A Hardware Oriented Method to Generate and Evaluate Nonlinear Interleaved Sequences with Desired properties

Quynh Le Chi[1] Cuong Nguyen Le[2] Thang Pham Xuan[2]
1. Van Lang University, 45 Tran Khac Nhu, TPHCM, Viet Nam
2. Electric Power University, 235 Hoang Quoc Viet Hanoi, Viet Nam

Abstract
It is well known that the combinatorial structure, algebraic structure and D-transform based method render the nonlinear sequences with good autocorrelation function (ACF) and great linear complexity (LC). However, "all sequences" are not equal even if they are "born" by the same method! In this paper the big inequalities regarding LC of these sequences are shown based on a hardware oriented method (D-transform). In order to get the right sequences some more extensive simulations and trade off are needed. That is why this paper is represented here with above Title.
Keywords: cryptography, mobile communications, security, watermarking, D-transform

1. Introduction

Binary sequences with large length (period), good autocorrelation function (ACF) and great linear complexity (LC) are most desired in such applications like cryptography, mobile communications security, watermarking… [1-6]. A lot of attentions have been paid to this issues. In general the mathematical tools for generating and analyzing such sequences can be classified as:

i. Combinatorial structure [7-12].
ii. Algebraic structure [1,2,3,6,13-15].
iii. The hard ware oriented or D-transform (time multiplexing)[16-19].

It can be seen that while the ACF are more or less the same in all constructions, the LC shows a big differences. The paper is organized like this: after reviewing the main concepts of sequence design in section 2, we will point out the differences in LC in section 3. Then, in the next section, section 4 we will show some trade off and remarks related to sequences selection.

2. Preliminary

For better understanding of problems encountered in selection of sequences, a broad view on sequences design methods is given.

2.1 The combinatorial approach

There is a one-to-one correspondence between cyclic difference sets and almost balanced binary sequences with the autocorrelation property [3,7]. Therefore, constructing all cyclic difference sets is equivalent to finding all almost-balanced binary sequences with the desired autocorrelation property.

Definition 1 [3] *difference set:* A set of distinct integers D={d_1,d_2,…d_k} modulo an integer υ is called integer difference set or difference set denoted by (υ, k, λ) if every integer b≠0 (mod υ) can be expressed in exactly λ way in the form d_i-d_j ≡b(mod υ), where d_i, d_j belong to the integer set D.

Example 1

i / j	1	3	4	5	9
1	0	2	3	4	8
3	9	0	1	2	6
4	8	10	0	1	5
5	7	9	10	0	4
9	3	5	6	7	0

D = {1,3,4,5,9} is a (11, 5, 2) – difference set λ=2.

It is well known [7,11] that CDS characteristic sequence of period υ defined by

$$s(t)=\begin{cases}0 & \text{for } t\in D\\ 1 & \text{for } t\notin D\end{cases} \quad (1)$$

Has the two-level autocorrelation function

$$R_s(\tau)=\begin{cases}\upsilon & \text{for } \tau\equiv 0(\text{mod}\,\upsilon)\\ \upsilon-4(k-\lambda) & \text{otherwise}\end{cases} \quad (2)$$

Example 2
Consider a CDS (15,7,3), and D = {0----5-7--10,11-13,14}.The corresponding sequence S(t) determined by (1) is:

S(t)= 011110101100100 and satisfies (2).

Note: The bit zeros correspond the positions of Digits in D!
Definition2-cyclic Hadamard difference set (CHDS): A cyclic difference set with $\upsilon=4^n-1$, $k=2^n-1$, $\lambda=n-1$ is called a cyclic Hadamard difference set, and it induces a binary sequence of period $\upsilon=4^n-1$ with the ideal autocorrelation, a Hadamard sequence [11,12]. Sequences generated based on CHDS draw a lot of attentions from many authors. These sequences include the well-known m-sequences and GMW sequences, quadratic residue difference set sequences, Hall's sextic residue difference set sequences, twin prime difference set sequences. Among the sequences related to CDS, the binary sequences of length 2^n-1 with two level ideal ACF are most widely used [7-12]. Therefore, our selection is concentrated on this kind of sequences.
Definition 3 CDS with Singer parameters [10,11]: Cyclic difference sets in $GF(2^n)$ with Singer parameters are those with parameters $(2^n - 1, 2^{n-1} - 1, 2^{n-2} - 1)$for some integer *n* or their complements.
Most of cyclic difference sets with Singer parameter were constructed from binary sequences, q-ary m-sequences, q-ary GMW sequences, and q-ary cascaded GMW sequences and therefore are having interleaved structure.
Note that (1) is the necessary and sufficient condition to generate sequences having almost ideal ACF(2).

2.2 Algebraic structure method: Trace function representation and analysis of interleaved Structure:
The concept of trace function is widely used in representing the sequences of length 2^n-1[1-4,7,9,16,20-22], and it is convenient to represent the interleaved structure. Let n= l.m> 1 for some positive integers l and m. The binary *GMW sequence* with these parameters and can be specified as

$b_i = Tr_l^m([Tr_m^n(\alpha^i)]^r)$, i=0,1,2,...

