Features of generation and analysis of pseudorandom sequences and codes based on them

Volodymyr Pelishok
National University
Lviv Polytechnic
Lviv, Ukraine
volodymyr.o.pelishok@lpnu.ua

Ihor Tchaikovskyi
National University
Lviv Polytechnic
Lviv, Ukraine
ihor.b.chaikovskyi@lpnu.ua
ORCID-0000-0003-0653-5121

Olena Horina
Lviv State University of Life Safety
35, Kleparivska Str., Lviv
79007, Ukraine
o.horina@ldubgd.edu.ua

Abstract—The paper analyzes the methods of generating pseudorandom sequences, which are basic for creating more complex sequences - Gold, Kasami and others. Special attention is paid to the generation method using a shift register, the structure of which uses a well-known forming polynomial. It is shown that certain contradictions arise when using the specified method, which can be the reason for obtaining erroneous results during the generation of M-sequences. The cause of these contradictions was investigated and an algorithm for their elimination was developed.

Keywords — M-sequences, Gold, Kasami, shift register with linear feedback, forming polynomials.

1.INTRODUCTION

Broadband systems are widely used in the development of radio communication systems [5, 6]. Their main advantages include:

- less sensitivity to various types of noise and distortions caused by the presence of multi-beam propagation of radio waves;
- the ability to hide and encrypt signals;
- formation of multiple access, in which several users can simultaneously use one frequency band with little mutual interference, etc.

Broadband systems belong to systems with an extended spectrum. One of the options for spectrum expansion is the direct sequence spread spectrum (DSSS) method. At the same time, each bit of primary useful information is matched by several bits of extended useful information that is actually transmitted. The expansion is carried out by using pseudorandom sequences (PRS), which are periodic. The degree of expansion is determined by the PRS length (that is, the number of bits L in one PRS period). For example, if L=15, then instead of one bit of primary useful information, 15 bits of extended useful information are transmitted. When implementing multiple access, an individual PRS is provided for each subscriber, which is characterized by the unique placement of N bits within the period. Then, in the case of receiving extended useful information by several subscribers, only the subscriber to whom it is addressed can extract the primary useful information from it (that is, which knows the individual PRS of this subscriber used by the transmitter).

In general, the PRS is required to fulfill mutually exclusive requirements:

- must contain a random series of binary zeros and ones;
- since the transmitter and receiver (as indicated above) must have their copies, the PRS generation must be carried out according to a certain algorithm.

Such an algorithm is deterministic, so the generated PRSs cannot be statistically random. But, with a sufficiently justified choice of the specified algorithm, the obtained PRS can successfully pass a number of randomness tests. That is why the considered sequences are called PRS. Next, such PRSs are considered, which are most often used in extended spectrum communication systems.

Among them, M-sequences (a maximum length sequence-MLS) occupy a particularly important place. They are used both as separate PRSs and basic for generating more complex PRSs (Gold codes, Kasami, etc.).

The most efficient way to generate MLS is to use maximal linear-feedback shift registers. The resulting sequences can appear almost random over a long enough time interval, causing a noise-like signal to form. In addition, shift registers are easy to implement at the hardware level. They can operate at quite a high speed, which is extremely important, since the expansion rate is much higher than the required data transfer rate. It is known that the output signal of the shift register is periodic.

It is always possible to form such a structure of the shift register, in which the period of the generated sequence is determined according to dependence (2). The sequence generated in this case is MLS.

The degree of similarity of signals can be characterized on the basis of their correlation functions. It is known [7] that the autocorrelation function of the MLS (one sharp peak) significantly simplifies the synchronization of the receiver.

More complex MLSs are even more effective. For example, with n=13 ($L=2^{13}$ -1= 8191), the cross correlation function of two MLS is 703. Similarly (with n=13), the specified function for Gold sequences is 129.

But during the generation of PVP, certain problems arise, which are discussed below.

2. CRITERIA FOR EVALUATING SEQUENCES BELONGING TO THE MLS

Below are some digital sequences (1), which at first glance are random, and possibly belong to the class of MLS.

