МЕТОДИКА ЗА СИНТЕЗ НА КОМПЛЕМЕНТАРНИ БИНАРНИ ФАЗОВО МАНИПУЛИРАНИ СИГНАЛИ С ДЪЛЖИНА N=1MOD4

Пламен Янакиев[1], Цветослав Цанков[2]
[1] *Шуменски университет „Епископ Константин Преславски“*
[2] *Шуменски университет „Епископ Константин Преславски“*

METHODOLOGY FOR SYNTHESIS OF COMPLEMENTARY BINARY PHASE MANIPULATED SIGNALS WITH LENGTH N=1MOD4

Plamen Yanakiev[1], Tsvetoslav Tsankov[2]
[1] *Konstantin Preslavsky University of Shumen*
[2] *Konstantin Preslavsky University of Shumen*

Abstract

The phase manipulated (PM) signals which periodic autocorrelation functions (PACF) have small side-lobes are very important for the radars, sonars, radio-navigation and radio-synchronization systems. Due to this reason in the paper a general methodology for synthesis of ideal binary complementary PM signals with lengths N=1mod4, N prime, is suggested. The results, obtained in the paper, could be applied in the process of development of new radio-communication devices, used for precise measurement of distances.

Keywords: ideal periodic autocorrelation functions; phase manipulated signals; synthesis of signals.

ВЪВЕДЕНИЕ

За радио-локационните, радио-навигационните и радио-синхронизиращите системи е много важно използваните сигнали да имат идеални периодични автокорелационни функции (ПАКФ), наподобяващи делта импулс. Основната причина за това е, че контрастът между основния (централния) лист и страничните листа на ПАКФ определя разделителната способност и полезния ефект от разделната обработка с последващо натрупване на радио сигналите, преминали по различни пътища [1].

От гледна точка на простотата и надеждността при практическата реализация, най-предпочитани са бинарните фазово манипулирани (ФМ) сигнали, чиято ПАКФ има странични листа с минимално възможно ниво. По тази причина те са обект на интензивни изследвания през последните шестдесет години, но откритите до момента класове от бинарни ФМ сигнали с идеална или перфектна ПАКФ не могат да задоволят потребностите на практиката [1], [2], [3]. Отчитайки тази ситуация, целта на доклада е да се направи детайлен анализ на класическия метод за синтез на така наречените сигнали на Льожандър с дължина $N = p \equiv 1\ mod\ 4$, който да послужи за основа за разработването на методика за синтез на комплементарни (допълнителни) бинарни ФМ сигнали и да доведе до изясняване на връзката между бинарните перфектни ФМ сигнали на Льожандър и на идеалните биунимодуларни ФМ сигнали на Бьорк с дължина $N = p \equiv 1\ mod\ 4$.

АНАЛИЗ НА КЛАСИЧЕСКИЯ МЕТОД ЗА СИНТЕЗ НА ПЕРФЕКТНИ БИНАРНИ ФАЗОВО МАНИПУЛИРАНИ СИГНАЛИ С ДЪЛЖИНА N=1 MOD4

За бинарните ФМ сигнали с дължина $N = p \equiv 1\ mod 4$ е в сила следната теорема [2].

Теорема 1: Бинарният ФМ сигнал, чиято дължина е просто нечетно число

$$N = p \equiv 1\, mod4, \tag{1}$$

а отчетите му са формирани по правилото (за кодиране)

$$s(0) = \pm 1,\ \ s(i) = (-1)^{ind_\theta i}, \tag{2}$$

$$i = 1, 2, \dots, p-1,$$

имат следната ПАКФ

$$s(0) = +1 \to Q_{ss}(r) =$$

$$= \begin{cases} N,\ r = 0, \\ 1, ind_\theta r \equiv 0 mod2, \\ -3, ind_\theta r \equiv 1 mod2, \end{cases} \tag{3}$$

$$s(0) = -1 \to Q_{ss}(r) =$$

$$= \begin{cases} N,\ r = 0, \\ 1, ind_\theta r \equiv 1 mod2, \\ -3, ind_\theta r \equiv 0 mod2. \end{cases} \tag{4}$$

