CDMA-BLAST space-time code scheme. Inform. Technol. J., 7: 1067-1071.

Pin-Hui, K.E., Z. Jie and W.E.N. Qiao-Yan, 2007. Further study of the trace representation of Bent sequences families. J. Commun., 28: 118-121.

Sengupta, K. and F. Porikli, 2009. Geometric sequence (GS) imaging with byesian smoothing for optical and capacitive imaging sensors. Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops, June 20-25, Cambridge, MA. USA., pp: 90-97.

Tachikawa, S., K. Toda, T. Isikawa and G. Manibayashi, 2007. Direct sequence/spread spectrum communication systems using chip interleaving and its applications for high-speed data transmissions on power lines. Electr. Commun. Jap. Part I: Commun., 75: 46-58.

Tachikawa, S.I., 2007. Recent spreading codes for spread spectrum communication systems. Electr. Commun. Jap. Part I: Commun., 75: 41-49.

Tanimoto, M., H. Sumiyoshi and M. Komai, 2008. Synchronous spread-spectrum multiplex communication system using a modified m-sequence. Electr. Commun. Jap. Part I: Commun., 76: 70-77.

Todorovic, B.M. and V.D. Orlic, 2009. Direct sequence spread spectrum scheme for an unmanned aerial vehicle PPM control signal protection. IEEE Commun. Lett., 13: 727-729.

Wen-Feng, W.J.Q., 2006. Construction of bent sequences and gold-like sequences. J. Electr. Inform. Technol., 28: 81-85.

Yang, T.C. and W.B. Yang, 2008. Performance analysis of direct-sequence spread-spectrum underwater acoustic communications with low signal-to-noise-ratio input signals. J. Acoust. Soc. Am., 123: 842-855.

Zhang, Z.X. and R.F. Hao, 2008. Time-hopping spread-spectrum based on balance gold sequences in ultra-wide band communications. Proceedings of the 4th International Conference on Wireless Communications, Networking and Mobile Computing, Oct. 12-14, pp: 1-5.