011001, 0110010, 011001010 (1)

All of them contain a different length L (the number of chips), which can take one of two values (0 or 1).

It is obvious that, according to the title of this paper, it is primarily of interest to determine whether they belong to MLS. For this, certain criteria are known [1] (Fig. 1).

Main (based on length L)	Additional (based on chip series placement)

Fig. 1. Criteria for detection of MLSs

But, even if a specific sequence satisfies the criteria (Fig. 1), it may not belong to MLS. The primary requirement is its periodicity, and the analyzed fragment is one of the periods of this sequence.

The length L of the M-sequence must satisfy the following condition

$$L=2^n-1 \quad (2)$$

where: n>1 is an integer.

Table 1 shows data on the length L for certain values of n.

TABLE 1. DATA ON THE LENGTH L FOR CERTAIN VALUES OF N

n	***2***	***3***	***4***	***5***	***6***	***7***	***8***	***9***	***10***
L	3	7	15	31	63	127	255	511	1023

Based on the data (Table 1), it is possible to make a obvious conclusion - the length of the MLS is always odd. That is, the first of sequences (1), for which L=6, belongs to MLS. Also, the third sequence in (1), for which L=9 (this value is not in table 1), does not belong to MLS.

It can be seen that the length L of each subsequent MLS is significantly greater than the length of the previous one (almost twice). This belongs to certain disadvantages of MLS. For example, a situation is possible when, for a certain communication system, it is sufficient to use MLS with a length of L of at least 600. In reality, in this case (according to Table 1), a much more complex sequence with a length of L=1023 will have to be used.

Additional criteria (Fig. 1) are as follows:

- the quantity of 1 is greater than the quantity of 0 by one unit;
- there is one series of 1 of length n, one series of 0 of length n-1, one series of 0 and 1 of length n-2 each, two series of 0 and 1 of length n-3 each, and 2^{n-1} series of 0 and 1 of length 1 each.

Although the second sequence in (1) contains the permitted length (L=7) according to Table 1, the number of 0s in it is greater than the number of 1s, which indicates that it does not belong to the MLS.

A different situation is possible when analyzing MLS. For example, the following PRSs are available

0010110011111000110111010100001

1000010010110011111000110111010 (3)

0100011101111100100110000101101

All of them, according to the criteria (Fig.1), belong to MLS. But the question arises - these are different MLSs, or some of them represent one and the same sequence (but the beginning of reading starts from different places). Obtaining the required answer, with a significant length of sequences, is quite time-consuming. For the sake of simplification, it is suggested to "reformat" the sequence data as follows - so that they all start with the series that contains the largest number of 1s (in this case, 11111)

1111100011011010100000100101100

1111100011011010100000100101100 (4)

1111100100110000101101010001110

From the obtained results of "reformatting" (4), it is clearly visible that the first two MLSs are actually one and the same sequence, and the last sequence is really different.

3. MLS GENERATION

The physical (hardware) generation of each MLS of the required length L (2) is carried out by a separate linear feedback shift register, LFSR [1]. It belongs to digital automata, which provides one of the main requirements for the obtained MLS - its periodicity. The main components of a shift register that generates an M-sequence of length L are the following:

- a line of serially connected n triggers (which perform the function of memory cells);
- a line of serially connected r (r<n) modulo 2 adders, which form a feedback channel;
- generator of clock pulses, when they are simultaneously applied to each trigger, the input signal of the trigger is moved to its output.

Fig. 2 shows one of the possible variants of the structure of LFSR, which can only potentially (but not necessarily) generate the MLS of length L=15. In order to generate the required M-sequence in the shift register, a necessary and sufficient condition must be fulfilled. The necessary condition is to satisfy requirement (2), which is fulfilled for this register (that is, it contains n=4 triggers). A sufficient condition is the correct choice of the structure of the feedback channel.

