МОСКОВСКИЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ СВЯЗИ И ИНФОРМАТИКИ

На правах рукописи

Кренгель Евгений Ильич

"ИССЛЕДОВАНИЕ И РАЗРАБОТКА НОВЫХ КЛАССОВ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ И УСТРОЙСТВ ИХ ГЕНЕРАЦИИ ДЛЯ СИСТЕМ С КОДОВЫМ РАЗДЕЛЕНИЕМ КАНАЛОВ"

Специальность 05.12.13 - Системы, сети и устройства телекоммуникаций

Диссертация

на соискание ученой степени кандидата технических наук

Научный руководитель:

д.т.н., профессор Мешковский К.А.

Москва - 2002

Содержание

Введение

Мир сегодня переживает поистине самую настоящую "бескровную" революцию в области информационно-телекоммуникационных технологий (ИТТ), которые становятся одним из наиболее важных факторов, влияющих на формирование общества 21 века. Их воздействием в значительной степени обусловлены наметившиеся тенденции к глобализации мировой экономики и к построению информационного общества. На состоявшемся в июле 2000г. на Окинаве форуме глав восьми индустриально развитых стран подчеркивалось возрастание роли ИТТ в реализации программы повышения уровня эффективности и конкурентоспособности национальных экономик, преодолении разрыва в развитии ряда стран и борьбе с бедностью. В принятой на этом форуме хартии открытого информационного общества говорится [1]:

"Суть стимулируемой ***ИТТ*** экономической и социальной трансформации заключается в ее способности содействовать людям и обществу в использовании знаний и идей. Информационное общество, как мы его представляем, позволяет людям шире использовать свой потенциал и реализовывать свои устремления. Для этого мы должны сделать так, чтобы ***ИТТ*** служили достижению взаимодополняющих целей обеспечения устойчивого экономического роста, повышения общественного благосостояния, стимулирования социального согласия и полной реализации их потенциала в области укрепления демократии, транспарентного и ответственного управления, международного мира и стабильности. Достижение этих целей и решение возникающих проблем потребует разработки эффективных национальных и международных стратегий". Важное место в дискуссии занял вопрос о преодолении электронно-цифрового разрыва внутри государств и между ними. Для этого повсеместно необходимо развивать современные цифровые средства и системы связи, обеспечивающие свободный и надежный обмен разнотипной информацией (речью, данными, мультимедийной информацией) из любой доступной точки планеты. Участники форума подтвердили свою приверженность предпринимаемым в настоящее время усилиям

по разработке и осуществлению последовательной стратегии, направленной на решение данного вопроса.

Основой экономического роста в последующие десятилетия станет создание единого общемирового информационного пространства, включающего в себя все виды телекоммуникационных сетей из радио, проводных и оптоволоконных кабельных линий связи. Важная роль в этом процессе принадлежит беспроводным технологиям связи, бурный рост которых совместно с последними достижениями микроэлектроники открывают уникальные возможности по созданию глобальной системы персональной связи. За прошедшее десятилетие беспроводная персональная связь прошла путь от неопределенной концепции до глобальной телекоммуникационной службы, основу которой в настоящее время составляют системы подвижной радиотелефонной связи 2-го поколения с почти 400 миллионами подписчиков. Однако несовместимость большинства существующих систем 2-го поколения, а также их ограниченные возможности по увеличению пропускной способности и предоставлению качественно новых видов услуг вызвали потребность в создании концепции единого стандарта на системы мобильной связи. Одним из самых амбициозных проектов конца 20 века является концепция IMT-2000 построения систем мобильной связи 3-го поколения (3G) [2,3], в основе которой лежит принцип мобильного доступа ко всем ресурсам единого общемирового информационного пространства из любой точки на поверхности Земли и в любое время. Согласно прогнозу UMTS возможное число абонентов в наземных сетях мобильной связи к 2005г. превысит 1700 миллионов, а к 2015г. ее абонентами могут стать 3 миллиарда человек [2].