Where α is a primitive element of $GF(2^n)$, and r is any integer relatively prime to $2^m -1$, $1<r<2^m -1$.
Example 3: The CDS and Trace function concepts for interleaved structure
Let consider the CDS(255,127,63). Its characteristic sequence of length 255=15.17 obviously has the interleaved structure. The way to decompose this into 17 subsequences, each of length 15 is represented in [4,10]. The trace representation is closely related to the coset mod 127. The coset leaders in z=127 are:
C_s={1,7,11,13,19,23,29,31,37,43,53,59,61,91,127}
The power series of x in trace representation corresponds to C_1 is {7,11,13,37} which present the GMW sequences of length 255. It's trace form is:
$S(x)=Tr^8{}_1(x^7+x^{11}+x^{13}+x^{37})$.
For C_7={1,19,53,91} the corresponding trace is $S(x)=Tr^8{}_1(x^1+x^{19}+x^{53}+x^{91})$.
In many papers published recently the trace representation are widely used to represent and analyze the sequences LC since it related to maximal sequences, easily implemented by linear feedback shift register (LFSR). However, it is not always easy to express the sequences in trace form .For details please refer to [4,10,11,12].

2.3 D-transfotmation and Technical oriented method
Definition 4 D-transform [2,16,17,18,19]**:** The D-transform of a sequence $\{b_n\}$ over GF(p) is denoted by $D[b_n]$ or F and designed by:

$$D[b_n] = F = \sum_{i=1}^{n} b_i D^i \qquad (3)$$

For example: let $\{b_n\}$ = 010111, D-transform of b_n is $D(b_n)=D+D^3+D^4+D^5$.
The inverse transform of D is $D^{-1}= \{b_n\}$
The D-transform of the generator sequence $\{b_n\}$ of a linear feedback shift register (LFSR) is then given by:

$$b(D) = \frac{S(D)}{G(D)} \qquad (4)$$

Where G(D) of degree n is the generating polynomial of a LFSR and S(D) of degree $\leq$ n -1 specifies the initial condition corresponding to a particular shifted version of $\{b_n\}$. When G(D) is primitive, the LFSR sequence is an m-sequence and there are 2^n-1 polynomials S(D) corresponding to 2^n-1 values of the initial states of that LFSR.
D-transform is based on the delay-operation and therefore most closely related to time-multiplexing technique as compaired to other matematical tools. That is why it is called Hardware oriented method. It can be also easily used to analyze the ACF as well as LC of the sequences [20].
Since all above mentioned methods render sequences with ideal two level ACF, we will just give one example here for reference.

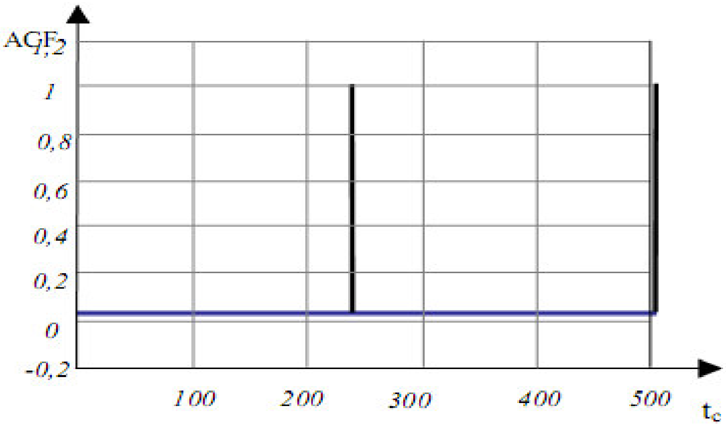

Figure 1. ACF diagram of the sequences pecified by $g(D) = 1 + D + D^2 + D^3 + D^4 + D^5 + D^6 + D^8 + D^9$, length L= 511.

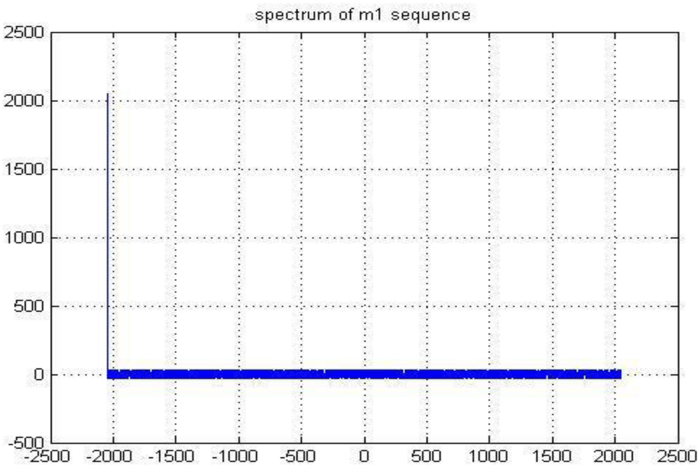

Figure 2. Spectrum of nonlinear interleaved sequence of length L=4096.

3. Profile of linear complexity of interleaved sequences of length 2^n-1

The linear complexity of a periodic sequence is considered as a primary measure of its randomness and strength against Berlekamp–Masey algorithm. Therefore, a lot of efforts have been made to generate sequences not only having good ACF but also large LC (nonlinear).

