Comparative analysis of pseudorandom sequences using modified Barker codes and M – sequences of the same length

Tatyana Sestacova, Gherman Sorochin

Technical University – Kishinev, The Republic of Moldova
E-mail: ger_sor@mail.ru

Abstract: *The paper discusses the correlation properties of pseudo-random sequences (PRS) used to form noise-like signals in high-speed data transmission systems. The most frequently used pseudo-random sequences are considered: modified Barker codes, M-sequences having the same length. In the Matlab medium a comparative analysis of the correlation properties of the PRS is done. It is shown, that modified Barker codes have unsatisfactory correlation properties. It is proved, that the use of M - sequences allows to obtain signals with the required correlation properties for communication systems, including systems with code division of channels. The directions of further research are determined.*

KEYWORDS: *NOISE-LIKE SIGNAL, PSEUDO-RANDOM SEQUENCES, MODIFIED BARKER CODES, M-SEQUENCES, AUTOCORRELATION FUNCTION, CROSS-CORRELATION FUNCTION*

1. Introduction

Currently, in radio systems (RS) is increasingly used a broadband (BB) signals or as they also called noise-like (NL) signals, which are based on pseudo-random sequences (PRS) [1-5]. Depending on the size of the alphabet and the method of construction, binary (size of the alphabet p = 2) and multi-value (size of the alphabet p > 2) PRS are distinguished.

Communication systems with NL signals are widely used for three reasons:

Firstly, the broadband signals generated by different PRSs can have the same center frequency, i.e. be transmitted in the same band.

The second reason why the use of NL signals is very profitable is its high resistance to the effects of both broadband and narrowband interference, which is very important in conditions of a tense electromagnetic environment in modern communication systems.

The third reason is the high energy secrecy of systems with NL signals and, as a result, the high confidentiality of the transmitted data. The essence of the above is that a broadband signal is not only difficult to decode - it is difficult to simply detect, i.e. identify the fact of the subscriber station.

In RS channels, as a rule, either a signal detection task or a signal discrimination task can be solved, which can be considered as a special case of the detection problem.

To solve these problems, the correlation technique should be applied in an optimal way. The correlation technique is the more effective, the more complex is the useful signal [7, 9].

The best signals are those in which the ratio of the main peak of the autocorrelation function (ACF) to the lateral is the largest.

However, most of the PRS, which found practical application in broadband systems, is not free from a number of disadvantages.

These and other factors prompt not only to search for ways to optimize ensembles of sequences with acceptable correlation properties, but also to explore new classes of SRP with the required correlation properties.

2. Preconditions and means for resolving the problem

2.1. Theoretical part

It is known that the rate of information transmission over the communication channel with additive Gaussian white noise is determined by the Shannon-Hartley theorem:

$$C = W_s \log_2\left(1 + \frac{P_s}{P_n}\right), \qquad (1.1)$$

where Ws is the bandwidth of the communication channel (Hz),

Ps is the average signal power (W),

Pn is the average noise power (interference) (W).

From “Eq. (1)” it follows that the same bandwidth C (bit / s) of the communication channel can be provided either by using a wide bandwidth Ws (Hz) with a small signal-to-noise ratio Ps/Pn, or - a narrow band Ws with higher signal-to-noise ratio Ps/Pn. Consequently, between the bandwidth of the communication channel W_s and the signal-to-interference ratio P_s/P_n interchange is possible.

An important parameter of a system using noise-like signals is processing gain. The processing gain (PG) shows the degree of improvement of the signal-to-noise ratio when converting the noise-like signal received by the receiver into the desired information signal. According to the classical definition, PG is equal to:

$$PG = 10\log (C_{ch}/C_{inf}), \qquad (1.2)$$

where Cch is the repetition rate of the pseudo-random sequence chips, chip/s.,

Cinf - information transfer rate, bits/s.

By this definition, a system that has a data transfer rate of 1 Mbps. and a chip repetition rate of 13 Mchip/s. (this means that each bit of information is encoded by a 13-bit Barker pseudo-random code sequence), will have a PG of 11.14 dB.

This result means that the performance of the information transmission system will be maintained with the same BER if the useful signal at the input decreases by 11.14 dB. If you increase the length of the code sequence to 64 chips per bit, then at the same information transfer rate of 1 Mbps, the processing gain will be 10 lg (64) = 18.0 dB.

In general, the following requirements are imposed on pseudo-random sequences (PSP) used to expand the spectrum of signals [1, 3, 4]:

- a large volume of the ensemble of sequences formed using a single algorithm;
- “good” auto- and cross-correlation properties of the sequences included in the ensemble;
- balance of structure;
- the maximum period for a given length of the shift register that forms the sequence;
- unpredictability of the sequence structure over its undistorted segment of limited length.

The autocorrelation function (ACF) of discrete signals is calculated by the formula:

$$R_u(n) = \sum_{j=-\infty}^{\infty} u_j\, u_{j-n}, \qquad (1.3)$$

where n is an integer, positive, negative or zero.