Доказателство: Както е известно, индексът на i по отношение на *примитивния елемент* (*корен*) θ на полето на Галоа $GF(p)$ $ind_\theta i$ е аналог на операцията логаритмуване (в безкрайните алгебрични полета) [4]. По-конкретно, във всяко крайно алгебрично поле $GF(p^n)$ съществува най-малко един примитивен елемент θ, който се характеризира с това, че редицата

$$\theta^1 = \theta, \theta^2, \dots, \theta^{p^n-1}, \tag{5}$$

съдържа всичките $p^n - 1$ ненулеви елементи на $GF(p^n)$ [4]. По тази причина, в случаите на прости алгебрични полета, когато $n = 1$, редицата

$$\theta^1 = \theta, \theta^2, \dots, \theta^{p-1}, \tag{6}$$

е просто някаква пермутация

$$\pi(1), \pi(2), \dots, \pi(p-1), \tag{7}$$

на числата

$$1, 2, \dots, p-1. \tag{8}$$

Следователно индексът на i по отношение на примитивния елемент (корен) θ се определя от равенствата

$$i = \theta^{\pi(i)} \to ind_\theta i =$$

$$= \pi(i),\ \ i = 1, 2, \dots, p-1. \tag{9}$$

За ПАКФ на бинарните ФМ сигнали с дължина $N = p \equiv 1\, mod4$ е в сила анализът, направен при доказателството на Теорема 2 от [5], при което е изпълнено

$$Q_{ss}(r) =$$

$$= -1 + s(0)\left[(-1)^{\pi(r)} + (-1)^{\pi(p-r)}\right]. \tag{10}$$

Сега обаче

$$\pi(-1) = \tfrac{p-1}{2} \equiv 1\, modp, \tag{11}$$

тъй като $p \equiv 1\, mod4$. Действително

$$p \equiv 1\, mod4 \to p = 4n + 1 \to$$

$$\to \tfrac{p-1}{2} = 2n \equiv 0 mod2. \tag{12}$$

Следователно

$$Q_{ss}(r) = -1 + s(0)(-1)^{\pi(r)}(1 + 1) =$$

$$= -1 + 2s(0)(-1)^{\pi(r)}, \tag{13}$$

което доказва теоремата.

Не е трудно да се провери, че Теорема 1 остава в сила, ако отчетите на ФМ сигнала с дължина $p \equiv 1\, mod4$ са формирани по правилото (за кодиране)

$$s(0) = \pm 1,\ \ s(i) = (-1)^{ind_\theta i + 1}, \tag{14}$$

$$i = 1, 2, \dots, p-1.$$

Теорема 1 ще бъде илюстрирана със следния пример.

Пример 1: Нека $\{s(i)\}_{i=0}^{N-1}$ е бинарен ФМ сигнал с дължина $N = p = 5 \equiv 1\, mod4$ като отчетите му са формирани по правилото (за кодиране) (14).

Както е известно, крайното алгебрично поле $GF(5)$ има два примитивни елемента

$$\theta_1 = 2,\ \ \theta_2 = 3. \tag{15}$$

Непосредствено се проверява, че последователните степени на $\theta_1 = 2$, $\theta_2 = 3$ представляват всички ненулеви елементи на $GF(5)$, макар и подредени в някакъв разбъркан ред

$$\theta_1^1 = \theta_1 = 2, \theta_1^2 = 4, \theta_1^3 = 3, \theta_1^4 = 1, \tag{16}$$

$$\theta_2^1 = \theta_2 = 3, \theta_2^2 = 4, \theta_2^3 = 2, \theta_2^4 = 1. \tag{17}$$

Последователностите (16) и (17) демонстрират Свойствата 1, 2, 3 и 4 на крайните алгебрични полета (*полетата на Галоа*) $GF(p^n)$, разгледани в [4]. Тук следва специално да се отбележи, че съгласно Свойство 4 при разбиването на елементите на $GF(p^n)$ на непресичащи се класове при

фиксирани стойности на множителите m, d класът $C_{cl}(1)$ не зависи от конкретния избор на примитивен елемент.

Следователно, Теорема 1 може да се преформулира по следния начин.

Теорема 1А: Бинарният ФМ сигнал, чиято дължина е просто нечетно число

$$N = p \equiv 1\ mod 4, \tag{18}$$

а отчетите му са формирани по правилото (за кодиране)

$$s(0) = \pm 1,\ \ s(i) = \begin{cases} 1, & i = a^2 \\ -1, & i \neq a^2, \end{cases} \tag{19}$$

$$i = 1, 2, \dots, p-1,$$

имат ПАКФ, съответстваща на ограниченията (3) или (4).

