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 9 (7): 1397-1402, 2010
ISSN 1812-5638

Fast Generation of Bent Sequence Family

[1]Fangfang Chen, [1]Jingyu Hua, [1]Cheng Zhao and [1,2]Shouli Zhou
[1]College of Information Engineering, Zhejiang University of Technology, Hangzhou, 310032, China
[2]State Key Laboratory of Information Engineering in Survey, Mapping and Remote Sensing, Wuhan University, Wuhan, China

Abstract: In modern spread spectrum communications, how to generate spread spectrum sequence quickly is important in system modeling and design and therefore has received wide attentions. Accordingly, this study investigates the fast generation of Bent sequences, where we use a single generator to generate multiple Bent sequences simultaneously and therefore significantly reduce the realization cost. The proposed fast generator comes from the intrinsic relations between the m-sequence and the Bent sequence, i.e., the m-sequence and its shift versions can construct a trace based generator of Bent sequence family with sequence number approaching $2^{n/2}$. Moreover, we realize such fast generators in Agilent ADS (Advanced Design System) 2005A software and two examples are provided: four order Bent sequence and twelve order Bent sequence. Then, both fast generators are verified by comparing the simulated autocorrelation and crosscorrelation with the corresponding theoretical values and the results prove that the proposed method is effective and beneficial for spread spectrum communications.

Key words: Bent function, fast sequence generation, m-sequence, spread spectrum, ADS2005A

INTRODUCTION

Spread spectrum communication systems have many advantages, such as security, Low Probability of Intercept (LPI) and strong anti-jamming ability. Hence, they had been widely used in modem military communications, accoustic communications and mobile communications (Britto and Sankaranarayanan, 2006; Tachikawa *et al*., 2007; Todorovic and Orlic, 2009; Mingxin *et al*., 2008; Yang and Yang, 2008). Since, the preformance of spread spectrum systems depend on the spread spectrum sequence significantly, studies on spread spectrum sequences have become important topics in spread spectrum systems (Tanimoto *et al*., 2008; Zhang and Hao, 2008; Tachikawa, 2007).

Conventionally, m-sequence and Gold sequence are widely exploited and in order to obtain better correlation properties as well as high security, people also studied m-sequence, GMW sequence and Bent sequence (Golomb and Gong, 2005). Among these sequences, the Bent sequence has large linear complexity, good balance characteristic and excellent pseudo-randomness (Kavut *et al*., 2007; No *et al*., 2003). Moreover, the number of nth-order Bent sequence can approach $2^{n/2}$ and the corresponding cross-correlation (autocorrelation) is triple valued and controllable. Therefore, Bent sequence is a kind of good spread spectrum sequence and receives much attention (Canteaut and Charpin, 2003; Budaghyan *et al*., 2006).

Generally, the study on Bent sequence can be classified as two types: Bent function construction and sequence generation. The former focused on the basic principle of Bent sequence, such as Izbenko *et al*. (2009), Budaghyan *et al*. (2006), Canteaut and Charpin (2003) and Kavut *et al*. (2007), while the latter emphasized on the realization and application of Bent sequence (Guo and Cai, 1993; No *et al*., 2003; Pin-Hei *et al*., 2007; Wen-Feng, 2006). In present study, we focus on the generation of Bent sequence.

Trace transform methods (No *et al*., 2003; Pin-Hui *et al*., 2007; Wen-Feng, 2006) and feed-forward generation method (Guo and Cai, 1993) are two most popular methods to generate Bent sequence. Generally, the trace transform method requires large implementation cost and the feed-forward method must design multiple feed-forward networks to account for multiple sequence generations.

In order to reduce the realization cost, this study presents a simple method to generate a family of Bent sequences (with number $2^{n/2}$), which combines the trace

Corresponding Author: Fangfang Chen, College of Information Engineering, Zhejiang University of Technology, Hangzhou, 310032, China

based method and the feed-forward network method, then produce multiple Bent sequence only through one feed-forward network. In fact, the proposed method exploits the intrinsic relations between the m-sequence and the Bent sequence, i.e., the m-sequence generator (trace based) and its shift versions (feed-forward network) can construct a generator for a certain Bent sequence family. Moreover, we realize such fast generators in Agilent ADS (Advanced Design System) 2005A software and two examples are provided: four order Bent sequence and twelve order Bent sequence. Then, both fast generators are verified by comparing the simulated autocorrelation and crosscorrelation with the corresponding theoretical values and the results validate its effectivity.