Ключевой проблемой при построении систем мобильной связи является выбор метода многостанционого доступа, характеризующего способность базовой станции одновременно передавать и принимать сигналы мобильных абонентов. В настоящее время все более широкое распространение в системах мобильной связи получает технология многостанционного доступа с кодовым разделением каналов (Code Division Multiple Access

или сокращенно CDMA), основными принципами которой являются расширение спектра в сочетании с кодовым разделением физических каналов за счет использования псевдослучайных последовательностей (ПСП). Изначально технология CDMA возникла в 50гг. применительно к военной области для обеспечения скрытности и эффективной работы систем связи в условиях радиопротиводействия и многолучевого распространения сигналов [4]. В течение нескольких десятилетий основным препятствием для внедрения технологии CDMA в коммерческие системы являлась ее значительная функциональная сложность. Достижения в области цифровой обработки сигналов и микроэлектроники в 90гг. положили начало процессу внедрения этой технологии в системах мобильной связи 2-го поколения. В существующих системах подвижной связи 2-го поколения технология CDMA (стандарт IS-95) обеспечивает более высокую пропускную способность по сравнению с другими известными технологиями Frequency Division Multiple Access (FDMA) и Time Division Multiple Access (TDMA) [5,6]. Сегодня из-за своих бесспорных преимуществ технология CDMA принята в качестве основной при разработке концепции IMT-2000.

Псевдослучайные последовательности по образному выражению С. Голомба составляют основу технологии CDMA [7], поскольку именно они обеспечивают расширение спектра и кодовое разделение каналов. Расширение спектра производится за счет модуляции несущего колебания по закону псевдослучайной последовательности, при этом используется прямой метод модуляции (Direct Sequence или сокращенно DS) и модуляция скачкообразным переключением частоты (Frequency Hopping или сокращенно FH). Получаемый в результате такого преобразования сигнал получил название широкополосного шумоподобного сигнала. Кодовое разделение или различение каналов в системе с CDMA осуществляется за счет присвоения каждому абонентскому каналу такой кодовой ПСП (в литературе такие последовательности получили название сигнатурных [8]), которая максимальным образом не коррелирована с сигнатурными последовательностями других абонентских каналов. Для мобильных систем CDMA это условие означает, что

значения взаимно-корреляционных функций (ВКФ) этих последовательностей при всех сдвигах должны быть малы. Для фиксированных систем CDMA достаточно обеспечить малую взаимную корреляцию последовательностей в одной точке. Очевидно, чем больше будет найдено сигнатурных последовательностей с минимальной взаимной корреляцией, тем больше может быть абонентов в системе. В большинстве CDMA систем синхронизация между базовыми и абонентскими станциями также обеспечивается посредством псевдослучайных последовательностей. Это могут быть как сигнатурные, так и специально выделенные пилот сигнальные последовательности с малыми значениями боковых выбросов их автокорреляционных функций (АКФ). В дальнейшем такие АКФ, равно как и ВКФ, будем называть хорошими. Заметим, что последовательности с хорошими АКФ и ВКФ требуются также для борьбы с многолучевостью. Еще одним важным требованием, предъявляемым к современным коммерческим системам с CDMA, является обеспечение конфиденциальности передачи. С этой целью в этих системах применяются ПСП с большим периодом и большой линейной сложностью [9].

Среди известных семейств ПСП длины 2^N-1 с близкой к идеальной автокорреляцией [10, 11, 12] (их еще называют последовательностями типа Адамара) наибольшее распространение в широкополосной связи получили m-последовательности, поскольку генерация этих последовательностей наиболее проста, а их свойства по сравнению с другими изучены намного лучше. В настоящее время в мире насчитывается не одна сотня работ по m-последовательностям и интерес к ним не ослабевает [7,13]. Однако, будучи линейными, m-последовательности характеризуются малым значением линейной сложности. Данного недостатка лишены некоторые другие последовательности типа Адамара и, прежде всего, последовательности GMW [14], интерес к которым, судя по имеющимся публикациям, сегодня значительно возрос. Кроме того, численность семейства последовательностей GMW при больших значениях N во много раз превышает число m-последовательностей. Построение таких ПСП существенно расширяет исходную базу для

формирования максимальных по объему подмножеств ПСП с приемлемым уровнем взаимной корреляции, что позволяет в одних случаях увеличивать число пользователей при заданной помехоустойчивости, а в других случаях снижать уровень взаимных помех при фиксированном числе пользователей. Таким образом, успешная работа систем с CDMA прямым образом зависит от возможности конструирования многочисленных ансамблей ПСП, удовлетворяющих всем вышеперечисленным требованиям при приемлемой аппаратной сложности их генерации.

