УНИВЕРСИТЕТ „ПРОФ.Д-Р АСЕН ЗЛАТАРОВ“
ФАКУЛТЕТ ТЕХНИЧЕСКИ НАУКИ
КАТЕДРА „КОМПЮТЪРНИ СИСТЕМИ И ТИХНОЛОГИИ“

инж. Лилия Анестиева Станева

АЛГОРИТМИ ЗА СИНТЕЗ И ОБРАБОТКА НА СЕМЕЙСТВА ОТ СЛОЖНИ СИГНАЛИ С ОПТИМАЛНИ КОРЕЛАЦИОННИ СВОЙСТВА

АВТОРЕФЕРАТ

на дисертация за присъждане на образователна и научна степен „доктор“

научно направление: 5.3
„Комуникационна и компютърна техника“
научна специалност:
„Компютърни системи и технологии“

Научни ръководители:

проф. дтн. Борислав Йорданов Беджев
доц. д-р Станислав Денчев Симеонов

БУРГАС, 2014

Защитата на дисертационния труд ще се състои на …….. от……. часа в зала …….. на Университет „Проф. д-р Асен Златаров“ (бул. „Проф. Якимов“ №1)

Дисертационният труд е обсъждан и насочен за защита от разширен катедрен съвет на катедра „Компютърни системи и технологии“, Университет „Проф. д-р Асен Златаров“ – Бургас на 20.06.2014 г.

Рецензенти:
1. проф. д-р инж. Румен Иванов Арнаудов, ТУ-София
2. проф. д-р инж. Иван Кръстев Цонев, ШУ "Епископ Константин Преславски"

Автор:

инж. Лилия Станева

Заглавие:

„Алгоритми за синтез и обработка на семейства от сложни сигнали с оптимални корелационни свойства“

Отпечатано в 10 броя

ОБЩА ХАРАКТЕРИСТИКА НА ДИСЕРТАЦИОННИЯ ТРУД

Актуалност на проблема

Преимуществата на широколентовите системи за връзка на основата на сложни сигнали (СС) са били добре известни на специалистите в средата на 60-те години на миналия век, като ефективно средство за борба със смущенията. Техническата реализация е бил основен проблем през тези години. За това СС първо са били използвани в радиолокационните военни и космическите системи, тъй като тук не е стоял проблема за големите размери и маса на устройствата. В тези системи са вложени най-добрата научна и инженерна мисъл. За хубаво или лошо те изцяло са променили днешния стандарт на живот на човека. Един от най-добрите примери за използване и предаване на информация е системата за мобилна връзка, базираща се на технологията Code Division Multiple Access (CDMA). В основата на тази система стои широколентовия сигнал (ШЛС). CDMA позволява постоянно всяка станция да осъществява предаване във всеки честотен диапазон.

Особено важно е да се отбележи, че развитието на средствата за връзка на основата на СС би било просто невъзможно, първо без ускоряване темпа на развитие на микроелектрониката и второ без разработката на оригинални алгоритми и методи за формиране, предаване и обработка на СС. Заедно с шумоустойчивото кодиране на тези системи действително заема почетното първо място в йерархията на системата за подвижни и персонални спътникови връзки.

Следователно на настоящия етап с голяма острота стои въпросът за систематизиране и унифициране на научните методи. Поради изключителното разнообразие в конструкцията и сферите на приложение на мобилните устройства, построяването на единен алгоритъм за тяхното изследване едва ли е възможен. Все пак с оглед на потребностите е необходимо да се направят усилия за намиране на общ алгоритъм поне за една от областите на приложение.

Цел и предмет на изследването

Основната цел на разработката е да се разработят алгоритми за синтез на дискретно честотни сигнали с ***P***-сложност, осигуряващи на съвременните мобилни комуникационни системи висока шумозащитеност, точност и разделителна способност по разстояние и по честота.

Предмет на дисертационния труд е синтезирането в общ вид на модели за обработка на дискретни честотни сигнали (ДЧС) и разработването на пакет от приложни програми за автоматизирано синтезиране на семейство от сложни ДЧС с оптимални автокорелационни свойства.

Публикации

Основните моменти от дисертационния труд са представени в три международни научни конференции: Научна конференция с международно участие - МАТТЕХ ШУ „Епископ Константин Преславски” 22-24.11.2012, Международна научна конференция „Образование, наука, икономика и технологии“, 17th Telecommunications forum TELEFOR 2009, една научна конференция "Защитата на личните данни в контекста на информационната сигурност" както и в научно списание „Information, Communication and Control Systems and Technologies”.

Структура и обем на дисертационния труд

Дисертационният труд се състои от увод, четири глави, заключение, списък на публикациите по темата и приложения.

В първа глава са изложени основните понятия и математически функции описващи корелационните свойства на сигналите. Представени са основните изисквания към сигналите. Анализирано е съвременното състояние на проблема на методите за синтез на дискретно – честотни сигнали и тяхното приложение в мобилните комуникационни системи. Формулирани са целите и задачите на дисертационния труд.

Във втора глава се прави обосновка на основните алгебрични методи за синтез на дискретно – честотни сигнали. Оценяват се съвременните методи за синтез на семейства от ДЧС и се построява алгоритъм за синтез на семейство от ДЧС притежаващи едновременно най-малка странична лента на техните ПАКФ и възможно най-малка лента на техните ПВКФ.

В трета глава са представени методите за синтез от семейства дискретни честотни акустични сигнали чрез масиви на Костас. Представени са резултати от изследването в рамките на тези семейства. Оценяват се съвременните методи за намиране на дискретно – честотни сигнали и се предлагат нови подобрени методи за тяхното намиране, който се отличава с малката си изчислителна сложност .

В четвърта глава е описана система за автоматизиран синтез на семейства от ДЧС с оптимална автокорелационна функция предложени във втора и трета глава. Представени са някои от най-добрите резултати от изследването. Описана е и компютърна софтуерна система за автоматизиран синтез на дискретно честотни сигнали с идеална или близка до идеалната автокорелационна функция (АКФ), разработена в средата на MATLAB.

Дисертационният труд съдържа 132 страници, от които 19 са приложения. Списъкът на използваната литература се състои от 144 заглавия, от които 12 на български, 9 на руски и 123 на английски език. Включени са 39 фигури и 20 таблици.

СЪДЪРЖАНИЕ НА ДИСЕРТАЦИЯТА

ГЛАВА ПЪРВА – СЪВРЕМЕННО СЪСТОЯНИЕ НА МЕТОДИТЕ ЗА СИНТЕЗ НА ДИСКРЕТНО – ЧЕСТОТНИ СИГНАЛИ

В тази глава е обоснована актуалността и мотивите за работа по темата на дисертацията. Обект на изследване в дисертационния труд са дискретно – честотни сигнали приложими в съвременните мобилни комуникационни системи.

1.1. Значение на дискретно – честотните сигнали за съвременните комуникационни системи

Необходимостта от практическо използване на дискретно честотни сигнали е тясно свързана с развитието на радиолокационните системи [67]. Както е известно, радиолокационните устройства възникват независимо и едновременно в средата на 30-те години на 20-ти век във водещите в радиоелектрониката страни: САЩ, Русия (тогава СССР), Германия, Великобритания, Япония, Италия и Франция. Тяхната поява е отговор на създаването в началото на 30-те години на тежките бомбардировачи с голям радиус на действие. Радиолокацията се използва за наблюдаване и за навигация, в това число и за осигуряване прелитането на самолетите над препятствия и за следване релефа на местността.

От средата на 50-те години на 20-ти век РЛК намират все по-широко приложение за мирни цели. РЛК решават такива всекидневни задачи като сондиране на йоносферата и наблюдение на метеорологичната обстановка. Когато предназначената за тези цели апаратура започва да се разработва и изпитва, нейните създатели (специалистите по радиолокация) вероятно не са имали и представа, за обичайното днес понятие "дистанционно сондиране на заобикалящата среда". Постепенно радиолокационните методи започват да се използват за изследване на метеори, полярни сияния и т.н., докато в наши дни идва ред на прилагането на радиолокаторите за проследяване миграцията на птиците и насекомите от орнитолозите и ентомолозите. Съвременният транспорт е немислим без РЛК. РЛК са изключително важен елемент от системите за управление на въздушния, морски и железопътен трафик на всички страни. Серийно произвежданите бордови радиолокатори измерват височината на самолета, откриват опасни буреносни зони, определят вектора на скоростта на самолета (с помощта на доплерови навигационни устройства), привързват се към наземни ориентири. Повечето морски съдове в наши дни са оборудвани с един или няколко радиолокатора, предназначени да предотвратят сблъсквания и за решаване на навигационни задачи. Те се отнасят към числото на най-евтините и в същото време твърде надеждни уст-

ройства, получили в количествено и качествено отношение широко разпространение. В последното десетилетие на 20^{ти} век радарни сензори започнаха все по-масово да се използват и в автомобилите, защото осигуряват на водачите ценна информация в дъжд, мъгла и при лоша осветеност на пътя. РЛК са задължителен елемент на космическите системи за сближаване, съединяване и приземяване на управляеми и автоматични орбитални модули. Не може да се подмине и ролята на РЛК за дистанционно сондиране на различни полезни изкопаеми, на археологически находки, на повредени тръбопроводи. Важна е ролята на РЛК и в системите за сигурност на частни домове, обществени сгради, банки, магазини и офиси, за контрол спазването на правилата за движение по пътищата, за проследяването на автомобили, за намирането на хора, пострадали от пожари, природни стихии или страдащи от тежки форми на склероза и т.н.

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).