The study of ACF plays an important role in the selection of code sequences from the point of view of the least probability of establishing false synchronization.

The cross-correlation function (CCF), on the other hand, is of great importance for systems with code division of subscribers, such as CDMA. The cross-correlation function between two discrete signals is calculated using the same “Eq. (1.3)” formula

$$R_{uv}(n) = \sum_{j=-\infty}^{\infty} u_j\, v_{j-n}, \qquad (1.4)$$

Correlation properties of code sequences used in BB systems depend on the type of code sequence, its length L, the frequency of
its characters and its character structure [3,9 -13].
Let us perform a comparative analysis of the correlation characteristics of the SRP, which are used to obtain noise-like signals. The characteristics of the PSP are the functions of autocorrelation (ACF) and cross-correlation (CCF), which are divided into periodic and aperiodic. ACF and CCF are calculated by counting the difference in the number of matching and non-matching bits of a PRS when one of them shifts. Periodic ACF (PACF) and CCF (PCCF) are calculated during the cyclic shift of the PRS, and aperiodic ACF (AACF) and CCF (ACCF) are calculated during the usual shift of the PRS (parts of the PRS of various lengths are compared - from maximum to minimum).
We study PRSs that have a length L ≈ 63.
Barker codes. Barker signals (codes) can be attributed to discrete signals with the best ACF structure. The Barker signal code sequence consists of N characters ± 1 and is characterized by a normalized ACF of the form:

$$R_u(n) = \begin{cases} 1, \text{ для } n = 0, \\ 0, \text{для } n = 2l + 1, \\ \pm 1/N, \text{для } n = 2l, \end{cases}$$

(1.5)
where l = 0, 1, ... (N-1)/2.
The sign in the last line depends on the value of N.
These signals have a unique property: regardless of the number of positions N in the code combination, the ACF values calculated by formula (1.3) do not exceed unity for all $n \neq 0$. At the same time, the energy of these signals, i.e. the value of $R_u(0)$ is numerically equal to N. Only seven Barker signals are known, the most complex of them consists of 13 characters and has a ratio of the height of the main ACF peak to the side peak equal to 13. This property allows reliable detection of such a signal at signal-to-noise ratios $P_s/P_n < 1$.
In particular, these codes are used in systems with the spread spectrum of the IEEE 802.11 standard.
However, in data transmission channels in which significant interference is present, even Barker signals do not provide the required reliability of their detection.
In [8, 11], to increase the signal-to-noise ratio and increase the probability of correct detection, it is proposed to use modified Barker signals — Barker – Volynskaya signals.
The method of obtaining such signals is based on the combination of Barker signals. The Barker sequence is taken as the "maternal" sequence, and then each symbol of the "maternal" sequence is replaced by a direct or inverse Barker "daughter" sequence, depending on whether zero or one in the "maternal" sequence.
In [8], it is stated that out of all possible pairwise combinations of "mother" and "daughter" sequences of Barker codes with the highest ratio of the central peak of ACF to the side lobes, only 10 sequences satisfy: 3×4.1; 3×3; 3×7; 3×11; 7×3; 7×7; 7×11; 11×3; 11×7; 11×11. However, combinations of pairwise combinations of Barker codes 13×3; 3×13; 5×13; 13×5 were not considered.
This paper investigates pseudo-random sequences that have a length of approximately 63. PRS, which has a length L ≈ 63, can be obtained using the proposed, modified Barker codes. They can have the following structures:
(5×13), (13×5), ((5×3) ×4), ((3×5) ×4), ((2×11) ×3), ((11×2) ×3).
The last four combinations are a combination of the "maternal" sequence in the form of Barker – Volynskaya codes, in which each character of this sequence is replaced by a direct or inverse "daughter" sequence of the Barker code. And this, in turn, depends on what value a symbol (zero or one) takes in the "maternal" sequence of the Barker-Volynskaya code. For example, for a 3×4.1 sequence, the "maternal" sequence is - 1 1 0, and the "daughter" sequence is – 1 0 1 1, then the new sequence has the form:

$$\underbrace{1011}_{\text{«1»}}\ \underbrace{1011}_{\text{«1»}}\ \underbrace{0100}_{\text{«0»}}$$