Целью диссертационной работы является конструирование новых классов ПСП большого объема с близкой к идеальной автокорреляцией и сложной имитационной структурой, исследование их основных параметров: общего количества, взаимной корреляции и линейной сложности, а также разработка методов и устройств их генерации для систем связи с многостанционным доступом и кодовым разделением каналов.

Решение этой проблемы для систем связи с CDMA расширяет возможность выбора максимального по объему множества сигналов с заданной помехоустойчивостью и облегчает построение устройств синхронизации абонентских приемников при заданном числе абонентов. На основе этих последовательностей могут быть синтезированы системы ортогональных кодовых последовательностей большой линейной сложности и осуществлено криптозащищенное скремблирование передаваемой информации.

Поставленная цель достигается решением следующих задач.

1. Анализ существующих классов ПСП и критериев их выбора для широкополосных систем связи на базе технологии DS-CDMA.
2. Систематизация известных и новых классов последовательностей GMW и нахождение общего числа этих последовательностей для всех возможных значений N.
3. Разработка новых методов оценки и расчета ЛС ПСП GMW, строящихся на основе различных базисных последовательностей не зингеровского типа.

4. Разработка методов исследования ВКФ последовательностей типа Адамара, включая оценки максимума взаимной корреляции классов m-последовательностей, последовательностей GMW, последовательностей Холла и Лежандра.
5. Разработка нового метода генерации ПСП GMW и его схемотехническое решение.
6. Использование исследуемых классов ПСП в системах с CDMA для:
   - формирования максимальных по объему подмножеств квазиоптимальных последовательностей;
   - формирования новых систем ортогональных сигналов большой ЛС;
   - повышения безопасности связи в системах на основе стандартов IS-95 и cdma2000;
7. Экспериментальные исследования разработанных систем ортогональных сигналов объема 128 на базе действующей радиосистемы многостанционного доступа "СТС-ИСТОК CDMA РРК 3/5.0"

Решение поставленной задачи достигается посредством анализа и учета взаимно исключающих требований, предъявляемых к псевдослучайным последовательностям: многочисленность ансамбля, хорошие корреляционные свойства, большая линейная сложность и простота аппаратной реализации.

В диссертации использовались следующие **методы исследования**:

1) комбинаторный анализ и теория конечных полей;
2) теория периодических дискретных сигналов;
3) теория передачи дискретных сообщений;
4) математическое моделирование.

В диссертационной работе впервые были получены следующие **новые научные результаты**.

1. На основе введенной классификации и найденных условий эквивалентности классов ПСП GMW с различной длиной базисных последовательностей, получена формула для расчета общего числа различных двоичных ПСП GMW.

2. Предложен и апробирован метод исследования ВКФ последовательностей типа Адамара на основе разбиения их изоморфных коэффициентов на смежные классы по подгруппе максимального порядка, позволяющий существенно сократить объем вычислений их ВКФ на компьютере.

3. Произведены оценки максимума ВКФ классов m-последовательностей, GMW, Холла и Лежандра. Полученные оценки могут быть использованы для формирования подмножеств последовательностей с заданными корреляционными свойствами.

4. Найдена верхняя граница и разработаны методы расчета ЛС двоичных ПСП GMW, строящихся на основе различных базисных последовательностей не зингеровского типа, позволившие впервые найти ЛС для всех 79-ти классов ПСП GMW длины 16383.

5. Разработан метод генерации двоичных последовательностей GMW на основе сдвинутых копий двоичной m-последовательности той же длины и его схемное решение.

6. Построены системы ортогональных сигналов большой линейной сложности на основе систем производных последовательностей, в которых исходной является m-последовательность, а производящей последовательность GMW.

7. Предложен метод защиты информации от несанкционированного доступа для систем связи CDMA на основе стандартов IS-95 и cdma2000, где в качестве скремблирующей последовательности предлагается ПСП GMW большой линейной сложности.

8. Построены производные системы ортогональных сигналов порядка 128 на основе последовательностей типа Адамара длины 127 для действующей радиосистемы многостанционного доступа "СТС-ИСТОК CDMA РРК 3/5.0".