1.2. Съвременно състояние на методите за синтез на дискретно – честотни сигнали

Анализът на работата на МКС показва, че използваните в тях системи от сигнали следва да:

- осигуряват висока шумозащитеност на комуникационните системи (включително и на РЛК);

- позволяват организирането на едновременната работа на много абонати в обща честотна лента при асинхронно-адресен принцип на работа на системата за свръзка на базата на кодовото разделяне на абонатите (т.е. на тях се базират CDMA технологиите, използвани широко в съвременните мобилни комуникации);

- позволяват успешна борба с негативните ефекти, породени от многолъчевото разпространение на радиовълните, чрез разделяне на преките и отразени лъчи;

- обезпечават електромагнитната съвместимост на радиоелектронната апаратура;

- осигуряват много добро използване на електромагнитния спектър.

Някои от тези изисквания могат да бъдат удовлетворени с едни и същи технически подходи. Ето защо горните изисквания могат да бъдат групирани и в резултат на това могат да бъдат преформулирани както следва.

Системите от сложни сигнали, използвани в съвременните МКС, трябва едновременно да отговарят на следните основни изисквания:

1. Да бъдат широколентови сигнали с:

- ниска спектрална плътност;

- висока структурна сложност,

осигуряващи скритост по отношение на радио-техническото разузнаване (РТР) поради *ниската вероятност за прехващането им* (*low probability for detection* (*interception*)).

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

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

От направените анализи в горния параграф могат да се направят следните изводи.

Извод 1: Проблемът за синтез на ДЧС с оптимални корелационни свойства, осигуряващи на МКС необходимите работни характеристики, от формално математическа гледна точка се свежда до намирането на всички възможни пермутации $a(1), a(2), \ldots, a(N)$ на числата $\{1, 2, \ldots, N\}$, при което сравнението (1.39) има минимален брой решения.

Анализът на специализираните литературните източници показва, че известните към момента методи за синтез на ДЧС с оптимални корелационни свойства [136], [139], [142] са приложими само, когато N е просто число или степен на просто число. Нещо повече, отчитайки големите усилия, полагани системно в целия свят по тези проблеми, може да се направи обосновано предположение, че намирането на всички възможни пермутации $a(1), a(2), \ldots, a(N)$ на числата $\{1, 2, \ldots, N\}$, при което сравнението (1.39) има минимален брой решения, е задача с много висока сложност.

В тази връзка следва да се припомни, че според сложността (трудността) им задачите се класифицират както следва [9].

P-задачи. Това са задачи, при които решението се намира за време

$$T_{\text{реш}} \sim a_n . V^n + a_{n-1} . V^{n-1} + \cdots + a_1 . V + a_0 . \qquad (1.41)$$

Тук $T_{\text{реш}}$ е времето за решаване на задачата, V е минималният обем от информация, необходим за решаване на задачата, а $a_n, a_{n-1}, \ldots, a_1, a_0$ са коефициенти.

Тъй като изразът в дясната част на (1.41) е полином, те се наричат задачи с *полиномиална сложност* (съкращението *P* идва от *polynomial*). От своя страна този клас е доста обширен тъй като в редица алгоритми участват и функции с асимптотично нарастване, което е по-ниско от това на линейната функция като например: *логаритмичната функция*, *обратната функция на Акерман* и др. [9].

NP-задачи. *NP* е съкращение от *non-deterministic polynomial time*, т.е. *полиномиално проверими* задачи. Дадена задача принадлежи към класа *NP*, ако е възможно с полиномиална сложност да се провери дали даден кандидат за решение действително е решение, без да се интересуваме колко време ще отнеме намирането на този кандидат. Така за *NP*-задачите е характерно, че ако веднъж успеем да "налучкаме" правилното решение, то лесно можем да го проверим.

Exp-time задачи. Това са задачи, при които времето за решение зависи експоненциално от обема на необходимата информация, т.е.

$$T_{\text{реш}} \sim e^{a.V}. \qquad (1.42)$$

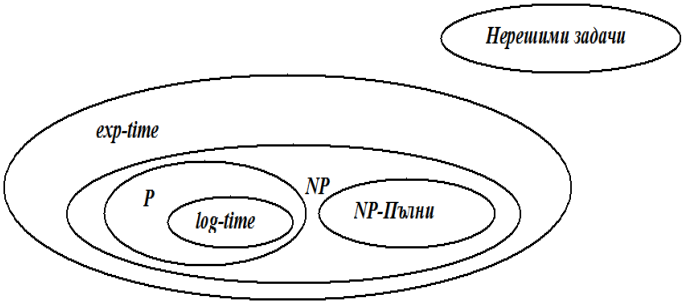
Този клас съдържа предишните три, но не е всеобхватен - има задачи, за които най-добрите алгоритми са със сложност по-висока от експоненциалната.

Space задачи. Това са задачи, при които критична е паметта, която използват (като функция от големината на входните данни). При тях не се интересуваме от сложността на алгоритъма за решаването им. Този клас може да се разпадне до няколко подкласа: *P-space* (задачи, за които е необходима полиномиална памет), *exp-space* (експоненциална памет) и др.

Ясно е, че изчислителната сложност на алгоритъма е винаги поне толкова, колкото е сложността по памет.

Нерешими задачи. Съществуват алгоритмични задачи, за които може да се докаже [9], че не могат да бъдат решени, независимо от това с колко време и памет разполагаме.

Някои от изброените класове от задачи (и връзките между тях) са показани схематично на фиг. 1.16.



Фиг. 1.16. Класове от задачи.

Един от основните открити въпроси на съвременната математика и теоретичната кибернетика е действително ли NP-пълните задачи са труднорешими. Повечето специалисти твърдят, че всички NP-пълни задачи са труднорешими. NP-пълнотата на задачите обаче означава, че за решаването им с полиномиални алгоритми е необходимо сериозно откритие.

1.3. Изводи, произтичащи от анализа на съвременно състояние на методите за синтез на дискретно честотни сигнали.

От анализа на съвременно състояние на методите за синтез на дискретно честотни сигнали, направен до тук, произтичат следните изводи.

Извод 1.1. В РЛС сложните сигнали:

1) позволяват едновременно да се постигнат висока разделителна способност по разстояние и по скорост, както и голяма зона на обзор;

2) осигуряват висока точност на измерванията на разстоянието до целите и техните радиални скорости.

Извод 1.2. ДЧС и производните от тях ДЧСС имат изключително висока структурна сложност и малка спектрална плътност, които им осигуряват много висока скритост по отношение на радио-техническото разузнаване на престъпни и терористични групи, а на тази основа - много висока устойчивост към опитите за неоторизиран достъп до ресурсите на комуникационните системи, използващи такива сигнали. По тази причина ДЧС и ДЧСС често се наричат *сигнали с малка вероятност за откриване* (*прехващане*) - *signals with low probability of detection* (*interception*) или съкратено *LPD* (*LPI*) *signals.*

Извод 1.3. Предвид на положителните им свойства и приложението им в радиолокационните системи на авиационния и морския транспорт, както и в комуникационните системи за управление на армията, полицията, гражданската отбрана и спасителните служби, проблемът за

разработване на алгоритми за синтез на ДЧС и ДЧСС има изключително голяма практическа значимост на съвременния етап.

Извод 1.4. Проблемът за синтез на ДЧС с оптимални корелационни свойства, осигуряващи на МКС необходимите работни характеристики, от формално математическа гледна точка се свежда до намирането на всички възможни пермутации $a(1), a(2), \ldots, a(N)$ на числата $\{1, 2, \ldots, N\}$, при което сравнението (1.39) има минимален брой решения.

Извод 1.5. Намирането на всички възможни пермутации $a(1), a(2), \ldots, a(N)$ на числата $\{1, 2, \ldots, N\}$, при което сравнението (1.39) има минимален брой решения, е задача с много висока сложност.

Предвид на тези изводи целта на дисертационния труд е:

Да се разработят алгоритми за синтез на дискретно честотни сигнали с ***P***-сложност, осигуряващи на съвременните МКС висока шумозащитеност, точност и разделителна способност по разстояние и по честота.

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

1. Да се анализира съвременното състояние на методите за синтез на дискретно честотни сигнали и да се формализират математически изискванията към тях.
2. Да се систематизират методите за изчисления в крайни алгебрични полета.
3. Да се разработят алгоритми за синтез на дискретни честотни радио сигнали.
4. Да се разработят алгоритми за синтез на дискретни честотни акустични сигнали.
5. Да се разработи система за автоматизиран синтез на предложените нови дискретно честотни сигнали, позволяваща да се анализират техните корелационни свойства.

ГЛАВА ВТОРА – АЛГОРИТМИ ЗА ИЗЧИСЛЕНИЯ В КРАЙНИТЕ АЛГЕБРИЧНИ ПОЛЕТА

При анализа, направен в глава първа, беше установено, че системите от дискретни честотни сигнали, използвани в съвременните комуникационни системи и в частност РЛК, притежават висока структурна сложност, осигуряваща ниски вероятности за прехващане на сигналите и за разкриване на принципите на модулация им, техните честотни и времеви параметри. На тази база се постига висока скритост по отношение на радио-техническото разузнаване. Синтезирането на системи от ДЧС обаче в много съществена степен се основава на използването на алгоритми за изчисления в крайни алгебрични полета. В тази връзка възниква проблемът за намаляване на изчислителната сложност на тези алгоритми и, естествено, той беше формулиран като втора основна задача на дисертационния труд.

