

Метод за синтез на сигнали с дължина от вида 3^{n-1} , притежаващи идеална периодична автокорелационна функция

Борислав Беджев, Стоян Йорданов

The Method for Synthesis of Signals with Length 3^{n-1} , Possessing Ideal Periodic Autocorrelation Function: The signals, possessing so named ideal periodic auto-correlation function (PACF), which resembles a delta pulse, play a key role in many applications. Due to this reason these signals have been intensively studied since 1950. Despite of all taken efforts at present few classes of phase manipulated signals with ideal PACF and with symmetric signal constellation are known. With regard to this situation in the paper a new method for synthesis of signals with length $3n-1$ and ideal PACF is presented.

Key words: phase manipulated signals, ideal periodic auto-correlation function

ВЪВЕДЕНИЕ

Сигналите, притежаващи така наречената идеална периодична автокорелационна функция (ПАКФ), имаща формата на делта импулс, играят изключително важна роля в области като радиолокация, радионавигация, синхронизация на електронни автоматични устройства, кодово разделяне на абонатите в съвременните мобилни комуникационни системи и др. [1], [2], [3], [4], [5]. По тази причина те са обект на интензивни изследвания от началото на 50-те години на миналия век до сега. Напоследък дори се извършва изчерпателно търсене на такива сигнали с помощта на компютри [5]. Независимо от системно полаганите усилия към момента е известен само един клас от фазово манипулирани (ФМ) сигнали със симетрично сигнално съзвездие и идеална ПАКФ [1], [2], [3], [4], [5]. Това са така наречените последователности на Задоф и Чу [5], [6]. Съществен недостатък при използването на ФМ сигнали от този вид е пряката зависимост между дължината N на сигнала и сложността на модулацията. По-конкретно, увеличаването на дължината N се постига с цената на увеличаване на количеството на възможните начални фази на елементарните фазови импулси, с което расте и сложността на използваната апаратура, както и вероятността за грешки при приемането на сигналите, а в резултат на това се влошава шумозащитеността на комуникационните системи [1], [2], [3], [4], [5]. Предвид на това в настоящия доклад се обосновава метод за синтез на сигнали с идеална ПАКФ с дължина от вида като елементарните фазови импулси (чипове) се формират чрез несложна фазова манипулация, тъй като началната фаза приема само 3 различни стойности, докато параметърът n може да бъде произволно голям. Ето защо предимството на синтезираните в доклада сигнали в сравнение със сигналите на Задоф и Чу и производните им сигнали е, че дължината на сигналите може да бъде произволно голяма като сложността на фазовата манипулация остава постоянна. Това съществено положително свойство се постига с цената на напълно приемливо от инженерна гледна точка нарушаване на симетрията на сигналното съзвездие.

МЕТОД ЗА СИНТЕЗ НА СИГНАЛИ С ДЪЛЖИНА ОТ ВИДА $3N-1$, ПРИТЕЖАВАЩИ ИДЕАЛНА ПЕРИОДИЧНА АВТОКОРЕЛАЦИОННА ФУНКЦИЯ

ФМ сигналите, формирани на базата на линейни рекурентни последователности (ЛРП) с максимална дължина (maximal length sequences), наричани кратко M – последователности (M -sequences), са открити в началото на 50-те години на миналия век. При това се използва някакво линейно рекурентно уравнение (ЛРУ) [3], [7], [8]:

$$u(i) = d_{n-1}u(i-1) + d_{n-2}u(i-2) + \dots + d_0u(i-n) \quad (1)$$

В (1) новият $(i+1)$ -ви елемент от ЛРП $u(i+1)$ се изчислява въз основа на елементите от разглежданата ЛРП, получени в предходните моменти от време $u(i-1), u(i-2), \dots, u(i-n)$ (необходимо е началните стойности $u(0), u(1), \dots, u(n-1)$ да са зададени). Освен това коефициентите $d_{n-1}, d_{n-2}, \dots, d_0$ принадлежат на крайното алгебрично поле $GF(p^s)$ и всички алгебрични операции в уравнение (2) са изпълнение в $GF(p^s)$ (т.е. по модул p , където p може да бъде произволно просто число, а s е произволно цяло положително число).