Основные положения, выносимые на защиту.

1. Проведенная систематизация и разбиение последовательностей GMW на классы позволяет найти общее количество этих последовательностей, а также применять к их классам одни и те же методы исследования.

2. Разработанный метод исследования периодических ВКФ последовательностей типа Адамара мощности M с помощью изоморфных коэффициентов позволяет в M-1 раз ускорить расчет их корреляционных параметров на компьютере.
3. Найденные пары m и GMW последовательностей с максимальными пиками взаимной корреляции и их свойства позволяют повысить эффективность отбора последовательностей для систем связи с CDMA с заданным уровнем взаимной корреляции за счет сокращения их области поиска по ансамблю до двух раз.
4. Применение разработанного метода генерации последовательностей GMW на основе сдвинутых копий двоичной m-последовательности той же длины позволяет значительно упростить реализацию последовательностей GMW по сравнению с методом Шольца-Велча, использующего для этой цели q-ичную m-последовательность.

Структура и объем работы.

Диссертация состоит из введения, 6-ти глав, заключения, библиографического списка использованной литературы и приложения. Основная часть работы изложена на 182 страницах и содержит 26 таблиц и 14 рисунков.

Краткое содержание работы.

Во введении обосновывается актуальность решаемой в диссертации научно-технической проблемы, сформулированы цель и задачи исследований, описывается научная новизна и основные положения, выносимые на защиту.

В первой главе, посвященной современным принципам конструирования ПСП для систем CDMA, изложены особенности построения широкополосных систем связи на базе технологии DS-CDMA. Дан краткий обзор известных и новых семейств двоичных ПСП с оптимальной ВКФ и показаны их недостатки по сравнению с последовательностями GMW. Рассмотрены критерии оптимального выбора последовательностей для систем связи с CDMA.

Во второй главе, посвященной математическим основам классов двоичных ПСП GMW, дано формальное определение этих ПСП, разработан общий алгоритм построения и проведена их систематизация посредством разбиения на классы. Получено выражение для вычисления общего числа этих ПСП при любом допустимом значении N. Найдена верхняя граница ЛС ПСП GMW. Разработаны методы расчета их ЛС для случаев, когда известные аналитические расчетные формулы не применимы. Приведены результаты расчета ЛС ПСП GMW для N=12, 16, 18, 20 и 24. Впервые сделан полный расчет ЛС для всех 79 различных классов этих ПСП длины 16383.

В третьей главе, посвященной взаимной корреляции последовательностей типа Адамара, рассмотрен метод исследования ПВКФ последовательностей типа Адамара с помощью изоморфных коэффициентов, позволяющий существенно ускорить их расчет на компьютере; найдены оценки максимума взаимной корреляции классов m и GMW последовательностей, а также последовательностей Холла и Лежандра. Подробно исследованы четные и нечетные ВКФ всех последовательностей типа Адамара длины 127 и их ЛС.

В четвертой главе, посвященной анализу существующих методов и схем генерации ПСП GMW, предложен новый простой метод генерации двоичных последовательностей GMW на основе генерации сдвинутых копий двоичной m-последовательности той же длины. Показано преимущество данного метода по сравнению с известным методом Велча-Шолца, основанного на генерации q-ичной m-последовательности.

В пятой главе, посвященной применению последовательностей типа Адамара в системах связи с CDMA, рассмотрен вопрос формирования максимальных по объему подмножеств квазиоптимальных последовательностей. На основе классов m-последовательностей и последовательностей GMW построены системы ортогональных сигналов большой ЛС. Разработан метод повышения безопасности передачи данных в системах CDMA на основе стандартов IS-95 и cdma2000, в котором в качестве

скремблирующей последовательности используется последовательность GMW с повышенной криптозащищенностью. Исследована генерация q-ичных m-подобных последовательностей большой ЛС, получаемых на основе двоичных m-последовательностей.

В шестой главе, посвященной экспериментальной проверке новых классов ПСП в сетях фиксированной радиосвязи многостанционного доступа "СТС-ИСТОК CDMA РРК 3/5.0", рассмотрены принципы и особенности построения систем ортогональных сигналов порядка 128 на основе последовательностей типа Адамара длины 127. Приведены результаты математического моделирования разработанных систем сигналов и их сравнительные характеристики.