Естествено, правилото (за кодиране) (19) може да се опише и чрез символа на Льожандър [2], [4], [5]

$$s(0) = \pm 1,\ \ s(i) = \left(\frac{i}{p}\right), \tag{20}$$

$$i = 1, 2, \dots, p-1.$$

Това дава основание ФМ сигналите, синтезирани по правилото (2) (или еквивалентните правила (19) и (20)), също да бъдат наричат *сигнали* (*последователности*) *на квадратичните остатъци* или *сигнали* (*последователности*) *на Льожандър с дължина* $N = p \equiv 1\ mod 4$.

Както се вижда от (3) и (4), половината от страничните листа на ПАКФ на сигналите на Льожандър имат ниво -3. В редица практически случаи обаче е необходимо ПАКФ на ФМ сигналите изобщо да нямат странични листа. При $N \equiv 1\ mod\ 4$ това може да се постигне само чрез използване на фазова манипулация, която е по-сложна от бинарната. Например в литературата е посочено следното правило (за кодиране)

$$s(0) = 1,\ \ s(i) = \begin{cases} s(i) = \begin{cases} x, & i = a^2, \\ x^*, & i \neq a^2, \end{cases} \end{cases}$$

$$i = 1, 2, \dots, p-1,\ N = p \equiv 3\ mod\ 4 \tag{21}$$

като тук x е комплексно число с модул 1:

$$x = cos\varphi + jsin\varphi = e^{j\varphi},\ j = \sqrt{-1},$$

$$x^* = cos\varphi - jsin\varphi = e^{-j\varphi}. \tag{22}$$

Правилото (за кодиране) (21) е установено от *Г. Бьорк* (*G. Bjorck*) през 80-те години на миналия век [6], но в Интернет няма ресурс, съдържащ неговата обосновка. Предвид на тази ситуация следва да се отбележи, че анализът на класическия метод за синтез на перфектни бинарни ФМ сигнали с дължина $N = p \equiv 1\ mod\ 4$, направен до тук в доклада, създава предпоставките правилото (за кодиране) (21) да бъде доказано строго в [7].

МЕТОДИКА ЗА СИНТЕЗ НА КОМПЛЕМЕНТАРНИ БИНАРНИ ФАЗОВО МАНИПУЛИРАНИ СИГНАЛИ С ДЪЛЖИНА N=1 MOD4

От (21) ясно се вижда, че при дължина на сигнала $N = p \equiv 1\ mod 4$ страничните листа на неговата ПАКФ се отстраняват по метода на Бьорк чрез използване на несиметрична троична фазова манипулация, която усложнява конструкцията на предавателите и приемниците и влошава шумоустойчивостта на радио- комуникационните системи. Предвид на това в настоящия параграф ще бъде обоснована методика за минимизиране на страничните листа на ПАКФ на сигналите на Льожандър с дължина $N = p \equiv 1\ mod 4$ при запазване на бинарната фазова манипулация.

По-конкретно, нека предавателят на радио-комуникационната система излъчва по два различни канала два сигнала на Льожандър с дължина $N = p \equiv 1\ mod 4$ като първият от тях $\{s_1(i)\}_{i=0}^{N-1}$ е формиран по правилото за кодиране

$$s_1(0) = +1,\ \ s_1(i) = (-1)^{ind_\theta i}, \tag{23}$$

$$i = 1, 2, \dots, p-1,$$

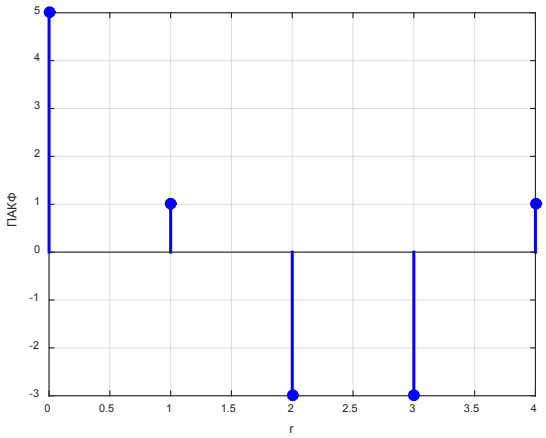
а вторият $\{s_2(i)\}_{i=0}^{N-1}$ – по правилото за кодиране