The nonlinear interleaved sequences having almost ideal ACF is introduced in 1984 by Sholtz and Welch, which turn out to be equivalent to the cyclic difference set of Gordon, Mills and Welchand called GMW sequences [1,2]. In 1985, a method to construct the nonlinear interleaved sequences with best possible ACF is introduced based on quite different approach: D-transformation (time multiplexing technique) and called an m-like sequence. Later on they are shown to be equivalent to GMW sequences [19,20]. However, due to differences in methodology the algorithm for calculation of LC are different.

In algebraic method, the LC of GMW sequence can be calculated either:

(i) By the minimum number of terms in its trace function expression (by the sum of elements in $GF(2^n)$). For example, the GMW sequence of period 63 given by $g(t)=Tr_1^3\left(\{Tr_3^6(\alpha^t)\}^3\right)$ can be expanded as [2,10,13,14,15]:

$$g(t)=Tr_1^6(\alpha^{3t})+Tr_1^6(\alpha^{5t}) = \alpha^{2^0.3t}+\alpha^{2^1.3t}+\alpha^{2^2.3t}+\alpha^{2^3.3t}+\alpha^{2^4.3t}+\alpha^{2^5.3t} +\alpha^{2^0.5t}+\alpha^{2^1.5t}+\alpha^{2^2.5t}+\alpha^{2^3.5t}+\alpha^{2^4.5t}+\alpha^{2^5.5t}$$

and LC=12, since there are 12 terms in that expansion or

(ii) Based on the Hamming weight of the decimation r (which creates the non-linearity) in the expression:

$$b_i = Tr_l^m\left(\left[Tr_m^n\left(\alpha^i\right)\right]^r\right)$$

And is determined as [1,2]: LC= $m.l^{w(i)}$ With l=n/m, w(i) is the Hamming weight of r (decimation).

In D-transform based method, a DFT (discrete fourier transformation) can be used to calculate the LC of periodical sequences [16]:

LC=$w(S^N)$ where w is the Hamming weight of the DFT S^N of the sequence S(t).

This is called Blahut theorem.

It is well known that most of the specific sequence of great length L has interleaved structure since L is composite number in most of the cases (L=T.N). For sequences of interleaved structure two simple operations are introduced before applying Euclid algorithm for LC calculation [17,18,19,20]:

(i) Time division: In the time frame T the consecutive bits of subsequences are separated by T time slots. In D-transform this equivalents to the operation $Z_i(D)=Z_i(d^T)$.

(ii) Timeslot assignment: This operation is equivalent to multiply the subsequences by D^i, therefore $b(D)=\sum_{i=0}^{T-1} d^i Z_i(d^T)$. According to theorem 1[17], if one want to get the nonlinear sequence C_n, $Z_i(d^T)$ must represent the particular phase shift (subsequences) of $\{e_n\}$, specified by I_p^T. Similarly to (4) we put: $Z_i(d^T)=\frac{S_{ei}(d^T)}{G_{es}(d^T)}$, where $S_{ei}(d^T)$ and $G_{es}(d^T)$ represent the initial state and generating polynomial for $\{e_n\}$ respectively. Then: $C(D)=\sum_{i=0}^{T-1} \frac{d^i S_{ei}(d^T)}{G_{es}(d^T)}$.

The Euclid algorithm applied on C(D) renders the least degree polynomial for C (D) and the LC is thus obtained. The simulation and hardware implementation in this paper is completely based on this method. Since the number of primitive polynomials of degree >12 is very large [21], we can only take 70 polynomials for degree n=12, 14 in this appendix. The results are listed in Appendix A.

Appendix A

The first column is the order number.

The second column list the primitive polynomials of degree n=lm, correspond to the sequences of interleaved structure.

The next columns list the polynomials of degree m of the subsequences. The binary values represent the feedback taps of the LFSR.

Remarks1: The set of {LC} It can be seen in Table 1,for n=12, m=6, LC={12,24,48,96,192}. In table 2a,2b,2c, for n=14,m=7 LC={14,28,56,112,224,448} similarly for n=16, m= 8, LC={16,64,128,256,1024}. In general $LC=m.2^{w(r)}$, W(r) is the Hamming distance of r, r being an integer (0<r<m, r is the decimation).

Remark 2: Relationship to subsequences $\{e_n\}$:

- Let $\{a_n\}$ denotes the original subsequences of length 2^m-1 in the interleaved sequence $\{b_n\}$[17,18,19,20].
- Let I_p^T denotes the interleaving order (time multiplexing) of $\{a_n\}$ to create $\{b_n\}$.
- Let $\{e_n\}$ denotes the subsequences of length 2^m-1 replacing $\{a_n\}$.

Then:

1) $LC=LC_{min}$ if $\{e_n\} = \{a_n\}$. That is clear since there is no change (nonlinear effect) in $\{b_n\}$. For n={12,14,16,18}, we have the value LC_{min} ={ 12,14,16,18} (linear).

