A Method for Synthesis of CAZAC Sequences with Period $7^n - 1$

Prof. Borislav Yordanov Bedzhev,
Member, IEEE
Faculty of Technical Sciences
University of Shumen -"Bishop Konstantin Preslavsky"
Shumen, Bulgaria

Stoyan Sabkov Yordanov,
Student Member, IEEE
Department of "Telecommunications"
University of Ruse -"Angel Kanchev"
Ruse, Bulgaria

Prof. Ivo Michailov Michailov
Faculty of Mathematics and Informatics
University of Shumen "Bishop Konstantin Preslavsky"
Shumen, Bulgaria

***Abstract*— A key role for the present wireless communications play families of signals with ideal periodic autocorrelation known as Constant Amplitude Zero Autocorrelation Code (CAZAC) sequences. They find many applications for synchronization, channel estimation, elimination of the negative effects, caused by the multipath spread of the electromagnetic waves, data protection and others. With regard in this paper we present a new method for synthesis of CAZAC sequences with small signal constellation. The method is based on a modification of the signal constellation of the classical maximal length sequences with period 7^n-1. The proposed method can be successfully used in the process of development of perspective wireless communication system, exploiting very effectively the limited natural resource – the electromagnetic spectra.**

Keywords- phase manipulated signals, synthesis of signals with ideal periodic autocorrelation function, crosscorrelation function

I. INTRODUCTION

Signals with ideal periodic autocorrelation function (PACF), resembling a delta pulse, find many applications in radars and in wireless communications for synchronization and for eliminating the negative effects, caused by the multipath spread of the electromagnetic waves. Due to this reason various methods for synthesis of families of such signals have been researched for the last 60 years. However, only a few classes of CAZAC signals are known. The most famous of them are the so - named Zadoff and Chu sequences [1], [2]. The main drawback of Zadoff and Chu sequences is the existence of a hard connection between the length N of the sequences and the size of the signal constellation (alphabet), consisting of a complex envelopes of the elementary phase pulses (chips). In other words, if longer sequences are needed a more complex modulation must be used.

With regard to this situation in the present paper we suggest a new method for synthesis of phase manipulated (PM) signals, possessing both an ideal PACF and a small signal alphabet. The new PM signals are derived by means of a modification of the classical maximal length sequences (*m* – sequences). As a result their signal alphabet is limited. On this base it is possible to synthesize families of PM signals with ideal PACF, low cross-correlation and unlimited lengths that could be successfully applied in the following directions [3], [4], [5], [6]:

- for synchronization and channel estimation [2];
- in an adaptive modulation schemes, where variable data rates according to channel characteristics are supported by means of PM signals with variable signal alphabet size [7];
- in a design of wideband signals with complex inner structure, which are suitable for the perspective communication systems, providing a very high level of the information protection.

The paper is organized as follows. First, in Section II the methods for transformation of the *m*-sequences with lengths (periods) $2^n - 1$, $3^n - 1$ and $5^n - 1$ into CAZAC sequences are recalled. After that in Section III the new method for synthesis of CAZAC sequences with period $7^n - 1$, is suggested. In Section IV results of investigation of cross-correlation properties of the new signals are presented. Conclusions of the paper are summarized in Section V.

II. METHODS FOR TRANSFORMATION OF M-SEQUENCES INTO CAZAC SEQUENCES

A. Basics of the Clasical m-sequences-theory

The linear recurring sequences (LRS) find wide implementation in many fields, especially for information protection and in communications [8], [9], [10], [11]. Due to this reason they have been extensively studied since the mid-20th century [8], [9], [10], [11].

LRSs are created by means of a linear recursive equation (LRE), which can be expressed as:

$$u(i) = d_{n-1}.u(i-1) + d_{n-2}.u(i-2) + ... + d_0.u(i-n), \quad (1)$$

where $u(i)$ is the new *i*-th element of the *LRS*, $u(i-1), u(i-2), ..., u(i-n)$ are elements of the considered *LRS*, obtained during the previous steps of the LRE (1) (the initial elements $u(0), u(1), ..., u(n-1)$ should be known), $d_{n-1}, d_{n-2}, ..., d_0$ are coefficients, belonging to a finite algebraic field (named *Galois Field* (*GF*)) and all algebraic operations in (1) are performed in $GF(p^m)$ (i.e. modulo *p*, where *p* can be an arbitrary prime integer).

After the substitution $u(i) = x^i$, $i = 0, 1, 2, ...$, Eq. (1) is transformed into the so-named *characteristic equation* (noted often as *the connection polynomial* of the linear feedback shift registers (LFSRs), which are the hardware, realizing the LRE (1)):

$$x^n - d_{n-1}.x^{n-1} - d_{n-2}.x^{n-2} - ... - d_0 = 0 \quad (2)$$

If the left side of the characteristic equation is a primitive irreducible polynomial over $GF(p^m)$, then the period of the LRS is maximal, namely $N = (p^m)^n - 1$ and it is called *maximal length sequence* (*m – sequence*).