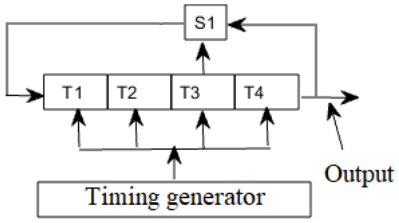

Fig. 2. One of the possible variants of the shift register for generating the MLS (L=15)

Feedback is carried out through one (or several serially connected) module 2 adders. Similarly, the output signal of the previous adder is the input signal of the next adder. The output signal of the last trigger must be fed to one of the inputs of the first adder, and the output of the last adder is fed to the input of the first trigger. The value of the output signal of the module 2 adder is given in Table 2.

TABLE 2. THE VALUE OF THE OUTPUT SIGNAL

a	**b**	**mod2(a,b)**
0	0	0
0	1	1
1	0	1
1	1	0

Timing pulses are applied to the shift register at certain time intervals. When each timing pulse is applied, the signals in the shift register move one chip to the right. In the time intervals between the supply of timing pulses, the shift register is characterized by a certain state - that is, the value of the signals (0 or 1) at the output of each of the triggers.

The choice of the structure of the feedback channel is quite complicated, therefore, several methods of its implementation

have been developed. One of the simplest, which does not require additional information (except for the one given in condition (2) and Table 1), is the method proposed in [3]. It consists of the following:

- a shift register is used in which the necessary condition (2) is fulfilled;
- one of the possible feedback options is formed;
- the sequence is generated using this shift register;
- on the basis of condition (2) and criteria (Table 1), it is determined whether the obtained sequence belongs to the MLS.

Table 3 shows an example of sequence generation using a shift register (Fig. 2)

TABLE 3. SEQUENCE GENERATION USING A SHIFT REGISTER

State number	Shift register status				mod 2 (T4, T3)	Output
	T1	T2	T3	T4		
1 (Beginning)	1	1	1	0	1	0
2	1	1	1	1	0	1
3	0	1	1	1	0	1
4	0	0	1	1	0	1
5	0	0	0	1	1	1
6	1	0	0	0	0	0
7	0	1	0	0	0	0
8	0	0	1	0	1	0
9	1	0	0	1	1	1
10	1	1	0	0	0	0
11	0	1	1	0	1	0
12	1	0	1	1	0	1
13	0	1	0	1	1	1
14	1	0	1	0	1	0
15	1	1	0	1	1	1
16 (The same as 1 state)	1	1	1	0	1	0

A special question has an initial state before the clock pulses are applied. It can be arbitrary, except for "zero" at the output of each of the triggers. In this case, when applying an arbitrary number of clock pulses, the output of the shift register is always 0, which is of no practical interest. In this case (Table 3), the initial state is provided in the form of 1110.

After applying each clock pulse, the initial state must change, which is true for state numbers 1..15 (Table 3). Until such a change occurs, sequence generation continues. However, after sending a certain number of clock pulses, the state of the shift register will necessarily be received, which was already encountered when the clock pulses were previously sent (in this case, #16 of the state of the register corresponds to #1). Then sequence generation stops. It can be seen that the following sequence of length L=15 is obtained.

$$B = [011110001001101] \quad (5)$$

When the following timing pulses are applied, the already obtained (5) sequence is periodically repeated.

The sequence (5), length L=15, is obtained using a shift register containing 4 triggers (i.e. n=4). and corresponds to dependence (2). Thus, the resulting sequence can be considered as MLS. In addition, it meets all additional requirements (Fig. 1), and therefore really belongs to the MLS..

In general, when using M-sequences, a significant number of them is required. Therefore, using the shift register (Fig. 2), with n=4 one can hope to obtain a different, compared to (3) MLS with length L=15.

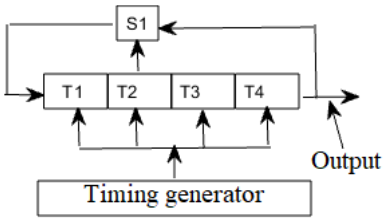

Fig. 3. Another possible variant of the shift register for generating the MLS (L=15)

Table 4 shows the results of sequence generation using this shift register at the initial state of 1110.