BENT SEQUENCE GENERATION

Definition of Bent sequence: In Galois Field (GF), the trace function maps $x \in GF(2^n)$ into GF(2) (Golomb and Gong, 2005):

$$tr_1^n(x) = \sum_{j=0}^{n-1} x^{2^j} \quad (1)$$

Then, the Bent sequence is defined as:

$$S_z(t) = f_z(tr_1^n(r_1\alpha^t), tr_1^n(r_2\alpha^t),....,tr_1^n(r_m\alpha^t))+tr_1^n(x_0^{-1}\alpha^t) \quad (2)$$

where, $z \in GF(2^m)$, $x0 \in GF(2^n)|GF(2^m)$, $n = 2m = 4k$ and k is any positive integer. Moreover, $r_1, r_2....,r_m$ are basises of $GF(2^m)$ over GF(2) and α is a primitive element of $GF(2^n)$.

Given $T = 2^m+1$, α^T is a primitive element of $GF(2^n)$ and $\{\alpha^0, \alpha^T....\alpha^{(m-1)T}\}$ also are basises of $GF(2^m)$. Accordingly, $X_0 = \alpha^{-1} \in GF(2^n)|GF(2^m)$ and Eq. 2 is equivalent to Eq. 3 (Golomb and Gong, 2005):

$$S_z(t) = f_z(tr_1^n(\alpha^t), tr_1^n(\alpha^{t+T}),....,tr_1^n(\alpha^{t+(m-1)T}))+tr_1^n(\alpha\ \alpha^t) \quad (3)$$

Combination of trace transform and feed-forward network: In Eq. 3, we have feed-forward function,

$$f_z(x) = f(x)+z^Tx \quad (4)$$

and m-sequence expression based on trace transform.

$$a_t = tr_1^n(\alpha^t) \quad (5)$$

where, f(x) is a bent function and $a_{t+T} = tr_1^n(\alpha^{t+T})$ is the T-step shift equivalent sequence of m-sequence (a_t), which means that the stage register to output a_{t+T} is T-step ahead that to produce a_t.

From Eq. 1-5, we explicitly see that the key of Bent sequence generation is generating iT-step shift equivalent sequence of m-sequence, where i = 1…m-1. As an example, we take the four order Bent sequence into consideration, i.e., n = 4, m = 2 and $T = 2^m+1 = 5$, then we have the primitive polynomial of the m-sequence x^4+x+1 (Golomb and Gong, 2005). Accordingly, we can derive,

$$\begin{aligned} a_{t+4} &= a_{t+3}+a_t,\ tr_1^n(\alpha^{t+T}) = tr_1^n(\alpha^{t+5}) \\ &= a_{t+5} \\ &= a_{t+4}+a_{t+1} \\ &= a_{t+3}+a_{t+1}+a_t \end{aligned} \quad (6)$$

From Eq. 6, we can obtain the iT-step shift equivalent sequence of m-sequence to generate Bent sequence. Moreover, the derivations in Eq. 6 can be extended to more general cases, i.e., any n. Due to the space limitation, we only provide such analogous derivations of four different n's in Table 1.