In communications the *m* - sequences are used for controlling the phase modulation of the PM signals. Due to the symmetric connection, the derivative PM signals are named *m* - sequences also. The main advantage of these signals is that their PACF is almost perfect, because the level of the side-lobes is constant and equal to -1, i.e.:

$$P_{\zeta\zeta}(r) = \sum_{i=0}^{N-1} \zeta(i).\zeta^*\langle i + r \rangle = \begin{cases} N, \ r = 0, \\ -1, \ r \neq 0. \end{cases} \quad (3)$$

In (3) $P_{\zeta\zeta}(r)$ is the PACF of the *m* - sequence $\{\zeta(i)\}_{i=0}^{N-1}$, $\boldsymbol{r}$ is the time shift, the symbol "$\langle\ \rangle$" means "summing modulo *p*", and symbol "*" – "complex conjugation".

The complex envelopes of the elementary phase impulses (chips) of the PM signal are described with the following equation (or *coding rule*):

$$\zeta(i) = e^{j\frac{2\pi l}{p}u(i)}, \ i = 0, 1, 2, ..., N-1, ... \quad (4)$$

Here $\boldsymbol{l}$, $1 \le l < p$, is an arbitrary integer and $u(i)$ are the elements of the *m*-sequence, controlling the phase modulation.

Another important advantage of *m* - sequences, is the possibility to obtain arbitrary long sequence length even though the size of the signal alphabet is small. This feature is essential if longer sequences are required.

B. *Methods of transformation of m-sequences into CAZAC sequenceses of period $2^n - 1$, $3^n - 1$ and $5^n - 1$*

In the paper [3] a method for modification of the binary *m* - sequences ($p = 2$), is recalled. It allows the almost perfect PACF of the *m* - sequences to be transformed into ideal PACF. In this method, (4) is substituted by the following equation for the chip generation (coding rule):

$$\xi(i) = e^{j.\psi.u(i)}, \ \psi = \arccos(-1 + 2^{-(n-1)}), \quad i = 0, 1, 2, ..., N-1, ... \quad (5)$$

As mentioned, the new PM signal has an ideal PACF:

$$P_{\xi\xi}(r) = \sum_{i=0}^{N-1} \xi(i).\xi^*\langle i + r \rangle = \begin{cases} N, \ r = 0, \\ 0, \ r \neq 0. \end{cases} \quad (6)$$

In two recent papers [4] and [5] the method of [3] has been developed for cases of *m* - sequences over *GF*(*3*) and *GF*(*5*). In the case of *m* - sequences over *GF*(*3*), the conventional chips

$$\forall \xi(i) \in \left\{ e^{j\frac{2\pi}{3}0} = 1, \ e^{j\frac{2\pi}{3}1}, \ e^{j\frac{2\pi}{3}2} \right\} \quad (7)$$

are substituted by the following "corrected" chips:

$$\forall \zeta(i) \in \left\{ x = e^{j\varphi_x}, y = e^{j\varphi_y}, y^{-1} = e^{-j\varphi_y} \right\}; \quad \varphi_x = \arccos\left(\frac{-1 + 3^{-(n-1)}}{\pm\sqrt{1 + 3^{-(n-1)}}} \right), \quad \varphi_y = \arccos\left(\frac{\pm\sqrt{1 + 3^{-(n-1)}}}{2} \right) \quad (8)$$

As a result the *m* - sequences are transformed into CAZAC sequences. In the case of *m* - sequences over *GF*(*5*), the conventional chips:

$$\forall \zeta(i) \in \left\{ 1, e^{j\frac{2\pi}{5}1}, e^{j\frac{2\pi}{5}2}, e^{j\frac{2\pi}{5}3}, e^{j\frac{2\pi}{5}4} \right\} \quad (9)$$

are substituted with the following "corrected" chips:

$$x = e^{j\varphi_x}, \ y = e^{j\varphi_y}, \ z = e^{j\varphi_z}, \quad y^{-1} = e^{-j\varphi_y}, \ z^{-1} = e^{-j\varphi_z} \quad (10)$$

Here the power coefficients are:

$$\varphi_x = \arccos\frac{-1+5^{-(n-1)}}{\pm\sqrt{1+3.5^{-(n-1)}}},$$
$$\varphi_y = \arccos\frac{\pm\left(1+3.5^{-(n-1)}\right)\pm\left(5-5^{-(n-1)}\right)}{4}, \quad (11)$$
$$\varphi_z = \arccos\frac{\pm\left(1+3.5^{-(n-1)}\right)\mp\left(5-5^{-(n-1)}\right)}{4}$$

Again, after the substitution of the chips the almost perfect PACF of the *m* - sequences is transformed into ideal PACF.

These modified *m* - sequences have several valuable positive features [3], [4], [5], [12], [13]:

- Constant zero autocorrelation except for the zero shift;
- Fixed small signal alphabet that does not restrict the increasing of the length of the sequences;
- Possibility for synthesis of families of PM signals with low cross-correlation.