2) $LC=LC_{max}$ if the hamming weight of r reach the maximal value = {192,448,1024,2304}.

It is clear that the nonlinear effect is created by replacing the subsequences $\{a_n\}$ by $\{e_n\}$ (decimation of $\{a_n\}$ by r) [1,17,18]. However, the effects on LC are not equal and depends on the particular subsequence pair $\{a_n\}$ and $\{e_n\}$! For example in table 1, for n=12, $\{b_n\}$ specified by 1100101000001=$1+D+D^4+D^6+D^{12}$; m=6 and $\{a_n\}$ specified by: 1100001 =$1+D+D^6$ then LC=12(linear). If $\{a_n\}$ is replaced by $\{e_n\}$ specified by 1000011 =$1+D^5+D^6$,then LC=192! a big difference!

4. Run distribution of nonlinear-interleaved sequences

In this section we want to check how far the nonlinear-interleaved sequences satisfy the randomness postulate r-2 about runs distribution. According to R-2 postulates: In every period, half the run have the length 1 (probability = 1/2), one fourth have the length 2 (probability=1/4), one eighth have length 3(probability 1/8) and so on. Here we will give a demonstration for n = 10 and see that the nonlinear interleaved sequences almost satisfied this R-2.

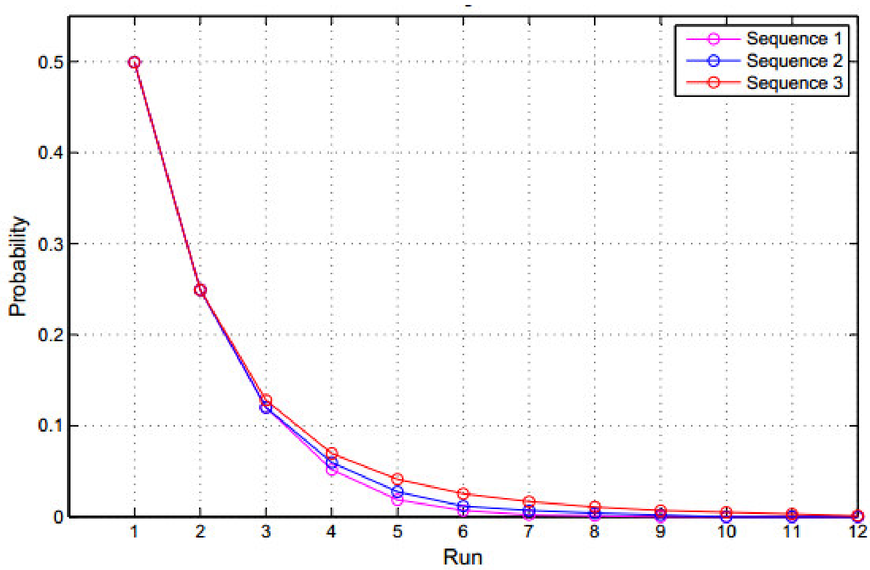

Figure 3. Runs of "0" distribution for

Sequence 1	Sequence 2	Sequence 3
- GF(2^{10}): $1 + d^3 + d^{10}$ - GF(2^5): $1 + d^2 + d^3 + d^4 + d^5$	- GF(2^{10}): $1 + d + d^3 + d^4 + d^{10}$ - GF(2^5): $1 + d + d^2 + d^3 + d^5$	- GF(2^{10}): $1 + d^4 + d^5 + d^8 + d^{10}$ - GF(2^5): $1 + d + d^2 + d^3 + d^5$

Note: All created sequences having LC = 80.

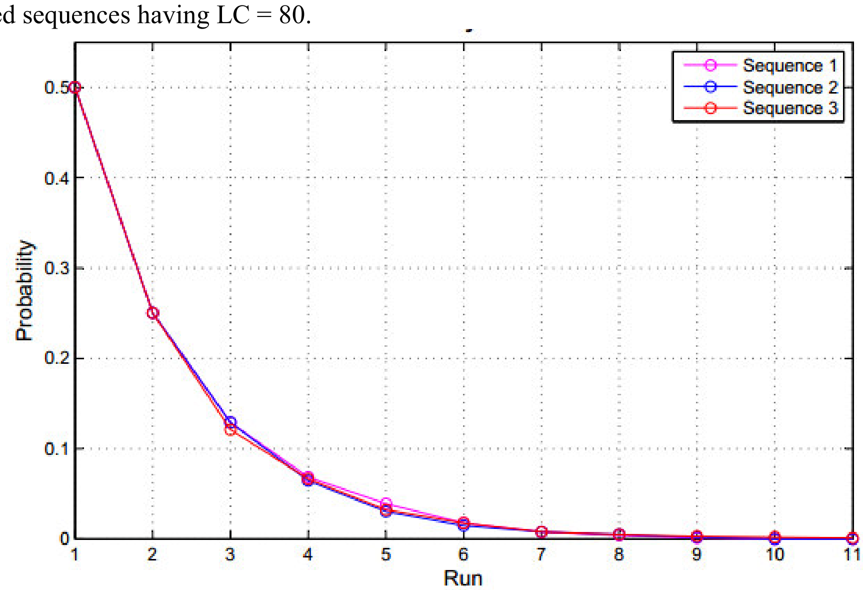

Figure 4. Runs of "1" distribution for the above sequences.