M - sequences. It should be noted the following - Barker codes are mainly used for high-speed BB systems designed to transmit information, but not for code separation of subscribers. Barker code sequences longer than 13 characters are unknown. Modified Barker codes allow increasing the length of the PRS, but at the expense of some deterioration in the correlation properties. Therefore, to obtain greater noise immunity, as well as for code division of channels, sequences of greater length are used, a significant part of which form M-sequences.
The sequences of maximum length or M - sequences are the sequences formed by shift registers with linear feedback and having a period $L = 2^n - 1$, where n is the length of the register. The most important feature of M - sequences is that their periodic autocorrelation function is optimal in the class of possible autocorrelation functions of binary sequences of length $L = 2^n - 1$.
Optimality here is understood in the sense of the minimum of the maximum value of the lateral outliers of the autocorrelation function. It is the good autocorrelation properties of M-sequences and the simplicity of their formation that led to their wide application in communication systems [1,3-5].
The law of the formation of linear PRS is determined by the linear recurrence relation:

$$a_j = \sum_{i=1}^{n} C_i\, a_{j-i},$$

(1.6)
where the addition is made by mod 2.
The coefficients C_i take the values 0 or 1 and are determined by the characteristic polynomial:

$$f(x) = x^n \oplus C_{n-1}x^{n-1} \oplus \ldots \oplus C_1 x \oplus 1. \qquad (1.7)$$

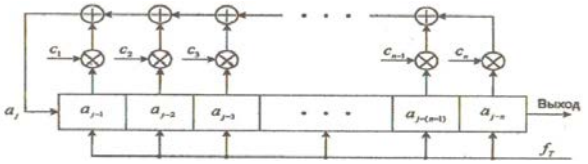


***Fig. 1. 1**. Scheme of PRS generator with linear feedback (LFSR)*

A necessary condition for obtaining an M-sequence using the characteristic polynomial (1.7) is its irreducibility. A polynomial f(x) of degree "n" is called irreducible if it cannot be decomposed into cofactor polynomials of lesser degree. For example, the polynomial $f(x) = x^5+x+1$ is reducible, since $x^5+x+1=(x^3+x^2+1) \times (x^2+x+1)$. If 2^n-1 is a prime number, then an irreducible polynomial generates an M-sequence.
An irreducible polynomial f(x) of degree "n" is called primitive if the period of coefficients 1/f(x) is 2^n-1. The primitiveness of the polynomial f(x) is a necessary and sufficient condition for obtaining an M - sequence. Primitive

polynomials exist for all n >1. the number of such polynomials is defined by the following expression:

$$N_p(n) = F_p(L)/n = (1/n)\prod_{i=1}^{k}(p_i - 1)\cdot p_i^{n_i-1},$$

(1.8)

where F_p (L) is the Euler function that determines the number of integers that are coprime and do not exceed L;

p_i-multipliers of numbers 2^n-1.

If L can be represented as a product of non-multiple multipliers, i.e. $n_i = 1$, then expression (1.8) takes the form:

$$N_p(n) = F_p(L)/n = (1/n)\prod_{i=1}^{k}(p_i - 1).$$

(1.9)

For example, for n = 8, we get L = 255 = 3×5×17 and the number of irreducible polynomials is N_p (n) = (1/8) (3 -1) (5 - 1) (17 - 1) = 16.

Table 1.1 shows some data regarding the number and numbers of taps of generators of M-sequences for a different number of bits of the shift register.

Table 1.1. *Numbers of taps and the number of M - sequences*

Number of digits, **n**	M – sequence period	Quantity M-sequences	Tap numbers register for the chain feedback
2	3	1	[2,1]
3	7	2	[3,2]; [3,1]
4	15	2	[4,3], [4,1]
5	31	6	[5,3], [5,2]
6	63	6	[6,5], [6,1]

As follows from the data given in table 1.1, the number of M-sequences increases with increasing "n".

Table 1.2 shows some irreducible polynomials and their binary equivalents.

Table 1.2 *Irreducible polynomials and their equivalents*

Degree	Irreducible polynomial	Binary sequence
4	$x^4 + x + 1$	10011
	$x^4 + x^3 + 1$	11001
5	$x^5 + x^2 + 1$	100101
	$x^5 + x^3 + 1$	101001
	$x^5 + x^3 + x^2 + x + 1$	101111
	$x^5 + x^4 + x^2 + x + 1$	110111
	$x^5 + x^4 + x^3 + x + 1$	111011
	$x^5 + x^4 + x^3 + x^2 + 1$	111101
6	$x^6 + x + 1$	1000011
	$x^6 + x^4 + x^2 + x + 1$	1010111
	$x^6 + x^4 + x^3 + x + 1$	1011011
	$x^6 + x^5 + 1$	1100001
	$x^6 + x^5 + x^2 + x + 1$	1100111
	$x^6 + x^5 + x^3 + x^2 + 1$	1101101
	$x^6 + x^5 + x^4 + x + 1$	1110011

The autocorrelation function of an M-sequence can be defined as:

$$R_u(n) = (k - l)/L = (L - 2d)/L,$$

(1.10)

where k is the number of matches;

l – number of mismatches;

L is the total number of characters;

d is the Hamming distance.