След полагането $u(i) = x^i$ и съкращаване на x^n от (1) се получава така нареченият характеристичен полином на съответната ЛРП:

$$x^n - d_{n-1} \cdot x^{n-1} - d_{n-2} \cdot x^{n-2} - \dots - d_0 \quad (2)$$

Ако (2) е примитивен неразложим полином над $GF(p^s)$, тогава периодът на ЛРП достига максимално възможната си стойност [4], [7]:

$$N = (p^s)^n - 1 \quad (3)$$

ЛРП намират широко приложение в редица области, особено при защита на данните от несанкциониран достъп [9], [10]. По-конкретно, значението на ЛРП за комуникационните системи произтича от факта, че на тяхна база се формират периодични ФМ сигнали с близка до идеалната ПАКФ, наричани кратко М-последователности. Това се постига като комплексните обвиващи на елементарните фазови импулси (чипове) на ФМ сигналите се формират по следното правило за кодиране:

$$\zeta(i) = \exp \left[j \frac{2\pi d}{p} u(i) \right], \quad i = 0, 1, 2, \dots, N-1, \dots \quad (4)$$

Тук $1 \leq l < p$ е произволно просто число, а $u(i)$ са елементи на ЛРП с максимален период (3), изчислени чрез ЛРУ от вида (1).

ПАКФ на М-последователностите имат странични листа с постоянно относително ниво -1 . Математически това се описва с равенството:

$$P_{\zeta\zeta}(r) = \sum_{i=0}^{N-1} \zeta(i) \cdot \zeta^* \langle i+r \rangle = \begin{cases} N, & r = 0, \\ -1, & r \neq 0. \end{cases} \quad (5)$$

В (5) $P_{\zeta\zeta}(r)$ е ПАКФ на М-последователността (4), r е отместването във времето, символът " $\langle \rangle$ " означава "сума по модул p ", а символът "*" – "комплексно спрягане".

Ако се избере $p = 2$, тогава комплексните обвиващи на елементарните фазови импулси на М-последователностите, съгласно (4), могат да бъдат само -1 и $+1$. Това означава, че в този случай М-последователностите могат да се формират много просто чрез бинарна фазова манипулация (binary phase shift keying-BPSK), при която стойностите на началната фаза на елементарните фазови импулси е 0 или π радиана.

Предвид на големия контраст между централния и страничните листа на ПАКФ и удобството на техническата реализация, бинарните (двоичните) М-последователности започват да се прилагат в инженерната практика още в началото на 50-те години на миналия век. Все пак обстоятелството, че страничните листа на ПАКФ на разглежданите бинарни М-последователности не е 0 , създава определени проблеми. По-конкретно, в общата теория на комуникационните системи е доказано, че оптималната процедура за откриване на сигнали на фона на бял шум в приемника се състои във формиране на корелационния интеграл на приетия и

еталонния сигнали, при което се получава ПАКФ на приетите сигнали [4]. При постъпване на няколко припокриващи се по време сигнала с различна енергия, страничните листа на ПАКФ на силните сигнали маскират централните листа на ПАКФ на слабите сигнали. Поради този негативен ефект вероятно в края на 50-те години на миналия век е бил разработен метод [8] за корекция на М-последователностите, така че страничните листа на ПАКФ на коригираните М-последователности изчезват (стават 0). При този метод комплексните обвиващи на елементарните фазови импулси (чиповете) на М-последователностите се формират по следното правило за кодиране [8]:

$$\xi(i) = \exp[j\psi u(i)], \quad \psi = \arccos(-1 + 2^{-(n-1)}), \quad i = 0, 1, 2, \dots, N-1, \dots \quad (6)$$

Следователно коригираните М-последователности се формират чрез бинарна фазова манипулация (BPSK), при която стойностите на началната фаза на елементарните фазови импулси е 0 или ψ радиана.

По-нататък в доклада ще бъде доказано, че М-последователностите в случая $p=3$ също могат да бъдат коригирани така, че тяхната ПАКФ да получи идеална форма, т.е. относителното ниво на страничните листа на ПАКФ от -1 да стане 0. При това ще бъде използвана следната теорема, доказана в [7].