2.1. Алгоритми за изчисления в крайни алгебрични полета

Математическият апарат на крайните алгебрични полета се оформя като относително самостоятелна научна дисциплина през 20-те и 30-те години на 20-ти век в резултат на радикално преустройство, което превръща алгебрата в теоретико-множествена, аксиоматична наука с основен предмет алгебричните операции, извършвани над елементи с произволна природа [12], [20], [21], [108]. Естествено тази промяна е подготвена от цялото предшестващо развитие на алгебрата през 19-ти век. Голям принос за нейното появяване имат плеяда велики математици като Гаус, Галоа, Дирихле, Кумер, Дедекинд, Грасман, Ньотер и Хилберт.

Възможностите на математическия апарат на крайните алгебрични полета за дълбоко, съдържателно и високоефективно изследване на широк кръг от задачи в теорията на комуникационните системи и на радиолокацията в частност са оценени в края на 50-те години на 20-ти век в резултат на успешното решаване на следните два изключително важни проблема. Първият от тях е проблемът за синтезирането на кодове на Хеминг [113], [110], поправящи две и повече грешки. Както е известно, кодовете на Хеминг, откриващи и поправящи една грешка, са предложени през 1942 г. в доклад, който е бил засекретен (поради Втората световна война) до 1949 г. В периода 1949 г. – 1959 г. най-изявените световни теоретици в областта на комуникационните системи хвърлят огромни усилия за да открият метод за синтез на кодове на Хеминг, откриващи и поправящи две грешки. Техните усилия се увенчават с успех едва през 1959 г., когато Боуз и Чоудхури решават проблема. Независимо от тях през 1960 г. Хоквингем получава аналогични резултати. Този успех оказва изключително впечатление върху научната общественост, защото от архивни материали става ясно, че Боуз е бил запознат с кодовете на Хеминг,

поправящи една грешка, още през 1942 г. Вторият случай, който демонстрира големия потенциал на математическия апарат на крайните алгебрични полета за решаване на тежки проблеми от теорията на комуникационните системи, е откриването на общ метод за синтез на сложни фазово манипулирани сигнали с почти идеална периодична автокорелационна функция, имаща форма на делта импулс. Както е известно, през 1953г. биват предложени така наречените кодове на Баркер, притежаващи почти идеална непериодична автокорелационна функция. В края на 50-те години на 20-ти век става ясно, че кодове на Баркер съществуват само за дължини не по-големи от 13 (т.е. броят на елементарните импулси в сигнала не е повече от 13). Този факт е доказан строго от Сторер и Тюрин (с уговорката, че дължината на кода е нечетно число) през 1961 г. Същевременно необходимостта от повишаване на енергетичния потенциал на РЛК без да се влошава тяхната разделителна способност по разстояние налага използването на много по-дълги сигнали. Този теоретичен проблем, имащ огромно практическо значение, се решава с откриването на последователностите с максимална дължина, наричани още М-последователности (maximal length sequences), от такива теоретици, използващи методите на съвременната алгебра, като Голомб [114], Алфред и Цирлер [77], [78], [81]. Въпреки че от изнамирането на М-последователностите до днес са изминали почти 50 години, те продължават да имат много голямо значение за комуникационните системи и РЛК.

След посочените две важни открития през 60-те години на 20-ти век започва процес на "алгебризация" на методите, използвани в теорията на комуникационните системи, който продължава и до днес.

От това, че класическият метод за директно изчисляване елементите на ЛРП остава в сила и в случая, когато ЛРП е дефинирана над крайно алгебрично поле, произтича следният алгоритъм за изчисления в крайни алгебрични полета

Алгоритъм за изчисления в крайни алгебрични полета

1. От справочници се взема примитивен неразложим полином над $GF(p)$ от желаната степен $\boldsymbol{n}$ (тук $\boldsymbol{p}$ 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:

$$u(0)=\begin{bmatrix}1\\0\\\dots\\0\end{bmatrix}=1,\ u(1)=\begin{bmatrix}0\\1\\\dots\\0\end{bmatrix}=\beta,\dots,u(n-1)=\beta^{n-1}=\begin{bmatrix}0\\0\\\dots\\1\end{bmatrix} \qquad 2.81$$

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

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

$$\beta^1,\beta^2,\ldots,\beta^{n-1},\beta^n,\beta^{n+1},\ldots,\beta^{p^n-1} \qquad 2.82$$

т.е. всички ненулеви елементи на $GF(p^n)$ са подредени в експоненциален ред.

6. На елемента 0 и на всеки елемент от степенния ред (2.82) се съпоставя число ***k*** в диапазона $\left[0,\ p^n-1\right]$ съгласно (2.35):

$$\begin{aligned}&\left[0,0,\ldots,0,\ldots,0,0\right]\Rightarrow k=0,\\ &\beta^j=\left[c_{n-1j},c_{n-2j},\ldots,c_{ij},\ldots,c_{1j},c_{0j}\right]\Rightarrow\sum_{i=0}^{n-1}c_{ij}.p^i=k\Rightarrow f_k(x=p),\\ &j=1,2,\ldots,p^n-1\end{aligned} \qquad 2.83$$

Това позволява да се формира лексикографския ред

$$0\Rightarrow f_0(x),\ 1\Rightarrow f_1(x),\ 2\Rightarrow f_2(x),\ldots,p^n-1\Rightarrow f_{p^n-1}(x) \qquad 2.84$$

на елементите на $GF(p^n)$, както и таблицата на техните целочислени логаритми (индекси) като се използва (2.83) в „обратна посока“, т.е.

$$\begin{aligned}&k=0\Rightarrow\beta^{-\infty}=\left[0,0,\ldots,0,\ldots,0,0\right]\Rightarrow ind_\alpha 0=-\infty,\\ &k\Rightarrow f_k(x=p)\Rightarrow\beta^j=\left[c_{n-1j},c_{n-2j},\ldots,c_{ij},\ldots,c_{1j},c_{0j}\right]\Rightarrow ind_\alpha f_k(x)=j,\\ &k=1,2,\ldots,p^n-1\end{aligned} \qquad 2.85$$

7. Ако трябва да се съберат (извадят) два елемента $f_k(x)$ и $f_l(x)$ на $GF(p^n)$, тогава се използва (2.9).

8. Ако трябва да се умножат (разделят) два елемента $f_k(x)$ и $f_l(x)$ на $GF(p^n)$, тогава

8.1) първо се проверява дали някой от тези елементи е 0; ако това е така:

- произведението на елементите е 0;
- и ако $f_k(x)=0$ тогава $\dfrac{f_k(x)}{f_l(x)}=0$;
- и ако $f_l(x)=0$ тогава делението $\dfrac{f_k(x)}{f_l(x)}$ е невъзможно;

8.2) ако и двата елемента не са 0, тогава се определят техните целочислени логаритми (индекси) чрез таблица (2.85), т.е.

$$f_k(x) \Rightarrow ind_\alpha f_k(x) = j_k,\ f_l(x) \Rightarrow ind_\alpha f_l(x) = j_l \qquad 2.86$$

8.3) след това индексите (2.86) се сумират (изваждат) по модул $q = p^n - 1$ (с това се отчита свойство (2.28) на ненулевите елементи на $GF(p^n)$), т.е.

$$f_k(x).f_l(x) \Rightarrow ind_\alpha f_k(x) + ind_\alpha f_l(x) = j_k + j_l = j_s \bmod q, \qquad 2.87$$
$$\frac{f_k(x)}{f_l(x)} \Rightarrow ind_\alpha f_k(x) - ind_\alpha f_l(x) = j_k - j_l = j_s \bmod q$$

8.4) накрая въз основа на изчисления в (2.87) индекс j_s и (2.85) се определя произведението (частното) на два елемента $f_k(x)$ и $f_l(x)$ на $GF(p^n)$ като степен на примитивния елемент β

$$j_s \Rightarrow f_k(x).f_l(x) = \beta^s, \qquad 2.88$$
$$j_s \Rightarrow \frac{f_k(x)}{f_l(x)} = \beta^s$$

Обоснованият до тук Алгоритъм за изчисления в крайни алгебрични полета е много ефективен от изчислителна гледна точка, тъй като използва само събиране на вектори-стълбове и умножение на числа с вектори-стълбове по модул $\boldsymbol{p}$. По тази причина той много лесно се реализира софтуерно, например с MATLAB. На неговата основа в следващия параграф и в Глава трета на дисертационния труд ще бъдат обосновани ефективни от изчислителна гледна точка алгоритми за синтез на дискретни честотни радио- и акустични сигнали.

2.2. Алгоритми за синтез на дискретни честотни радио сигнали

В §1.2 на дисертационния труд беше показано, че при синтеза на ДЧС следва да се разглеждат два основни случая.

Първо, в комуникационните системи, използващи радиосигнали, относителното изменение на носещата честота на сигналите в резултат на ефекта на Доплер е малко и в редица случаи може да се пренебрегне.

Второ, в комуникационните системи, използващи акустични сигнали, относителното изменение на носещата честота на сигналите в резултат на ефекта на Доплер е голямо и не може може да се пренебрегне.

Предвид на това и в изпълнение на третата основна задача на дисертационния труд в настоящия параграф ще бъде обоснован алгоритъм с *P*-сложност за синтез ДЧС за комуникационни системи, използващи радиосигнали.

Общ алгебричен метод за синтез на семейства от ДЧС

Стъпка 1: Синтезира се цикличният код $(N, M_{CC}, N-C; n)$;

Стъпка 2: Множеството от M_{CC} кодови думи се разделя на класове, съдържащи *еквивалентни кодови думи* (две кодови думи от един цикличен код са *еквивалентни*, ако едната кодова дума може да бъде получена чрез циклично отместване на другата кодова дума; по тази причина различните класове от еквивалентни кодови думи се наричат *орбити* [49]);

Стъпка 3: От всяка орбита с дължина *N* се взима само една кодова дума (т.е. взима се само по един представител от всяка орбита);

Стъпка 4: Кодовите думи, избрани на стъпка 3, се трансформират в ДЧС (2.89). Всеки символ на всяка кодова дума се замества с елемент от множеството $F = \{f_{\pi(0)}, f_{\pi(1)}, \ldots, f_{\pi(n-1)}\}$, използвайки произволна пермутация $\{\pi(0), \pi(1), \ldots, \pi(n-1)\}$ на числата $\{0,1, \ldots, n-1\}$.