According to the previous derivation, we can conclude that the m inputs of $f_z(x)$ are a_t, a_{t+T}, a_{t+2T},… $a_{t+(m-1)T}$

Table 1: iT-step shift equivalent sequence of m-sequence

n	m	$T = 2^m+1$	Primitive polynomial	The T-step shift equivalent sequence
4	2	5	x^4+x+1	$a_{t+5} = a_{t+3}+a_{t+1}+a_t$
8	4	17	$x^8+x^4+x^3+x^2+1$	$a_{t+17} = a_{t+7}+a_{t+4}+a_{t+2}+a_{t+1}+a_t$
				$a_{t+34} = a_{t+7}+a_{t+5}+a_{t+4}+a_{t+3}+a_{t+2}$
				$a_{t+51} = a_{t+6}+a_{t+3}+a_{t+2}+a_t$
12	6	65	$x^{12}+x^6+x^4+x+1$	$a_{t+65} = a_{t+10}+a_{t+9}+a_{t+8}+a_{t+6}+a_{t+5}+a_{t+4}+a_{t+2}$
				$a_{t+130} = a_{t+11}+a_{t+10}+a_{t+4}+a_{t+3}+a_{t+1}$
				$a_{t+195} = a_{t+11}+a_{t+10}+a_{t+9}+a_{t+8}+a_{t+7}+a_{t+4}$
				$a_{t+260} = a_{t+11}+a_{t+10}+a_{t+8}+a_{t+7}+a_{t+6}+a_{t+4}+a_{t+1}+a_t$
				$a_{t+325} = a_{t+11}+a_{t+10}+a_{t+9}+a_{t+8}+a_{t+7}+a_{t+5}+a_{t+1}$
16	8	257	$x^{16}+x^{12}+x^9+x^6+1$	$a_{t+257} = a_{t+15}+a_{t+13}+a_{t+9}+a_{t+7}+a_{t+5}+a_t$
				$a_{t+514} = a_{t+12}+a_{t+8}+a_{t+6}+a_{t+4}+a_{t+2}+a_{t+1}+a_t$
				$a_{t+771} = a_{t+15}+a_{t+13}+a_{t+10}+a_{t+9}+a_{t+8}+a_{t+7}+a_{t+6}+a_{t+4}+a_t$
				$a_{t+1028} = a_{t+15}+a_{t+12}+a_{t+10}+a_{t+9}+a_{t+7}+a_{t+6}$
				$a_{t+1285} = a_{t+15}+a_{t+13}+a_{t+9}+a_{t+7}+a_{t+6}+a_{t+5}+a_{t+4}+a_{t+1}+a_t$
				$a_{t+1542} = a_{t+14}+a_{t+11}+a_{t+8}+a_{t+7}+a_{t+6}+a_{t+4}+a_{t+2}+a_{t+1}$
				$a_{t+1799} = a_{t+15}+a_{t+14}+a_{t+12}+a_{t+9}+a_{t+8}+a_{t+4}+a_{t+3}+a_{t+1}$

and z^Tx denotes the combinations of these inputs. Since z has $2^{n/2}$ values, the number of such a Bent sequence family is $2^{n/2}$.

Fast generation of Bent sequence family: In order to show the generation process clearly, we study the example in the above subsection again, where the Bent function is $f(x) = x_1x_2$. After some tedious derivations, we obtain Table 2, where the inputs a_t, a_{t+5} can replace x_2, x_1 during the generation process and the Bent sequence is obtained by XOR a_{t+1} and the outputs of $f_z(x)$.

It's easy to find in Table 2 that Bent 2 = Bent 1+a_{t+5}, Bent 3 = Bent 1+a_t and Bent 4 = Bent 1+a_t+a_{t+5}. Hence, we conclude that one Bent sequence XOR any combination of a_t, a_{t+T}, a_{t+2T}, …, $a_{t+(m-1)T}$ produces another Bent sequence of the same family. In this way, we can generat $2^{n/2}$ Bent sequences quickly and avoid constructing many feed-forward networks, thus the proposed method is superior to conventional ones (Pin-Hui *et al*., 2007; Wen-Feng, 2006; Guo and Cai, 1993).

Table 2: Four-order Bent sequence (Modulo-2)

z	$fz(x) = f(x)+z^Tx$	Bent sequences
0 0	x_1x_2	Bent 1 = a_t a_{t+5}+a_{t+1}
0 1	x_1x_2+x_2	Bent 2 = a_t a_{t+5}+a_{t+5}+a_{t+1}
1 0	x_1x_2+x_1	Bent 3 = a_t a_{t+5}+a_t+a_{t+1}
1 1	x_1x_2+x_1+x_2	Bent 4 = a_t a_{t+5}+a_t+a_{t+5}+a_{t+1}

BENT SEQUENCE GENERATOR IN ADS2005A

Before detailed descriptions, we must highlight that modelling and simulation are necessary for spread-spectrum systems. Therefore, this section will demonstrate the Bent sequence generator in ADS2005A, which is a popular software in communication modelling and simulation.