Therefore, the ACF can only take two values:

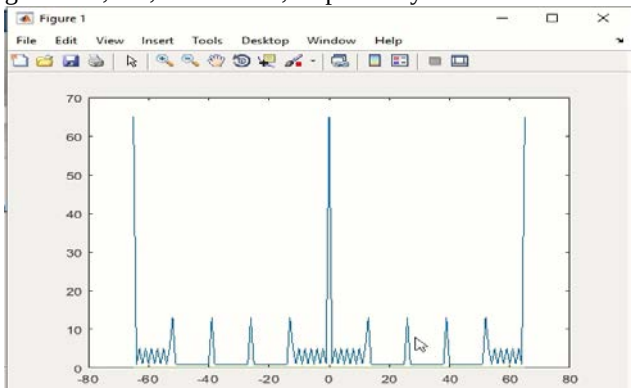
$$R_u(n) = \begin{cases} 1, & n = 0 \bmod L, \\ -1/L, & n \neq 0 \bmod L. \end{cases}$$

(1.11)

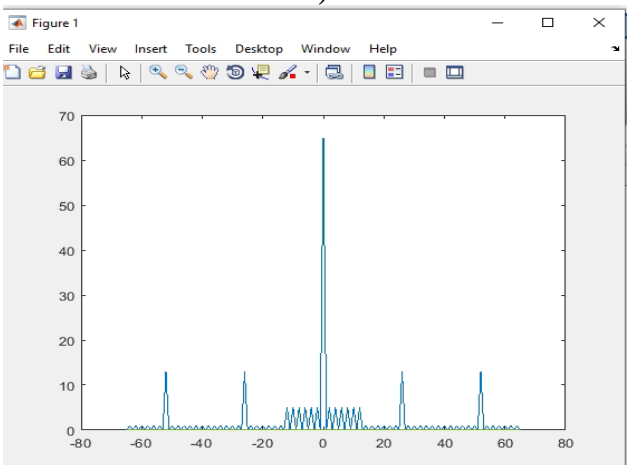
2.2. Experimental data

The correlation characteristics of PRSs are better studied in the Matlab - Simulink environment, especially if the PRSs have a long length. This can be done in two ways: using blocks from the Simulink library to build a generator for the corresponding pseudo-random sequence, or programmatically.

The correlation properties of broadband signals of modified Barker codes, which are presented above, were studied in the Matlab environment [6], the results of which are presented in figures 1.2, 1.3, 1.4 and 1.5, respectively.

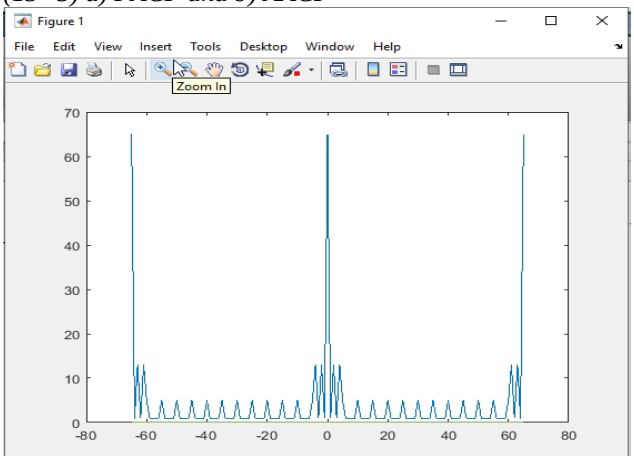


a)

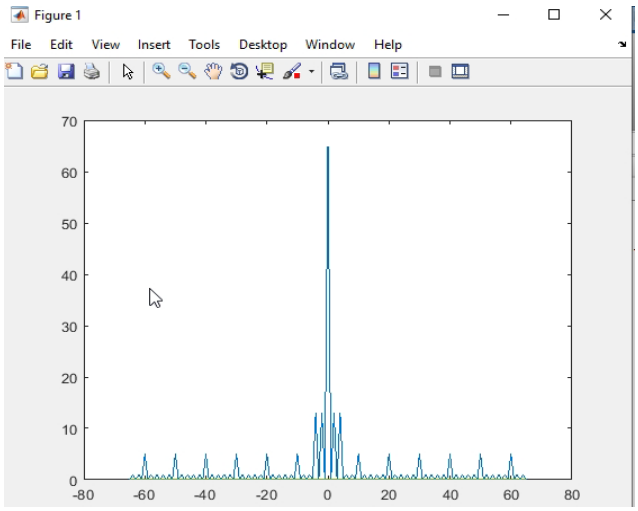


b)

Fig. 1.2. *Correlation functions of modified Barker codes (13×5) a) PACF and b) AACF*



a)



b)

Fig. 1. 3. *Correlation functions of modified Barker codes (5×13) a) PACF and b) AACF*

Fig. 1.4 shows the cross- correlation function of these two signals.