III. New Method for Sinthesis of Cazac Sequences with Period 7^N-1

Now we shall suggest a new method for modification of *m* - sequences with period 7^n-1. Here the chips of conventional *m* – sequences over *GF*(*7*):

$$\forall\zeta(i)\in\left\{1, e^{j\frac{2\pi}{7}1}, e^{j\frac{2\pi}{7}2}, e^{j\frac{2\pi}{7}3}, e^{j\frac{2\pi}{7}4}, e^{j\frac{2\pi}{7}5}, e^{j\frac{2\pi}{7}6}\right\} \quad (12)$$

are substituted by the following "modified"chips:

$$\forall\xi(i)\in\left\{x, y, z, u, y^{-1}, z^{-1}, u^{-1}\right\}, \quad (13)$$

where:

$$x = e^{j\varphi_x}, y = e^{j\varphi_y}, z = e^{j\varphi_z}, u = e^{j\varphi_u},$$
$$y^{-1} = e^{-j\varphi_y}, z^{-1} = e^{-j\varphi_z}, u^{-1} = e^{-j\varphi_u}.$$

In order to transform the almost perfect PACF of the conventional *m* – sequences over *GF*(*7*) into an ideal PACF, the following theorem should be used.

Theorem (Zierler, [10]): Let $\{u(i)\}_{i=0}^{N-1}, N = p^n - 1$ be a *m* – sequence over *GF(p)*. Then the pairs $\{u(i), u(i+r)\}, i = 0,1,...,N-1$ have the following distribution.

First, in the case of $r \neq s(\mathrm{mod}N), s = (p^n - 1)/(p-1)$ all possible pairs $\{0,1\},\{0,2\},...,\{0,p-1\},\{1,0\},\{1,1\},...,\{1,p-1\},...,\{p-1,0\},\{p-1,1\},...,\{p-1,p-1\}$ appear p^{n-2} times, and the pair $\{0,0\}$ appears $p^{n-2}-1$ times.

Second, in the case of $r \equiv s(\mathrm{mod}N), s = (p^n - 1)/(p-1)$ the pairs satisfying the relation $u(i) - u(i+r) = a,\ a \in \{0,1,2,...,p-1\},\ i = 0,1,2,...,N-1$ appear p^{n-1} times, and the pair $\{0,0\}$ appears $p^{n-1}-1$ times. According to the of Zierler's theorem and (13) we can write four equations with four indeterminates:

$$r \neq ks \Rightarrow 7^{(n-2)}(x + y + y^{-1} + z + z^{-1} + u + u^{-1})(x^{-1} + y^{-1} + z + z^{-1} + u + u^{-1}) - 1 = 0 \quad (14)$$

$$r = s \Rightarrow 7^{(n-1)}(yu^{-1} + y^{-1}z^{-1} + yz + y^{-1}u + z^{-1}u + zu^{-1} + 1) - 1 = 0 \quad (15)$$

$$r = 2s \Rightarrow 7^{(n-1)}(yu + y^{-1}u^{-1} + zu + z^{-1}u^{-1} + yz^{-1} + y^{-1}z + 1) - 1 = 0 \quad (16)$$

$$r = 3s \Rightarrow 7^{(n-1)}(y^2 + y^{-2} + z^2 + z^{-2} + u^2 + u^{-2} + 1) - 1 = 0 \quad (17)$$

Here it should be pointed out that in general the PACF is a complex - symmetric function (i.e. $P_{\zeta\zeta}(r) = P^*_{\zeta\zeta}(N-r),\ r = 1,2,...,N-1$) and as a result the cases $r = 4s, 5s, 6s$ are complex conjugated with the above cases (namely $r = 3s, 2s, 1s$).

The equations (14), (15), (16) and (17) can be transformed as follows:

$$(y + y^{-1} + z + z^{-1} + u + u^{-1})(x + x^{-1}) + (y + y^{-1} + z + z^{-1} + u + u^{-1})^2 + xx^{-1} = 7^{-(n-2)} \quad (18)$$

$$yu^{-1} + y^{-1}z^{-1} + yz + y^{-1}u + z^{-1}u + zu^{-1} = -1 + 7^{-(n-1)} \quad (19)$$

$$yu + y^{-1}u^{-1} + uz + z^{-1}u^{-1} + yz^{-1} + zy^{-1} = -1 + 7^{-(n-1)} \quad (20)$$

$$y^2 \pm 2 + y^{-2} + z^2 \pm 2 + z^{-2} + u^2 \pm 2 + u^{-2} = -1 + 7^{-(n-1)} \pm 6 \quad (21)$$

From (21) two possible equations are got:

$$(y + y^{-1})^2 + (z + z^{-1})^2 + (u + u^{-1})^2 = 5 + 7^{-(n-1)} \quad (22)$$

$$(y - y^{-1})^2 + (z - z^{-1})^2 + (u - u^{-1})^2 = -7 + 7^{-(n-1)}. \quad (23)$$

The sum of (19) and (20) is

$$(y+y^{-1})(u+u^{-1})+(y+y^{-1})(z+z^{-1})+ \\ +(z+z^{-1})(u+u^{-1})=-2+2.7^{-(n-1)} \quad (24)$$