TABLE 4. THE RESULTS OF SEQUENCE GENERATION

State number	Shift register status				mod 2 (T4, T2)	Output
	T1	T2	T3	T4		
1 (Beginning)	1	1	1	0	1	0
2	1	1	1	1	0	1
3	0	1	1	1	0	1
4	0	0	1	1	1	1
5	1	0	0	1	1	1
6	1	1	0	0	1	0
7 (The same as 1 state)	1	1	1	0	1	0

In this case, with n=4, the following periodic sequence of length L=6 is obtained

$$D = [011110] \quad (6)$$

The obtained sequence does not satisfy the condition (2), therefore it is not MLS.

Thus, the considered method has a number of advantages and disadvantages. The advantages include the fact that after analyzing (analogous to table 3, table 4) all possible variants of feedback in the shift register, at a given value of n, it is possible to obtain all variants MLS of length L (2). The disadvantages include the fact that this method is not very effective. At the same time, it is necessary to carry out a time-consuming analysis (similarly to Table 3, Table 4) of a significant number of possible feedback structures, as a result of which only a small number of MLS can actually be obtained.

4. CONTRADICTION DURING THE GENERATION OF MLS AND THEIR ELIMINATION

A more effective way of generating MLS is proposed in [1,2]. At the same time, forming polynomials (FP) are used to construct the structure of the feedback channel. For example, with n=4, there are two FPs.

$$1+X+X^4 \quad (7,a)$$

$$1+X^3+X^4 \quad (7,b)$$

A complete list of FPs, at different values of n, is given in [4].

FPs indicate which trigger signals form the feedback channel. There are certain signal designations for each trigger. But different authors interpret in different ways, which causes certain contradictions.

For example, in [1], the placement of signals in the shift register is accepted as follows

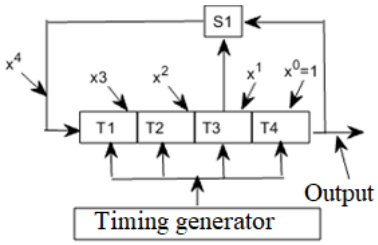

Fig. 4. The shift register, formed on the basis of the FP $1+X+X^4$ with increasing powers of the addends of the FP "from right to left".

It can be seen that in this case (Fig. 4) the signals marked as "x^4", "x", "1" are involved in the feedback channel. Such addends are in FP (7,a). Therefore, in [1] it is indicated that the shift register (Fig. 4, similar to Fig. 2) is formed on the basis of FP (7,a).

On the contrary, in [2], the placement of signals in the shift register is accepted according to (Fig. 5).

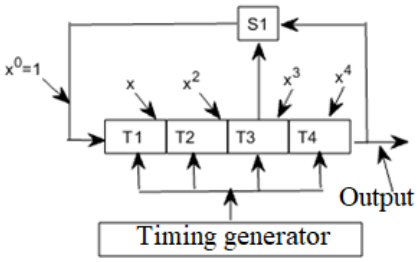

Fig. 5. The shift register formed on the basis of FP $1+X^3+X^4$ with increasing powers of the addends of the FP "from left to right".

It can be seen that in this case (Fig. 5) the signals marked as "x^4", "x^3", "1" are involved in the feedback channel. Such the addends are present in the FP (7,b). Therefore, it is indicated in [2] that the shift register (Fig. 5, similar to Fig. 2) is formed on the basis of FP (7, b).

Thus, one of the variants (Fig. 4, Fig. 5) of forming the structure of the shift register based on the known FP is erroneous. At the same time, there are a number of significant shortcomings (Fig. 6) related to MLSs.

1. When using two different FP, one sequence will be obtained (it is not known how to obtain the second).	2.It is also unknown on the basis of which FP a specific sequence was obtained, which makes it impossible to use it for the generation of Gold codes (which uses MLS obtained only on the basis of known recommended FPs).

Fig. 6. Disadvantages of MLS generation caused by existing contradictions

Therefore, the problem of detecting a false result and developing recommendations for the correct formation of the structure of the shift register based on the known FP is relevant. First, it is necessary to find out what MLS can actually be obtained when using each of the FPs (for example, 7a and 7b).

It is known [1] that based on the analysis of the used FP, it is possible to unambiguously determine the actually obtained MLS - as the value of the inverse of the FP.

