ШУМЕНСКИ УНИВЕРСИТЕТ
„ЕПИСКОП КОНСТАНТИН ПРЕСЛАВСКИ“

Цветослав Станиславов Цанков

АЛГОРИТМИ ЗА СИНТЕЗ НА ПЕРИОДИЧНИ ШУМОПОДОБНИ ФАЗОВО МАНИПУЛИРАНИ СИГНАЛИ С ВИСОКА СТРУКТУРНА СЛОЖНОСТ

АВТОРЕФЕРАТ

на дисертация

за получаване на образователна и научна степен „доктор“

по научна специалност: Радиолокация и радионавигация

Научен ръководител:
проф. дтн инж. Борислав Йорданов Беджев

Рецензенти:
проф. д-р инж. Михаил Петков Илиев
проф. д-р инж. Иван Кръстев Цонев

Шумен, 2014 г.

Дисертацията е разработена в Шуменския университет „Епископ Константин Преславски“. Дисертантът работи в същия университет. Дисертационният труд е обсъден и насрочен за защита на разширено заседание на катедра „Комуникационна и компютърна техника“ към Факултета по технически науки на 22 май 2014 г.

Дисертационния труд съдържа 180 страници, от които 65 са приложения. Включени са 27 фигури и 13 таблици. Списъкът на използваната литература се състои от 118 заглавия, от които 7 на български, 22 на руски и 89 на английски език.

Защитата на дисертационния труд ще се състои на 11.07.2014 г. от 11:00 ч. в зала С5 на корпус „С“.

Материалите по защитата са на разположение в Шуменския университет „Епископ Константин Преславски“, ул. „Университетска“ №115, корпус 1, каб. 107, както и в сайта на университета – http://shu.bg/.

Съдържание на дисертационния труд

Обща характеристика на дисертационния труд

Актуалност на проблема

Съвременните комуникационни системи непрекъснато разширяват количеството и качеството на услугите, които предлагат. Поставят се все по-високи изисквания към осигуряването на подходяща среда за пренос на данни. В последните години броят на потребителите на мобилни комуникации драстично е нараснал. Същевременно е налице тенденцията на ориентирането на потребителското търсене от услуги, свързани с пренос на речеви данни към такива, при които водещ е обмена на мултимедийни данни при възможно по-високи скорости. Това налага използването на сложни сигнали, притежаващи така наречената идеална периодична автокорелационна функция (ИПАКФ), имаща формата на делта импулс. Тези сигнали играят изключително важна роля в областта на радиолокацията и радионавигацията, а също и при синхронизация на електронни автоматични устройства, кодово разделяне на абонатите, синхронизация и оценка на канала в съвременните мобилни комуникационни системи. Така сега особено актуален е въпросът за синтезиране на системи от сигнали с подходящи авто- и взаимно-корелационни свойства за осигуряване на среда за достъп на по-голям брой потребители на комуникационните системи при по-висока скорост на обмен на данни.

Цел на изследването

Целта на дисертационния труд е да се разработят алгоритми за синтез на периодични шумоподобни фазово манипулирани сигнали с висока структурна сложност, чието приложение да доведе до повишаване на капацитета и шумозащитеността при проектирането и разработването на съвременни комуникационни системи.

Предмет на изследване и разработка

Предмет на дисертационния труд е синтезът на сложни шумоподобни сигнали, осигуряващи висока скритост и разделителна способност по разстояние на радиолокационните комплекси.

Структура и обем на дисертационния труд

Дисертационният труд се състои от увод, четири глави, заключение, литературни източници и приложения.

В първа глава са изложени теоретичните основи в обработката на радиолокационната информация. Изясняват се качествените показатели на радиолокационната информация. Формулирани са целите и задачите на дисертационния труд.

Във втора глава се решава проблемът за количественото измерване на структурната сложност на равномерните ФМ сигнали чрез рекурентни последователности. Оценяват се съвременните методи за измерване на структурната сложност на тези сигнали.

В трета глава са обосновани алгоритми за синтез на периодични ФМ сигнали с висока структурна сложност, при които използването на филтър, потискащ страничните листа (ФПСЛ) е съпроводено с малки загуби в отношението сигнал/шум. Обърнато е внимание и на влиянието на коефициента на загубите върху големината на зоната на обзор на радиолокационните станции (РЛС).

В четвърта глава е описана системата за автоматизиран синтез на двойки „периодичен шумоподобен ФМ сигнал с висока структурна сложност – филтър за потискане на страничните листа на ПАКФ“. Представени са някои от най-добрите резултати от изследването.

Основните резултати по дисертационния труд паралелно са изнесени на международни научни конференции в България и чужбина и са публикувани в специализирани списания.

Глава I

Съвременно състояние на методите за синтез на периодични шумоподобни фазово манипулирани сигнали с висока структурна сложност

Най-сложните РЛК, използвани на съвременния етап от развитието на науката и техниката, са РЛК, използвани за целите на противовъздушната отбрана (ПВО) и за управление на въздушното движение (УВД). По тази причина по-нататък в настоящия параграф основното внимание ще бъде фокусирано върху обработката на радиолокационната информация (ОРЛИ) в РЛК за УВД.

От функционална гледна точка РЛК се състоят от следните компоненти:

1. Измервателен РЛК, включващ една или няколко радиолокационни станции (РЛС), които измерват плоските или пространствените координати на въздушните обекти;
2. Комплекс от изчислителни средства за ОРЛИ;
3. Комплекс от средства за предаване на информация между елементите на РЛК и към потребителите;
4. Средства за управление, предназначени за обезпечаване съгласуваната работа на всички елементи.

Оценките на ефективността на системите се правят с цел обосноваване на проектно-конструкторските решения за създаване на нови или модернизиране на вече съществуващите системи. Стремежът

при проектирането така да се изберат параметрите на новата система, така че тя да има най-голяма ефективност произтича от необходимостта търсенето на оптимални решения да бъде пренесено от евристическа на строго математическа основа.

От най-общи позиции се приема, че ефективността на дадена система е мяра за съответствието на резултатите от функционирането на системата на поставените й за изпълнение задачи и на направените разходи за обезпечаване на това функциониране. В повечето случаи паричното измерване на разходите не е трудно. Сложността на количественото определяне на ефективността произтича от твърде разнообразния характер на задачите, които се възлагат на големите системи. Много от тези задачи, като например ценността на спасените човешки животи, политическият авторитет и престиж и др., въобще нямат паричен еквивалент.

Всяка голяма система е изградена от редица подсистеми. По тази причина ефективността на всяка подсистема се определя от частта, която тя внася в общата ефективност на системата от по-висок порядък.

При повишаване ефективността на системите се използват два основни подхода:

- повишаване ефективността на системата чрез подобряване качеството на изпълнение на възложените й задачи, при което материалните разходи не превишават някакъв разумен предел;
- повишаване ефективността на системата чрез намаляване на материалните разходи за нейното изграждане и поддържане без да се влошава качеството на функционирането й.

Много често за създаване на критерий за ефективност на дадена система, отговарящ на горните изисквания, се въвеждат междинни параметри, които обикновено се наричат показатели за качеството на системата:

1. Зона на наблюдение на РЛК.
2. Пълнота на изображението.
3. Точност на изображението.
4. Пропускателна способност.
5. Достоверност на изображението.
6. Шумозащитеност.
7. Експлоатационна надеждност на РЛК.
8. Своевременност.
9. Стойност.
10. Критерий за ефективност.

Тези показатели са значително по-малко от общия брой параметри, от които зависи ефективността на системата, но всеки един от

тях описва достатъчно пълно част от съществените й особености. Критерият се конструира като функция, чиито аргументи са показателите за качество на системата.

След откриване на типа и местоположението на РЛК от ПВО или УВД за тяхното радиоелектронно подавяне или физическо унищожение се използват следните средства: активните смущения, пасивните средства за РЕП, мощните йонизиращи лъчения, стелт технологиите, непреднамерените смущения. Използването на РЕП от злонамерени лица, престъпни и терористични групи влияе отрицателно върху всички показатели на качеството на РЛК. Ето защо:

– радиоелектронната защита трябва да бъде комплексна и всеобхватна;

– РЛК трябва да са построени на такива технически принципи, че злонамерените лица (респективно престъпните и/или терористичните групи) да бъдат максимално затруднени в организирането и провеждането на РЕП.

Развитието и широкото внедряване на "ударната радиолокация" в момента се затруднява от няколко технологични проблема като например: сложността и все още високата цена на апаратурата за генериране и обработка на сигналите, намаляването на коефициента на полезно действие на антените при намаляване дължината на вълната и др. Ето защо, основно направление за развитие на РЛК на настоящия етап е използването на сложни сигнали със свръх голяма база, получени в резултат на разширяване на спектъра чрез дискретна вътрешноимпулсна честотна или фазова манипулация.