5. Conclusion and Further work

With D-transform the direct connection between the algorithm and the time multiplexing technique can be easily established. Therefore the hardware implementation is clear. It can also be seen that while ACF is identical for any interleaving, the distribution of runs is almost random and the LC shows a great differences! There need be some more investigation and trade off regarding the choice of subsequences. We hope to prove the relation between the decimation r and the linear complexity in the next paper.

We express our gratitude to the reviewer for improving the paper.

References

[1] Fan.P.Z and Darnell.M (1996), "Sequence Design for Communications Applications", New York: Wiley, 1996.

[2] Golomb S. W and. Gong. G (2005), "Signal Design for Good Correlation - for Wireless Communication, Cryptography and Radar", Cambridge University Press, 2005.

[3] Lin. X.D and Chang K.H, (1997), "Optimal PN Sequence Design for Quasi synchronous", IEEE TRANSACTIONS ON COMMUNICATIONS, VOL. 45, NO. 2, FEBRUARY 1997 p 222-226.

[4] Hieu l .M et al (2015), “Design and Analysis of Ternary m-sequences with Interleaved Structure by d-Transform”, Journal of Information Engineering and Applications 8/2015 p 93-101.
[5] A. Patel, B. Kosko (2011), “Noise Benefits in Quantizer-Array Correlation Detection and Watermark Decoding”, IEEE Trans on signal processing, VOL. 59, NO. 2, FEBRUARY 2011, pp 488-505.
[6] M.K.Simon, J.Komura, R.A.Sholz, B.K.Levitt (2002), “Spread spectrum communications Handbook”, McGraw-Hill 2002.
[7] B. Gordon, W. H. Mills and L. R. Welch (1962), “Some new difference sets”, Canad. J. Math., Vol. 14, 1962, pp 614–625.
[8] L. D. Baumert, Cyclic Difference Sets (1971), “Lecture Notes in Mathematics”, Springer Verlag 1971.
[9] C. Ding, T. Helleseth, and W. Shan (1998), “On the linear complexity of Legengdre sequences”, IEEE Trans. Inf. Theory, Vol. 44,N3,1998, pp 1276–1278.
[10] C.-Y. Lai and C.-K. Lo (2002), “Nonlinear orthogonal spreading sequence design for third generation DS-CDMA systems”, IEE Proceeding commun. vol 149 n2 2002, pp 405-410.
[11] J. Kim and H.Y.Song (1999), “Existence of Cyclic Hadamard Difference Sets and its Relation to Binary Sequences with Ideal Autocorrelation”, JOURNAL OF COMMUNICATIONS AND NETWORKS, Vol.1, No.1, MARCH 1999, pp 14-18.
[12] J.No (2004), “New Cyclic Difference Sets with Singer Parameters Constructed from d-Homogeneous Functions Designs”, Codes and Cryptography, 33, pp 199–213, 2004.
[13] A. Klapper, A. H. Chan and M. Goresky (1993), “Cascaded GMW sequences”, IEEE Trans. Information theory, Vol.39,1993, pp 177–18.
[14] Z.Dai, G.Gong, H.Y.Song, D.Ye (2011), “Trace Representation and Linear Complexity of Binary eth Power Residue Sequences of Period P”, IEEE Trans. on information theory, Vol.57, No.3, March 2011, pp 1530-1547.
[15] J.S.No, S.W.Golomb, G.Gong, H.K.Lee, P.Gal (1998), “Binary pseudorandom sequences of period 2^n-1 with ideal autocorrelation”, IEEE Trans. Inf. Theory 44, 1998, pp 814-817.
[16] J.M.Massey, S.Secornek (1998), “A Fourier transform approach to the linear complexity of the nonlinearly filtered sequences”, Swiss fegeral institute of technology 1998 pp 332-340.
[17] L.C.Quynh, S. Prasad (1985), “A class of binary cipher sequences with best possible correlation function”, IEEE Proceeding Part F .Dec 1985. Vol 132, pp 560-570.
[18] L.M Hieu, L.C.Quynh (2005), “Design and Analysis of Sequences with Interleaved Structure by d-Transform”, IETE Journal of Research, vol. 51, no. l, pp 61-67, Jan-Feb. 2005.
[19] N. L Cuong P. X Thang, L.C Quynh (2015), “On the Comparative Study of Some Mathematical Tools for Specific Sequences Design”, Journal of information Engineering and Applications Vol.5, No.12, 2015, pp 1-10.
[20] Cuong.N.L, Hieu L.M and Quynh L.C (2016), “On the relations between D-transform based and other Approach for interleaved sequence design”, submitted to IETE technical Review 4-2016.
[21] Peterson R.Ziemer.R.E,Borth.D.E (1995), “Introduction to spread spectrum communication”, Prentice Hall International 1995.