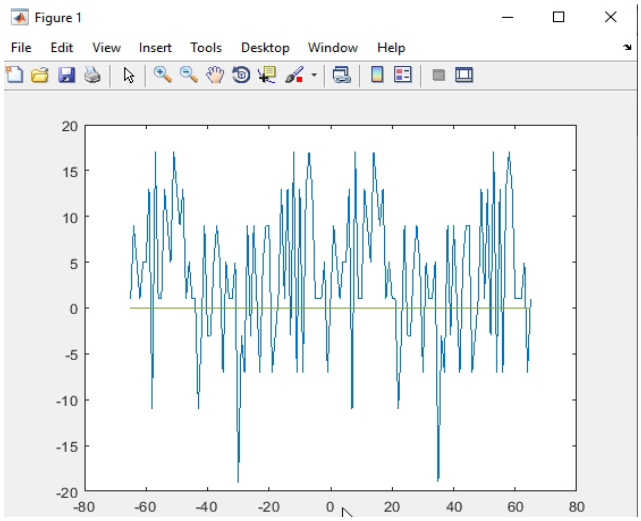
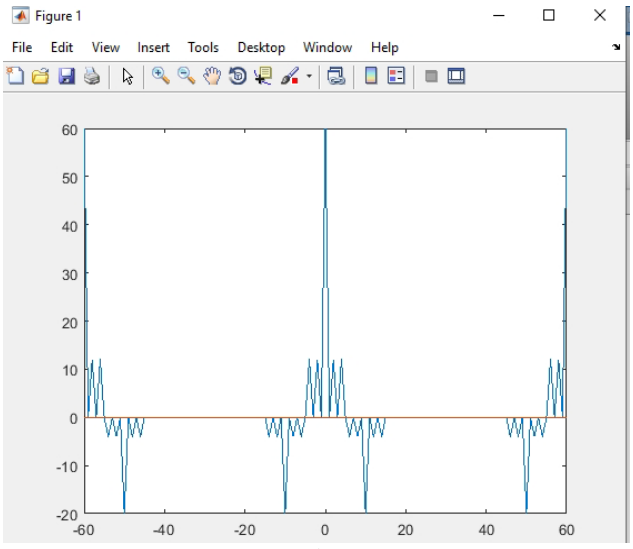
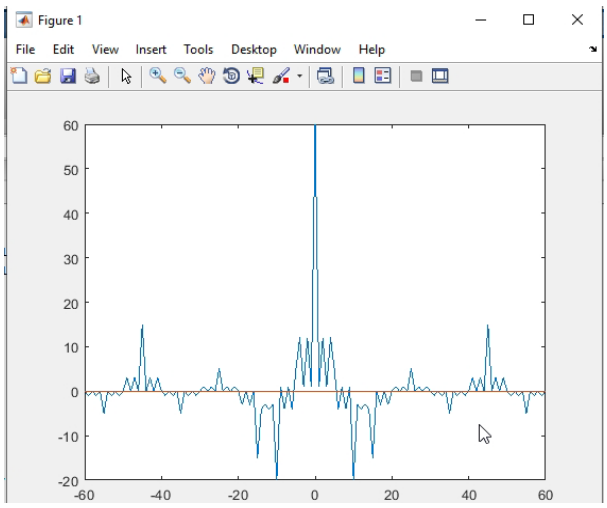


Fig. 1.4. *CCF modified Barker codes (13 × 5) and (5 × 13)*



a)



b)

Fig. 1.5. *Correlation functions of modified Barker codes (5×13) ×4 a) PACF and b) AACF*

Fig. 1.6 shows the CCF of modified Barker codes ((3×5×4) and ((5×3×4)