Ако в РЛК се използват сложни сигнали, тогава те ще имат висока скритост и шумоустойчивост, т.е. висока шумозащитеност. Освен подобряването на шумозащитеността, използването на СС в комуникационните системи позволява да се води борба с негативните ефекти, породени от многолъчевото разпространение на радиовълните. Многолъчевостта възниква в такива случаи, когато радиовълните отиват в точката на приемане, отразявайки се от различни препятствия по пътя на разпространение (слоевете на йоносферата, сгради, хълмове и т.н). Различията в дължината на пътищата на тези вълни довежда до различното им закъснение в точката на приемане. В резултат, ако сигналите идват по различни пътища и се препокриват във времето, то между тях възниква интерференция, която на свой ред предизвиква затихване на резултантния сигнал на входа на приемника.

В съвременните комуникационни системи най-голямо приложение намират следните сложни сигнали:

- честотно-модулирани (ЧМ) сигнали;

- фазоманипулирани (ФМ) сигнали (direct sequence (DS) complex signals);

- дискретни честотни (ДЧ) сигнали (наричани още честотно манипулирани (ЧМ) сигнали или frequency hopping (FH) complex signals);

- дискретни честотни съставни (ДЧС) сигнали, (frequency hopping-direct sequence (FH-DS) complex signals; frequency hopping-frequency hopping (FH-FH) complex signals).

Към системите от сигнали, използвани в съвременните комуникационни системи и в частност РЛК, се поставят следните основни изисквания:

1. Да бъдат системи от широколентови сигнали с:

1.1. ниска спектрална плътност;

1.2. висока структурна сложност,

осигуряващи скритост по отношение на радио-техническото разузнаване (РТР). Както беше посочено, тези свойства осигуряват на сигналите *ниска вероятност за прехващане – low probability for interception* (or *detection*) (LPI, LPD).

2. Да притежават така наречените *оптимални корелационни свойства* (ОКС), чрез които се постига:

2.1. Висока *разделителна способност по разстояние* (*high time or distance resolution*), позволяваща разделна обработка на лъчите, преминали по различни пътища (в противен случай възниква *самосмущаване* (*fading*) (*self interference* – SE), предизвикано от интерференцията на сигналите, преминали по различни пътища (ехото на предхождащите символи се наслагва върху пристигащите в момента следващи символи от съобщенията).

2.2. Възможност за едновременна работа на много потребители при допустимо ниво на *взаимните смущения* (*multi access interference* – MAI), т.е. добра електромагнитна съвместимост.

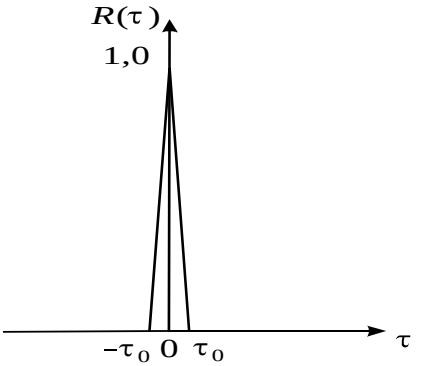
3. Процесите на генерация и обработка на сигналите трябва да могат да се реализират практически чрез апаратура с приемливи размери и цена.

Изискването 2.1. за високата разделителна способност по разстояние е много важно за РЛК, тъй като в съответствие с теорията на оптималното приемане, обработката на приетите сигнали в комуникационните системи се осъществява с оптимален приемник. В най-общ случай напрежението на изхода на оптималния приемник има вида, показан на фиг. 1.3.1. В процеса на работа на РЛК е напълно възможно на един и същи азимут да има няколко цели в интервал по разстояние с размери от порядъка на

$$\Delta d \approx T.(c/2), \qquad (1)$$

като тук ***c*** е скоростта на разпространение на електромагнитните вълни, а ***T*** е продължителността на сондиращия импулс на РЛС. В такава ситуация продуктите от свиването на ехо-сигналите се смесват на изхода на оптималния приемник, при което е възможно страничните листа на АКФ на ехо-сигналите от цел с голяма *ефективна отразяваща повърхност* (ЕОП), да са по-големи от главния лист на АКФ на ехо-сигналите от малоразмерна цел. В резултат на това ехо-сигналите от малоразмерната цел, която може да представлява много по-съществена опасност, няма да бъдат открити. За да се избегне този крайно нежелателен ефект на маскиране на ехо-сигналите, е необходимо СС, използвани в РЛК, да осигуряват висока разделителна способност по
разстояние. От направения анализ се вижда, че всъщност изискването 2.1. се свежда до изискванията:

2.1.1. Сигналите, използвани от РЛК, следва да имат АКФ с така наречената *идеална форма* подобна на *делта-импулс*, показана на фиг. 1, която осигурява максимално възможната *разделителна способност по разстояние* Δd поради отсъствието на странични листа (пикове);



Фиг. 1: *Автокорелационна функция на сложен сигнал с идеална форма*

2.1.2. Продължителността $2\tau_0$ на основния лист на АКФ на сигнала трябва да бъде възможно най-малка.

От анализа на свойствата на сложните шумоподобни сигнали, направен до тук, произтичат следните изводи.

Извод 1. Структурната сложност на ЧМ сигналите е малка. Освен това формата на техните АКФ се влияе съществено от измененията в честотата на ехо-сигналите, причинени от *ефекта на Доплер*. По тази причина ЧМ сигналите почти не се използват в РЛК за ПВО и УВД, проектирани и произведени след 1990 г.

Извод 2. Изискване 2.1.2. се удовлетворява сравнително лесно при използването на равномерни ФМ, ДЧ или ДЧС сигнали, тъй като при тях

$$\tau_0 = \tau_{ch},\ T = N.\tau_{ch}, \tag{2}$$

като тук $\boldsymbol{T}$ е продължителността на сондиращия импулс, а $\boldsymbol{N}$ е броят на елементарните импулси (чиповете) в него.

От (1) и (2) се вижда, че ако в РЛК се използват равномерни ФМ, ДЧ или ДЧС сигнали, висока точност се постига като се скъсява продължителността τ_{ch} на елементарните импулси (чиповете). Освен това разделителната способност по разстояние Δd се подобрява като се използват сигнали с АКФ с идеална форма (фиг. 1), тъй като в този случай

$$\Delta d \approx \tau_{ch}.(c/2), \tag{3}$$

при което зоната Δd се скъсява $N = T/\tau_{ch}$ пъти.

Извод 3. Синтезирането на равномерни ФМ, ДЧ или ДЧС с идеална АКФ като показаната на фиг. 1, осигуряваща максимално възможната разделителна способност по разстояние при зададена продължителност τ_{ch} на елементарните импулси (чиповете), е много сложен и нерешен до край проблем в теорията на комуникационните системи, поради което въпреки интензивните изследвания през последните 50 години, в настоящия момент са известни само малък брой такива сигнали.

Извод 4. Равномерните ФМ сигнали отговарят във висока степен на всички изисквания към системите от сигнали, използвани в съвременните РЛК. Осен това те имат следните предимства в сравнение с другите основни типове сложни сигнали.

Първо, на настоящия етап са известни няколко класа равномерни ФМ сигнали, притежаващи много висока структурна сложност, която им

осигурява много висока скритост за РТР. Характерна черта за тези класове е използването на силно нелинейни преобразования и функции в процеса на техния синтез.

Второ, равномерните ФМ сигнали се открояват и с относителната простотата на процесите на генерация и обработка, което позволява да се реализират практически с малка по габарити апаратура и на ниска цена. Ето защо равномерните ФМ сигнали намират широко приложение в най-различни РЛК и особено в безпилотните самолети и роботите с дистанционно управление, които в момента се развиват много динамично в количествено и качествено отношение.

Извод 5. Равномерните ФМ сигнали отстъпват на ДЧ и ДЧС сигналите единствено по показателите 2.1.1. и 2.2., които изискват листата (без централния лист) на АКФ и на взаимно-корелационните функции (ВКФ) на всички двойки сигнали от едно семейство, да бъдат малки. Тук следва да се има предвид, че в теорията на сигналите са доказани така наречените *граници на Уелч* и *на Сидельников*. Съгласно тези граници, ако дължината на равномерните ФМ сигнали в семейството е N, тогава максималният брой K сигнали в семейството е:

$$K = \sqrt{N}\,, \tag{4}$$

а минималното ниво на листата на АКФ (без централния лист) и ВКФ е:

$$C_{\min} \geq \sqrt{N}\,. \tag{5}$$

Ограниченията (4) и (5) обаче са в сила при обработката на приетите ФМ сигнали с *оптимален* (наричан още *съгласуван*) *филтър*. Ето защо те могат да бъдат преодолени, ако се използват *несъгласувани филтри*.

Извод 6. Използването на специално подбрани несъгласувани филтри позволява получаването на отклик (реакция) с идеалната форма на делта-импулс, както това е показано на фиг. 1, за голям брой равномерни ФМ сигнали. Предвид на това закономерно възниква проблемът за откриване на такива класове равномерни ФМ сигнали, при които обработката с несъгласувани филтри е съпроводено с минимални загуби в отношението *сигнал*/*шум* (С/Ш, *signal-to-noise ratio* – SNR).

Предвид на тези изводи целта на дисертационния труд е:

Да се разработят алгоритми за синтез на периодични шумоподобни фазово манипулирани сигнали с висока структурна

сложност и съответните несъгласувани филтри, осигуряващи на съвременните РЛС висока шумозащитеност, точност и разделителна способност по разстояние.