Multiply (24) with 2 and add to (22):

$$[(y+y^{-1})+(z+z^{-1})+(u+u^{-1})]^2=1+5.7^{-(n-1)} \quad (25)$$

Now, subtract (20) from (19):

$$(yu^{-1}+y^{-1}u-yu-y^{-1}u^{-1})+(yz^{-1}-y^{-1}z+ \\ +yz-y^{-1}z^{-1})+(uz^{-1}+u^{-1}z-uz-u^{-1}z^{-1})=0 \Leftrightarrow \\ \Leftrightarrow -(y-y^{-1})(u-u^{-1})+(y-y^{-1})(z- \\ -z^{-1})-(z-z^{-1})(u-u^{-1})=0 \quad (26)$$

Next, multiply (26) with 2 and add to (23):

$$[(y-y^{-1})+(z-z^{-1})-(u-u^{-1})]^2=-7+7^{-(n-1)} \quad (27)$$

Add (25) to (27):

$$y+z+u^{-1}=\frac{\pm\sqrt{1+5.7^{-(n-1)}}\pm\sqrt{-7+7^{-(n-1)}}}{2} \quad (28)$$

In order to keep the compact size of the next calculations, the following substitutions will be made:

$$E=\frac{\pm\sqrt{1+5.7^{-(n-1)}}\pm\sqrt{-7+7^{-(n-1)}}}{2}, \quad (29)$$

$$x_1=x+x^{-1}, y_1=y+y^{-1}, z_1=z+z^{-1}, u_1=u+u^{-1}, \quad (30)$$

$$C=y_1+z_1+u_1. \quad (31)$$

From (14) and (31) an equation is obtained that contains only the indeterminate x:

$$7^{(n-2)}(x+C)(x^{-1}+C)-1=0. \quad (32)$$

Below the indeterminates y_1 and z_1 will be expressed via u_1. After the addition of (15) with (16) the result is:

$$7^{(n-1)}(y_1u_1+z_1u_1+y_1z_1+2)-2=0. \quad (33)$$

Apply the substitutions (30) in (22):

$$7^{(n-1)}(y_1^2+z_1^2+u_1^2-5)-1=0. \quad (34)$$

Here we put:

$$A=y_1u_1+z_1u_1+y_1z_1, \quad (35)$$

$$B=y_1^2+z_1^2+u_1^2, \quad (36)$$

whence we have for (33) and (34) respectively:

$$7^{(n-1)}(A+2)-2=0 \Rightarrow A=\frac{2}{7^{(n-1)}}-2, \\ 7^{(n-1)}(B-5)-1=0 \Rightarrow B=\frac{1}{7^{(n-1)}}+5. \quad (37)$$

From (31), (35) and (36) we find

$$C^2=(y_1+z_1+u_1)^2=B+2A \Rightarrow C=\pm\sqrt{B+2A}. \quad (38)$$

Here we put

$$a=y_1+z_1. \quad (39)$$

From (31) we get

$$a=C-u_1. \quad (40)$$

Then (35) can be transformed into

$$y_1z_1=A-(y_1+z_1)u_1=A-(C-u_1)u_1=A-au_1=b, \quad (41)$$

where we put

$$b=A-au_1. \quad (42)$$

From (29) the results are:

$$y_1-y-y^{-1}=0,\ z_1-z-z^{-1}=0. \quad (43)$$

After multiplication with y and z we obtain respectively:

$$y_1y-y^2-1=0,\ z_1z-z^2-1=0. \quad (44)$$

Hence y and z can be easily expressed by y_1 and z_1:

$$y=\frac{y_1\pm\sqrt{y_1^2-4}}{2} \text{ and } z=\frac{z_1\pm\sqrt{z_1^2-4}}{2}. \quad (45)$$

Here $y_1^2 - 4$ and $z_1^2 - 4$ are the discriminants of (44). From (28), (39) and (45) we obtain

$$\frac{1}{2}(y_1 + z_1 \pm \sqrt{y_1^2 - 4} \pm \sqrt{z_1^2 - 4}) + u^{-1} = E \quad =>$$
$$=> \pm \sqrt{y_1^2 - 4} \pm \sqrt{z_1^2 - 4} = 2E - 2u^{-1} - a . \quad (46)$$

After squaring of (46) the result is

$$y_1^2 - 4 + z_1^2 - 4 \pm 2\sqrt{(y_1^2 - 4)(z_1^2 - 4)} = , \quad (47)$$
$$= (2E - 2u^{-1} - a)^2 = F$$

where we put:

$$F = (2E - 2u^{-1} - a)^2 . \quad (48)$$

From (39) and (41) we get:

$$y_1^2 + z_1^2 = (y_1 + z_1)^2 - 2y_1 z_1 = a^2 - 2b . \quad (49)$$

The accounting (49) in (47) leads to:

$$\pm 2\sqrt{(y_1^2 - 4)(z_1^2 - 4)} = F - a^2 + 2b + 8 ,$$

and after squaring the result is

$$(y_1^2 - 4)(z_1^2 - 4) = \frac{1}{4}(F - a^2 + 2b + 8)^2 . \quad (50)$$

Denote by G the left side of (50). Then from (48) it follows that:

$$G = \frac{1}{4}(F - a^2 + 2b + 8)^2 = \frac{1}{4}(4E^2 + 4u^{-2} + . \quad (51)$$
$$+ a^2 - 8Eu^{-1} - 4Ea + 4u^{-1}a - a^2 + 2b + 8)^2$$