$$s_2(0) = -1,\ \ s_2(i) = (-1)^{ind_\theta i}, \tag{24}$$

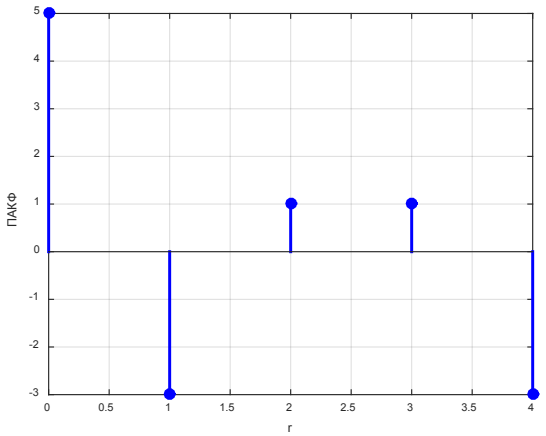
$$i = 1, 2, \dots, p-1.$$

ФМ сигналите $\{s_1(i)\}_{i=0}^{N-1}$ и $\{s_2(i)\}_{i=0}^{N-1}$ се приемат и обработват в приемника в два различни канала, след което се сумират на междинна или видео честота. От (3) и (4) се вижда, че сумарната ПАКФ на сигналите (23) и (24) става еквивалентна на ПАКФ на сигналите на Льожандър с дължина $N = p \equiv 3\ mod 4$, тъй като

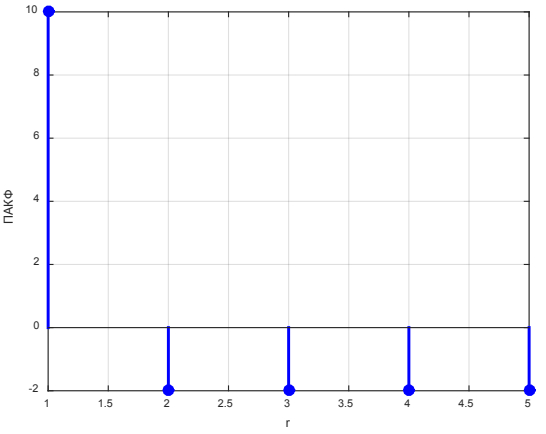
$$Q_{sum}(r) = Q_{s_1 s_1}(r) + Q_{s_2 s_2}(r) = \\ = \begin{cases} 2N, & r = 0, \\ -2, & r \neq 0. \end{cases} \quad (25)$$



а) ПАКФ на ФМ сигнала $\{s_1(i)\}_{i=0}^{N-1}$



б) *ПАКФ на ФМ сигнала* $\{s_2(i)\}_{i=0}^{N-1}$



в) *Сума на ПАКФ на ФМ сигналите* $\{s_1(i)\}_{i=0}^{N-1}$ *и* $\{s_2(i)\}_{i=0}^{N-1}$

Фиг. 1. *ПАКФ на сигналите на Льожандър с дължина* $N = p = 5 \equiv 1 \; mod4$*, чиито отчети са формирани по правилата (23) и (24)*

Този извод се пояснява на фиг. 1.

Напълно аналогичен резултат се получава, ако вместо (23) и (24) се използват следните правила за кодиране

$$s_1(0) = +1, \;\; s_1(i) = (-1)^{ind_\theta i + 1}, \quad (26)$$

$$i = 1, 2, \ldots, p-1,$$

$$s_2(0) = -1, \;\; s_2(i) = (-1)^{ind_\theta i + 1}, \quad (27)$$

$$i = 1, 2, \ldots, p-1.$$

Методът за елиминиране на страничните листа на ПАКФ чрез сумиране на ПАКФ на два бинарни ФМ сигнала е изобретен от *М. Голай* (*M. Goley*) [2], [3]. По тази причина те се наричат *комплементарни* (или *допълнителни*) *двойки* (*complementary pairs*) или *двойки на Голай* (*Goley's pairs - GPs*). В класическото определение на комплементарните сигнали [2] се изисква страничните листа на ПАКФ на бинарните ФМ сигнали от двойката да се компенсират напълно, т.е.

$$Q_{GP}(r) = Q_{s_1 s_1}(r) + Q_{s_2 s_2}(r) = \\ = \begin{cases} 2N, & r = 0, \\ 0, & r \neq 0. \end{cases} \quad (28)$$

Тук $Q_{s_1 s_1}(r)$ и $Q_{s_2 s_2}(r)$ са r –тите отчети на ПАКФ на ФМ сигналите от комплементарната двойка, а $Q_{GP}(r)$ е тяхната сума.