В заключении изложены основные результаты, полученные автором при исследовании последовательностей Адамара, а также показана их научная и практическая значимость.

Настоящая диссертация является частью работ по разработке и исследованию новых эффективных классов нелинейных последовательностей, а также методов и устройств их генерации для систем многостанционного доступа с кодовым разделением каналов, проводимых на кафедре МЭС МТУСИ и Государственном предприятии ЦКТ "Силикон-Телеком-Софт".

Глава 1. Современные принципы конструирования последовательностей для систем радиодоступа с кодовым разделением каналов

1.1. Особенности построения широкополосных систем связи на базе технологии CDMA

Впервые широкополосные методы передачи были применены в конце 2-й мировой войны в военных радиотехнических системах для обеспечения высокого разрешения по дальности и борьбы с преднамеренными помехами противника [4]. В течение последующих десятилетий широкополосная техника использовалась исключительно в военных целях, и только в последние годы значительное распространение получили коммерческие широкополосные системы связи. Отличительной особенностью широкополосных систем является то, что используемая в них полоса частот намного больше, чем минимально требуемая для передачи информации с данной скоростью.

Системы, определяемые как широкополосные, должны удовлетворять следующим требованиям:

1) Сигнал должен занимать полосу частот во много раз превышающую минимально необходимую для этой передачи;
2) Расширение спектра осуществляется посредством широкополосного кодового сигнала, который не зависит от передаваемых данных.

Восстановление переданных данных на приемной стороне осуществляется посредством корреляции принятого широкополосного сигнала с опорным кодовым сигналом, используемым для расширения спектра. Любая помеха, в том числе и сосредоточенная по спектру "перемалывается" на выходе корреляционного приемника за счет своей несхожести по форме с полезным сигналом.

Основными преимуществами методов широкополосной передачи являются:

1) Спектр сигналов широкополосных систем может перекрываться со спектрами сигналами других систем без заметного снижения их качества работы;
2) широкополосные сигналы позволяют эффективно бороться с помехами, вызванными многолучевым распространением сигнала;
3) широкополосные системы характеризуются хорошим качеством работы в условиях частотно-селективных замираний;
4) широкополосные системы обеспечивают высокую помехозащищенность в условиях действия преднамеренных помех;
5) широкополосные системы обладают повышенной скрытностью и конфиденциальностью передачи;
6) широкополосные системы обладают высокой электромагнитной совместимостью с другими системами.

Важными параметрами, характеризующими работу широкополосных систем связи, являются выигрыш обработки G_P и запас по помехе или помехозащищенность J [15]. Выигрыш обработки G_P есть отношение сигнал/шум на выходе к сигнал/шум на входе и для широкополосных систем равен

$$G_P = \frac{W_{SS}}{B_I} \quad , \quad (1.1)$$

где W_{ss} – есть ширина полосы частот широкополосного сигнала, а B_I – ширина полосы частот информационного сигнала. Запас помехоустойчивости J, выраженный в децибелах, определяется как

$$J=G_P - [L_{sys} + (E_b/N_0)_{треб.}] \quad , (1.2)$$

где L_{sys} – аппаратурные потери, $(E_b/N_0)_{треб.}$ – отношение сигнал-шум на входе демодулятора, требуемое для обеспечения заданной вероятности ошибки.

Следует заметить, что эти параметры не зависят от типа выбранного широкополосного метода, включая и кодирование, и поэтому могут быть использованы для сравнения работы различных систем связи.

Широкополосные методы эффективно используются для многостанционного доступа при разделении ограниченных коммуникационных ресурсов между большим числом их пользователей. Метод, при котором каждый пользователь одновременно использует свой уникальный широкополосный кодовый сигнал, получил название кодового разделения каналов с многостанционным доступом. Теоретические основы разделения каналов были сформулированы Д.В. Агеевым еще в 1935г. в работе [16], посвященной теории линейной селекции сигналов. Пусть на входе приемника действует групповой сигнал s(t), представляющий сумму всех канальных сигналов вида $s_k(t)=C_k\psi_k(t)$, k=1, 2,...,N, где $\psi_k(t)$ – функция переносчика сигнала k-го канала, а C_k – некоторый коэффициент, отображающий передаваемое по данному каналу сообщение. Агеев предложил для разделения N канальных сигналов на приемной стороне использовать N разделяющих приемных устройств, причем каждое k-е разделяющее устройство, описываемое линейным оператором разделения π_k, должно реагировать только на сигнал $s_k(t)$ и давать нулевые отклики на сигналы всех других каналов. В соответствии с этим сигналы $s_k(t)$ и операторы π_k в общем виде должны удовлетворять следующим условиям линейного разделения сигналов [16]