Общият алгебричен метод за синтез на семейства от ДЧС, разгледан по-горе, може да бъде приложен по различни начин в практиката, тъй като съществуват много методи за синтез на циклични кодове и $n!$ пермутации на индексите на честотите от библиотеката (множеството) F. Ето защо по-нататък в параграфа ще бъде обоснован алгоритъм за синтез на семейства от ДЧС, който е ефективен от изчислителна гледна точка. Алгоритъм се базира на известния *код на Рид – Соломон* (*Reed – Solomon* (RS)) [125], [127].

Алгоритъм 1
за синтезиране на семейства от ДЧС с оптимални корелационни свойства

Стъпка 1: Създава се последователност от вида (2.107), използвайки линейното рекурентно уравнение

$$u(i) = -g_{m-1}.u(i-1) - g_1.u(i-2) - \ldots - g_0.u(i-m), \qquad (2.125)$$
$$i = m, m+1, \ldots, q-2$$

Тук, съгласно <u>*Твърдение 2.3*</u> от по горе, новият ***i***-ти елемент $u(i) = \alpha^i$ от последователността се изчислява на базата на елементите $u(i-1) = \alpha^{i-1}, u(i-2) = \alpha^{i-2}, \ldots, u(i-m) = \alpha^{i-m}$, получени на предишните стъпки на рекурсията, а началните елементи $u(0), u(1), \ldots, u(m-1)$ трябва да бъдат

$$u(0)=\begin{bmatrix}1\\0\\\dots\\0\end{bmatrix}=\alpha^0,\ u(1)=\begin{bmatrix}0\\1\\\dots\\0\end{bmatrix}=\alpha^1,\dots,u(0)=\begin{bmatrix}0\\0\\\dots\\1\end{bmatrix}=\alpha^{m-1} \qquad (2.126)$$

Освен това коефициентите $g_{m-1}, g_{m-2},\dots,g_0$ са дефинирани от генераторния полином (2.106) на полето $GF(q)$, α е произволна нула на генераторния полином (2.106) и всички аритметични операции в (2.125) се изпълняват по модул $\boldsymbol{p}$ [3], [85], [134], [144].

Стъпка 2: Формира се 2-децимация на последователността (2.125)

$$v(i)=u\langle 2.i\rangle_N,\ i=0,1,\dots,q-2=N-1. \qquad (2.127)$$

Стъпка 3: Формират се всички различни циклични отмествания на последователността (2.125)

$$\{u\langle i+1\rangle\}_{i=0}^{q-2},\{u\langle i+2\rangle\}_{i=0}^{q-2},\dots,\{u\langle i+N-1\rangle\}_{i=0}^{q-2} \qquad (2.128)$$

Стъпка 4: Формира се множеството от $M=q+1$ последователности

$$\begin{aligned}
&A_0=\{v(i)\}_{i=0}^{q-2}+\{u(i)\}_{i=0}^{q-2},\\
&A_1=\{v(i)\}_{i=0}^{q-2}+\{u\langle i+1\rangle\}_{i=0}^{q-2},\\
&\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots,\\
&A_{q-2}=\{v(i)\}_{i=0}^{q-2}+\{u\langle i+q-2\rangle\}_{i=0}^{q-2},\\
&A_{q-1}=\{v(i)\}_{i=0}^{q-2},\\
&A_q=\{u(i)\}_{i=0}^{q-2}
\end{aligned} \qquad (2.129)$$

Стъпка 5: Последователностите (2.129) се трансформират в ДЧС (2.89) всеки символ на всяка последователност се замества с елемент от множеството $F=\{f_{\pi(0)},f_{\pi(1)},\dots,f_{\pi(n-1)}\}$, използвайки произволна пермутация $\{\pi(0),\pi(1),\dots,\pi(n-1)\}$ на числата $\{0,1,\dots,n-1\}$.

Стъпка 6:

6.1) От ДЧС, съответстващ на полинома $h_{q-1}(x)=x^2$, се взема едната половина и се формира един нов ДЧС с дължина

$$N_r=N/2=(p^m-1)/2; \qquad (2.143)$$

6.2) Всички останали ДЧС се разделят на две половини, от които се формират два нови ДЧС с дължина (2.143).

2.3.Изводи по глава втора

От анализа, направен в глава втора произтичат следните изводи.

Извод 2.1: Математическият апарат на крайните алгебрични полета е мощно средство за дълбоко, съдържателно и високоефективно изследване на широк кръг от задачи в теорията на комуникационните системи и на радиолокацията, включително и за анализ и синтез на семейства от ДЧС с оптимални корелационни свойства.

Извод 2.2:Обоснованият в § 2.1 *Алгоритъм за изчисления в крайни алгебрични полета* дава възможност съществено да се намали изчислителната сложност на операциите при практическата реализация на математическия апарат на крайните алгебрични полета и се реализира лесно с компютърни системи с матрични процесори.

Извод 2.3:Обоснованият на базата на Твърдения 2.3 и 2.4 в § 2.2 *Алгоритъм 1* позволява да се синтезират оптимални в смисъла на границата на Сингълтън семейства от ДЧС с оптимални корелационни свойства с дължина $N = 2^m - 1$, които могат да намерят успешно приложение в съвременните радиокомуникационни, радиолокационни и радионавигационни системи.

Извод 2.4:От доказаното в § 2.2 Твърдение 2.5 следва, че *Алгоритъм 1* от в § 2.2 може успешно да се прилага и за синтезирането на оптимални в смисъла на границата на Сингълтън семейства от ДЧС с оптимални корелационни свойства с дължина $N = p^m - 1$ като $p > 2$ е произволно просто число.

ГЛАВА ТРЕТА – МЕТОДИ И АЛГОРИТМИ ЗА СИНТЕЗ НА МАСИВИ НА КОСТАС

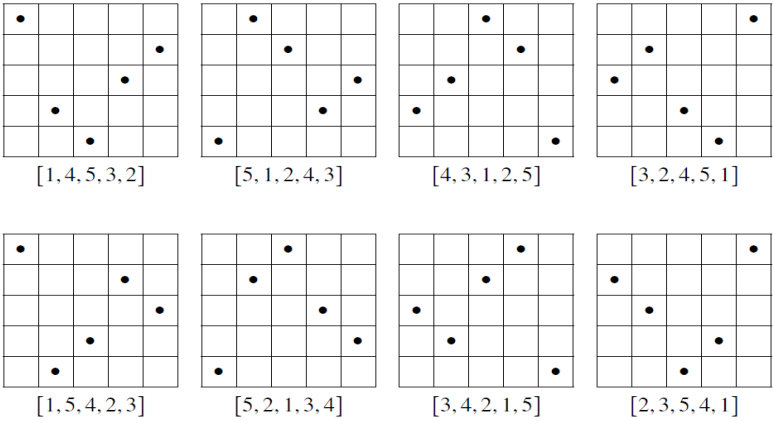
3.1. Масиви на Костас. Основни понятия и определения

При анализа, направен в глава първа, беше показано, че при синтеза на системи от ДЧС следва да се отчита средата на разпространение на сигналите. По – конкретно, при радио-сигналите изменението $f_d = \pm f_0 \frac{2.V_r}{c}$ на носещата честота, предизвикано от ефекта на Доплер, може да се пренебрегне тъй като радиалната скорост V_r на предавателя спрямо приемника е малка в сравнение със скоростта c на разпространение на радио-вълните. При акустичните сигнали обаче, скоростта на разпространение е от порядъка на няколко стотин или хиляди $\left[\frac{m}{s}\right]$ и изменението f_d на носещата честота трябва да се отчита. Този по-сложен случай при синтеза на системи от ДЧС беше формулиран като четвърта основна задача на дисертационния труд. Тя се решава в настоящата трета глава на базата на систематизиране и обобщаване на представените в редица литературни източници частни резултати.

Следва да се отбележи, че в специализираната литература акустичните ДЧС се наричат *масиви на Костас* на името на американския теоретик *Джон Костас* [36], [40], [53], [55], който е един от първите изследователи заедно с Л. Е. Варакин и В. Н. Власов (1960 г. - [8]), започнали работа в тази област в началото на 60-те години на миналия век.

3.2. Еквивалентност на масивите на Костас относно действието на групата D_4

Изчислителната сложност на синтеза на ДЧС, които са масиви на Костас, може да се намали, като се отчита, че един масив на Костас A може да се получи от друг масив чрез завъртане и/или огледално отразяване на A. Действително, посочените операции запазват геометричните съотношения, използвани в *Определение 3.5.* и в резултат втората (производната) матрица също е масив на Костас. Като се вземат предвид всичките осем симетрии на квадрата, които формират така наречената *група* D_4, се вижда, че от един предварително известен масив на Костас A при действието на D_4 се получава семейство от масиви на Костас, наречено *орбита на A под действието на D_4* [88], [97], [98]. Такова семейство е показано на фиг. 3.9 като масивите, получени от предварително известния първи масив чрез завъртания на 90°, 180° и 270° в посока, обратна на движението на часовниковата стрелка (ОЧС), са поставени на първия ред. На втория ред на фиг. 3.9 са разположени масивите, получени от предварително известния първи масив чрез диагонални, хоризонтални, вертикални и антидиагонални отражения.