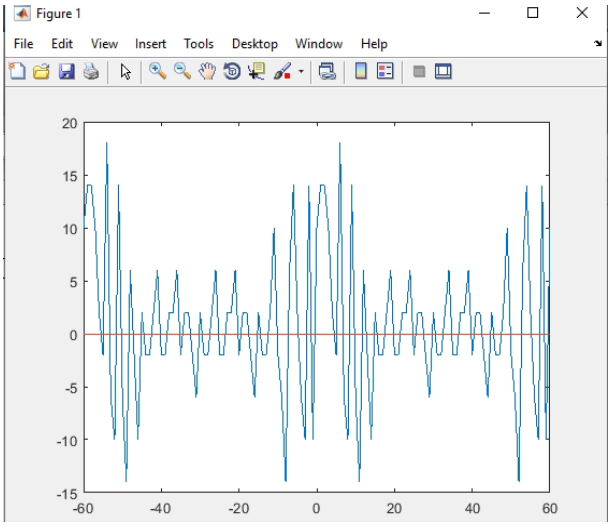
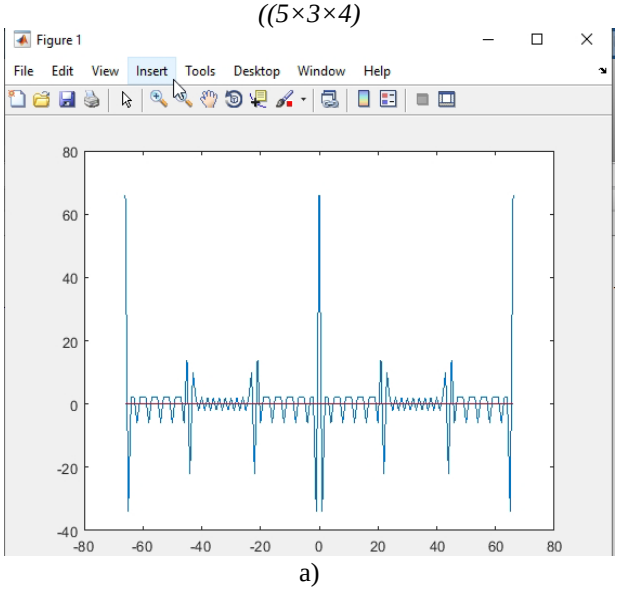
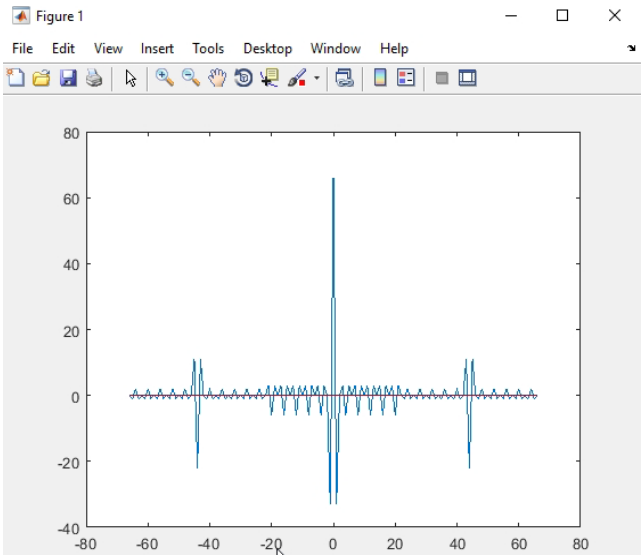


Fig. 1.6. *CCF modified Barker codes ((3×5×4) and ((5×3×4)*



a)



b)

Fig. 1.7. *Correlation functions of modified Barker codes (2×11) ×3 a) PACF and b) AACF*

Fig.1.8 shows the CCF of the modified Barker codes ((2×11) ×3) and ((11×2) ×3)

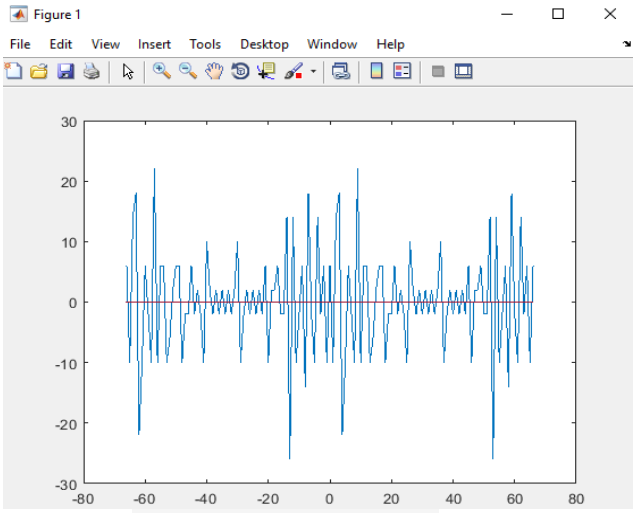


Fig. 1.8. *CCF modified Barker codes ((2×11) ×3) and ((11×2) ×3)*

From Fig. 1.2, ..., Fig.1.8 it can be seen that the use of modified Barker signals leads to an increase in the amplitude of the central peak of the ACF, but there are side outliers that can lead to errors in the processing of input signals. The cross- correlation functions of the considered signals have a large unevenness, which can lead to an increase in the level of interference of multiple access.

The Matlab environment also investigated the correlation properties of M - sequences with polynomials $f_1(x) = x^6 + x + 1$, $f_2(x) = x^6 + x^4 + x^3 + x + 1$, $f_3(x) = x^6 + x^5 + 1$ and $f_4(x) = x^6 + x^5 + x^4 + x + 1$, which have a length equal to $2^6 - 1 = 63$.

The graphs of the aperiodic autocorrelation functions listed above for M-sequences are shown in Fig.1.9, …., Fig.1.12, respectively.