APPENDIX

Table 1 LC of m-like sequences of length 2^{12}-1

Order	$GF(2^{12})$	$GF(2^6)$					
		1100001	1000011	1101101	1011011	1110011	1100111
1	1100101000001	12	192	48	48	24	96
2	1000001010011	192	12	48	48	96	24
3	1001011000001	192	12	48	48	96	24
4	1000001101001	12	192	48	48	24	96
5	1101111000001	12	192	48	48	24	96
6	1000001111011	192	12	48	48	96	24
7	1011111000001	48	48	24	96	192	12
8	1000001111101	48	48	96	24	12	192
9	1001100100001	192	12	48	48	96	24
10	1000010011001	12	192	48	48	24	96
11	1000101100001	48	48	96	24	12	192
12	1000011010001	48	48	24	96	192	12
13	1101011100001	96	24	192	12	48	48
14	1000011101011	24	96	12	192	48	48
15	1110000010001	24	96	12	192	48	48
16	1000100000111	96	24	192	12	48	48
17	1111100010001	192	12	48	48	96	24
18	1000100011111	12	192	48	48	24	96
19	1100010010001	12	192	48	48	24	96
20	1000100100011	192	12	48	48	96	24
21	1101110010001	12	192	48	48	24	96
22	1000100111011	192	12	48	48	96	24
23	1111001010001	48	48	24	96	192	12
24	1000101001111	48	48	96	24	12	192
25	1110101010001	48	48	96	24	12	192
26	1000101010111	48	48	24	96	192	12
27	1101011010001	48	48	96	24	12	192
28	1000101101011	48	48	24	96	192	12
29	1010000110001	192	12	48	48	96	24
30	1000110000101	12	192	48	48	24	96
31	1100110110001	96	24	192	12	48	48
32	1000110110011	24	96	12	192	48	48
33	1001101110001	96	24	192	12	48	48
34	1000111011001	24	96	12	192	48	48
35	1111101110001	48	48	24	96	192	12
36	1000111011111	48	48	96	24	12	192
37	1011000001001	48	48	24	96	192	12
38	1001000001101	48	48	96	24	12	192
39	1110110001001	48	48	96	24	12	192
40	1001000110111	96	24	192	12	48	48
41	1011110001001	96	24	192	12	48	48
42	1001000111101	24	96	12	192	48	48
43	1110011001001	24	96	12	192	48	48
44	1001001100111	24	96	12	192	48	48
45	1100111001001	48	48	96	24	12	192
46	1001001110011	48	48	24	96	192	12
47	1111111001001	192	12	48	48	96	24
48	1001001111111	12	192	48	48	24	96
49	1001110101001	24	96	12	192	48	48
50	1001010111001	96	24	192	12	48	48
51	1101001101001	96	24	192	12	48	48
52	1001011001011	24	96	12	192	48	48

Order	GF(2^{12})	GF(2^6)					
		1100001	1000011	1101101	1011011	1110011	1100111
53	1111000011001	192	12	48	48	96	24
54	1001100001111	12	192	48	48	24	96
55	1011100011001	48	48	96	24	12	192
56	1001100011101	48	48	96	24	12	192
57	1001110011001	12	192	48	48	24	96
58	1001100111001	192	12	48	48	96	24
59	1111110011001	24	96	12	192	48	48
60	1001100111111	96	24	192	12	48	48
61	1011001011001	24	96	12	192	48	48
62	1001101001101	96	24	192	12	48	48
63	1100010111001	48	48	96	24	12	192
64	1001110100011	48	48	24	96	192	12
65	1110000000101	192	12	48	48	96	24
66	1010000000111	12	192	48	48	24	96
67	1110110000101	24	96	12	192	48	48
68	1010000110111	96	24	192	12	48	48
69	1111001000101	48	48	96	24	12	192
70	1010001001111	48	48	24	96	192	12

Table 2a LC of m-like sequences of length 2^{14}-1

Order	GF(2^{14})	GF(2^7)					
		11000001	10000011	10010001	10001001	11110001	10001111
1	110101000000001	14	448	56	112	28	224
2	100000000101011	448	14	112	56	224	28
3	100111000000001	14	448	56	112	28	224
4	100000000111001	448	14	112	56	224	28
5	110010100000001	224	28	224	28	56	112
6	100000001010011	28	224	28	224	112	56
7	111110100000001	112	56	28	224	28	224
8	100000001011111	56	112	224	28	224	28
9	110111100000001	112	56	112	56	14	448
10	100000001111011	56	112	56	112	448	14
11	100101010000001	448	14	112	56	224	28
12	100000010101001	14	448	56	112	28	224
13	111101010000001	28	224	224	28	56	112
14	100000010101111	224	28	28	224	112	56
15	110111010000001	112	56	56	112	112	56
16	100000010111011	56	112	112	56	56	112
17	101111010000001	14	448	56	112	28	224
18	100000010111101	448	14	112	56	224	28
19	111100110000001	56	112	56	112	112	56
20	100000011001111	112	56	112	56	56	112
21	110101110000001	112	56	28	224	28	224
22	100000011101011	56	112	224	28	224	28
23	110011110000001	224	28	224	28	56	112
24	100000011110011	28	224	28	224	112	56
25	101100001000001	224	28	224	28	56	112
26	100000100001101	28	224	28	224	112	56
27	110010001000001	56	112	112	56	56	112
28	100000100010011	112	56	56	112	112	56
29	110111001000001	56	112	112	56	56	112
30	100000100111011	112	56	56	112	112	56
31	110000101000001	112	56	448	14	224	28
32	100000101000011	56	112	14	448	28	224