Фиг. 3.9. Клас от еквивалентни масиви на Костас, представляващи една пълна орбита при действието на групата на симетриите на квадрата D_4

Всяка орбита представлява един клас на еквивалентност и се казва, че масивите на Костас в даден еквивалентен клас са еквивалентни под действието на D_4. *Твърдение 3.3*. показва, че един клас от еквивалентни масиви на Костас има четири или осем члена (елемента), в зависимост от това дали предварително известният първи масив A има диагонална или антидиагонална симетрия. В различни ситуации, като например, при изчерпателно търсене и изброяване на масиви на Костас [50], е удобно да се разглежда само по един представител от всеки клас на еквивалентност. Обикновено се избира представител, който е най-напред измежду членовете на орбитата при лексикографското подреждане на пермутациите.

3.3. Методи за синтез на масиви на Костас

На фиг. 3.10 са показани известните към момента основни алгоритми за синтез на масиви на Костас. Първо е обоснована конструкцията на Лемпел. След това са открити конструкциите на Уелч и на Голомб като втората е обобщение на конструкцията на Лемпел.

Фиг. 3.10. Основни алгоритми за синтез на масиви на Костас

Посочените конструкции се основават на свойствата на крайните алгебрични полета и чрез тях могат да се синтезират масиви на Костас за безкрайно множество от стойности на дължината N на ДЧС (размера масива $n = N$), но не за всички.

Следва специално да се отбележи, че от публикуването на статията [81] до момента не са открити принципно нови конструкции. Поточно, през последните 30 години са разработени алгоритми, чрез които масиви на Костас, синтезирани посредством конструкциите на Лемпел, Уелч и Голомб [44] се трансформират в нееквивалентен масив на Костас с по-малък или по-голям размер. Ето защо по-нататък в този параграф се прави кратък анализ на посочените на фиг. 3.10 конструкции.

3.4. Алгоритми за синтез на семейства от масиви на Костас

Анализираните в § 3.3 конструкции позволяват създаването на отделни масиви на Костас с размер (дължина) n. От друга страна синтезирането на семейства от масиви на Костас притежаващи добри взаимнокорелационни свойства има голямо практическо значение, тъй като много често радарите и сонарите са обединени в сложни комплекси, където възникват взаимни смущения в резултат на едновременната им работа. Ето защо този проблем се анализира в повече детайли по-нататък в параграфа.

Алгоритъм 2
за синтезиране на семейства от масиви на Костас с оптимални корелационни свойства

Стъпка 1: За дадено n, удовлетворяващо условията $n = p - 1$ или $n = p^m - 2$, p е просто число, се построява семейство от $S = \varphi(q-1), q = p$ или $S = [\varphi(q-1)]^2, q = p^m$ масива на Костас по формула (3.13) или формула (3.14) като се използват всички примитивни корени на $GF(p)$ или $GF(q), q = p^m$ съответно;

Стъпка 2: Семейството от масиви на Костас, създадено на предходната стъпка, се разделя на всички възможни $\frac{S(S-1)}{2}$ двойки от масиви;

Стъпка 3: Изчисляват се взаимните функции на неопределеност (ВФН) за всичките двойки от масиви на Костас, формирани на предходната стъпка;

Стъпка 4: Всички масиви на Костас, които образуват двойки с максимално ниво на ВФН над прага $\sqrt{n}$, се отхвърлят;

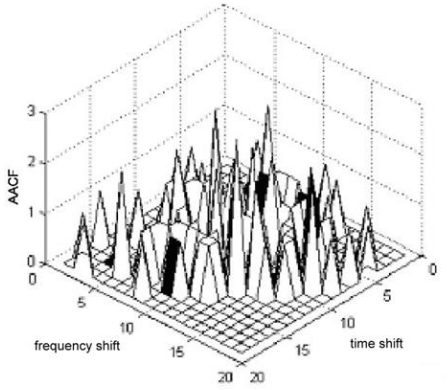
Следва да се отбележи, че стойността $\sqrt{n}$ е избрана като максимално допустимо ниво на ВФН на двойките от масиви на Костас по следните причини.

Първо, минималната стойност $L_{\min max}$ на максималните листа на взаимно-корелационните функции (ВКФ) ниво на семейство от K фазово манипулирани сигнала с дължина n се подчинява на следното неравенство [138]:

$$L_{\min max} \geq n\sqrt{\frac{1-(1/K)}{n-(1/K)}}[V] \approx \sqrt{n}\,[V] \tag{3.22}$$

Второ, натрупаният практически опит при експлоатацията на реални системи показва, че ако максималните листа на ВФН на всички двойки от сигнали, използвани в комуникационната система, е $\sqrt{n}$, взаимните смущения, предизвикани от едновременната работа на абонатите, не оказват съществено вредно влияние.

Обоснованият по-горе Алгоритъм 2 за синтез на семейства от масиви на Костас ще бъде илюстриран с конкретен пример, при който $n = 10$. В този случай $p = 11$ и съгласно (3.21), съществуват $S = 4$ примитивни елемента на полето $GF(11)$. Поради тази причина се използва формула (3.13) за да се синтезира семейство от 4 масива на Костас, които формират шест двойки без повторения.

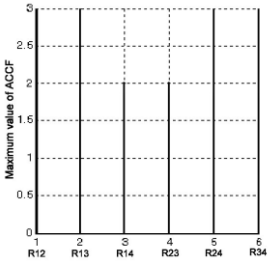


Фиг. 3.14. Общ вид на ВФН на семейство от масиви на Костас с дължина $n = 10$

Общият вид на ВФН на всички двойки ДЧС от семейството е показан на фиг. 3.14, а на фиг. 3.15 са представени техните максимални нива (R_{kl} е максималното ниво на ВФН на k – тия и l – тия ДЧС от семейството).

От фиг. 3.14 и фиг. 3.15. се вижда, че максималните нива на ВФН на всички двойки масиви на Костас от разглежданото семейство не пре-

вишават прага $\sqrt{11} = 3{,}316$, и следователно, синтезираното с Алгоритъм 2 семейство от масиви на Костас притежава оптимални корелационни свойства.



Фиг. 3.15. Максимални нива на ВФН на двойките масиви на Костас с дължина $n = 10$

Следва дебело да се подчертае, че на първата стъпка на Алгоритъм 2 може да се използва Алгоритъм 1 от § 2.2 за да се формира началното множество от ДЧС сигнали. При това обаче трябва да се изследват и ФН на ДЧС от семейството. По тази причина на втората стъпка на Алгоритъм 2 трябва да се формират всички двойки с повторения на ДЧС (т.е. трябва да се формират S^2 двойки от сигнали).

В заключение на параграфа ще бъде обоснован още един алгоритъм за синтез на семейства от ДЧС с оптимални корелационни свойства. Той се основава на факта, че доказателството на конструкцията на Уелч остава вярно, ако вместо просто алгебрично поле $GF(p)$ се използва разширено алгебрично поле $GF(p^m)$. Този факт ще бъде илюстриран с най-простия възможен случай, когато $p = m = 2$. В тази ситуация може да се използва *Пример 2.1* от § 2.2, при което се получава следната пермутация

$$\{d_j\}_{j=0}^{2} = \left\{\alpha^0 = \begin{bmatrix}1\\0\end{bmatrix}, \alpha^1 = \begin{bmatrix}0\\1\end{bmatrix}, \alpha^2 = \begin{bmatrix}1\\1\end{bmatrix}\right\}. \tag{3.23}$$

Тук $\alpha = \begin{bmatrix}0\\1\end{bmatrix}$ е първата нула на неразложимия примитивен над $GF(2)$ полином $g(x) = x^2 + x + 1$ (другата нула на този полином е $\alpha^2 = \begin{bmatrix}1\\1\end{bmatrix}$).

Пермутацията (3.23) е *обобщен масив на Костас*, защото в редовете на нейния триъгълник на разликите няма повтарящи се елементи

$$t_{1,1}(d) = \begin{bmatrix}0\\1\end{bmatrix} - \begin{bmatrix}1\\0\end{bmatrix} = \begin{bmatrix}1\\1\end{bmatrix}, t_{1,2}(d) = \begin{bmatrix}1\\1\end{bmatrix} - \begin{bmatrix}0\\1\end{bmatrix} = \begin{bmatrix}0\\1\end{bmatrix}, \tag{3.24}$$
$$t_{2,1}(d) = \begin{bmatrix}1\\1\end{bmatrix} - \begin{bmatrix}1\\0\end{bmatrix} = \begin{bmatrix}0\\1\end{bmatrix}.$$

Обобщената конструкция на Уелч следва да се обозначава с $W_1(p^m, \alpha, c)$.

За съжаление пермутацията (3.23) не може да се използва директно в инженерната практика тъй като нейните елементи не са обикновени числа. Този проблем може да се преодолее, ако всеки елемент

$$f_i(x) = c_{m-1,i}x^{m-1} + c_{m-2,i}x^{m-2} + \cdots + c_{1,i}x + c_{1,i} \qquad (3.25)$$

на полето $GF(p^m)$ се замени число по формулата

$$f_i(p) = c_{m-1,i}p^{m-1} + c_{m-2,i}p^{m-2} + \cdots + c_{1,i}p + c_{1,i}. \qquad (3.26)$$

В резултат на тази операция пермутациите (3.13) се трансформират в пермутации на числа. Така например при $p = 2, m = 3$ елементите на (3.13) са елементи на полето $GF(2^3)$ и може да се използва *Таблица 2.1* от § 2.1, след което лесно се установява, че пермутацията (3.13) се трансформира както следва

Таблица 3.5

Трансформиране на елементите на пермутацията (1) *в числа при* $p = 2, m = 3$

№	α^i	$[c_2, c_1, c_0]$	$c_2 2^2 + c_1 2 + c_0$
0	α^0	[0, 0, 1]	1
1	α^1	[0, 1, 0]	2
2	α^2	[1, 0, 0]	4
3	α^3	[0, 1, 1]	3
4	α^4	[1, 1, 0]	6
5	α^5	[1, 1, 1]	7
6	α^6	[1, 0, 1]	5

Таблицата на Юнг на пермутацията в последната колона на *Таблица 3.5* е следната.