Note that Fig. 3 and 4, the X-coordinate and the Y-coordinate denote the sequence shift and the value of correlation, respectively.

Four-order Bent sequence: The schematic diagram of four-order Bent sequence family is shown in Fig. 1, where we exploit two kinds of kernel devices, i.e., delay device (InitDelay) and XOR device (LogicXOR2). In Fig. 1, first we explicitly see that there is only one feed-forward network by which four Bent sequences are produced at the same time and then we can derive the logic relations of Bent 1~4 as:

$$\begin{aligned} &a_{t+5} = a_{t+3}+a_{t+1}+a_t,\\ &\text{Bent 1} = a_t\,a_{t+5}+a_{t+1},\\ &\text{Bent 2} = \text{Bent 1}+a_{t+5},\\ &\text{Bent 3} = \text{Bent 1}+a_t,\\ &\text{Bent 4} = \text{Bent 1}+a_t+a_{t+5} \end{aligned} \tag{7}$$

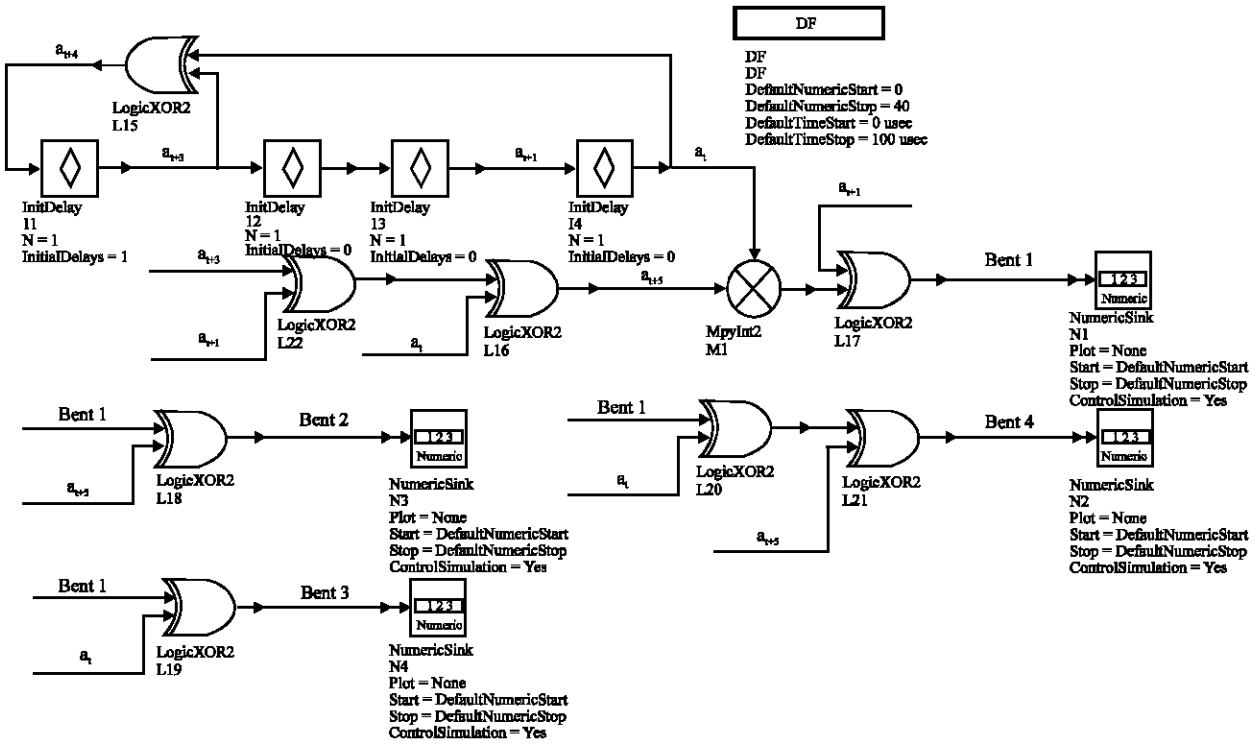

Fig. 1: The schematic diagram of four-order Bent sequence family in ADS2005A

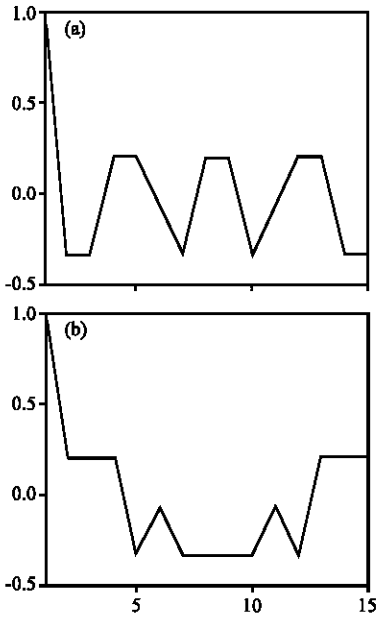

Fig. 2: The auto-correlation characteristics, (a) Bent 1 and (b) Bent 2

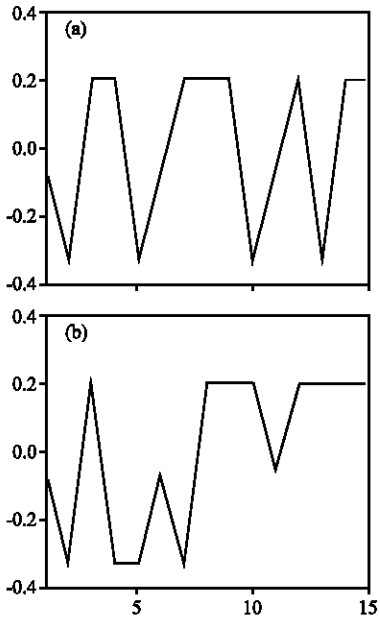

Fig. 3: The cross-correlation characteristics, (a) Bent 1 and 4 and (b) Bent 2 and 3

Besides kernel devices, Fig. 1 also utilizes DF (data flow control device) and NumericSink (data terminal device). In order to verify our design, we further run simulations and compare sequences' auto/cross correlation with corresponding theoretical values. According to previous presentations, the four-order Bent sequence (period fifteen) should have triple-valued auto/cross-correlation sidelobes, i.e., 3/15, -1/15 and -5/15.