За постигане на тази цел е необходимо да се решат следните основни задачи:

1. Да се анализира съвременното състояние на методите за синтез на периодични шумоподобни ФМ сигнали с висока структурна сложност и да се обосноват перспективните пътища за тяхното развитие.

2. Да се систематизират методите за количествена оценка на структурната сложност на равномерните ФМ сигнали.

3. Да се разработят алгоритми за синтез на периодични шумоподобни ФМ сигнали с висока структурна сложност и съответните несъгласувани филтри, осигуряващи идеална форма на периодичната АКФ (ПАКФ) при минимални загуби в отношението сигнал/шум.

4. Да се разработи система за автоматизиран синтез на предложените нови периодични шумоподобни ФМ сигнали с висока структурна сложност и съответните несъгласувани филтри, позволяваща да се анализират техните корелационни свойства.

Глава II

Методи за количествено измерване на структурната сложност на равномерни фазово манипулирани сигнали

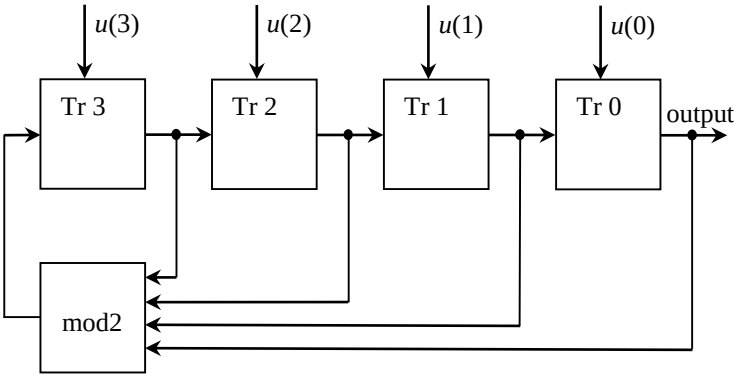
В съвременните комуникационни системи се използват два основни метода за формиране на степенните последователности на равномерните ФМ сигнали. Първият от тях е разработен в началото на 50-те години на миналия век и се основава на така наречените *линейните рекурентни последователности* (ЛРП).

ЛРП намират широко приложение в математиката, защитата на информацията, синтеза на сложни сигнали за съвременните комуникационни системи и др. области на науката и техниката. За тяхното генериране се използва някакво линейно рекурентно уравнение (ЛРУ), чиито общ вид е:

$$u(i) = a_{n-1}.u(i-1) + a_{n-2}.u(i-2) + ... + a_0.u(i-n) \quad (1)$$

В (1) новият *i*-ти елемент $u(i)$ от ЛРП се изчислява въз основа на елементите $u(i-1), u(i-2), ..., u(i-n)$ от разглежданата ЛРП, получени в предходните моменти от време (необходимо е началните стойности $u(0), u(1), ..., u(n-1)$ да са зададени). Освен това се счита,

че операциите в (1) и коефициентите $a_{n-1}, a_{n-2}, ..., a_0$ са дефинирани в някакво алгебрично поле, което може да бъде безкрайно (числово) или крайно (поле на Галоа).



Фиг. 1: *Електрическа схема, реализираща ЛРП от ЛРУ* $u(i) = u(i-1) + u(i-2) + u(i-3) + u(i-4)$ *, когато началните елементи на ЛРП са от полето* $GF(2)$

Предвид на структурата им, електрическите схеми, реализиращи ЛРП, е прието да се наричат *преместващи регистри с линейни обратни връзки* (*ПРЛОВ*), а съответният английски термин е *linear feedback shift registers* (LFSRs).

Алгоритъм за подреждане на елементите на крайно алгебрично поле по степените на примитивен елемент

1. От справочници се взема примитивен неразложим полином над $GF(p)$ от желаната степен ***n*** (тук ***p*** е произволно просто число).

2. Избраният полином се приравнява на 0 и се разглежда като характеристичен полином на ЛРП.

3. За начални елементи на ЛРП се вземат елементите:

$$u(0) = \begin{bmatrix} 1 \\ 0 \\ ... \\ 0 \end{bmatrix} = 1, \; u(1) = \begin{bmatrix} 0 \\ 1 \\ ... \\ 0 \end{bmatrix} = \beta, ..., u(n-1) = \beta^{n-1} = \begin{bmatrix} 0 \\ 0 \\ ... \\ 1 \end{bmatrix}. \qquad (2)$$

4. Последователно се изчисляват елементите $u(n),u(n+1),...,u(p^n-1)$ на ЛРП.

5. Редицата $u(1),u(2),...,u(n-1),u(n),u(n+1),...,u(p^n-1)$ представлява последователните степени на примитивния елемент β :

$$\beta^1,\beta^2,...,\beta^{n-1},\beta^n,\beta^{n+1},...,\beta^{p^n-1},$$

която съдържа всички ненулеви елементи на $GF(p^n)$ в някакъв псевдо-случаен ред.

Алгоритъмът се характеризира със следните положителни свойства:

Първо, алгоритъмът е много ефективен от изчислителна гледна точка, тъй като използва само събиране на вектори-стълбове и умножение на числа с вектори-стълбове по модул ***p***. По тази причина той много лесно се реализира софтуерно, например с Matlab.

Второ, чрез алгоритъма всъщност се синтезират степенните последователности на равномерните ФМ сигнали с *максимална дължина* (*maximal length sequences*), наричани кратко *М-последователности* (*M-sequences*), които са открити в началото на 50-те години на миналия век. Както е известно, при М-последователностите не се налага сигналното съзвездие (или броят на възможните стойности, които началната фаза на ФМ сигнала приема) да бъде усложнявано за да се увеличи тяхната база. Освен това *периодичните автокорелационни функции* (ПАКФ) на М-последователностите имат странични листа с постоянно относително ниво -1. С други думи, ПАКФ на М-последователностите имат близка до идеалната форма, осигуряваща максимално възможната разделителна способност по разстояние при зададена стойност на продължителността на елементарните фазови импулси (чиповете) τ_{ch} . По тази причина М-последователностите започват да се прилагат в радиолокационните и радионавигационните системи още в началото на 50-те години на миналия век.

Трето, подреждането на елементите на крайно алгебрично поле по степените на примитивен елемент е основна стъпка при синтезирането и на други сложни псевдо-случайни радио сигнали като например GMW сигнали (това са сигнали, чиито степенни последователности са последователности на Gordon-Mills-Welch), дискретно-честотни сигнали (масиви на Костас) и др.

Доказват се следните твърдения:

Твърдение 1: Всяка ЛРП освен чрез ЛРУ от вида (1) може да се генерира и чрез следното деление на полиноми

$$\begin{aligned}&\frac{B(x)}{D(x)} = U(x) = \\ &= u(0) + u(1).x + ... + u(i-n).x^{i-n} + ... \\ &+ u(i-1).x^{i-1} + u(i).x^{i} + ...\end{aligned} \tag{3}$$

като тук знаменателят $D(x)$ е реципрочният полином на характеристичното уравнение (5) на ЛРП, а коефициентите на числителя $B(x)$ се определят еднозначно от известните начални стойности (елементи) $u(0),u(1),...,u(n-1)$ на ЛРП и от коефициентите на знаменателят $D(x)$.

Твърдение 2: Ако степента на полинома $B(x)$ е строго по-малка от степента на полинома $D(x)$ и $d_n \neq 0$ в резултат на тяхното деление се получава безкрайна последователност, която може да се формира и чрез ЛРУ от вида (1). При това $D(x)$ е реципрочният полином на характеристичното уравнение на ЛРУ (1), а началните стойности $u(0),u(1),...,u(n-1)$ на ЛРП се определят от системата:

$$\left|\begin{array}{c} u(0) = b_0 / d_n \\ u(1) = \left[b_1 - u(0).d_{n-1}\right] / d_n \\ ..... \\ u(n-1) = \left[b_{n-1} - u(0).d_1 - u(1).d_2 - ... - u(n-1).d_{n-1}\right] / d_n \end{array}\right. \tag{4}$$

Вторият основен метод за формиране на степенните последователности на равномерните ФМ сигнали в съвременните комуникационни системи се основава на така наречените *полиномиални функции* и е разработен в началото на 80-те години на миналия век.

По-конкретно при този метод елементите на степенните последователности на равномерните ФМ сигнали се определят чрез някаква *полиномиална функция* (или просто полином), чиито общ вид е:

$$f(x)=\sum_{i=0}^{M} a_i . x_{n-1}^{c_{n-1,i}} . x_{n-2}^{c_{n-2,i}} ... x_1^{c_{1,i}} x_0^{c_{0,i}} \ . \qquad (5)$$

Полиномиалната функция (5) съпоставя на всеки елемент от разширеното крайно алгебрично поле $GF(p^n)$ един елемент от простото крайно алгебрично поле $GF(p)$.

От гледна точка на практическото синтезиране на равномерни ФМ сигнали с помощта на компютри, преминаването на аргумента $x=(x_{n-1}, x_{n-2},..., x_0)$ на полиномиалната функция (5) в експоненциален ред през елементите на $GF(p^n)$ има следните предимства:

Първо, експоненциалното подреждане на елементите на $GF(p^n)$ се реализира лесно с алгоритъма, използващ свойствата на ЛРП.