Теорема (Zierler): Нека $\{u(i)\}_{i=0}^{N-1}$, $N = p^n - 1$ е ЛРП с максимален период, чиито елементи се изчисляват по правилото (1) като аритметичните операции се извършват в GF(p). Тогава двойките $\{u(i), u(i+r)\}$, $i = 0, 1, \dots, N-1$ имат следното разпределение.

Първо, при $r \not\equiv s \pmod{N}$, $s = (p^n - 1)/(p - 1)$ всички възможни двойки $\{0, 1\}, \{0, 2\}, \dots, \{0, p-1\}, \{1, 0\}, \{1, 1\}, \dots, \{1, p-1\}, \dots, \{p-1, 0\}, \{p-1, 1\}, \dots, \{p-1, p-1\}$ се срещат по p^{n-2} пъти, а двойката $\{0, 0\}$ - $p^{n-2} - 1$ пъти.

Второ, при $r \equiv s \pmod{N}$, $s = (p^n - 1)/(p - 1)$ двойките, за които е изпълнено:

$$u(i) - u(i+r) = a, \quad a \in \{0, 1, 2, \dots, p-1\}, \quad i = 0, 1, 2, \dots, N-1 \quad (7)$$

се срещат по p^{n-1} пъти, а двойката $\{0, 0\}$ - $p^{n-1} - 1$ пъти.

В случая $p=3$ е очевидно, че всички операции в (1) следва да се извършват в GF(3) и са в сила следните съотношения:

$$N = 3^n - 1, \quad \forall u(i) \in \{0, 1, 2\} \quad (8)$$

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

М-последователностите при $p=3$ лесно могат да бъдат коригирани така, че комплексните обвиващи на техните елементарни фазови импулси да се описват с множеството (10) вместо с множеството (9):

$$\forall \zeta(i) \in \left\{ x = e^{j\varphi_x}, y = e^{j\varphi_y}, y^{-1} = e^{-j\varphi_y} \right\} \quad (10)$$

От Теоремата на Zierler се получава система от 2 уравнения, от които неизвестните комплексни обвиващи на елементарните фазови импулси x и y могат да се определят така, че относителното ниво на страничните листа на коригираните М-последователности от -1 да стане 0. При $p=3$ броят на уравненията е 2 по следната причина. По принцип съгласно Теоремата на Zierler би следвало да се

анализират в случаите:

$$r \neq s, r = 1.s, r = 2.s, \dots, r = (p-1).s \quad (11)$$

Известно е обаче, че ПАКФ на сигналите е комплексно-симетрична, т.е. [4], [8]:

$$P_{\zeta\zeta}(r) = P^*_{\zeta\zeta}(N-r), \quad r = 1, 2, \dots, N-1 \quad (12)$$

С оглед на (12), вместо всички възможни случаи (11) е достатъчно да бъдат разгледани само $(p+1)/2$ случая:

$$r \neq s, r = 1.s, r = 2.s, \dots, r = [(p-1)/2].s \quad (13)$$

При $p = 3$ това са случаите $r \neq s, r = 1.s$, които водят до следната система от 2 уравнения с 2 неизвестни, принадлежащи на множеството (10):

$$\begin{cases} 3^{(n-2)}(x+y+y^{-1}).(x^{-1}+y+y^{-1})-1=0 \\ 3^{(n-1)}(y^2+y^{-2})-1=0 \end{cases} \quad (14)$$

Като се отчете, че $2.y.y^{-1} = 2$ изразът в скобите във второто уравнение на (14) се допълва до точен квадрат, при което се получава:

$$y + y^{-1} = \pm \sqrt{1 + 3^{-(n-1)}} \quad (15)$$

След отчитане на равенство (15) в първото уравнение на (14), резултатът е:

$$3^{(n-2)}(x \pm \sqrt{1 + 3^{-(n-1)}}).(x^{-1} \pm \sqrt{1 + 3^{-(n-1)}}) - 1 = 0 \quad (16)$$

След разкриване на скобите в (16) се вижда, че:

$$x + x^{-1} = \frac{-2 + 2.3^{-(n-1)}}{\pm \sqrt{1 + 3^{-(n-1)}}} \quad (17)$$

Сега като се отчете, че $x + x^{-1} = 2 \cos \varphi_x$, $y + y^{-1} = 2 \cos \varphi_y$ окончателно се получава:

$$\varphi_x = \arccos \left(\frac{-1 + 3^{-(n-1)}}{\pm \sqrt{1 + 3^{-(n-1)}}} \right), \quad \varphi_y = \arccos \left(\frac{\pm \sqrt{1 + 3^{-(n-1)}}}{2} \right) \quad (18)$$