Looking at Fig. 2, we find that zero shift causes the largest autocorrelation and non-zero shifts significantly reduce the autocorrelation, where the three sidelobes are valued (3/15, -1/15, -5/15), which is consistent with theoretical results. Meanwhile, Fig. 3 shows the crosscorrelation of different Bent sequences, where X-coordinate denotes shift between two sequences and Y-coordinate represents the values of correlation. From Fig. 3, we can conclude that different Bent sequences produce small crosscorrelations and the crosscorrelation value are triple-valued and consistent with the theoretical result.

Twelve-order Bent sequence: Next, we further construct a twelve-order Bent sequence generator in ADS2005A, where the detailed schematic diagram isn't presented due to the space limitation.

The proposed Bent sequence generator uses the Bent function $f(x)=x_1x_4+x_2x_5+x_3x_6$ and without loss of generality, we only provide results of auto/cross correlation of Bent 5 and 6, where,

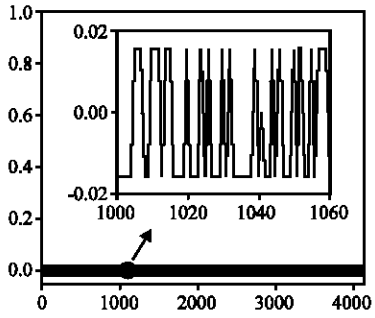

Fig. 4: The autocorrelation of Bent 5

- z = [0 0 0 0 0 0] for Bent 5, results in feed-forward function $f_z(x) = f(x)$
- z = [0 0 0 0 0 1] for Bent 6, results in feed-forward function $f_z(x) = f(x)+x_6$= Bent 5+x_6