Второ, експоненциалното подреждане на елементите на $GF(p^n)$ е трудно за предвиждане дори при неголеми стойности на ***p*** и ***n***.

Трето, съществуват голям брой различни експоненциални подреждания на елементите на $GF(p^n)$, чиито общ вид е:

$$(\alpha^d)^0, (\alpha^d)^1, \ ..., (\alpha^d)^{n-2}. \qquad (6)$$

Тук *d* е произволно цяло число, което е взаимно-просто с p^n-1. Известно е, че *d* може да бъде избрано по $\varphi(p^n-1)$ различни начина. При това $\varphi(l)$ е така наречената *фи-функция на Ойлер*, която дава броя на всички естествени числа, които са по-малки и взаимно-прости с ***l***

$$\varphi(l)=\left(p_1^{c_1}-p_1^{c_1-1}\right)\left(p_2^{c_2}-p_2^{c_2-1}\right)..\left(p_k^{c_k}-p_k^{c_k-1}\right). \qquad (7)$$

Използването на експоненциално подреждане на елементите на $GF(p^n)$ при синтеза на равномерни ФМ сигнали затруднява много

работата на противниковото радио-електронно разузнаване, тъй като за него конкретният вид на генераторния полином и стойността на $\boldsymbol{d}$ са неизвестни параметри.

Скритостта е фактор от първостепенно значение за ефективността на РЛК. При това изхождайки от задачите, които решава РТР, скритостта се класифицира като *енергетическа*, *структурна* и *информационна* (т.е. *криптоустойчивост*). *Енергетическата скритост* се характеризира със способността системата да остане незабелязана от разузнавателните приемни устройства. *Структурната скритост* характеризира способността на системата да затрудни максимално разкриването на принципите на модулация на сигнала, неговите честотни и временни параметри. Следователно за увеличаване на структурната скритост е необходимо в системата да могат да се използват голям брой сигнали, както и да е възможно достатъчно бързо да се изменя формата на сигналите. *Информационната скритост* се характеризира със способността на системата да противостои на мерките, насочени към разкриване на смисъла на предаваната с помощта на сигнали информация. Информационната скритост се нарича още *криптоустойчивост* и представлява важен самостоятелен научен проблем, но тя има съществено значение за РЛК само в режим на *активен отговор* от съпровожданите обекти. Следователно в режим на *пасивен отговор*, който е основен за повечето РЛК, анализът на скритостта без загуба на общност може да се сведе само до тяхната енергетическа и структурна скритост. Енергетическата и структурната скритост обаче са много тясно свързани и взаимно обусловени. По-конкретно, използваните в момента широколентови шумоподобни сигнали имат много ниска спектрална плътност, която им осигурява много висока енергетична скритост. Оттук закономерно произтича извод.

Извод 1: На съвременния етап повишаването на скритостта на РЛК в максимална степен се основава на използване на сигнали с висока структурна сложност.

Предвид на този извод естествено възниква проблемът за количествена оценка на структурната сложност на сигналите, използвани в радиолокационните комплекси. За неговото решаване основна роля има следното твърдение.

Твърдение 1: Степенната последователност на всеки периодичен равномерен ФМ сигнал може да се формира чрез ЛРП.

$$V(x) = \frac{B_0(x)}{D_0(x)}. \tag{8}$$

Определение 1: Степента на полинома в знаменателя на (8) се нарича *линейна сложност* (*linear complexity*) на периодичната последователност.

Синоним на понятието *линейна сложност* (*linear complexity*) е изразът *линеен обхват* (*linear span*).

Практическото значение на величината линейна сложност произтича от това, че в средата на 60-те години на миналия век американските теоретици *Берлекемп* (*Berlekamp*) и *Меси* (*Massey*) създават алгоритъм, наречен по-късно на техните имена – *алгоритъм на Берлекемп-Меси* (*Berlekamp-Massey algorithm*), който позволява да се определи ЛРУ, формиращо произволна целочислена периодична последователност

$$S = \{s(0), s(1), ..., s(N-1), s(N), s(N+1), ..., s(2N-1), ...\} = \{s(i)\}_{i=0}^{\infty}, \quad \forall i,\ s(i) \in \{0,1,..., p-1\} = Z_p \tag{9}$$

на базата на известни $2\boldsymbol{n}$ произволни последователни елемента от нея

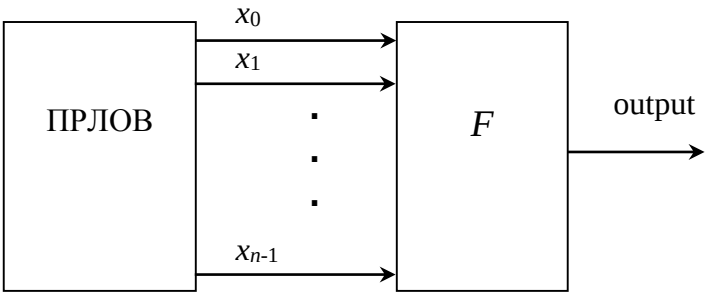
$$\left\{ \begin{matrix} s(j), s(j+1), ..., s(j+n-1), \\ s(j+n), s(j+n+1), ..., s(j+2n-1) \end{matrix} \right\}. \tag{10}$$

В (10) $\boldsymbol{n}$ е линейната сложност на последователността (9).

Извод 2: Нека $\boldsymbol{n}$ е линейната сложност на степенната последователност на равномерен периодичен ФМ сигнал, използван от някакъв РЛК. Тогава ако радио-електронното разузнаване правилно регистрира (прихване) произволни $2\boldsymbol{n}$ последователни елементарни импулса (чипа) от ФМ сигнала, тогава злонамерените лица, престъпните и/или терористичните групи, използвайки алгоритъма на Берлекемп-Меси, ще могат да имитират абсолютно точно ФМ сигнала на РЛК и вредният ефект за РЛК от радио-електронното подавяне ще бъде максимален.

Извод 3: За да се осуети използването на атаката на Берлекемп-Меси от злонамерените лица, престъпните и/или терористичните групи е достатъчно равномерните ФМ сигнали, използвани от РЛК, да имат висока структурна сложност, осигуряваща висока линейна сложност на степенната последователност на ФМ сигнала.

Предвид на Извод 3, общата схема на генераторите на степенни последователности на равномерни ФМ сигнали, има вида, показан на фиг. 2.



Фиг. 2: *Обща схема на генераторите на степенни последователности на равномерни ФМ сигнали с висока структурна сложност*

Тук блокът ПРЛОВ представлява преместващ регистър с линейни обратни връзки. Този блок формира в експоненциален ред елементите на $GF(p^n)$

Извод 4: За да се затрудни максимално работата на радиоелектронното разузнаване, е необходимо степенните последователности на равномерните ФМ сигнали, използвани от РЛК, да се формират чрез обработка на съдържанието на регистрите на ПРЛОВ от схемата на фиг. 2 с нелинейни функции, устойчиви към всички известни в момента криптоаналитични атаки.

От анализа, направен в глава втора произтичат следните изводи.

1.На съвременния етап се използват два основни метода за формиране на степенните последователности на равномерните ФМ сигнали. Първият от тях е разработен в началото на 50-те години на миналия век и се основава на така наречените линейните рекурентни последователности. При втория метод, предложен в началото на 80-те години на миналия век, се използват полиномиални функции.

2.В режим на пасивен отговор, който е основен за повечето РЛК, скритостта всъщност се свежда само до тяхната енергетическа и структурна скритост. При това е достатъчно вниманието на конструкторите на РЛК да бъде фокусирано върху осигуряването на висока структурна сложност на използваните сигнали, тъй като

периодичните шумоподобни ФМ сигнали по принцип притежават много ниска спектрална плътност, която обуславя висока енергетична скритост.

3.Структурната сложност на равномерните ФМ сигнали се определя от параметъра линейна сложност, който представлява алгебричната степен на характеристичното уравнение на ЛРП, формиращо степенната последователност на ФМ сигнала. При това на базата на доказаните Твърдения в Глава II се обосновава универсален метод за количествено измерване на структурната сложност не само на равномерните ФМ, но и на равномерните ДЧ сигнали, тъй като конкретната физическа природа на сигнала няма значение при извеждането на формула (9).

4.За да се затрудни максимално работата на радиоелектронното разузнаване, е необходимо степенните последователности на равномерните ФМ сигнали, използвани от РЛК, да се формират чрез обработка на съдържанието на регистрите на ПРЛОВ от схемата на фиг. 2 с нелинейни функции, устойчиви към всички известни в момента крипто-аналитични атаки.

