

Алгоритъм за синтез на системи от сигнали с оптимални корелационни свойства

Борислав Беджев, Стоян Йорданов

***The Algorithm for Synthesis of Systems of Signals with Optimal Correlation Properties:** A key role for the present wireless communications play the systems (families) of signals, possessing so named optimal correlation properties. With regard in the paper an algorithm for synthesis of systems of phase manipulated signals with length p^{n-1} , possessing ideal periodic auto-correlation function (PACF), is presented. The algorithm could be used in the process of developing of new wireless communication systems, providing ultra high rate of information transmission.*

Key words: phase manipulated signals, signals with optimal correlation properties.

ВЪВЕДЕНИЕ

За съвременните безжични комуникационни системи изключително важна роля имат корелационните свойства на използваните системи (семейства) от сигнали, тъй като те осигуряват едновременно достъп на потребителите до ресурсите на системите. Тази ситуация обуславя изключителния интерес към проблема за синтез на семейства, състоящи се от сигнали, които притежават едновременно идеална периодична автокорелационна функция (ПАКФ) с формата на делта импулс и нулева периодична взаимно – корелационна функция (ПВКФ) между всички двойки от сигнали в семейството [1], [2], [3], [4], [5]. Установените чрез теоретичен анализ ограничения показват [1], [2], [3], [4], [5], [6], че само семействата от комплементарни сигнали, наричани още сигнали на Голай, притежават посочените корелационни свойства. Тези семейства от сигнали се реализират практически само чрез едновременно използване на поне два типа модулация (например честотна и фазова, поляризационна и фазова и т.н.), което е съпроводено със съществено усложняване на предавателната и приемната апаратура на комуникационните системи. По тази причина в момента се извършват интензивни изследвания, целящи откриването на семейства от фазово манипулирани (ФМ) сигнали, при които максималното ниво на ПАКФ (без централния лист) и ПВКФ са възможно най-малки, а сложността на фазовата манипулация е приемлива от икономическа гледна точка [1], [2], [3], [4], [5]. Отчитайки теоретичните ограничения, зададения вид на фазовата манипулация и дължината на сигналите N , посоченият проблем се свежда до намирането на множество (система от сигнали) Φ (K, N, C), съдържащо максимално възможния брой K от ФМ сигнали, така че максималното относително ниво на листата на ПАКФ (без централния лист) и ПВКФ да не превишава величината [1], [2], [3], [4], [5]:

$$C = \alpha \sqrt{N} \quad (1)$$

Тук α е коефициент, а дължината N показва количеството на елементарните фазови импулси (чипове), съдържащи се във всеки сигнал от семейството.

Следва да се отбележи, че посоченият проблем в много случаи не може да се реши на базата само на теоретични анализи [1], [2], [3], [4], [5], [6]. Предвид на това в настоящия доклад се обосновава алгоритъм за синтез на системи (семейства) от ФМ сигнали с дължина от вида $N = p^n - 1$ като тук p е просто число, а n е произволно цяло положително число. ФМ сигналите от синтезираните семейства се характеризират с идеална ПАКФ, имаща формата на делта импулс, а максималното относително ниво на ПВКФ не превишава величината (1). Предвид на изложеното по – горе, резултатите от изследването могат да се използват в процеса на разработване на нови безжични комуникационни системи, осигуряващи свръхвисока скорост на предаване на информацията.

Алгоритъм за синтез на системи от сигнали с оптимални корелационни свойства

ФМ сигналите, формирани на базата на линейни рекурентни последователности (ЛРП) с максимална дължина (maximal length sequences), наричани кратко М – 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]:

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

където новият $(i+1)$ -ви елемент $u(i+1)$ от ЛРП се пресмята на базата на елементите $u(i-1), u(i-2), \dots, u(i-n)$ от разглежданата ЛРП, получени в предходните моменти от време (необходимо е началните стойности $u(0), u(1), \dots, u(n-1)$ да са задаени).