For example, when using an FP of the form $1+X^3+X^4$, the actually obtained MLS is defined as $1/(1+X^3+X^4)$. The division procedure is shown in Fig. 7, as a result of which it is obtained

$$1 + 0*X + 0*X^2 + 1*X^3 + 1*X^4 + 0*X^5 + 1*X^6 + 0*X^7 + 1*X^8 + 1*X^9 + 1*X^{10} + 1*X^{11} + 0*X^{12} + 0*X^{13} + 0*X^{14} \quad (8)$$

This means that when using the FP of the form $1+X^3+X^4$, the following periodic MLS of length L=15 is obtained

$$G=[100110101111000] \quad (9)$$

It should be noted that the division was not carried out in a completely usual way, which takes into account the peculiarities of using modulo 2 operations.

$$\begin{array}{l|l} 1 & 1+X^3+X^4 \\ - & \hline 1 + 0*X + 0*X^2 + 1*X^3 + 1*X^4 + \\ 1+X^3+X^4 & 0*X^5 + 1*X^6 + 0*X^7 + 1*X^8 + 1*X^9 + \\ \hline X^3+X^4 & 1*X^{10} + 1*X^{11} + 0*X^{12} + 0*X^{13} + 0*X^{14} \end{array}$$

$$\begin{array}{l} - \\ X^3 + X^6 + X^7 \\ \hline X^4 + X^6 + X^7 \\ - \\ X^4 + X^7 + X^8 \\ \hline X^6+X^8 \\ - \\ X^6 + X^9 + X^{10} \\ \hline X^8 + X^9 + X^{10} \\ - \\ X^8 + X^{11} + X^{12} \\ \hline X^9 + X^{10} + X^{11} + X^{12} \\ - \\ X^9 + X^{12} + X^{13} \\ \hline X^{10} + X^{11} + X^{13} \\ - \\ X^{10} + X^{13} + X^{14} \\ \hline X^{11} + X^{14} \\ - \\ X^{11} + X^{14} + X^{15} \\ \hline X^{15} \\ - \\ X^{15} + X^{18} + X^{19} \\ \hline X^{18} + X^{19} \end{array}$$

Fig. 7. The result of division $1/(1+X^3+X^4)$

Similarly, when using a FP of the form $1+X+X^4$, the formed MLS is defined as the result (10) of division $1/(1+X+X^4)$.

$$1 + 1*X + 1*X^2 + 1*X^3 + 0*X^4 + 1*X^5 + 0*X^6 + 1*X^7 + 1*X^8 + 0*X^9 + 0*X^{10} + 1*X^{11} + 0*X^{12} + 0*X^{13} + 0*X^{14} \quad (10)$$

This means that when using the FP of the form $1+X+X^4$, the following periodic MLS of length L=15 is obtained.

$$H=[111101011001000] \quad (11)$$

The results of the analysis of the indicated contradictions are given in Table 5.

TABLE 5. THE ANALYSIS OF THE INDICATED CONTRADICTIONS

	Result
The actual MLS, obtained as the inverse of the FP, that is $1/(1+x^3+x^4)$	100110101111000 (9) or after reformatting 111100010011010
Generated on the basis of FP $1+x^3+x^4$ by the shift register of Fig. 5, (analogous to Fig. 2), in which powers the addends of the FP increase "from left to right"	011110001001101 (5) or after reformatting 111100010011010, that is corresponds to the actual
Generated on the basis of FP $1+x+x^4$ by the shift register of Fig. 4, (analogous to Fig. 2), in which powers of the addends of the FP increase "from right to left"	111101011001000 (11), that is no corresponds to the actual

Thus, it is shown that the shift register (Fig. 2) can be obtained only on the basis of the FP of the form $1+x^3+x^4$, and the powers of the addends of the FP in this register increase "from left to right" (Fig. 5). That is, with respect to the indicated contradictions, the result given in [2] is correct, and in [1] it is wrong.

Using a similar algorithm, the structure of wrong shift register (Fig. 4) can be adjusted in the manner (Fig. 7).