Таблица 3.6

Таблицата на Юнг на пермутацията $[1, 2, 4, 3, 6, 7, 5]$

	1	2	4	3	6	7	5
t_1	1	2	-1	3	-1	-2	
t_2	3	1	2	4	-1		
t_3	2	4	3	2			
t_4	5	5	1				
t_5	6	3					
t_6	4						

Както се вижда от *Таблица 3.6*, трансформираната пермутация има максимално ниво 2 на листата на ФН, т.е. тя практически много малко отстъпва на един истински масив на Костас. Ето защо при разработването на дисертационния труд беше направено обширно изследване и моделиране с компютър за голям брой стойности на p и m. Получените резултати показват, че трансформираните пермутации (3.26) имат оптимални корелационни свойства и могат да се използват за синтезиране на семейства от ДЧС. Ето защо обоснованият по-горе Алгоритъм 2 може да се преобразува в следния Алгоритъм 3.

Алгоритъм 3
за синтезиране на семейства от ДЧС с оптимални корелационни свойства

Стъпка 1: За дадено n, удовлетворяващо условията $n = p - 1$ или $n = p^m - 1$, p е просто число, се построява семейство от $S = \varphi(q-1), q = p^m$ обобщени ДЧС по формула (3.13) като се използват всички примитивни корени на $GF(q), q = p^m$;

Стъпка 2: Всеки обобщен ДЧС от семейството, създадено на предходната стъпка, се трансформира в обикновен ДЧС по формула (3.25);

Стъпка 3: Семейството от ДЧС, създадено на предходната стъпка, се разделя на всички възможни S^2 двойки от ДЧС с повторения.

Стъпка 4: Изчисляват се ФН и ВФН за всичките двойки от ДЧС, формирани на предходната стъпка.

Стъпка 5: Всички ДЧС, чиито ФН или ВФН имат максимално ниво над прага $\sqrt{n}$, се отхвърлят.

3.5.Изводи по глава трета

От анализа, направен в глава трета произтичат следните изводи.

Извод 3.1: При акустичните сигнали поради относително ниската скорост на разпространение на вълните следва да се отчита изменението на носещата честота, предизвикано от ефекта на Доплер. Този посложен случай при синтеза на системи от ДЧС е прието да се нарича *проблем за синтезирането на масиви на Костас.*

Извод 3.2: Масивите на Костас са ДЧС със сложна вътрешна структура, осигуряваща им устойчивост в условията на радио-електронно противодействие. Освен това тяхното прилагане в сонарите води до значително разширяване на обхвата на действие, подобряване на точността и разделителната способност по разстояние, както и точността на измерване на радиалната скорост на обектите.

Извод 3.3: Към момента са известни 3 конструкции, които позволяват синтезирането на масиви на Костас за дължини на сигналите

почти изключително от вида $n = p - 1$ или $n = p^m - 2$, като p е просто число.

Извод 3.4: В § 3.4 са обосновани два алгоритъма (Алгоритъм 2 и Алгоритъм 3) с полиномиална сложност за синтез на семейства от ДЧС с оптимални корелационни свойства. Синтезираните с тези алгоритми семействата от ДЧС осигуряват възможност на комуникационните системи да работят устойчиво в сложни условия като многолъчево разпространение на вълните, взаимни смущения и активно радио-електронно противодействие. Следователно Алгоритъм 2 и Алгоритъм 3 могат да се използват успешно при разработката на комуникационни системи, за които функционалната надеждност е от приоритетно значение.

ГЛАВА ЧЕТВЪРТА – ОСНОВНИ РЕЗУЛТАТИ ОТ ИЗСЛЕДВАНЕТО, ПРОВЕДЕНО ПО ДИСЕРТАЦИОННИЯ ТРУД

4.1. Софтуерна система за автоматизиран синтез на семейства от ДЧС с оптимална автокорелационна функция

За решаване на петата основна задача на дисертационния труд беше разработена компютърна софтуерна система за автоматизиран синтез на семейство от ДЧС с оптимални автокорелационни свойства [15]. Тази система се състои от няколко универсални компютърни програми, работещи в средата на MATLAB, която осигурява практическото използване на Алгоритъм 1 от §2.2 и Алгоритми 2 и 3 от §3.4 съответно.
Работата на първата универсална програма, реализираща Алгоритъм 1 от §2.2., се пояснява с блок – схемата от фиг. 4.1 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 бяха използвани стойностите

$$p = 2, 3, 5 \tag{4.1}$$

които намират най-голямо практическо приложение предвид на простотата на практическата реализация;

- ***m*** – ***степен*** на разширение на простото поле на Галоа, която следва да бъде цяло число, $m \geq 1$;

$$m = 2, 3, 4 \ldots \tag{4.2}$$

които осигуряват постигането на целта на дисертационния труд, като този въпрос ще бъде анализиран в по-подробно в следващия § 4.2.;

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

Следва да се отбележи специално, че:

- ***p*** и ***m*** определят най-важните параметри на семейство ДЧС сигнали, а именно

$$q = p^m,\ N = q-1, M.N = q^k - 1, d = N - k + 1, n = q \tag{4.3}$$

- ако параметрите не са въведени съгласно ограниченията и изискванията към ***k***, програмата изисква тяхното коригиране.

2) На базата на въведения неразложим над $GF(p)$ примитивен полином от ***m***-та степен чрез Алгоритъма за изчисления в крайните алгебрични полета от § 2.1. се формира експоненциален ред на ненулевите елементи $\alpha^0 = 1, \alpha^1, \ldots, \alpha^{q-2}$ на разширеното поле $GF(p^m)$ (тук α е коя да е от нулите на $g(x)$). Както беше изяснено в § 2.1., посоченият алгоритъм всъщност се свежда до изчисляване на елементите на ЛРП като се използва общата структурна схема от фиг. 2.2., която се реализира много просто с компютърна система с матричен процесор.

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

$$0 = \begin{bmatrix} 0 \\ 0 \\ \ldots \\ 0 \end{bmatrix} \tag{4.4}$$

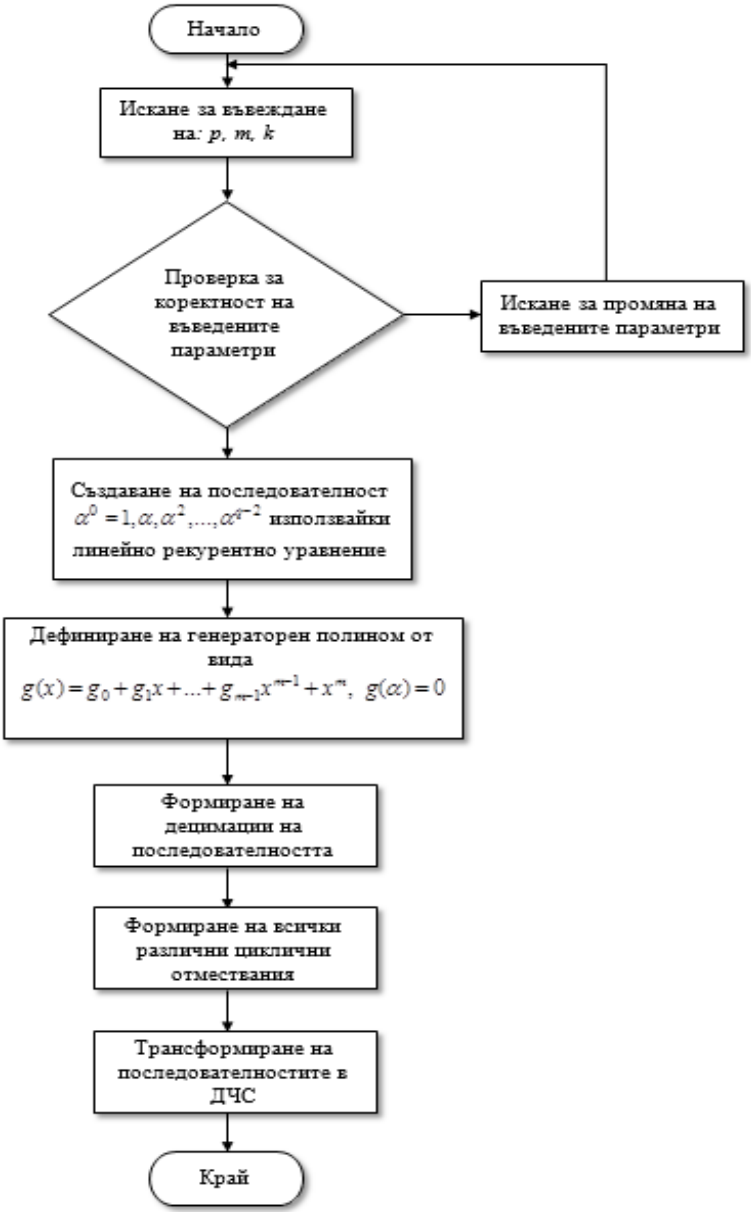
В резултат се получава експоненциалният ред на всички елементи на $GF(2^m)$

$$0, \alpha^0, \alpha^1, \ldots, \alpha^{q-2} \tag{4.5}$$

3) Създават се последователности от вида (2.19) като се прилага линейното рекурентно уравнение. След което се формират и децимациите на последователностите съгласно (2.39).