Глава III

Алгоритми за синтез на периодични шумоподобни фазово манипулирани сигнали с висока структурна сложност

Периодичните шумоподобни ФМ сигнали отговарят във висока степен на всички изисквания към системите от сигнали, използвани в съвременните РЛК. Всъщност ФМ сигналите отстъпват на ДЧ и ДЧС сигналите единствено по показателите от параграф 1.4.поради ограниченията, произтичащи от така наречените граници на Уелч и на Сидельников. Тези ограничения могат да бъдат преодолени, ако се използват несъгласувани филтри, позволяващи получаването на отклик (реакция) с идеалната форма на делта-импулс. Предвид на това и на положителните свойства на ФМ сигналите е необходимо да се разработят алгоритми за синтез на периодични шумоподобни ФМ сигнали с висока структурна сложност и съответните несъгласувани филтри, осигуряващи идеална форма на ПАКФ при минимални загуби в отношението сигнал/шум. Това е третата задача на дисертационния труд и тя се решава в настоящата трета глава чрез компютърно моделиране и изследване на ФМ сигнали, формирани чрез използване на силно нелинейни функции.

Изчисляването на ПАКФ на сигналите в приемниците на комуникационните системи и в частност на РЛС е основна процедура, тъй като в теорията на оптималното приемане е доказано, че при това се

максимизира отношението *сигнал/шум* (С/Ш-*signal-to-noise ratio* (SNR))в най-типичния практически случай, когато смущенията представляват *адитивен бял гаусов шум* (АБГШ – *additive white Gaussian noise* (AWGN)). Ето защо формата на ПАКФ на използваните сигнали оказва съществено влияние върху тактико-техническите параметри на РЛС. В тази връзка следва е важно да се припомни, че съгласно анализа, направен в параграф 1.4., страничните листа на ПАКФ, предизвикани от ехо-сигналите от цел с голяма *ефективна отразяваща повърхност* (ЕОП), могат да маскират ехо-сигналите от малка по размери цел, ако разстоянието между целите е по-малко от

$$\Delta d = N.\tau_{ch}.(c/2). \qquad (1)$$

Тук $\boldsymbol{N}$ е броят на елементарните импулси (чиповете), формиращи сложния сондиращ сигнал на РЛС, τ_{ch} е продължителността на елементарните импулси (чиповете), а $\boldsymbol{c}$ е скоростта на разпространение на електромагнитната енергия (т.е. скоростта на светлината).

За да се избегнат нежелателните последици от маскирането на сигналите, изразяващи се в пропускане на малоразмерни цели (например самолети на наркотрафиканти), необходимо е да се използват такива методи за обработка на приетите ехо-сигнали в РЛС, така че да се премахнат страничните листа на ПАКФ на сигналите. Това може да се постигне чрез така наречената несъгласувана обработка на ехо-сигналите в приемниците на РЛС.

Оттук произтича следният метод за несъгласуваната цифрова обработка на ехо-сигналите в приемниците на РЛС.

Първо, приетите ехо-сигнали се преобразуват в цифров вид. При това, ако се пренебрегнат изкривяванията, породени от шумовете и смущенията, може да се приеме, че:

$$\zeta_i = U_{mi}.e^{j\frac{2\pi}{p}s(i)}, \; i = 0,1,...,N-1, \qquad (2)$$

като тук $s(i)$ е $\boldsymbol{i}$-тият елемент на степенна последователност на приетия ФМ сигнал

$$S = \{s(0), s(1),..., s(N-1)\}, s(i) \in \{0,1,..., p-1\} = Z_p. \qquad (3)$$

Второ, получават се N уравнения

$$C_l.D_l^* = N,\ l = 0,1,...,N-1, \tag{4}$$

като тук $\{C_0, C_1, ..., C_{N-2}, C_{N-1}\}$ е дискретния спектър на Фурие на приетия сигнал, а $\{D_0, D_1, ..., D_{N-2}, D_{N-1}\}$ е дискретната честотна характеристика на несъгласувания приемен филтър, чрез който страничните листа на реалната ПАКФ на приетия сигнал се отстраняват, а

$$Q_{\zeta\zeta}(x) = 0.x^{N-1} + 0.x^{N-2} + ... + 0.x + N \quad \mathrm{mod}(x^N - 1) \tag{5}$$

е полиномът, съответстващ на ПАКФ с идеална форма.

След като предварително се изчислят $C_l, l = 0,1,...,N-1$ могат да се определят отчетите

$$D_l = \left(\frac{N}{C_l}\right)^*,\ l = 0,1,...,N-1. \tag{6}$$

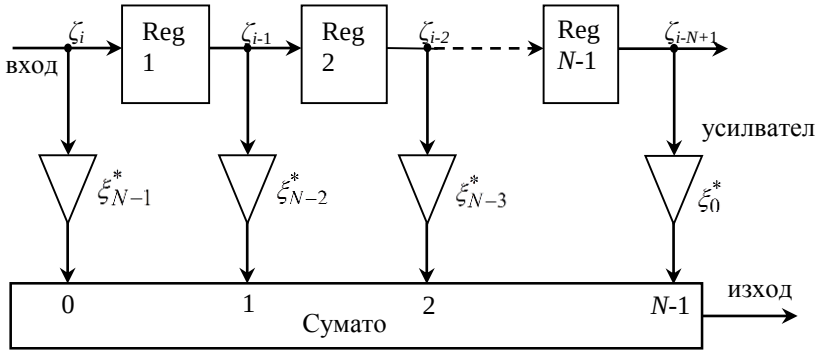
Използването на уравненията (6) не представлява никакъв проблем, ако всички отчети $C_l, l = 0,1,...,N-1$ са различни от 0 (т.е. ако в дискретния спектър на Фурие на приетия сигнал няма нули).

Трето, използвайки последователността $\{D_0, D_1, ..., D_{N-2}, D_{N-1}\}$ чрез обратното преобразование на Фурие се изчисляват отчетите на преходната характеристика на несъгласувания филтър, т.е.:

$$\xi_l = \frac{1}{N}\left\{D_{N-1}\left(e^{-j\frac{2\pi}{N}l}\right)^{N-1} + D_{N-2}\left(e^{-j\frac{2\pi}{N}l}\right)^{N-2} + ... + D_1\left(e^{-j\frac{2\pi}{N}l}\right) + D_0\right\}, \tag{7}$$
$$l = 0,1,...,N-1$$

Четвърто, на базата на (7) несъгласуваният цифров филтър, който премахва всички странични листа на реалната ПАКФ на приетия

ехо-сигнал, лесно се реализира като *цифров филтър с крайна импулсна характеристика* (наричан за краткост КИХ-филтър) по следната схема



Фиг. 1: *КИХ-филтър, премахващ страничните листа на ПАКФ на ехо-сигналите*

На фиг. 1 регистрите $\mathrm{Re}\, g_1, \mathrm{Re}\, g_2, ..., \mathrm{Re}\, g_{N-2}, \mathrm{Re}\, g_{N-1}$ задържат отчетите на входния сигнал на един такт τ_{ch}, а коефициентите на усилване на усилвателите са комплексно-спрегнатите стойности на отчетите $\xi_l = h_l.e^{j\varphi_l}, l = 0,1,..., N-1$, изчислени от (7), т.е.

$$\xi_l^* = h_l.e^{-j\varphi_l},\ l = 0,1,..., N-1. \tag{8}$$

Обобщавайки изложеното, следва да се подчертае, че страничните листа на ПАКФ на приетите ехо-сигнали могат да бъдат отстранени, ако съгласуваният филтър с преходна характеристика

$$\left\{\xi_0^*,\ \xi_1^*, ..., \xi_{N-2}^*,\ \xi_{N-1}^*\right\} \tag{9}$$

се замени с несъгласуван филтър с преходна характеристика

$$\left\{\xi_0^*,\ \xi_1^*, ..., \xi_{N-2}^*,\ \xi_{N-1}^*\right\}, \tag{10}$$

чиито отчети се изчисляват чрез (7).

Разгледаният несъгласуван филтър се нарича *филтър, потискащ страничните листа* (ФПСЛ, *side lobe suppression filter* (SLSF)).

За съжаление този изключително полезен от практическа гледна точка резултат се получава за сметка на известно влошаване на отношението сигнал/шум по мощност q^2 .

Следните бент-функции имат различна алгебрична степен и по тази причина са *афинно нееквивалентни*

$$\begin{aligned}
&f_0(x) = x_0x_m + x_1x_{m+1} + \ldots + x_{m-1}x_{2m-1},\\
&f_1(x) = x_0x_m + x_1x_{m+1} + \ldots + x_{m-1}x_{2m-1} + x_0x_1x_2,\\
&f_2(x) = x_0x_m + x_1x_{m+1} + \ldots + x_{m-1}x_{2m-1} + x_0x_1x_2x_3,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,\\
&f_{m-2}(x) = x_0x_m + x_1x_{m+1} + \ldots + x_{m-1}x_{2m-1} + x_0x_1x_2..x_{m-1}
\end{aligned}, \qquad (11)$$

От анализа произтичат следните изводи.

Извод 1. Коефициентът на загубите винаги е по-голям от или равен на 1. Неговата стойност е толкова по-близка до 1, колкото по-равномерен е енергетичният спектър на използваните от РЛС ФМ сигнали.

Извод 2. При синтеза на равномерни ФМ сигнали с висока структурна сложност най-голяма практическа значимост за РЛК имат сигналите, при които коефициентът на загубите има стойност близка до 1.