On the other hand, we can express G by a and b in this way:

$$y_1^2 z_1^2 - 4(y_1^2 + z_1^2) + 16 = G => b^2 - 4(a^2 - 2b) + 16 = G . \quad (52)$$

From (40) and (42) we obtain

$$a^2 - 2b = C^2 - 2A - u_1^2 . \quad (53)$$

Now, put

$$H = 4E^2 + 4u^{-2} - 8Eu^{-1} - 4Ea + 4u^{-1}a . \quad (54)$$

From (51) and (54) the result is:

$$G = \frac{1}{4}(H + 2b + 8)^2 = \frac{1}{4}(H^2 + 4b^2 +$$
$$+ 64 + 4Hb + 16H + 32b) =>$$
$$=> -4(C^2 - 2A - u_1^2) = \frac{1}{4}H^2 + H(b + 4) + 8b . \quad (55)$$

Applying (40) in (54) we obtain:

$$H = 4E^2 - 8Eu^{-1} - 4E(C - u - u^{-1}) + 4u^{-1} + 4u^{-2}C - . \quad (56)$$
$$- 4 - 4u^{-1} = 4Eu + 4(C - E)u^{-1} + 4E^2 - 4 - 4EC$$

Finally, taking into account (55), (56) and the substitutions (37), (38), (40), (42), the following polynomial for u is obtained:

$$4\left[(\sqrt{\frac{1}{7^{n-1}} + 5 + 2(\frac{2}{7^{n-1}} - 2)})^2 - 2(\frac{2}{7^{n-1}} - 2) - (u + u^{-1})^2\right] +$$
$$+ \frac{1}{4}\left[4(\frac{\sqrt{1 + 5.7^{-n+1}} + \sqrt{-7 + 7^{-n+1}}}{2})^2 - 4 - \right.$$
$$- 4(\frac{\sqrt{1 + 5.7^{-n+1}} + \sqrt{-7 + 7^{-n+1}}}{2})(\sqrt{\frac{1}{7^{n-1}} + 5 + 2(\frac{2}{7^{n-1}} - 2)}) +$$
$$+ 4(\frac{\sqrt{1 + 5.7^{-n+1}} + \sqrt{-7 + 7^{-n+1}}}{2})u +$$
$$\left. + 4(\sqrt{\frac{1}{7^{n-1}} + 5 + 2(\frac{2}{7^{n-1}} - 2)} - \frac{\sqrt{1 + 5.7^{-n+1}} + \sqrt{-7 + 7^{-n+1}}}{2})u^{-1}\right]^2 +$$
$$+ (4(\frac{\sqrt{1 + 5.7^{-n+1}} + \sqrt{-7 + 7^{-n+1}}}{2})^2 -$$
$$- 4 - 4(\frac{\sqrt{1 + 5.7^{-n+1}} + \sqrt{-7 + 7^{-n+1}}}{2})(\sqrt{\frac{1}{7^{n-1}} + 5 + 2(\frac{2}{7^{n-1}} - 2)}) +$$
$$+ 4(\frac{\sqrt{1 + 5.7^{-n+1}} + \sqrt{-7 + 7^{-n+1}}}{2})u + 4(\sqrt{\frac{1}{7^{n-1}} + 5 + 2(\frac{2}{7^{n-1}} - 2)} -$$
$$- \frac{\sqrt{1 + 5.7^{-n+1}} + \sqrt{-7 + 7^{-n+1}}}{2})u^{-1})((\frac{2}{7^{n-1}} - 2 - \quad (57)$$
$$- (\sqrt{\frac{1}{7^{n-1}} + 5 + 2(\frac{2}{7^{n-1}} - 2)} - (u + u^{-1}))(u + u^{-1})) + 4) +$$
$$+ 8(\frac{2}{7^{n-1}} - 2 - (\sqrt{\frac{1}{7^{n-1}} + 5 + 2(\frac{2}{7^{n-1}} - 2)} -$$
$$- (u + u^{-1}))(u + u^{-1})) = 0$$

It seems that it is not possible to simplify further this polynomial manually. With the aid of the computer program

Maple, we were able to calculate the roots of the polynomial (57) for $1 \le n \le 10$. After that we have found the rest of the indeterminates as roots of the three quadratic polynomials determined by (32), (39) and (41).

In Table I the solutions for n=1÷10 are presented (the rounding of the digits and the range of n are sufficient in respect to the present and near future needs of the communications systems, where the period of sequences usually is lower than 1.10^6). The presented solutions are in compliance with the theory of PM signals, because the chips must be complex numbers with unit magnitude.