$$\pi_k\left\{\sum_{i=1}^{N} s_i(t)\right\}=\gamma_{ik}=\begin{cases}\neq 0 & i=k\\ =0 & i\neq k\end{cases}, \quad (1.3)$$

где γ_{ik} – отклик оператора π_k на канальный сигнал $s_i(t)$.

Д. В. Агеевым также впервые было доказано, что необходимым и достаточным условием разделимости сигналов линейными устройствами является условие их линейной независимости. Частным случаем линейной независимости сигналов являются ортогональные сигналы, широко использующиеся в системах с частотным, временным и кодовым разделением каналов. В последнем случае сигналы можно передавать

одновременно и они могут иметь перекрывающиеся частотные спектры. Главное здесь - форма сигналов, благодаря которой обеспечиваются условия их ортогональности. При этом в синхронных системах, в которых моменты начала и конца тактовых интервалов сигналов всех каналов строго синхронизированы и совмещены в точке приема, условия ортогональности сводятся к ортогональности в одной точке, совпадающей с началом сигнала. В асинхронных системах связи, когда каналы не синхронизированы между собой во времени, обеспечить ортогональность при любом временном сдвиге сигналов практически невыполнимо. Вместе с тем можно сформировать такие сигналы, для которых ортогональность при любых временных сдвигах выполняется приближенно, т.е. в том смысле, что их скалярное произведение при любом сдвиге по времени оказывается намного меньше энергии сигнала. По своим свойствам такие квазиортогональные сигналы приближаются к белому шуму и поэтому их часто называют шумоподобными.

CDMA системы по способу модуляции могут подразделяться [17] на системы:

- с модуляцией прямыми последовательностями (DS-CDMA) ;
- с модуляцией "перескоком" по частоте (FH-CDMA);
- с модуляцией "перескоком" по времени (TH-CDMA);
- гибридные.

В DS-CDMA системах расширение спектра осуществляется за счет перемножения информационного сигнала с псевдослучайной последовательностью. В случае FH-CDMA псевдослучайная последовательность определяет закон изменения мгновенной частоты передачи. Ширина полосы в каждый момент времени небольшая, но в целом на длительности символа может быть очень большой. Частота "прыганья" может быть или быстрой (несколько перескоков за символ) или медленной (один перескок за несколько символов). В системах с TH-CDMA моменты передачи определяются псевдослучайной последовательностью. В гибридных CDMA могут использоваться два и более из выше перечисленных способов модуляции.

В связи с тем, что настоящая диссертация в основном посвящена исследованию ПСП, применяемых в системах с DS-CDMA , остановимся более подробно на свойствах этих систем. Наиболее важными из них являются:

- множественность доступа;
- эффективное функционирование в условиях многолучевости;
- противодействие узкополосным и широкополосным помехам;
- скрытность и конфиденциальность.

Множественность доступа. Возникает при одновременной работе нескольких пользователей в одном канале, сопряженного с кодовой последовательностью одного какого-нибудь выделенного пользователя. Если сигналы остальных пользователей используют кодовые последовательности, мало коррелируемые с кодовой последовательностью этого выделенного пользователя, то при корреляционном приеме только небольшая часть мощности их сигналов попадет в информационную полосу выделенного пользователя. В случае большого числа пользователей их общая интерференционная помеха может быть интерпретирована как гауссовский шум. С учетом этого и в предположении равенства мощностей сигналов всех пользователей на входе приемника, максимальное число K пользователей системы определяется следующей формулой [15]

$$K \approx \frac{G_P}{(E_b/N_0)_{треб.}\,\alpha} \quad , (1.4)$$

где α - активность пользователя.