Изводи от Глава III:

1. Страничните листа на ПАКФ на сондиращите сигнали влошават разделителната способност по разстояние на РЛС, в резултат на което се пропускат ехо-сигналите на важни обекти с малка ефективна отразяваща повърхност. По тази причина задача с голямо практическо значение е разработването и внедряването на методи за обработка на приетите ехо-сигнали в РЛС, отстраняващи страничните листа на ПАКФ на сигналите. Един от основните методи за решаване на посочената задача е несъгласувана обработка на ехо-сигналите в приемниците на РЛС посредством така наречените филтри, потискащи страничните листа (ФПСЛ) на ПАКФ.
2. Използването на ФПСЛ вместо съгласувани филтри в приемниците на РЛС винаги е съпроводено с влошаване на отношението сигнал/шум. Предвид на това в световен мащаб се провеждат интензивни научни изследвания, насочени към синтезирането на периодични ФМ сигнали, осигуряващи висока

скритост на работата на РЛС, при които коефициентът на загубите при обработката с ФПСЛ е малък. Резултатите, публикувани в откритата литература обаче показват, че този проблем е сложен и към момента е далече от окончателното си решение.

3. С оглед на положителните свойства на метода за несъгласувана обработка на ехо-сигналите в приемниците на РЛС в глава III на дисертационния труд са обосновани 2 алгоритъма за синтез на периодични ФМ сигнали с висока структурна сложност, при които използването на ФПСЛ е съпроводено с малки загуби в отношението/сигнал шум.

- При Алгоритъм 1 се използват нелинейни функции, изобразяващи директно елементите на $GF(p^n)$ в елементите на простото алгебрично поле $GF(p)$.
- При Алгоритъм 3 се прилагат композиции на равномерни и нелинейни функции. При това на първия етап чрез някаква равномерна функция $h(x)$ елементите ***x*** на $GF(p^n)$ се изобразяват в елементите ***y*** на междинното алгебрично поле $GF(p^m)$ като тук ***m*** е нетривиален делител на ***n*** (т.е. ***m*** е делител на ***n***, който е различен от 1 и ***n***). След това чрез нелинейна функция $f(y)$ на всеки елемент ***y*** от $GF(p^m)$ се съпоставя някакъв елемент ***z*** от простото алгебрично поле $GF(p)$.

4. При практическото използване на посочените Алгоритъм 1 и Алгоритъм 3 възникват няколко проблема, които също са решени в глава III на дисертационния труд. По-конкретно, анализирано е влиянието на коефициента на загубите върху големината на зоната на обзор на РЛС. Разработени са ефективни от изчислителна гледна точка алгоритми (Алгоритъм 2 и Алгоритъм 4) за определяне на линейната сложност на ФМ сигналите, синтезирани посредством Алгоритъм 1 и Алгоритъм 3.

Глава IV

Основни резултати от изследването, проведено по дисертационния труд

Синтезът на периодични шумоподобни ФМ сигнали, осигуряващи скритост по отношение на радиотехническото разузнаване (РТР) е сложен научен проблем, чието решаване е възможно само чрез

използване на компютърни системи. Естествено при това възниква необходимост от автоматизация на процеса на синтез на периодични шумоподобни ФМ сигнали с висока структурна сложност. Следва специално да се отбележи, че при практическото използване на разработената софтуерна система за автоматизиран синтез на двойки „периодичен шумоподобен ФМ сигнал с висока структурна сложност – ФПСЛ на ПАКФ“ бяха получени редица неизвестни до момента периодични шумоподобни ФМ сигнали с висока структурна сложност и с малък коефициент на загубите, които представляват основните резултати от изследването, проведеното по дисертационния труд.

За решаване на четвъртата основна задача на дисертационния труд беше разработена компютърна софтуерна система за автоматизиран синтез на двойки „периодичен шумоподобен ФМ сигнал с висока структурна сложност – ФПСЛ на ПАКФ“. Тази система се състои от 2 универсални компютърни програми, работещи в средата на Матлаб, които осигуряват практическото използване на Алгоритъм 1 от § 3.2. и Алгоритъм 3 от § 3.3. на ДСТТ съответно.

Работата на първата универсална програма, реализираща Алгоритъм 1 от § 3.2., се пояснява с блок-схемата от фиг. 1 и може да се опише както следва.

1) В началото на програмата се задават стойности на параметрите:

- ***p*** – характеристика на полето на Галоа, която трябва да бъде просто число; при изследванията в дисертационния труд беше използвана само стойността

$$p = 2\,, \tag{1}$$

която съответства на бинарна фазова манипулация (*Binary Phase Shift Keying – BPSK*), намираща най-голямо практическо приложение предвид на простотата на практическата ѝ реализация;

- ***n*** – ***степен*** на разширение на простото поле на Галоа, която съгласно анализа, направен в § 3.2. на ДСТТ, следва да бъде четно число; при изследванията в дисертационния труд бяха използвани стойностите

$$n = 4,6,8,10,12\,, \tag{2}$$

които осигуряват постигането на целта на дисертационния труд;

Фиг. 1: *Блок-схема на универсална програмата, реализираща Алгоритъм 1.*

- въвежда се неразложим над $GF(p)$ примитивен полином $g(x)$ от n-та степен.

Следва да се отбележи специално, че:

- параметрите ***p*** и ***n*** определят дължината и базата на синтезираните ФМ сигнали

$$B = N = p^n; \tag{3}$$

- ако параметрите не са въведени съгласно посочените ограничения, програмата изисква тяхното коригиране.

2) На базата на въведения неразложим над $GF(p)$ примитивен полином от ***n***-та степен чрез Алгоритъма за подреждане на елементите на крайно алгебрично поле по степените на примитивен елемент от § 2.1. на ДСТТ се формира експоненциален ред на ненулевите елементи $\alpha^0 = 1, \alpha^1, ..., \alpha^{n-1}$ на разширеното поле $GF(p^n)$ (тук α е коя да е от нулите на $g(x)$). Както беше изяснено, посоченият алгоритъм всъщност се свежда до изчисляване на елементите на ЛРП като се използва общата структурна схема от фиг. 2.1.3., която се реализира много просто с компютърна система с матричен процесор.

Накрая пред вече изчислените ненулеви елементи на $GF(p^n)$ се добавя и нулевият елемент

$$0 = \begin{bmatrix} 0 \\ 0 \\ ... \\ 0 \end{bmatrix}. \tag{4}$$

В резултат се получава експоненциалният ред на всички елементи на $GF(2^n)$

$$0, \alpha^0, \alpha^1, ..., \alpha^{n-1}. \tag{5}$$

3) Въвежда се поредната конкретна формула от списъка на афинно нееквивалентните бент-функции. Тази конкретна формула се

допълва, при което се получава множество от 2^n афинно еквивалентни бент-функции, в които последователно се заместват стойностите (5). В резултат се получават 2^n степенни последователности с дължина (3).

4) Чрез формираните на предходната стъпка 2^n степенни последователности с дължина (3) се генерират 2^n ФМ сигнали.

Разгледаните до тук Стъпки 1, 2, 3 и 4 са пояснени с Пример 1 от § 3.3. на ДСТТ, при който $p = 2,\ n = 2$ и $g(x) = x^2 + x + 1$. В тази ситуация експоненциалният ред (5) на всички елементи на $GF(2^2)$ е

$$0 = \begin{bmatrix} 0 \\ 0 \end{bmatrix},\ \alpha^0 = \begin{bmatrix} 1 \\ 0 \end{bmatrix},\ \alpha^1 = \begin{bmatrix} 0 \\ 1 \end{bmatrix},\ \alpha^2 = \begin{bmatrix} 1 \\ 1 \end{bmatrix}. \tag{6}$$

От друга страна списъкът на бент-функции тук съдържа само 1 формула

$$f_0(x) = x_0 x_1, \tag{7}$$

от която се получава множество от $2^2 = 4$ афинно еквивалентни бент-функции

$$\begin{aligned} f_{0ae,0}(x) &= f_0(x) = x_0 x_1, \\ f_{0ae,1}(x) &= f_0(x) + x_0 = x_0 x_1 + x_0, \\ f_{0ae,2}(x) &= f_0(x) + x_1 = x_0 x_1 + x_1, \\ f_{0ae,1}(x) &= f_0(x) + x_1 + x_0 = x_0 x_1 + x_1 + x_0. \end{aligned} \quad . \tag{8}$$

След заместване на стойностите (6) в (8) се получават $2^2 = 4$ степенни последователности $S_{f_{0ae,l}}, l = 0,1,2,3$ с дължина $N = 2^2 = 4$. От тях по формула се генерират $2^2 = 4$ ФМ сигнала $\{\varsigma_l(i)\}_{i=0}^{3}, l = 0,1,2,3$. Всичко това е представено в табл. 1.