Директното изследване при различни стойности на n доказва, че М-последователностите при $p = 3$ могат да бъдат коригирани така, че тяхната ПАКФ да получи идеална форма. За целта комплексните обвиващи на техните елементарни фазови импулси в процеса на фазовата манипулация трябва да получат вида (10) като началните фази φ_x и φ_y се определят от равенства (18).

ЗАКЛЮЧЕНИЕ

В настоящия доклад е представен метод за синтез на ФМ сигнали като комплексните обвиващи на техните елементарни фазови импулси приемат само 3 различни стойности. Синтезираните сигнали притежават следните предимства:

1. Тяхната ПАКФ е идеална, т.е. има формата на делта импулс. В резултат на това значително се намалява риска от маскиране на слабите сигнали от по-силните в приемниците на комуникационните системи. Този положителен ефект се постига с напълно приемливо от инженерна гледан точка нарушаване на симетрията на сигналното съзвездие.

2. За разлика от сигналите на Задоф и Чу, при предложените в доклада сигнали не съществува връзка между дължината на сигналите и сложността на модулацията.

ЛИТЕРАТУРА

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

[2] Zhelev S., O. Fetfov, Advantages of ultra wide band technology in reconnaissance work, 3rd International Conference, Military Technical Faculty of National Defence University, Budapest, 2005

[3] Желев С., Спътникови комуникации, Университетско издателство "Еп. К. Преславски", Шумен, 2012, ISBN978-954-577-619-9

[4] Варакин Л. Е., Системы связи с шумоподобными сигналами - М.: Радио и связь, 1985. – 384 с.

[5] Benedetto J. J., J. J. Donatelli, Ambiguity function and frame-theoretic properties of periodic zero-autocorrelation waveforms, IEEE J. of Selected Topics in Signal Processing, vol.1, No.1, pp. 6-20, June 2007.

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

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

[8] Bedzhev B. Y., 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

[9] Станев С., С. Железов, Т. Великова, М. Иванова, За ефективността на стеганографските програми, Сборник трудове на национална конференция с международно участие „40 години Шуменски университет“, ФМИ, Шумен, 2011

[10] Станев С., И. Якимов, С. Железов, Реализация на паралелен стеганализ с клъстерна система, Международна научна конференция "Съвременни методи и технологии в научните изследвания", Варна, 2012 (под печат)

За контакти:

проф. дтн инж. Борислав Йорданов Беджев, Катедра "Телекомуникации", Русенски университет "Ангел Кънчев", E-mail: bedzhev@abv.bg

инж. Стоян Събков Йорданов, докторант в Катедра "Телекомуникации", Русенски университет "Ангел Кънчев", E-mail: stoyan.yordanov1000@abv.bg

Докладът е рецензиран.



**РУСЕНСКИ УНИВЕРСИТЕТ „АНГЕЛ КЪНЧЕВ”
UNIVERSITY OF RUSE „ANGEL KANCHEV“**

ДИПЛОМА

**Програмният комитет на
Научната конференция РУ&СУ'12
награждава с КРИСТАЛЕН ПРИЗ
“THE BEST PAPER”**

**проф. д-тн БОРИСЛАВ БЕДЖЕВ и
инж. СТОЯН ЙОРДАНОВ**

автори на доклада

**“Метод за синтез на сигнали с дължина от вида 3^{n-1} ,
притежаващи идеална
периодична автокорелационна функция”**

DIPLOMA

**The Programme Committee of
the Scientific Conference RU&SU'12
Awards the Crystal Prize "THE BEST PAPER"
to Prof. BORISLAV BEDZHEV, Dsc and
Eng. STOYAN YORDANOV
authors of the paper**

**“Method for Synthesis of Signals with Length 3^{n-1} ,
Possessing Ideal Periodic Autocorrelation Function”**

**РЕКТОР
RECTOR**

**проф. д.т.н. Христо Белоев
Prof. DSc Hristo Beloev, DHC**

30.10.2012