Эффективное функционирование в условиях многолучевости. Если кодовая последовательность имеет идеальную (близкую к идеальной) функцию автокорреляции, тогда эта функция равна нулю (близка к нулю) вне интервала $[-T_c, T_c]$, где T_c – есть длительность элемента кодовой последовательности или чипа. Реально это означает, что если сигнал и его задержанная копия имеют относительную задержку более, чем на T_c , то только малая часть мощности этой копии "проходит" в информационную полосу основного

сигнала. Этим достигается разделение принимаемых лучей. Кроме того, создается возможность объединения энергии нескольких лучей многоканальным рэйк-приемником, что позволяет добиться увеличения отношения сигнал-помеха на выходе приемника.

Противодействие узкополосным и широкополосным помехам. При корреляционном приеме происходит умножение принятого сигнала с сигналом опорной кодовой последовательности. В случае узкополосной помехи ее спектр в результате умножения становится широкополосным и его воздействие на полезный сигнал уменьшается в G_p раз.

Скрытность и конфиденциальность. Скрытность связи обеспечивается работой ниже уровня шумов вследствие существенного расширения спектра при фиксированной передаваемой мощности. Конфиденциальность обеспечивается за счет выбора уникальных кодовых последовательностей, обладающих высокой степенью непредсказуемости символов. Все это позволяет добиться высокой степени защиты от несанкционированного доступа к радиоканалу.

В настоящее время технология CDMA получила широкое распространение в системах сотовой подвижной и фиксированной связи. Большие заслуги по созданию систем на основе технологии CDMA принадлежат компании Qualcomm. В 1991г. эта компания разработала проект стандарта IS-95 и прототипное оборудование систем сотовой подвижной связи с CDMA. В 1992г. проект IS-95 дорабатывается в подкомитете TR-45.5 TIA (Ассоциации производителей оборудования связи), и в 1993г. базовая версия стандарта была утверждена TIA. На сегодня установлено, что в системе CDMA, построенной по стандарту IS-95, базовая станция с всенаправленной антенной на одной несущей при ширине канала в 1,25МГц может предоставить каналы связи одновременно примерно 20 подвижным абонентам и до 40 фиксированным абонентам. При этом максимальная скорость передачи по одному каналу составляет 14,4 кбит/с. В последующих версиях этого стандарта, в частности в стандарте IS-95B, предусмотрено существенное увеличение верхней границы скорости передачи данных. Так благодаря возможности объединения до 8 каналов трафика скорость

передачи может достигать значения 115 кбит/с. Стандарт IS-95C также направлен на повышение частотной эффективности и емкости системы. Для этого используемый набор из 64 кодов Уолша будет дополнен группой из 64 кодов, передаваемых по квадратурному каналу. Ожидаемое повышение эффективности спектра составит от 1,5 до 2 раз по сравнению с предыдущими версиями стандарта.

При разработке будущих систем подвижной и фиксированной связи 3-го поколения на основе технологи CDMA выдвигаются дополнительные требования гибкости в предоставлении широкого ассортимента услуг и адаптации системы к различным условиям работы. Набор услуг, предоставляемых этими системами, должен включать услуги мультимедиа со скоростями передачи до 2 Мбит/с в условиях низкой подвижности и до 144 Кбит/с в условиях высокой подвижности, высококачественную речевую связь при низких битовых скоростях, передачу данных с широким диапазоном скоростей в режиме коммутации каналов и пакетов, организацию несимметричных каналов в прямом и обратном направлениях и т.д. [6]. В начале разработка единого стандарта на системы CDMA 3-го поколения происходила в рамках рекомендаций Международного союза электросвязи (МСЭ) и получила название IMT-2000, где число 2000 указывает на используемый частотный диапазон. Однако в последнее время при переходе от этапа разработки концепций к созданию конкретных спецификаций стало очевидно, что интересы различных региональных организации невозможно объединить в рамках единого стандарта, и в настоящее время выдвинута "концепция семейства" систем 3-го поколения, членами которой могут стать отвечающие ряду обязательных требований региональные и национальные стандарты.