TABLE I. SOLUTIONS OF THE SYSTEM

n	x, y, z, u

2	x= (-0.6546536707-j*0.7559289460);
	y/z=(0.3471711849+j*0.9378017747);
	z/y=(0.9013754162-j*0.4330385187);
	u= (-0.5938929307-j*0.8045440864);

3	x= (-0.9331389496-j*0.3595159255);
	y/z=(0.2435483813+j*0.9698887493);
	z/y=(0.9010031349-j*0.4338125758);
	u=(-0.6196608572-j*0.7848696848);

4	x=(-0.9898956688-j*0.1417976191);
	z/y=(0.2256133101+j*0.9742169339);
	y/z=(0.9009736542-j*0.4338738001);
	u=(-0.6229558346-j*0.7822570090);

5	x=(-0.9985443305-j*0.05393718641);
	z/y=(0.2229646028+j*0.9748265416);
	y/z=(0.9009695515-j*0.4338823198);
	u=(-0.6234138087-j*0.7818920790);

6	x=(-0.9997917955-j*0.02040504156);
	z/y=(0.2225843541+j*0.9749134348);
	y/z=(0.9009689657-j*0.4338835361);
	u=(-0.6234789516-j*0.7818401351);

7	x=(-0.9999702513-j*0.007713392085);
	z/y=(0.2225299949+j*0.9749258440);
	y/z=(0.9009688818-j*0.4338837103);
	u=(-0.6234882519-j*0.7818327185);

8	x=(-0.9999957501-j*0.002915442792);
	z/y=(0.2225222285+j*0.9749276166);
	y/z=(0.9009688697-j*0.4338837351);
	u=(-0.6234895804-j*0.7818316590);

9	x=(-0.9999993929-j*0.001101936748);
	z/y=(0.2225211184+j*0.9749278701);
	y/z=(0.9009688685-j*0.4338837379);
	u=(-0.6234897702-j*0.7818315077);

10	x=(-0.9999999133-j*0.0004164931013);
	z/y=(0.2225209607+j*0.9749279061);
	y/z=(0.9009688677-j*0.4338837394);
	u=(-0.6234897973-j*0.7818314861);

The direct examination of the results in Table I proves the correctness of the above suggested method for modification of the m - sequences over $GF(7)$ into CAZAC sequences.

Below an example simulated in *Matlab*, using a sequence with length N=7^3-1= 342, is presented. It could be seen from Fig. 1 that PACF is ideal (i. e. after the correction of the signal alphabet the side-lobes of the PACF of the sequence vanish). Also the signal constellation of the new (corrected) sequence posses an acceptable asymmetry (Fig. 2) from an implementation point of view.

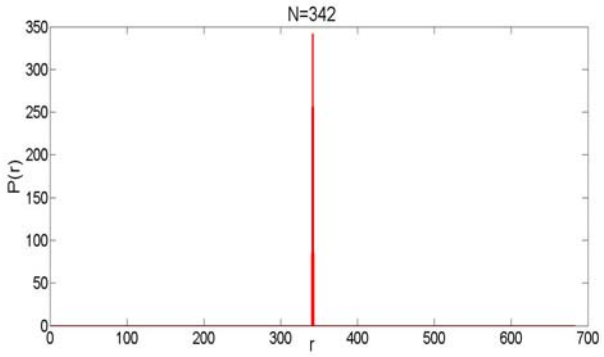

Figure 1. PACF of a corrected m - sequence with period N=7^3-1

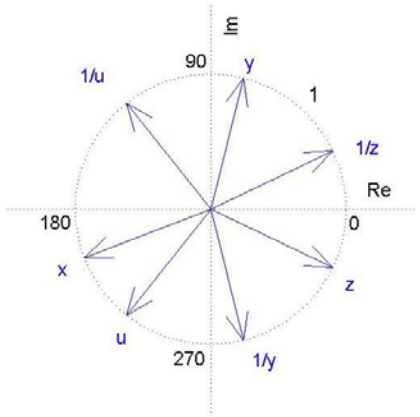

Figure 2. Signal constellation of the corrected m - sequence with period N=7^3-1

IV. CROSSCORELATION PROPERTIES OF SIGNALS WITH PERIOD 7^N -1 AND IDEAL PACF

The main problems in the wireless communication systems are the signal distortions, caused by the multipath spreading of the electromagnetic waves and the mutual interferences due to the simultaneous work of multiple users. The general method for solving of these problems is usage of families of signals, possessing both ideal PACF and low mutual Periodic Cross-correlation (LPCC) between all pairs of signals. The last one can be mathematically described as follows. Let F(K, N, C) be a set of ***K*** signals with period ***N*** and with maximal level ***C*** of the cross-correlation side-lobes:

$$C \le \alpha\sqrt{N}\,. \qquad (58)$$

Here α is a coefficient with relatively low value. In this case F(K, N, C) is named *family of signals with LPCC* [11].

With regard to the impact of the correlation properties of the signals over the performance of the communication

systems we shall show, that the method from the previous section can be developed for synthesis of families of signals with LPCC.

It should be pointed out that the decimations of the signals preserve their correlation properties. More specifically, let $\{\xi(i)\}_{i=0}^{N-1}$ be a signal with ideal PACF. Then the derivative signals $\{\xi_k(i)\}_{i=0}^{N-1}$, obtained by the rule:

$$\xi_k(i) = \xi\langle d_k . i\rangle_{\mathrm{mod}\, N},\ d_k = 1,2,...,N_t,\ i = 0,1,2,...,N-1,... \quad (59)$$

have also ideal PACF [11]. Here the decimation coefficients $d_k, k = 1,2,...,N_t$ are the all possible positive integers smaller than ***N*** and co-prime to ***N***, and the symbol "$\langle d_k . i\rangle_{\mathrm{mod}\, N}$" means "multiplication modulo p".