Figure 4 and 5 show the autocorrelation of Bent 5 and 6, where we explicitly see that zero shift produces the largest autocorrelation and non-zero shifts produce small and triple-valued autocorrelations, i.e., 63/4095, -1/4095 and -65/4095 as predicted by theoretical analysis. These results prove that the Bent sequence has excellent pseudo-randomness.

Figure 6 shows crosscorrelations of Bent 5 and 6. Though, the sequence shift only ranges from zero to one hundred for the sake of good curve resolution, we point out that other shifts lead to the same results as Fig. 6.

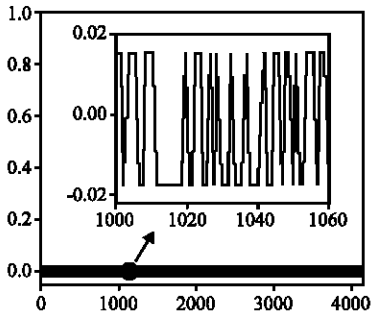

Fig. 5: The autocorrelation of Bent 6

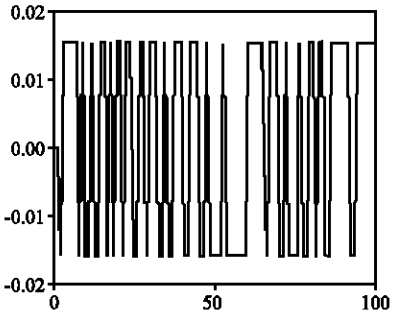

Fig. 6: The crosscorrelation of Bent 5 and 6

From Fig. 6, we explicitly see that Bent sequences have small cross-corrrelations. Most importantly, the crosscorrelation is consistent with the theory derivation, i.e., 63/4095, -1/4095 and -65/4095. Taken into consideration both Fig. 5 and 6, we know that the Bent sequence has excellent autocorrelation and crosscorrelation performance and thus is suitable for spread spectrum communications.

To summarize, the proposed fast generation method constructs a compact architecture to generate $2^{n/2}$ Bent sequences simultaneously, which not only avoids duplication of multiplication, but also eliminates the resource waste of constructing many feed-forward functions. Hence, the proposed method is much simpler than conventional methods (Pin-Hui *et al*., 2007; Wen-Feng, 2006; No *et al*., 2003; Guo and Cai, 1993).

CONCLUSIONS

Spread spectrum sequences require both excellent correlation performance and large sequence numbers. Meeting these requirements, Bent sequence, including its fast generation, has received much attention. Accordingly, this study presents a fast Bent sequence generation method, which can simply and effectively generate many Bent sequences simultaneously. As an application, this method has been implemented and evaluated in ADS2005A, the results show that it can completely achieve the theoretical performance and have a smaller computing load for multiple sequence generation. Furthermore, the Agilent ADS is a powerful design software in wireless system, hence designing Bent sequence generator will benefit the simulation of spread spectrum systems in ADS.

ACKNOWLEDGMENTS

This study is sponsored by science foundation for the excellent youth scholars of Zhejiang province (2010), Zhejiang provincial NSF of China under Grant No. Y1090645 (2010-2011) and the open fund of state key laboratory of information engineering in survey, mapping and remote sensing, Wuhan university, China (No. (08)03).

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.

Canteaut, A. and P. Charpin, 2003. Decomposing bent functions. IEEE Trans. Inform. Theory, 49: 2004-2019.

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

Guo, B.A. and C.N. Cai, 1993. Backforward generation of binary Bent sequences. Acta Electr. Sinica, 21: 101-103.

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.

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.

No, J.S., G.M. Gil and D.J. Shin, 2003. Generalized construction of binary Bent sequences with optimal correlation property. IEEE Trans. Inform. Theor., 49: 1769-1780.

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.

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

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.

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.