Таблица 1

Степенни последователности и ФМ сигнали, генерирани чрез функциите (8)

$\{x_1, x_0\}$	$S_{f_{0ae},0}$	$\{\varsigma_0(i)\}_{i=0}^{3}$	$S_{f_{0ae},1}$	$\{\varsigma_1(i)\}_{i=0}^{3}$	$S_{f_{0ae},2}$	$\{\varsigma_2(i)\}_{i=0}^{3}$	$S_{f_{0ae},3}$	$\{\varsigma_3(i)\}_{i=0}^{3}$
{0, 0}	0	1	0	1	0	1	0	1
{0, 1}	0	1	1	-1	0	1	1	-1
{1, 0}	0	1	0	1	1	-1	1	-1
{1, 1}	1	-1	0	1	0	1	1	-1

5) За всеки от генерираните на Стъпка 4 ФМ сигнали се синтезира съответния ФПСЛ и се изчисляват:

- съответния коефициент на загубите като се използва методът от § 3.1. на ДСТТ;

- линейната сложност n_{lc} като се прилага обоснования Алгоритъм 2.

6) От множеството от бинарни ФМ сигнали, генерирани на Стъпка 4, се изключват всички сигнали, за които коефициентът на загубите превишава $\gamma_{загдоп}$ или линейната сложност е по-малка от $n_{lc\,доп}$.

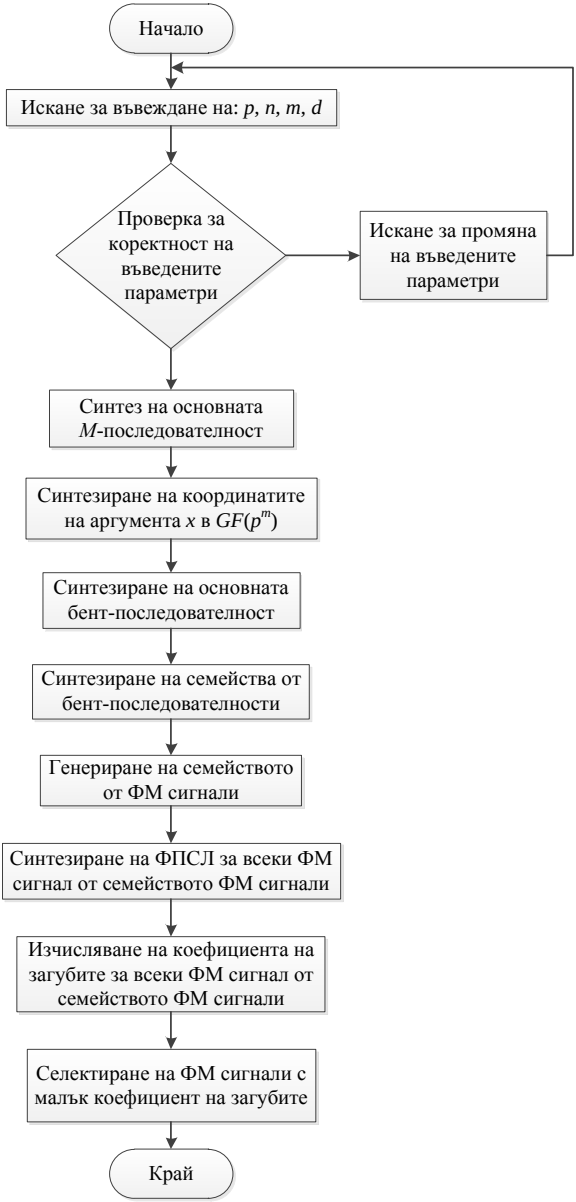
Следва да се отбележи, че в разгледания по-горе пример коефициентът на загубите $\gamma_{заг}$ е 1 и ФПСЛ всъщност съвпада със съответния съгласуван филтър. Това обаче е възможно единствено и само за бинарни ФМ сигнали с дължина $N = 4$. Във всички останали случаи коефициентът на загубите $\gamma_{заг}$ е по-голям от 1.

Работата на втората универсална програма, реализираща Алгоритъм 3 от § 3.3. на ДСТТ, се пояснява с блок-схемата от фиг. 2 и може да се опише както следва.

1) В началото на програмата се задават стойности на параметрите ***p***, ***n***, ***m*** и ***d***, както и неразложим над $GF(p)$ примитивен полином $g(x)$ от ***n***-та степен.

При това параметрите ***p*** и ***n*** имат разгледания по-горе смисъл.

Съгласно фиг. 3.2.2 от ДСТТ параметърът ***m*** задава на междинното поле на Галоа $GF(p^m)$ и трябва да бъде собствен делител на ***n***.



Фиг. 2: *Блок-схема на универсалната програма, реализираща Алгоритъм 3.*

На свой ред параметърът ***d*** трябва да бъде избран така, че $\beta = \alpha^d$ да бъде примитивен елемент на $GF(p^m)$ (тук α е коя да е нула на полинома $g(x)$, т.е. някой от примитивните елементи на $GF(p^n)$). От равенствата

$$\begin{aligned} &n = m.l, \\ &p^n - 1 = (p^m - 1)(p^{m(l-1)} + p^{m(l-2)} + ... p^m + 1) \end{aligned}, \tag{9}$$

следва, че

$$d = p^{m(l-1)} + p^{m(l-2)} + ... p^m + 1, \tag{10}$$

(тъй като при това се осигурява $\beta^{p^m-1} = \alpha^{d(p^m-1)} = \alpha^{p^n-1} = 1$).

Предвид на изложеното в изследването в дисертационния труд бяха използвани следните стойности на параметрите ***p***, ***n***, ***m*** и ***d***.

Таблица 2

*Стойности на параметрите **p**, **n**, **m** и **d**, използвани в изследването в дисертационния труд*

№	***p***	***n***	***m***	***d***
1	2	4	2	5
2	2	6	3	9
3	2	8	4	17
4	2	8	2	85
5	2	10	5	341
6	2	12	2	1365
7	2	12	3	585
8	2	12	4	273
9	2	12	6	65

Следва да се отбележи специално, че:

- параметрите ***p*** и ***n*** определят дължината и базата на синтезираните ФМ сигнали

$$B = N = p^n - 1; \tag{11}$$

- ако параметрите не са въведени съгласно посочените ограничения, програмата изисква тяхното коригиране.

2) На базата на въведения неразложим над $GF(p)$ примитивен полином от ***n***-та степен чрез Алгоритъма за подреждане на елементите на крайно алгебрично поле по степените на примитивен елемент от § 2.1. на ДСТТ се формира експоненциален ред на ненулевите елементи

$$\alpha^0 = 1, \alpha^1, ..., \alpha^{n-1} \tag{12}$$

на разширеното поле $GF(p^n)$ (тук α е коя да е от нулите на $g(x)$). Посоченият алгоритъм всъщност се свежда до изчисляване на елементите на ЛРП като се използва общата структурна схема от фиг. 2.1.3., която се реализира много просто с компютърна система с матричен процесор.

3) На базата на (12) се изчисляват множествата от стойности на координатите на ненулевите елементи междинното поле на Галоа $GF(p^m)$

$$x_0 = tr_1^n(\beta_0.\alpha^i), x_1 = tr_1^n(\beta_1.\alpha^i), ..., x_{m-1} = tr_1^n(\beta_{m-1}.\alpha^i). \tag{13}$$

Следва дебело да се подчертае, че в най-обща ситуация изчисленията по формули (13) са сложни. В дисертационния труд обаче бяха използвани следните факти, установени при анализа в § 2.1. на ДСТТ:

- тъй като $\beta^0 = 1$ всъщност $x_0 = tr_1^n(\beta_0.\alpha^i)$ е М-последователност и предвид на фиг. 2.1.3 на ДСТТ, в качеството на x_0 просто може да се вземе първата координата не елементите (12);

- координатите $x_l = tr_1^n(\beta_l.\alpha^i), l = 1, 2, ..., m-1$ също са М-последователности, които са циклични завъртания на М-последователността x_0 на ld позиции надясно.

Посочените факти позволиха значително ускоряване на изпълнението на универсалната програма, представена на фиг. 2.

4) По формули се формират всички афинно нееквивалентни бент-функции, изобразяващи елементите на $GF(2^m)$ в елементите на $GF(2)$.

5) На базата на всяка бент-функция, формирана на Стъпка 4, се генерират по 2^m афинно еквивалентни бент-функции.

6) Генерират се последователностите за всяка бент-функция, формирана на Стъпка 5.

7) Формира се множеството от бинарни ФМ сигнали като последователностите се използват като степенни последователности. Изчисляват се комплексните обвиващи на елементарните импулси на бинарните ФМ сигнали.

8) Синтезират се ФПСЛ за всички бинарни ФМ сигнали от множеството, формирано на Стъпка 7 и се изчислява съответния коефициент на загубите. От това множество от бинарни ФМ сигнали се изключват всички сигнали, за които коефициентът на загубите превишава $\gamma_{загдоп}$ или линейната сложност е по-малка от $n_{lcдоп}$.

Следва специално да се отбележи, че установените при изследването по дисертационния труд неизвестни до момента ФМ сигнали могат да се използват като градивни компоненти за синтезиране на ФМ сигнали с произволно висока структурна сложност и малък коефициент на загубите при обработка с ФПСЛ чрез използване на следната теорема, доказана от руския теоретик В. Ипатов.