The main problem here is finding of proper decimation coefficients that lead to generation of families of signals with LPCC. With regard to this we have conducted an exhaustive computer investigation of all possible decimation coefficients and corresponding cross-correlations. This survey has been realized by a computer program in *Matlab* environment. It can be explained by the block-scheme, shown on Fig. 3. As shown, the algorithm of the computer program consists of the following steps:

- Generation of a conventional *m*-sequence;
- Modification of the chosen *m*-sequence into CAZAC sequence;
- Decimation of the corrected sequence by all possible decimation coefficients and calculation of periodic cross-correlation functions (PCCF) of each pair of PM signals;
- The signals, which lead to PCCFs with side-lobes, exceeding the restriction (58), are excluded. As a result, after "filtering" the initial set of signals is transformed in a family of signals with LPCC.

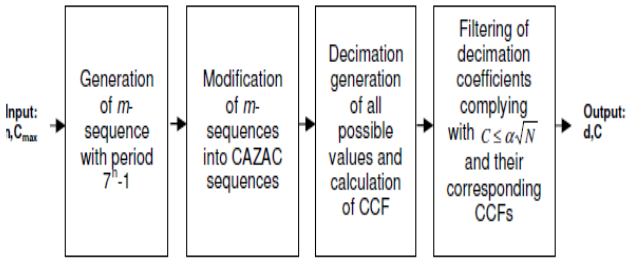

Figure 3. The algorithm of the computer program for synthesis of families of PM signals with LPCC

The results of our survey of the new sequences for the sequence lengths *N=48÷117648*, are given in table II. In the column *K* the sizes of the derived families are presented. It must be emphasized that the maximal cross-correlation (C) of the investigated families of PM signals can be minimized up to min. $P_{s(t),s(dt)}(\tau)$), but this leads to a diminishing of the family sizes.

TABLE II. RESULTS OF THE SURVEY OF THE CROSS-CORRELATION PROPERTIES OF THE FAMILIES OF PM SIGNALS, WHICH ARE CORRECTED M-SEQUENCES WITH PERIOD 7^N -1

Length of the sequences N=7^n-1		**Investigation of crosscorrelation of corrected *m*-sequences**				
		Minimal cross-correlation in the family F		**Maximal cross-correlation in the family F**		**size of F**
n	N	min $P_{s(t),s(dt)}(\tau)$	f($\sqrt{N}$)	C	f($\sqrt{N}$)	*K*
2	48	13.71	$2\sqrt{N-1}$	27.43	$4\sqrt{N-1}$	8
3	342	38.38	$2.08\sqrt{N-1}$	125.63	$6.80\sqrt{N-1}$	36
4	240	97.96	$2\sqrt{N-1}$	124.49	$25\sqrt{N-1}$	160
5	16806	328.12	$2.53\sqrt{N-1}$	5700.15	$43.97\sqrt{N-1}$	*
6	117648	685.99	$2\sqrt{N-1}$	58995.5	$172\sqrt{N-1}$	*
7	823542	1815.62	$2\sqrt{N-1}$	275200.78	$303.25\sqrt{N-1}$	*

From the obtained results it can be concluded that there exist families of new CAZAC signals with LPCC. Moreover, the lower bound of *C* is only $2\sqrt{N-1}$ in the case of even exponents (i.e. $n = 2k$).

V. CONCLUSION

In the paper a method for synthesis of PM signals with ideal PACF has been proposed. It allows synthesizing of CAZAC sequences with unlimited lengths by means of a small signal alphabet. Besides, applying the so-named Ipatov's theorem [16], [17] the new PM signals with ideal PACF, presented in table I, can be used as initial sequences for synthesis of longer PM signals with ideal PACF.

As a result, the practical implementation of the method for synthesis of families of PM signals, proposed in the paper, will lead to:

-a significant diminishing of the negative effects, caused by the multipath spread of the electromagnetic waves [18];

- a great improvement of the signal-to-noise ratio in the output of the receivers [18], which is a very important necessary condition for providing both very high rate of information transmission and data protection in the wireless communication systems.

REFERENCES

[1] H. Holma and A. Toskala, *LTE for UMTS - OFDM and SC - FDMA Based Radio Access*, Chichester, UK, John Wiley & Sons Ltd, 2009.- 452 pp.

[2] D. C. Chu, 'Polyphase codes with good periodic correlation properties,' *IEEE Transactions Information Theory*, vol. 18, pp. 531–532, July 1972.