В теоретичните изследвания е доказано следното необходимо условие за съществуване на класически комплементарни двойки от бинарни ФМ сигнали [2]

$$(K_{1+} - K_{1-})^2 + (K_{2+} - K_{2-})^2 = 2N \; . \quad (29)$$

Тук K_{1+} и K_{1-} са количествата на $+1$ –ците и -1 –ците в първия бинарен ФМ сигнал, а K_{1+} и K_{1-} са количествата на $+1$ –ците и -1 –ците във втория бинарен ФМ сигнал от комплементарната двойка. Освен това

$$K_{1+} + K_{1-} = K_{2+} + K_{2-} = N \; . \quad (30)$$

От (29) и (30) следва, че мрежата от стойности на дължината N в диапазона $1 \leq N \leq 50$, за които могат да съществуват комплементарни двойки от бинарни ФМ сигнали, е

$$N = 1, 2, 4, 8, 10, 16, 20, 26, 34, 40, 50 \; . \quad (31)$$

От (31) се вижда, че при нарастване на дължината N, гъстотата на мрежата от възможни стойности бързо намалява. В съвре-

менните радио-комуникационни системи обаче се използват ФМ сигнали, съдържащи хиляди отчети, тъй като при технологията *директно разширяване на спектъра* (*direct spreading of the spectrum*) подобряването на отношението сигнал/шум по мощност на изхода на приемника е [3]

$$\frac{q^2_{\text{изх пр}}}{q^2_{\text{вх пр}}} = 2N_{\text{c}} . \qquad (32)$$

Тук $q^2_{\text{вх пр}}$ и $q^2_{\text{изх пр}}$ са отношенията сигнал/шум по мощност на входа и изхода на приемника съответно, а N_{c} е броят на отчетите (чиповете) на използвания бинарен ФМ сигнал (ако ФМ сигналите са комплементарна двойка, то очевидно $N_{\text{c}} = 2N$). В англоезичната литература коефициентът (32) е прието да се нарича *processing gain*.

От (32) следва, че при проектирането на съвременни радио-комуникационни системи е необходимо мрежата от стойности на дължината N на ФМ сигналите да бъде достатъчно плътна в диапазона $1000 \le N \le 1000000$. Ето защо двойките от сигнали на Льожандър, формирани по правилата за кодиране (23), (24) или (26), (27), могат успешно да се използват за повишаване шумоустойчивостта на радио-комуникационните системи, използващи технологията директно разширяване на спектъра.

От изложените аргументи произтича коректността и практическата значимост на следната методика.

Методика за синтез на комплементарни бинарни фазово манипулирани сигнали с дължина $N = p \equiv 1\, mod 4$

Стъпка 1: Задаване на дължината $N = p \equiv 1\, mod\, 4$ на ФМ сигналите от комплементарната двойка.

Стъпка 2: Изчисляване на квадратите на всички числа $\{1, 2, \dots, p-1\}$ по $mod\ p$, т.е.

$$a_i \equiv i^2 mod\ p,\ i = 1, 2, \dots, p-1. \qquad (33)$$

Стъпка 3: От числата a_i, изчислени на предходната стъпка, се взема един пълен комплект от $N_a = (p-1)/2$ на брой различни числа. Този комплект представлява класа

$$d = 2,\ C_{cl}(1) = \{a_{i_0}, a_{i_1}, \dots, a_{i_{N_a-1}}\} \qquad (34)$$

на квадратичните остатъци по $mod\ p$.

Стъпка 4: Отчетите на бинарните ФМ сигнали $\{s_1(i)\}_{i=0}^{N-1}$ и $\{s_2(i)\}_{i=0}^{N-1}$ от комплементарната двойка се изчисляват по правилата (за кодиране) (23), (24) или (26), (27) съответно.