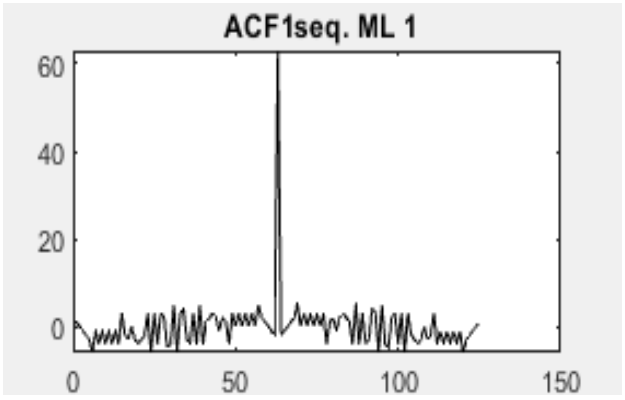


Fig. 1. 9. *Aperiodic ACF M-sequences with a verification polynomial* $f_1(x) = x^6 + x + 1$

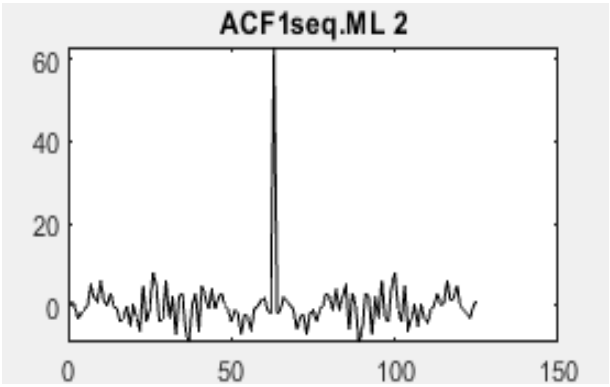


Fig. 1. 10. *Aperiodic ACF M-sequences with a verification polynomial* $f_2(x) = x^6 + x^4 + x^3 + x + 1$

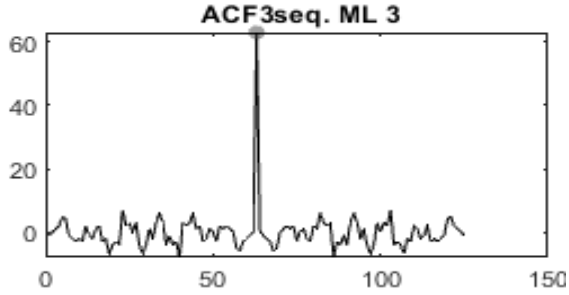


Fig. 1. 11*. Aperiodic ACF M-sequences with a verification polynomial* $f_3(x) = x^6 + x^5 + 1$

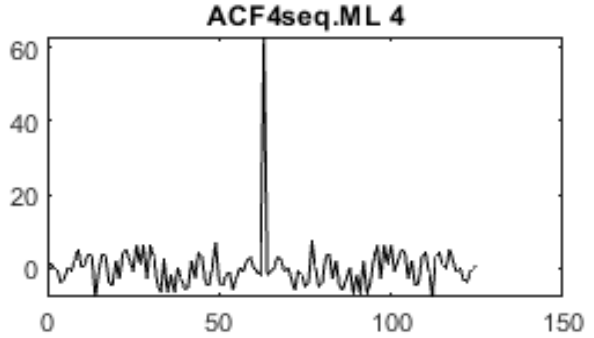


Fig. 1. 12. Aperiodic ACF M-sequences with a verification polynomial $f_4(x) = x^6 + x^5 + x^4 + x + 1$

Fig. 1.13 and Fig.1.14 show the cross- correlation functions of M-sequences $f_1(x) = x^6 + x + 1$, $f_2(x) = x^6 + x^4 + x^3 + x + 1$ and $f_3(x) = x^6 + x^5 + 1$, $f_4(x) = x^6 + x^5 + x^4 + x + 1$, respectively.

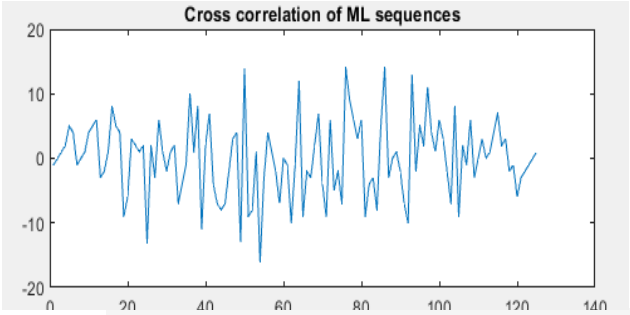


Fig. 1.13. *CCF M - sequences with verification polynomials* $f_{1}(x) = x^6 + x + 1$ and $f_{2}(x) = x^6 + x^4 + x^3 + x + 1$

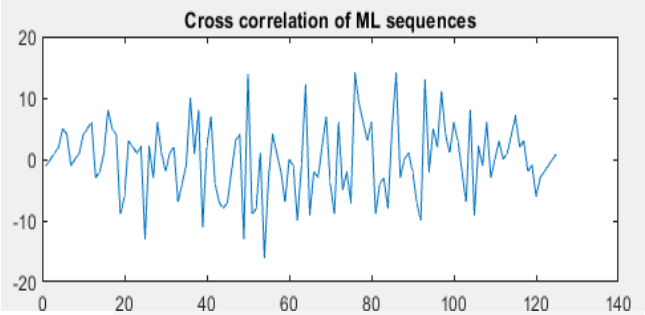


Fig. 1.14*. CCF M - sequences with verification polynomials* $f_{3}(x) = x^6 + x^5 + 1$ and $f_{4}(x) = x^6 + x^5 + x^4 + x + 1$