[3] B. Y. Bedzhev, Zh. N. Tasheva, B. P. Stoyanov, The Method for Synthesis of Perfect Two-Dimensional Arrays, Bergel House Inc., USA, *Journal of Automation and Information Science*, vol. 38, № 10, 2006, pp. 56 – 62

[4] B. Y. Bedzhev, S. Yordanov, A Method for synthesis of signals with a length of type 3^n-1, that possess an ideal periodical autocorrelation function, *International Scientific Conference of the University of Ruse "Angel Kanchev"*, Ruse, 26-27.10.2012 (In Bulgarian)

[5] B. Y. Bedzhev, S. Yordanov, A Method for synthesis of signals with a length of type 5^n-1, that possess an ideal periodical autocorrelation function, *International Scientific Conference "Mathtech 2012"*, Shumen, 22-24.11.2012 (In Bulgarian)

[6] B. Y. Bedzhev, S. Yordanov, An Algorithm for synthesis of system of signals with optimum correlation properties, *International Scientific Conference of the University of Ruse "Angel Kanchev"*, Ruse, 26-27.10.2012 (In Bulgarian)

[7] N. Y. Yu and G. Gong, "Multiplicative characters, the Weil bound, and polyphase sequence families with low correlation," *IEEE Trans. Inf. Theory*, (submitted)

[8] S. Stanev, S. Zhelezhov, T. Velikova and M. Ivanova, For the efficiency of the steganography programs, *Proceedings of the national conference with an international participation "40 years University of Shumen"*, Faculty of Mathematics and Computer Science, Shumen, 2011 (In Bulgarian)

[9] S. Stanev, I. Yakimov and S. Zhelezhov, A realization of parallel steganoanalysis with a cluster system, *International Scientific Conference "Modern methods and technologies in the scientific researches"*, Varna, 2012 (In Bulgarian)

[10] Zierler N., Linear recurring sequences, *J. Soc. Ind. Appl. Math.*, 7 (1959), №1, pp. 31–48

[11] S. Golomb and G. Gong, *Signal design for good correlation for wireless communications, cryptography and radar*, Cambridge University Press, 2005, 455 pp.

[12] S. Yordanov, A Statistical analysis of mutual correlation properties of signals with a length of type 2^n-1 и 3^n-1, that possess an ideal periodical autocorrelation function, *International Scientific Conference of the University of Ruse "Angel Kanchev"*, Ruse, 26-27.10.2012 (In Bulgarian)

[13] S. Yordanov, A Statistical analysis of mutual correlation properties of signals with a length of type 5^n-1, that possess an ideal periodical autocorrelation function, *International Scientific Conference "Mathtech 2012"*, Shumen, 22-24.11.2012 (In Bulgarian)

[14] M. B. Sverdlik, Optimal discrete signals, Moscow, Sovetskoe radio, 1975, 200 pp. (In Russian)

[15] G. Bjorck, "Functions of modulus one on Zn whose Fourier transforms have constant modulus, and cyclic n-roots," 1990, pp. 131–140.

[16] V. P. Ipatov, "Contribution to the theory of sequences with perfect periodic autocorrelation properties," *Radio Engineering and Electronic Physics*, vol. 25, pp. 31 – 34, Apr. 1980.

[17] Borislav Y .Bedzhev, Mihail P.Iliev, Stoyan S. Yordanov, Victor V. Hadzhivasilev, A Method for synthesis of signals possess ideal periodical autocorrelation function and small alphabet, Information, Comunication and Control Systems and Technologies", Year I, No 1/2012, 2012.

[18] John J. Benedetto and Jeffrey J. Donatelli, 'Ambiguity Function and Frame-Theoretic Properties of Periodic Zero-Autocorrelation Waveforms,' *IEEE Journal of Selected Topics in Signal Processing*, vol. 1, No1, pp. 6–20, June 2007.

AUTHORS PROFILE

Borislav Yordanov Bedzhev is currently a full professor in the University of Shumen "Bishop Konstantin Preslavsky" and University of Ruse "Angel Kanchev", Bulgaria. In 1991 he obtained a Ph.D. degree in communications. In 2004 he was awarded by the Bulgarian Academy of Sciences with the academic degree Doctor of Sciences in communications. He is IEEE Member since 1998. Address: University of Shumen "Bishop Konstantin Preslavsky", Faculty of Technical Sciences, Department "Communication and Computer Techniques", 115 Universitetska Str., Shumen, Bulgaria, Email: bedzhev@abv.bg, Mob tel: +359888745681

Stoyan Sabkov Yordanov received the M.Sc. engineering degree in telecommunications from the Technical University of Varna, Bulgaria, in 2009. Currently, he is a Ph.D student in the Department of Telecommunications, University of Ruse "Angel Kanchev", Russe, Bulgaria, E-mail: stoyan.yordanov1000@abv.bg , Mob tel: +359882027272

Ivo Michailov Michailov is currently a full professor in the University of Shumen "Bishop Konstantin Preslavsky". In 2001 he obtained a Ph.D. degree in algebra and number theory. In 2012 he was awarded by the Bulgarian Academy of Sciences with the academic degree Doctor of Sciences in algebra and number theory. Address: University of Shumen "Bishop Konstantin Preslavsky", Faculty of Mathematics and Informatics, Sector "Algebra and Geometry", 115 Universitetska Str., Shumen, Bulgaria, Emails: ivo@fmi.shu-bg.net ; ivo_michailov@yahoo.com , Mob tel: +359889834196, Web homepage: http://shu.bg/faculties/fmi/prepodavateli?faculty=fmi&teacherId=260#publications