Order	GF(2^{14})	GF(2^7)					
		11000001	10000011	10010001	10001001	11110001	10001111
33	110110011000001	28	224	112	56	112	56
34	100000110011011	224	28	56	112	56	112
35	101110011000001	112	56	448	14	224	28
36	100000110011101	56	112	14	448	28	224
37	111001011000001	448	14	112	56	224	28
38	100000110100111	14	448	56	112	28	224
39	101101011000001	28	224	28	224	112	56
40	100000110101101	224	28	224	28	56	112
41	101011011000001	56	112	224	28	224	28
42	100000110110101	112	56	28	224	28	224
43	101010111000001	112	56	56	112	112	56
44	100000111010101	56	112	112	56	56	112
45	100110111000001	112	56	28	224	28	224
46	100000111011001	56	112	224	28	224	28
47	100011111000001	56	112	112	56	56	112
48	100000111110001	112	56	56	112	112	56
49	101100000100001	224	28	224	28	56	112
50	100001000001101	28	224	28	224	112	56
51	111010100100001	56	112	56	112	448	14
52	100001001010111	112	56	112	56	14	448
53	100001100100001	112	56	56	112	112	56
54	100001001100001	56	112	112	56	56	112
55	111111100100001	224	28	224	28	56	112
56	100001001111111	28	224	28	224	112	56
57	101000010100001	448	14	112	56	224	28
58	100001010000101	14	448	56	112	28	224
59	101110010100001	448	14	112	56	224	28
60	100001010011101	14	448	56	112	28	224
61	111000110100001	28	224	224	28	56	112
62	100001011000111	224	28	28	224	112	56
63	110100110100001	224	28	28	224	112	56
64	100001011001011	28	224	224	28	56	112
65	101100110100001	448	14	112	56	224	28
66	100001011001101	14	448	56	112	28	224
67	110001110100001	56	112	56	112	112	56
68	100001011100011	112	56	112	56	56	112
69	100101110100001	56	112	56	112	112	56
70	100001011101001	112	56	112	56	56	112

Table 2b LC of m-like sequences of length 2^{14}-1

Order	GF(2^{14})	GF(2^7)					
		10111001	10011101	11100101	10100111	11010101	10101011
1	110101000000001	224	28	112	56	28	224
2	100000000101011	28	224	56	112	224	28
3	100111000000001	224	28	112	56	28	224
4	100000000111001	28	224	56	112	224	28
5	110010100000001	112	56	112	56	224	28
6	100000001010011	56	112	56	112	28	224
7	111110100000001	112	56	14	448	224	28
8	100000001011111	56	112	448	14	28	224
9	110111100000001	56	112	112	56	56	112
10	100000001111011	112	56	56	112	112	56
11	100101010000001	28	224	56	112	224	28
12	100000010101001	224	28	112	56	28	224

Journal of Information Engineering and Applications
ISSN 2224-5782 (print) ISSN 2225-0506 (online)
Vol.6, No.7, 2016

Order	$GF(2^{14})$	$GF(2^7)$					
		10111001	10011101	11100101	10100111	11010101	10101011
13	111101010000001	56	112	224	28	112	56
14	100000010101111	112	56	28	224	56	112
15	110111010000001	448	14	224	28	112	56
16	100000010111011	14	448	28	224	56	112
17	101111010000001	224	28	112	56	28	224
18	100000010111101	28	224	56	112	224	28
19	111100110000001	28	224	112	56	448	14
20	100000011001111	224	28	56	112	14	448
21	110101110000001	112	56	14	448	224	28
22	100000011101011	56	112	448	14	28	224
23	110011110000001	112	56	112	56	224	28
24	100000011110011	56	112	56	112	28	224
25	101100001000001	112	56	112	56	224	28
26	100000100001101	56	112	56	112	28	224
27	110010001000001	14	448	28	224	56	112
28	100000100010011	448	14	224	28	112	56
29	110111001000001	14	448	28	224	56	112
30	100000100111011	448	14	224	28	112	56
31	110000101000001	224	28	56	112	56	112
32	100000101000011	28	224	112	56	112	56
33	110110011000001	112	56	28	224	112	56
34	100000110011011	56	112	224	28	56	112
35	101110011000001	224	28	56	112	56	112
36	100000110011101	28	224	112	56	112	56
37	111001011000001	28	224	56	112	224	28
38	100000110100111	224	28	112	56	28	224
39	101101011000001	56	112	56	112	28	224
40	100000110101101	112	56	112	56	224	28
41	101011011000001	56	112	448	14	28	224
42	100000110110101	112	56	14	448	224	28
43	101010111000001	448	14	224	28	112	56
44	100000111010101	14	448	28	224	56	112
45	100110111000001	112	56	14	448	224	28
46	100000111011001	56	112	448	14	28	224
47	100011111000001	14	448	28	224	56	112
48	100000111110001	448	14	224	28	112	56
49	101100000100001	112	56	112	56	224	28
50	100001000001101	56	112	56	112	28	224
51	111010100100001	112	56	56	112	112	56
52	100001001010111	56	112	112	56	56	112
53	100001100100001	448	14	224	28	112	56
54	100001001100001	14	448	28	224	56	112
55	111111100100001	112	56	112	56	224	28
56	100001001111111	56	112	56	112	28	224
57	101000010100001	28	224	56	112	224	28
58	100001010000101	224	28	112	56	28	224
59	101110010100001	28	224	56	112	224	28
60	100001010011101	224	28	112	56	28	224
61	111000110100001	56	112	224	28	112	56
62	100001011000111	112	56	28	224	56	112
63	110100110100001	112	56	28	224	56	112
64	100001011001011	56	112	224	28	112	56
65	101100110100001	28	224	56	112	224	28
66	100001011001101	224	28	112	56	28	224