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:

$$u(i) = x^i \quad (3)$$

и съкращаване на x^n , се получава така нареченият характеристичен полином на съответната ЛРП (2):

$$x^n - d_{n-1}x^{n-1} - d_{n-2}x^{n-2} - \dots - d_0 \quad (4)$$

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

$$N = (p^s)^n - 1 \quad (5)$$

От (2) и (4) се вижда, че ако е известен характеристичният полином на някаква ЛРП, чрез него много лесно се възстановява съответното ЛРУ, при което става възможно да се изчисляват всички елементи на ЛРП.

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:

$$\zeta(i) = \exp\left[j\frac{2\pi d}{p}u(i)\right], \quad i = 0, 1, 2, \dots, N-1, \dots \quad (6)$$

Тук $1 \leq l < p$ е произволно просто число, а $u(i)$ са елементи на ЛРП с максимален период (5), изчислени чрез ЛРУ от вида (2).

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

$$P_{\zeta\zeta}(r) = \sum_{i=0}^{N-1} \zeta(i) \cdot \zeta^*(i+r) = \begin{cases} N, & r = 0, \\ -1, & r \neq 0. \end{cases} \quad (7)$$

В (7) $P_{\zeta\zeta}(r)$ е ПАКФ на М-последователността (6), 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 (6), 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 при разграничаването (разделянето) в приемника на няколко припокриващи се по време сигнала с различна енергия. Поради този негативен ефект вероятно в края на 50-те години на миналия век е бил разработен метод [8] за корекция на кодовата последователност, така че страничните листа на ПАКФ на коригираната М-последователност изчезват (стават 0). При този метод комплексните обвиващи на елементарните фазови импулси (чиповете) на М-последователностите се формират по следното правило за кодиране, при което стойностите на началната фаза на елементарните фазови импулси е 0 или радиана:

$$\xi(i) = \exp[j\psi \cdot u(i)], \quad \psi = \arccos(-1 + 2^{-(n-1)}), \quad i = 0, 1, 2, \dots, N-1, \dots \quad (8)$$

Аналогично, в [11] е обоснован метод за коригиране на М-последователностите при $p = 3$. Съгласно този метод комплексните обвиващи на елементарните фазови импулси (чипове) на М-последователностите се формират по следното правило за кодиране:

$$\begin{aligned} \forall \zeta(i) \in \left\{ x = e^{j\varphi_x}, y = e^{j\varphi_y}, y^{-1} = e^{-j\varphi_y} \right\}; \\ \varphi_x = \arccos\left(\frac{-1 + 3^{-(n-1)}}{\pm \sqrt{1 + 3^{-(n-1)}}}\right), \quad \varphi_y = \arccos\left(\frac{\pm \sqrt{1 + 3^{-(n-1)}}}{2}\right) \end{aligned} \quad (9)$$

Следва да се отбележи, че от всяка М-последователност може да се формира множество (семејство) $U(N_t, N)$ от N_t на брой сигнали като предварително се разместят елементите на съответната ЛРП с максимален период (кодова последователност) по следния начин [7]:

$$u_j(i) = u\langle d_j \cdot i \rangle_{\text{mod } N}, \quad d_j = 1, 2, \dots, N_t, \quad i = 0, 1, 2, \dots, N-1, \dots \quad (10)$$

Тук $d_j, j = 1, 2, \dots, N_t$ са всички положителни цели числа, които са по-малки от N и са взаимно прости с N , а символът $\langle d_j \cdot i \rangle_{\text{mod } N}$ означава, че произведението $d_j \cdot i$ се привежда по модул N . Както е известно [4], [5], [6], [7], N_t се изчислява чрез

така наречената φ -функция на Ойлер, т.е. $N_t = \varphi(N) = \prod_{k=1}^L (p_k^{e_k} - p_k^{e_k-1})$ като тук

$N = p_1^{e_1} \cdot p_2^{e_2} \cdot \dots \cdot p_L^{e_L}$ е представянето на дължината на М-последователността като произведение от прости числа.