4) Формират се всички различни циклични отмествания на създадените на предходната стъпка последователности като се използва формула (2.40) и се формира множеството от $M = q + 1$ последователности по формула (2.41).

5) Получените последователности от различни орбити се трансформират в ДЧС, използвайки произволна пермутация на числата $\{0, 1, \ldots, n-1\}$



Фиг. 4.1. Блок – схема на универсална програма, реализираща Алгоритъм 1 от §2.2

4.2. Основни резултати от изследването, проведено по дисертационния труд

В резултат от използването на представения в предходния параграф универсална програма бяха синтезирани семейства от ДЧС с оптимални корелационни свойства. Някои от тези ДЧС сигнали са представени в *Таблица 4.5.* и *Таблица 4.6.*

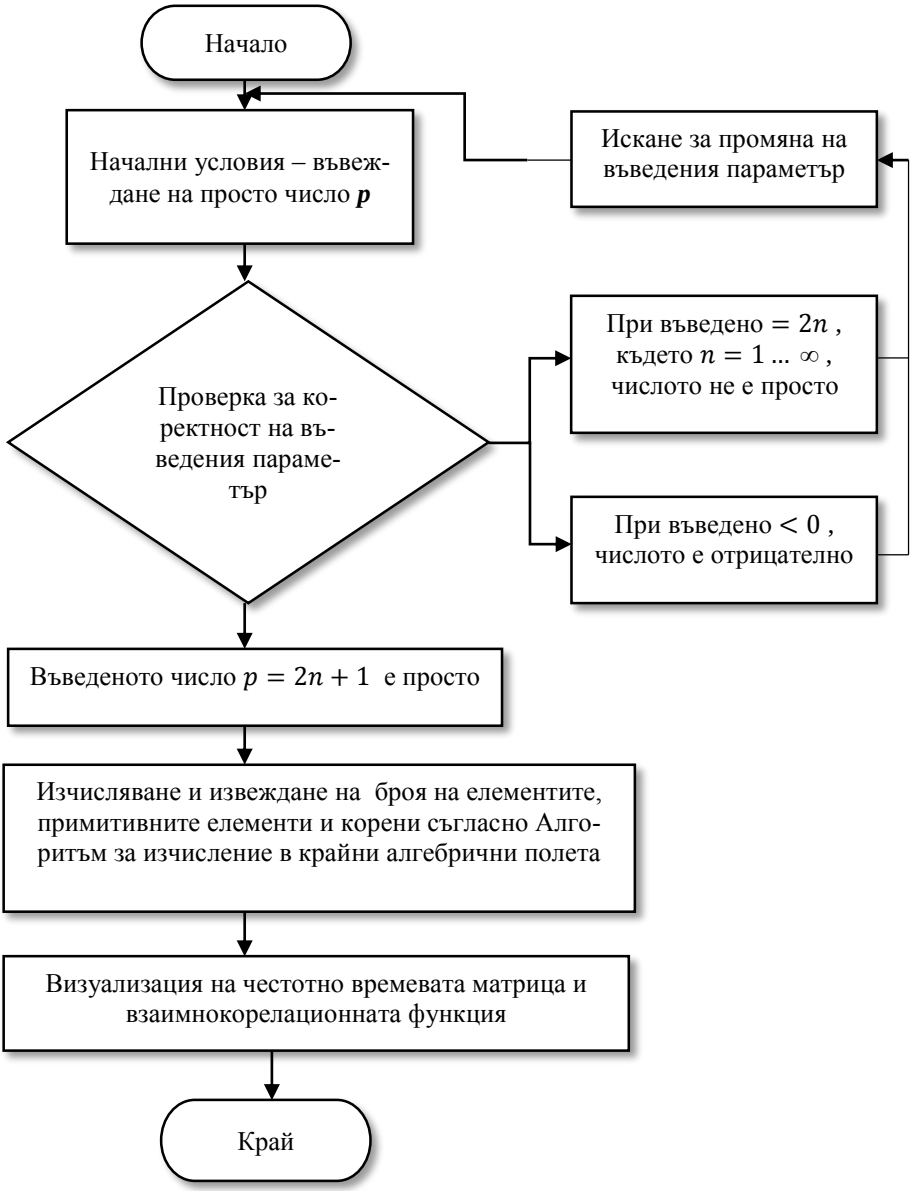
4.3. Приложение на алгоритъма за синтез на ДЧС сигнали с идеална или близка до идеалната АКФ

За решаване на петата основна задача на дисертационния труд беше разработена компютърна софтуерна система за автоматизиран синтез на дискретно честотни сигнали с оптимални корелационни свойства [14]. Тази система се състои от две универсални компютърни програми, работещи в средата MATLAB, които осигуряват практическото използване на Алгоритъм за изчисления в крайни алгебрични полета и Алгоритми 2 и 3 от §3.3.

За да се решат задачите за намиране на примитивните елементи на простите полета на Галоа и построяването на честотно-времевата матрица и взаимно корелационна функция на масиви на Костас е целесъобразно прилагането на следната последователност от действия (фиг. 4.2) [14], [15], [16]:

Прилагане на алгоритъма:

Прилага се алгоритъма от Фиг. 4.2 за да се намерят примитивните корени и примитивните елементи на числото 11 и да се построи честотно-времевата матрица и взаимнокорелационната функция на масива на Костас. Прилага се методът на Ойлер. В *Таблица 4.7* са изчислени всичките примитивни елементи по mod 11. Проверката е извършена чрез реализираната в среда Matlab CUI програма.



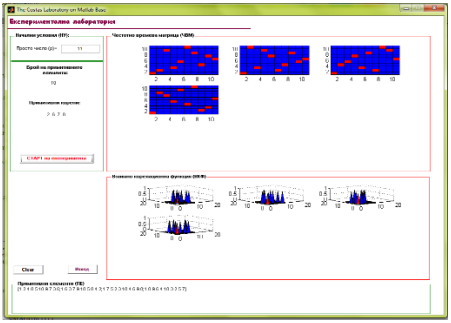
Фиг. 4.2. Блок схема на Алгоритъм за визуализация на честотно-време-вата матрица (ЧВМ) и взаимнокорелационна функция (ВКФ)

Таблица 4.7.

Степени на $\boldsymbol{a^i}$ по $\boldsymbol{mod\ 11}$

a / i	1	2	3	4	5	6	7	8	9	10
1	1	2	3	4	5	6	7	8	9	10
2		4	9	5	3	3	5	9	4	1
3		8	5	9	4	7	2	6	3	
4		5	4	3	9	9	3	4	5	
5		10	1	1	1	10	10	10	1	
6		9				5	4	3		
7		7				8	6	2		
8		3				4	9	5		
9		6				2	8	7		
10		1				1	1	1		
P_i	1	10	5	5	5	10	10	10	5	2

В този случай, когато $P_m(a) = \varphi(m)$, a се нарича примитивен корен по модул m. В примера, примитивни корени са числата 2, 6, 7 и 8. На Фиг. 4.5 са визуализирани примитивните елементи и корени по mod 11, както и ЧВМ и ВКФ.



Фиг. 4.5. Визуализация на примитивните елементи, корени и характеристики при p=11

Опитът показва, че използването на компютърна лаборатория за решаване на задачи за определяне простотата на число и за визуализирането на примитивните елементи и корени, с чиято помощ се построяват взаимнокорелационната функция и честотно-временната матрица, е бързо и ефективно. Тази лаборатория може непрекъснато да се надгражда и да се обновява с цел по-ефективна работа. При изследвания на малки прости положителни числа, изискванията към компютърната конфигурация не са големи. В тези случаи компютърната лаборатория може да работи успешно и с по-стари компютърни конфигурации. Разбира се, за намиране на примитивните елементи и корени на по-големи положителни прости числа е необходима по мощна конфигурация, подходяща най-вече за научни и изследователски цели.

Въз основа на полученото до тук и желанието да се постигне визуализирането на няколко двойки масиви на Костас върху една автокорелационна функция е предложен подобрен метод за синтезиране на семейства масиви на Костас. Използват се конструкциите Уелч и Голомб [82], [86], [87]. На фиг. 4.6 е показан алгоритъмът на работа на програмата (Алгоритъм 2 от §3.4.).