Теорема на Ипатов: Нека са дадени два ФМ сигнала с идеална ПАКФ $\{\xi(i_1)\}_{i_1=0}^{N_1-1}$ и $\{\zeta(i_2)\}_{i_2=0}^{N_2-1}$, чиито дължини са взаимно прости числа, т.е. $(N_1, N_2) = 1$. Тогава ФМ сигналът, получен чрез умножаване на елементарните импулси на изходните ФМ сигнали по правилото:

$$\varsigma(i) = \xi(i_1).\zeta(i_2),\ i = 0,1,...,N_1.N_2 - 1,\ \ i \equiv \begin{cases} i_1 \bmod N_1 \\ i_2 \bmod N_2, \end{cases} \qquad (14)$$

също има ПАКФ с идеална форма.

От тази теорема произтича следното твърдение, също доказано от Ипатов.

Твърдение на Ипатов: Ако $\{\xi(i_1)\}_{i_1=0}^{N_1-1}$ и $\{\zeta(i_2)\}_{i_2=0}^{N_2-1}$ са 2 ФМ сигнала с коефициенти на загубите $\gamma_{заг1}$ и $\gamma_{заг2}$ съответно, чиито дължини са взаимно прости числа, тогава производният ФМ сигнал с дължина $N = N_1.N_2$, синтезиран по правилото (14), има коефициент на загубите

$$\gamma_{заг} = \gamma_{заг1}.\gamma_{заг2}. \quad (15)$$

Освен това линейната сложност на производния сигнал е от порядъка на произведението на линейните сложности на компонентните сигнали.

Изводи:

1. При синтеза на периодични шумоподобни ФМ сигнали с висока структурна сложност възниква необходимост от автоматизация на процеса на изследване на техните свойства. По тази причина е разработена софтуерна система за автоматизиран синтез на двойки „периодичен шумоподобен ФМ сигнал с висока структурна сложност – ФПСЛ на ПАКФ“. При практическото използване на системата са получени редица неизвестни до момента периодични шумоподобни ФМ сигнали с висока структурна сложност и с малък коефициент на загубите.
2. Полезният ефект от резултатите, получени при изследванията по дисертационния труд съществено може да бъде увеличен чрез прилагане на Твърдението на Ипатов.
3. Изследванията по дисертационния труд могат да бъдат доразвити като се използва схемата от фиг. 4.2.1 на ДСТТ.

СПРАВКА ЗА ПРИНОСНИТЕ МОМЕНТИ В ДИСЕРТАЦИОННИЯ ТРУД

I. НАУЧНИ ПРИНОСИ

1. Доказани са два алгоритъма (Алгоритъм 1 от § 3.2. и Алгоритъм 3 от § 3.3. на ДСТТ) за синтезиране на ФМ сигнали с висока структурна сложност и с малък коефициент на загубите при обработка с ФПСЛ, които са универсални по отношение на вида фазовата манипулация.

2. В резултат на практическото използване на посочените Алгоритъм 1 и Алгоритъм 3 са установени нови неизвестни до момента бинарни ФМ сигнали с висока структурна сложност и с малък коефициент на загубите при обработка с ФПСЛ (§ 4.2., Табл. 1 и Табл. 2 на ДСТТ).

II. НАУЧНО-ПРИЛОЖНИ ПРИНОСИ

1. Разработен е Алгоритъм за подреждане на елементите на крайно алгебрично поле по степените на примитивен елемент (§ 2.1. на ДСТТ), който лесно се реализира практически с компютърни системи с матрични процесори.

2. Обоснован е ефективен от изчислителна гледна точка Алгоритъм 2 за оценка на линейната сложност на степенни последователности на ФМ сигнали с дължина $N = p^n$ (p е просто число, а n е произволно цяло положително число).

III. ПРИЛОЖНИ ПРИНОСИ

1. Анализирано е съвременното състояние на методите за синтез на периодични шумоподобни ФМ сигнали с висока структурна сложност и са обосновани перспективните пътища за тяхното развитие.

2. Анализирани са факторите, от които зависят допустимите стойности на коефициента на загубите $\gamma_{загдоп}$ и на линейната сложност $n_{lсдоп}$ при синтеза на периодични ФМ сигнали с висока структурна сложност, предназначени за използване в радиолокационни системи с пасивен отговор.

3. Синтезиран е ефективен от изчислителна гледна точка Алгоритъм 4 за оценка на линейната сложност на степенни последователности на ФМ сигнали с дължина $N = p^n - 1$ (p е просто число, а n е произволно цяло положително число).

4. На базата на Алгоритъм 1 от § 3.2. и Алгоритъм 3 е разработена система за автоматизиран синтез на периодични шумоподобни ФМ сигнали с висока структурна сложност и съответните несъгласувани филтри, позволяваща да се анализират техните корелационни свойства.

ПУБЛИКАЦИИ ПО ТЕМАТА НА ДИСЕРТАЦИОННИЯ ТРУД

1. Беджев Б. Й., Цанков Цв. С., Станева Л. Ан., Метод за приложение на сигнали с висока структурна сложност в радиолокационни системи, Научна конференция на тема "Защитата на личните данни в контекста на информационната сигурност", 2013, Шумен
2. Беджев Б. Й., Цанков Цв. С., Станева Л. Ан., Свиващ генератор на псевдослучайни последователности, формирани чрез нелинейни функции, Научна конференция на тема "Защитата на личните данни в контекста на информационната сигурност", 2013, Шумен
3. Беджев Б. Й., Йорданов С. С., Цанков Цв. С., Станева Л. Ан., Приложение на линейните рекурентни последователности над крайни полета при синтеза на сложни широколентови сигнали, MATTEX'2012, Шумен
4. Беджев Б. Й., Станева Л. Ан., Цанков Цв. С., Метод синтеза пар „сигнал с высокой структурной сложностью – приемный фильтр", 9th International Conference on Bionics and Prosthetic, Biomechanics and Mechanics, Mechatronics and Robotics, 2013, Riga, vol. 9, pp. 158 – 161
5. Николов Н. Р., Цанков Цв. С., Хардуерна реализация на генератор на псевдослучайни последователности описван с полином от 1024 степен и програмно управление на обратните връзки, Научна сесия на факултет „Артилерия, ПВО и КИС", 2010, Шумен
6. Цанков Цв. С., Компютърна лаборатория за автоматизиран синтез на сигнали с висока структурна сложност, MATTEX'2012, Шумен
7. Цанков Цв. С., Трифонов Т. С., Алгорифм для вычисления линейной сложности сигналов, 10th International Conference on Bionics and Prosthetic, Biomechanics and Mechanics, Mechatronics and Robotics, 2014, Liepaya, под печат
8. Bedzhev B. Y., Yordanov S. S., Tsankov Ts. S., A Method for Synthesis of Signals Possessing Almost Ideal Periodic Autocorrelation Function, 9th International Conference on Bionics

and Prosthetic, Biomechanics and Mechanics, Mechatronics and Robotics, 2013, Riga, vol. 9, pp. 166 – 169

9. Trifonov T. S., Staneva L. A., Tsankov Ts. S., A survey of phase manipulated signals with high structural complexity and small loses after processing with mismatched filters, Journal "Scientific and applied research", 2013, Shumen
10. Trifonov T. S., Tsankov Ts. S., Staneva L. A., An algorithm for synthesis of phase manipulated signals with high structural complexity, Journal "Scientific and applied research", 2013, Shumen

ANNOTATION

Dissertation:
Algorithms for synthesis of periodic pseudo-noise phase manipulated signals with high structural complexity

Author: M.Sc. Eng. Tsvetoslav Stanislavov Tsankov

The families of phase manipulated (PM) signals with an ideal periodic autocorrelation function (PACF), resembling a delta-pulse, find many applications for: synchronization, channel estimation, elimination of the negative effects, caused by the multipath spread of the electromagnetic waves, radars, radio-navigation systems and others. Due to this reason various methods for synthesis of families of such signals have been researched for the last 60 years. However, at the present moment only a few classes of PM signals with ideal PACF are known. With regard to this problem in the dissertation new algorithms for synthesis of pairs "PM signal with high structural complexity – side-lobe suppression filter (SLSF)" are developed. They could be useful in the development of new radars and other wireless systems with high resistance to the attempts for unauthorized access to the system resources.

In Chapter 1 a brief analysis of the present state of the problem is made. The basic terms and their mathematic descriptions are exposed. The main approaches for synthesis of pairs "PM signal with high structural complexity –SLSF" are analyzed. On this base the aim and main problems of the dissertation are formulated.

In Chapter 2 the quantity methods for measurement of the structural complexity of the uniform PM are analyzed. An algorithm for generating the elements of limited algebraic fields, according the powers of a primitive element. The algorithm can be easily performed by computer systems with matrix processors. Besides, it is used as an important building block in the next chapters of the dissertation.

In Chapter 3 two new algorithms for synthesis of pairs "PM signal with high structural complexity –SLSF" are developed. Besides, two algorithms for measurement of the structural complexity of the uniform PM are suggested.

In Chapter 4 a software system for automated synthesis of pairs "PM signal with high structural complexity –SLSF" is developed. New unknown PM signal with high structural complexity, which can be processed by SLSF with small losses in the signal-to-noise ratio, are presented.