Разместването (пермутацията) на елементите на някоя ЛРП (респективно на някоя М-последователност) по правилото (10) се нарича децимация. Теоретично е доказано [4], [5], [6], [7], че децимираните М-последователности (ФМ сигнали), запазват формата на ПАКФ (т.е. страничните листа на ПАКФ остават с постоянно

относително ниво -1). Ето защо М-последователностите от дадено множество $U(N_t, N)$ могат да се коригират, аналогично на (8) и (9), при което страничните листа на техните ПАКФ изчезват. При това очевидно ще се изпълнява условието (1) по отношение на максималните нива на страничните листа на ПАКФ. Оттук произтича следният Алгоритъм.

Алгоритъм за синтез на системи от сигнали с оптимални корелационни свойства

Първо, от справочници (например [4], [6], [7]) се избират примитивни неразложими полиноми над $GF(p)$ като на p се дават стойности $n = n_0, n_0 + 1, \dots, n_{\max}$. Тук n_0 се определя от необходимата минимална шумозащитеност на комуникационната система [4], а $n_{\max}$ се ограничава от максималната дължина на ФМ сигналите, която може да се използва практически със съвременните технологии.

Второ, предвид на еднозначно обратимото съответствие между характеристикния полином на дадена ЛРП и нейното ЛРУ, от всеки избран на предходната стъпка примитивен неразложим полином се получава ЛРУ (2), чрез което се изчисляват елементарните фазови импулси на М-последователностите при всяка от стойностите на p .

Трето, изчислените на предходната стъпка М-последователности се децимират по правилото (10) като се използват съответните децимационни коефициенти $d_j, j = 1, 2, \dots, N_t$ и така за всяка стойност на p се формира по едно множество $U(N_t, N)$ от децимирани М-последователности.

Четвърто, М-последователностите (ФМ сигналите) от множествата $U(N_t, N)$ се коригират, съгласно (8) и (9), в резултат на което страничните листа на ПАКФ на М-последователностите от множествата $U(N_t, N)$ изчезват (стават 0).

Пето, с помощта на компютри се изчисляват ПВКФ на всички възможни двойки коригирани М-последователности от множествата $U(N_t, N)$. На тази база се отстранява минимално възможното количество коригирани М-последователности от множествата $U(N_t, N)$, така че останалите М-последователности да представляват системи (семейства) $\Phi(K, N, C)$, съдържащи максимално възможния брой K от ФМ сигнали, при което максималното относително ниво на листата на ПВКФ да не превишава величината (1).

ЗАКЛЮЧЕНИЕ

В настоящия доклад е обоснован алгоритъм за синтез на системи (семейства) от сигнали с оптимални корелационни свойства. Семействата се състоят от максимално възможния брой K от ФМ сигнали с дължина $N = p^n - 1$ като максималното относително ниво на листата на ПАКФ (без централния лист) и ПВКФ не превишава величината (1).

Обоснованият в доклада алгоритъм притежава следните предимства:

1. ПАКФ на ФМ сигналите от всяко синтезирано семейство 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.

2. Чрез алгоритъма могат да се синтезират всички възможни системи от коригирани М-последователности. Това е така, тъй като е доказано [7], че всяка ЛРП над $GF(p)$ с характеристикен полином от n -та степен, е еквивалентна на ЛРП над $GF(p)$ с характеристикен полином е от sn -та степен.

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] Hellesteth T, P. V. Kumar, Sequences with low correlation, Chapter in: Handbook in Coding Theory. (Eds. V.S. Pless and W.C. Huffman), Elsevier 1998.
- [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)
- [11] Беджев Б., С. Йорданов, Метод за синтез на сигнали с дължина от вида $3n-1$, притежаващи идеална периодична автокорелационна функция, Международна научна конференция на РУ „А. Кънчев“, Русе, 26-27.10.2012 (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.