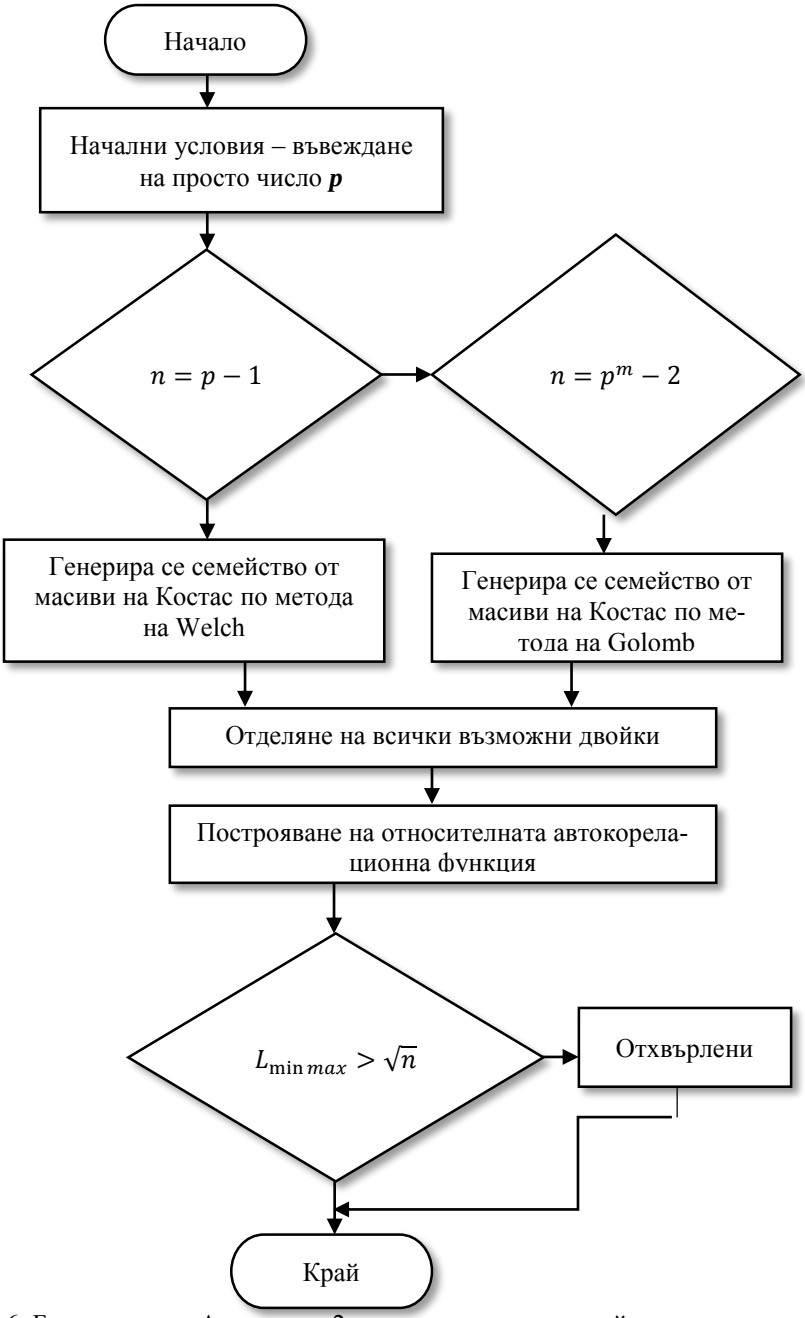
Алгоритъм е изпълнява на четири стъпки

Първа стъпка: Въвежда се просто число $\boldsymbol{p}$ и ако е изпълнено едно от двете условия [107] се генерира семейство от масиви на Костас съответно по формула (3.13) или (3.14);

Втора стъпка: Всички масиви на Костас от семейството се разделят на двойки;

Трета стъпка: Изчисляват се ФН и ВФН на всички двойки от масиви на Костас, формирани на предишната стъпка;

Четвърта стъпка: Всички масиви на Костас, образуващи двойки, при които максималното ниво на ВФН надвишава прага $\sqrt{n}$ се отхвърлят.



Фиг. 4.6. Блок схема на Алгоритъм 2 за синтезиране на семейства от масиви на Костас

4.4. Изводи по четвърта глава

Извод 4.1.: При синтеза на ДЧС 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 семейства от ДЧС с оптимални корелационни свойства. При практическото използване на системата са получени редица неизвестни до момента ДЧС с висока структурна сложност и оптимални корелационни свойства (*Таблица 3.3. и Таблица. 3.4.* от §3.4).

Извод 4.2.: Резултатите, получени при изследванията по дисертационния труд, могат да използвани при разработката на комуникационни системи, които трябва да могат да работят устойчиво в сложни условия като многолъчево разпространение на вълните, взаимни смущения и активно радио-електронно противодействие.

ЗАКЛЮЧЕНИЕ

В резултат на изследванията в рамките на дисертационния труд са получени следните:

I. НАУЧНИ ПРИНОСИ

1. Синтезирани са два алгоритъма (Алгоритъм 1 от § 2.2. и Алгоритъм 3 от §3.4.) полиномиална сложност за синтезиране на дискретни честотни сигнали.

2. В резултат на практическото използване на посочените Алгоритъм 1 и Алгоритъм 3 са установени нови неизвестни до момента семейства дискретни честотни сигнали с оптимални корелационни свойства (§ 4.2., Табл. 4.5 и Табл. 4.6).

II. НАУЧНО-ПРИЛОЖНИ ПРИНОСИ

1. Разработен е Алгоритъм за изчисления в крайни алгебрични полета (§ 2.1.), който лесно се реализира практически с компютърни системи с матрични процесори.

2. Обоснован е алгоритъм с полиномиална сложност (Алгоритъм 3 от § 3.4.) за синтез на семейства от дискретни честотни сигнали с дължина $N = p^n - 1, p^n - 2$ (***p*** е просто число, а ***n*** е произволно цяло положително число).

III. ПРИЛОЖНИ ПРИНОСИ

1. Анализирано е съвременното състояние на методите за синтез на семейства от дискретни честотни сигнали и са обосновани перспективните пътища за тяхното развитие (§ 1.2).

2. Анализирани са факторите, от които зависят максималните нива на листата на ПАКФ и ПВКФ на семействата от дискретни честотни сигнали, синтезирани с Алгоритъм 3 от § 3.2.

3. Анализирани са факторите, от които зависят максималните нива на листата на ПАКФ и ПВКФ на семействата от дискретни честотни сигнали, синтезирани с Алгоритъм 3 от § 3.2.

4. На базата на Алгоритъм 1 от § 2.2 и Алгоритми 2 и 3 от § 3.4 е разработена система за автоматизиран синтез на дискретни честотни сигнали, позволяваща да се анализират техните корелационни свойства (§4.1.).

БЛАГОДАРНОСТИ

Изказвам своята искрена признателност и благодарност на научния си ръководител проф. дтн Борислав Беджев за неговите ценни напътствия, професионална компетентност и съдействие при провеждане на настоящите изследвания и при подготовката на дисертацията. Изключително благодаря и за неговата неоценима морална подкрепа и за проявеното търпение.

Благодаря от цялото си сърце на човека - колега и приятел, доц. д-р Тодор Иванов, за безкрайната му всеотдайност и съдействие. Той повярва в мен, като до сетния си дъх ме насърчаваше. Поклон пред светлата му памет.

Благодаря на всички колеги от катедра „Компютърни системи и технологии“ към факултет по Технически науки за оказаното съдействие и подкрепа.

Не на последно място благодаря специално на семейството и приятелите си за тяхното търпение и стимулиращи напътствия.

СПИСЪК НА ПУБЛИКАЦИИТЕ ПО 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, Научна конференция с

международно участие - МАТТЕХ ШУ „Епископ Константин Преславски 22-24.11.2012, Шумен
[4] **Станева Л. Ан.**, Беджев Б., Симеонов С., Някои методи за синтез на дискретно честотни сигнали, Международна научна конференция „Образование, наука, икономика и технологии“, том VIII(1), 2012, Бургас
[5] **Станева Л. Ан.**, Цанков Ц., Компютърна лаборатория за синтез на сложни дискретно честотни сигнали, Научна конференция с международно участие - МАТТЕХ ШУ „Епископ Константин Преславски 22-24.11.2012, Шумен
[6] **Станева Ан. Л.**, Алгоритми за построяване на масиви на Костас, Научна конференция с международно участие - МАТТЕХ ШУ „Епископ Константин Преславски 22-24.11.2012, Шумен
[7] Iliev M, B. Bedzhev, T. Trifonov, **L. Staneva**, An algorithm for synthesis of families of frequency hopping signals with ideal periodic correlation properties, Information, Comunication and Control systems and Technologies, Year II, No.1/2013, Ruse.
[8] Mutkov V, N. Nikolov, R. Tsakov, **L. Staneva**, An Improved Method for Synthesis of Families of Costas Arrays, 17th Telecommunications forum TELEFOR 2009, Serbia, Belgrade, November 24 – 26, 2009

ANNOTATION

Dissertation:

ALGORITHMS FOR SYNTHESIS AND PROCESSING OF FAMILIES OF COMPLEX SIGNALS WITH OPTIMAL CORRELATION PROPERTIES

Author: M.Sc. Eng. Liliya Anestieva Staneva

A key role for the present wireless communications plays families of signals with optimal correlation properties. They find many applications for synchronization, channel estimation, elimination of the negative effects, caused by the multipath spread of the electromagnetic waves, data protection, code division multiple access 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 signals are known. Some of the most famous of them are the so – named families of Costas arrays and frequency hopping (FH) signals. With regard to this problem in the dissertation new algorithms for synthesis of families of FH signals and Costas Arrays with optimal correlation properties are developed. They are applicable in the fourth and next generation mobile communications or other wireless systems, using pseudo-noise signals.

In Chapter 1 the basic concepts and mathematical functions, describing the correlation properties of the signals, are outlined. The contemporary state of the methods for synthesis of FH signals and their applications in the mobile communication systems are analyzed. On this base the aim and the objectives of the dissertation are formulated.

In Chapter 2 the present computer methods for calculations in finite algebraic structures are systematized and analyzed. Using these results an algorithm for synthesis of families of FH radio-signals with ideal periodic correlation properties is suggested.

In Chapter 3 methods for synthesis of families of FH acoustic signals, which are Costas arrays, are systematized and analyzed. On this base two algorithms for synthesis of families of Costas arrays with optimal correlation properties are developed.

In Chapter 4 a software system for synthesis of families of FH radio- and acoustic signals, implemented in MATLAB environment, is presented. It automatizes all procedures in the process of analysis and synthesis of families of FH signals with optimal correlation properties.

The suggested in the dissertation algorithms could be useful in the development of communication systems, which must have very high functional reliability and ability to operate properly in very severe conditions of multipath spreading of the waves and radio-electronic counter-measurement.