От (25) се вижда, при използването на комплементарната технология бинарните сигнали на Льожандър с дължина $N = p \equiv 1\, mod 4$ стават еквивалентни на бинарните сигнали на Льожандър с дължина $N = p \equiv 3\, mod 4$. Действително, отношенията (контрастите) между основния (централния) лист и максималния страничен лист на ПАКФ на бинарните сигнали на Льожандър с дължина $N = p \equiv 1\, mod 4$ и $N = p \equiv 3\, mod 4$ са съответно

$$C_{p\equiv 1} = \frac{Q_{SS}(0)}{\underset{i\neq 0}{max}|Q_{SS}(i)|} = \frac{2N}{2} = N, \qquad (35)$$

$$C_{p\equiv 3} = \frac{Q_{SS}(0)}{\underset{i\neq 0}{max}|Q_{SS}(i)|} = \frac{N}{1} = N. \qquad (36)$$

От друга страна, практическото използване на комплементарната технология води до усложняване на предавателите и приемниците на радио-комуникационните системи. Този негативен ефект обаче може да се пренебрегне предвид на следните факти. Първо, двата комуникационни канала, по които се предават и обработват двата комплементарни бинарни ФМ сигнала, могат да се изградят от унифицирани компоненти с ниска цена. Второ, на практика дължината на сигналите се удвоява и, следователно, отношението сигнал/шум по мощност на изхода на приемника също се удвоява.

ЗАКЛЮЧЕНИЕ

През изминалите петдесет години методите за синтез на ФМ сигнали са били разработвани най-често като решения на частни инженерни проблеми. Днес обаче теорията на синтеза на ФМ сигнали трябва да може да обясни свойствата на различните класове ФМ сигнали от възможно най-общи позиции. Предвид на тази необходимост в доклада е направен детайлен анализ на класическия метод за синтез на перфектни бинарни ФМ сигнали с дължина $N = p \equiv 1\, mod\ 4$. На тази основа са получени два основни резултата.

Първо, обоснована е методика за синтез на комплементарни бинарни ФМ сигнали с дължина $N = p \equiv 1\ mod\ 4$, която се характеризира с простота, универсалност и ефективност от изчислителна гледна точка. Методиката дава възможност да се използва комплементарна технология, при която отношението (контрастът) между основния (централния) лист и максималния страничен лист на ПАКФ на бинарните сигнали на Льожандър с дължина $N = p \equiv 1\ mod 4$ се повишава от $C_{p\equiv 1} = \frac{N}{3}$ на $C_{p\equiv 1} = N$.

Второ, създадени са предпоставките за изясняване на връзката между бинарните перфектни ФМ сигнали на Льожандър и на идеалните би-унимодуларни ФМ сигнали на Бьорк с дължина $N = p \equiv 1\ mod\ 4$.

БЛАГОДАРНОСТИ

Настоящата статия се реализира във връзка с Проект РД-08-144/08.02.2018 г. – Интегрирана развойна тестова среда за информационна сигурност, финансиран от ШУ „Епископ Константин Преславски“.

REFERENCE

[1] N. Levanon and E. Mozeson, Radar signals, Wiley-Interscience, 2004, 427 pp.

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

[3] V. P. Ipatov, Spread spectrum and CDMA. Principles and Applications, Willey, 2006. - 373 pp.(in Russian)

[4] R. Lidl and H. Niederreiter, Finite fields, London: Addison-Wesley Publishing Company, 1983, 818 pp.

[5] P. Yanakiev and Ts. Tsankov, Methodology for synthesis of perfect phase manipulated signals with length N=3 mod 4, In: Proceedings of the International scientific conference UNITECH 2018, 16-17.11.2018, Gabrovo, Bulgaria (in press)

[6] B. Saffari, Some polynomial extremal problems which emerged in the twentieth century, In: Twentieth century harmonic analysis-a celebration, pp. 201-233, Kluwer Academic Publishers, 2001

[7] B. Bedzhev and P. Yanakiev, A survey of methods for synthesis of ideal phase manipulated signals with length N=1 mod 4, In: Proceedings of the International scientific conference MATTECH 2018, 25-27.10.2018, Shumen, Bulgaria (in press)