3. Conclusion

Analysis of the correlation properties of modified Barker codes allows us to draw the following conclusions:

- Increasing the length of the modified Barker sequence increases the amplitude of the central peak of the ACF, but also increases the amplitudes of the side outliers of the ACF. This can lead to a failure of synchronization, errors in the processing of input data.
- Modification of the Barker sequence leads to complication of circuit solutions in the construction of pseudo-random sequence generators based on such Barker codes.
- Modified Barker codes can be used in high-speed data transmission systems, taking into account the influence of the side outliers of the ACF.

The investigated M sequences, which have the same length as the modified Barker codes, have better autocorrelation and cross-correletion properties. M-sequences have a better balance of zeros and ones than modified Barker codes, and also have the least equivalent linear complexity. Therefore, M-sequences are preferable for high-speed data transmission systems.

However, for multichannel data transmission systems with code division multiplexing, it is necessary to use a large number of PRSs that differ from each other. Modified Barker codes cannot provide such an amount of PRS. The number of distinguishable M-sequences increases only with increasing bit depth n of the shift register. For example, if n = 6 there are only 6 such sequences, and if n = 10 there are 60 such sequences.

In addition, to reduce interference from multiple access, these generators of the PRS must have certain properties - the cross-correlation function of the generated pseudo-random sequences should be relatively uniform with minimal levels of side lobes.

However, only a small number of the entire ensemble of M-sequences with a given period has satisfactory correlation properties. An increase in the degree of the polynomial leads to an increase in the number of "good" sequences, however, the period of the M - sequence is significantly increased. And this, in turn, leads to an increase in chip speed and the expansion of the width of the spectrum of a noise-like signal more than acceptable. In order to compromise between the level of interference of multiple access and the bandwidth of the communication channel in some cases use "truncated" M - sequence. These sequences have slightly worse correlation properties, but allow you to achieve the desired compromise. The scope of M-sequences is huge and diverse. By selecting the appropriate properties of the M - sequence, a satisfactory result can be achieved in most cases of the operation of broadband systems. Therefore, obtaining ensembles of M-sequences of arbitrary length is an actual practical task.

Therefore, further careful study of the properties of M-sequences is required to solve the corresponding applied problems.

4. References

Books:

1. Варакин Л.Е. Системы связи с шумоподобными сигналами. – М.: Радио и связь, 1985. – 348с.
2. Solomon W. Golomb and Guang Gong. Signal Design for Good Correlation, Cambridge, Cambridge University Press, 2005, 458 p.
3. Феер К. Беспроводная цифровая связь, методы модуляции и расширения спектра. Перевод с англ. / Под ред. В.И.Журавлева. – М.: Радио и связь, 2000.
4. Гантмахер В.Е., Быстров Н.Е., Чеботарев Д.В. Шумоподобные сигналы. Анализ, синтез и обработка — Спб.: Наука и техника, 2005. —400 с.
5. Урядников Ю.Ф., Аджемов С.С. Сверхширокополосная связь. Теория и применение. — М.: СОЛОНПресс, 2005. —368 с.
6. Popa, Cristina. Tehnici de modelare şi simulare: Aplicaţii MATLAB / Cristina Popa, Bogdan Doicin. - Ploieşti : Editura Universitatii PetrolGaze din Ploieşti, 2018. - 161 p; fig., tab. - Bibliogr.: p. 161.

Journal published papers:

7. Кислов В.Я. и др. Корреляционные свойства шумоподобных сигналов, генерируемых системами с динамическим хаосом // Радиотехника и электроника, 1997. Том 42, № 11. С. 1341 – 1349.
8. Волынская А.В., Калинин П.М. Новые помехоустойчивые сигналы для интеллектуального канала телемеханики // Фундаментальные исследования. – 2012. – № 11-4. – С. 922-926;
9. Сарвате Д.В., Персли М.Б. Взаимно-корреляционные свойства псевдослучайных и родственных последовательностей // Труды Института Инженеров по Электротехнике и Радиоэлектронике. 1980. № 5. с. 59-90.
10. Рахматуллин А.Ф., Сперанский В.С. Сравнительный анализ кодовых последовательностей для СШП сигналов //Т – Comm – Телекоммуникации и транспорт.2012. № 9.

Symposia volumes:

11. Т.Шестакова, Г.Сорокин Особенности корреляционных свойств шумоподобных сигналов, The 6thInternational Conference on Telecommunications, Electronics and Informatics. – Chisinau: Tehnica – UTM, 2018, pp. 194-199.