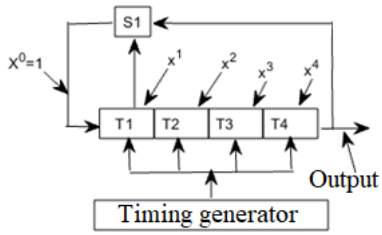

Fig. 7. The shift register formed on the basis of FP $1+X+X^4$ with increasing powers of FP addends "from left to right"

It can be seen that in this case (Fig. 7) the signals marked as "x^4", "x", "1" are involved in the feedback channel. Such addends are present in the FP (7,a).

Table 6 shows an example of sequence generation using a shift register (Fig. 7).

Thus, in this case, the following sequence is obtained

$$Q = [011110101100100] \quad (12)$$

The results of the MLS generation analysis using FP of the type $1+x+x^4$ are given in Table 5. It can be seen that in this case, the shift register (Fig. 7) generated an actual MLS, which is provided by the FP of the form $1+x+x^4$.

Thus, using this algorithm, the wrong result given in [1] was corrected. The shift register (Fig. 4) was changed to the correct one (Fig. 7).

TABLE 6. AN EXAMPLE OF SEQUENCE GENERATION USING A SHIFT REGISTER

State number	**Shift register status**				**mod 2 (T4, T3)**	**Output**
	T1	**T2**	**T3**	**T4**		
1 (Beginning)	1	1	1	0	1	0
2	1	1	1	1	0	1
3	0	1	1	1	1	1
4	1	0	1	1	0	1
5	0	1	0	1	1	1
6	1	0	1	0	1	0
7	1	1	0	1	0	1
8	0	1	1	0	0	0
9	0	0	1	1	1	1
10	1	0	0	1	0	1
11	0	1	0	0	0	0
12	0	0	1	0	0	0
13	0	0	0	1	1	1
14	1	0	0	0	1	0
15	1	1	0	0	1	0
16 (The same as 1 state)	1	1	1	0	1	0

The results of the analysis are given in Table 7.

TABLE 7. THE RESULTS OF THE ANALYSIS

	Result
The actual MLS, obtained as the inverse of the FP, that is $1/(1+x^1+x^4)$	111101011001000 (11)
Generated on the basis of FP $1+x+x^4$ by the shift register of Fig. 7, in which powers of the addends of the FP increase "from left to right"	011110101100100 (12) or after reformatting 111101011001000, that is no corresponds to the actual

CONCLUSIONS

1. It is shown that in a number of works there is an erroneous formation of the structure of the shift register obtained on the basis of the known FP of the form $1+x+x^2+x^3+...x^n$.

2. For the correct formation of the specified structure, the following algorithm is recommended:

- for each of the possible addends of the FP ($x^0+x+x^2+x^3+...x^n$) indicate its location points in the triggers of the shift register, and the power of the addends should increase "from left to right" (for example, Fig. 5 when using the FP of the 4th power) ;
- for the feedback loop, use signals from those points that correspond to the addends in the given FP (for example, Fig. 5 when using the FP of the form $1+x^3+x^4$.

REFERENCES

[1] William Stallings. Wireless Communications and Networks. 2nd Edition, Pearson College, 559 p. 2004.

[2] I. A. Hepko, V. F. Oleynyk, Yu. D. Chaika, A. V. Bondarenko. Modern wireless networks: state and development prospects. - K.: "EKMO", 2009. - 672 p.

[3] Bernard Sklar. Digital Communications: Fundamentals and Applications. Pirson Prentice Hall, ISBN-10: 0-13-458856-8,2013.

[4] Varakin L. E. Communication systems with noise-like signals. - M.: Radio and communication, 1985. - 384 p.

[5] Ipatov V. Broadband systems and code division multiplexing. Principles and applications. - M.: Tekhnosfera, 2007. –488 p.

[6] Volkov L. N. Digital radio communication systems: basic methods and characteristics: textbook / Volkov L. N., Nemirovsky M. S., Shinakov Yu. S. - M .: Eco-Trends, 2005. - 392 p.