Order	$GF(2^{14})$	$GF(2^7)$					
		10111001	10011101	11100101	10100111	11010101	10101011
67	110001110100001	28	224	112	56	448	14
68	100001011100011	224	28	56	112	14	448
69	100101110100001	28	224	112	56	448	14
70	100001011101001	224	28	56	112	14	448

Table 2c LC of m-like sequences of length 2^{14}-1

Order	$GF(2^{14})$	$GF(2^7)$					
		11111101	10111111	11010011	11001011	11110111	11101111
1	110101000000001	112	56	56	112	56	112
2	100000000101011	56	112	112	56	112	56
3	100111000000001	112	56	56	112	56	112
4	100000000111001	56	112	112	56	112	56
5	110010100000001	56	112	14	448	56	112
6	100000001010011	112	56	448	14	112	56
7	111110100000001	112	56	112	56	112	56
8	100000001011111	56	112	56	112	56	112
9	110111100000001	28	224	224	28	28	224
10	100000001111011	224	28	28	224	224	28
11	100101010000001	56	112	112	56	112	56
12	100000010101001	112	56	56	112	56	112
13	111101010000001	112	56	112	56	448	14
14	100000010101111	56	112	56	112	14	448
15	110111010000001	56	112	224	28	224	28
16	100000010111011	112	56	28	224	28	224
17	101111010000001	112	56	56	112	56	112
18	100000010111101	56	112	112	56	112	56
19	111100110000001	224	28	112	56	28	224
20	100000011001111	28	224	56	112	224	28
21	110101110000001	112	56	112	56	112	56
22	100000011101011	56	112	56	112	56	112
23	110011110000001	56	112	14	448	56	112
24	100000011110011	112	56	448	14	112	56
25	101100001000001	56	112	14	448	56	112
26	100000100001101	112	56	448	14	112	56
27	110010001000001	112	56	28	224	28	224
28	100000100010011	56	112	224	28	224	28
29	110111001000001	112	56	28	224	28	224
30	100000100111011	56	112	224	28	224	28
31	110000101000001	224	28	112	56	56	112
32	100000101000011	28	224	56	112	112	56
33	110110011000001	14	448	224	28	56	112
34	100000110011011	448	14	28	224	112	56
35	101110011000001	224	28	112	56	56	112
36	100000110011101	28	224	56	112	112	56
37	111001011000001	56	112	112	56	112	56
38	100000110100111	112	56	56	112	56	112
39	101101011000001	112	56	448	14	112	56
40	100000110101101	56	112	14	448	56	112
41	101011011000001	56	112	56	112	56	112
42	100000110110101	112	56	112	56	112	56
43	101010111000001	56	112	224	28	224	28
44	100000111010101	112	56	28	224	28	224
45	100110111000001	112	56	112	56	112	56
46	100000111011001	56	112	56	112	56	112

Order	GF(2^{14})	GF(2^7)					
		11111101	10111111	11010011	11001011	11110111	11101111
47	100011111000001	112	56	28	224	28	224
48	100000111110001	56	112	224	28	224	28
49	101100000100001	56	112	14	448	56	112
50	100001000001101	112	56	448	14	112	56
51	111010100100001	224	28	28	224	224	28
52	100001001010111	28	224	224	28	28	224
53	100001100100001	56	112	224	28	224	28
54	100001001100001	112	56	28	224	28	224
55	111111100100001	56	112	14	448	56	112
56	100001001111111	112	56	448	14	112	56
57	101000010100001	56	112	112	56	112	56
58	100001010000101	112	56	56	112	56	112
59	101110010100001	56	112	112	56	112	56
60	100001010011101	112	56	56	112	56	112
61	111000110100001	112	56	112	56	448	14
62	100001011000111	56	112	56	112	14	448
63	110100110100001	56	112	56	112	14	448
64	100001011001011	112	56	112	56	448	14
65	101100110100001	56	112	112	56	112	56
66	100001011001101	112	56	56	112	56	112
67	110001110100001	224	28	112	56	28	224
68	100001011100011	28	224	56	112	224	28
69	100101110100001	224	28	112	56	28	224
70	100001011101001	28	224	56	112	224	28