В качестве основы для стандарта подвижной связи 3-го поколения (UMTS) в Европе сегодня выбраны две технологии радиодоступа: в режиме частотного дуплекного разноса – широкополосная система CDMA (W-CDMA), а в режиме временного дуплексного разделения - гибридная широкополосная система с временным разделением сигналов

(W-TDMA/CDMA). В США также предполагается использовать несколько моделей построения систем 3-го поколения на основе технологии CDMA. Это, прежде всего, преемственный с IS-95 базовый сетевой стандарт cdma2000, предусматривающий расширение полосы до 20 МГц за счет использования в режиме множественных несущих ПСП, цифровых фильтров и радиоканала, полностью совпадающих с базовым стандартом IS-95. Частота следования чипов во всех режимах cdma2000 кратна частоте следования чипов IS-95, что также обеспечивает построение двухрежимных базовых станций и абонентских терминалов. Все это позволит строить двухрежимные (cdma2000/Is-95) базовые станции и абонентские терминалы с минимальными затратами. Предполагается, что при внедрении систем 3-го поколения по технологии CDMA одновременно с ними в течение какого-то времени будут существовать и системы связи 2-го поколения, которые со временем будут вытеснены. При этом ожидаемый экономический эффект от эксплуатации такого рода систем может составить многие миллиарды долларов США.

1.2. Последовательности для систем связи по технологии DS-CDMA

Используемые в современных системах CDMA последовательности предназначены в основном для расширения спектра и кодового разделения каналов и разделяются на псевдослучайные последовательности и ортогональные коды. Основное отличие ПСП от ортогональных кодов состоит в том, что взаимная корреляция ортогональных кодов строго равна нулю. Поэтому их наиболее целесообразно применять в синхронных системах. В основном это прямые каналы CDMA. В DS-CDMA передатчике происходит расширение спектра информационного сигнала за счет его модуляции кодовой последовательностью. Соответственно на приемной стороне осуществляется обратная задача свертки принятого сигнала при его корреляционной обработке. При этом очень важно обеспечить низкую

взаимную корреляцию между сигналами пользователей, ведущую к снижению интерференционных помех. С другой стороны для надежного и быстрого вхождения в синхронизм требуются последовательности с хорошими автокорреляционными свойствами. В противном случае большие боковые лепестки автокорреляционной функции могут привести к принятию ошибочных решений и, как следствие, к увеличению времени вхождения в синхронизм. Кроме того, хорошие автокорреляционные свойства важны и для надежного разделения многолучевых компонент сигнала. Заметим, что АКФ и ВКФ ансамблей детерминированных последовательностей связаны таким образом, что в них невозможно достигнуть одновременно хорошей авто и взаимной корреляции, тогда как для ансамблей случайных последовательностей эти функции в достаточной степени усреднены. Примерами таких последовательностей являются m&GMW последовательности, свойства которых подробно рассматриваются в 2-й и 3-й главах настоящей диссертации.

Используемые в системах связи последовательности условно можно разделить на линейные и нелинейные последовательности, а их символы на двоичные и недвоичные (соответственно бинарные и не бинарные). В силу важности этих понятий приведем их определение так, как они даются в [13,18].

Определение.

Линейной последовательностью памяти N над полем GF(q) называется последовательность $\{b_n\}=\{b_n : n=\ldots,-1,0,1\ldots\}$ элементов поля GF(q), в которой n-ый член связан с N предыдущими линейным разностным уравнением:

$$b_n=c_{N-1}b_{n-1}+c_{N-2}b_{n-2+\ldots}+c_0b_{n-N} \quad , (1.5)$$

где коэффициенты $c_i \in GF(q)$, а $c_0 \neq 0$.

Все, не удовлетворяющие данному определению последовательности, принято относить к нелинейным последовательностям [13]. Видное место среди нелинейных последовательностей занимают семейства нелинейных последовательностей с внешней логикой (NLFFL), строящиеся на основе линейных последовательностей. В самом общем

виде блок-схемы генераторов линейных и нелинейных последовательностей с внешней логикой представлены на Рис.1.1 и Рис.1.2. Здесь $f(x_1,x_2,\ldots,x_N)$ есть линейная функция обратной связи, а $g(x_1,x_2,\ldots,x_N)$ – нелинейная функция внешней логики. Впервые основные положения теории линейных и нелинейных последовательностей были изложены С. Голомбом в его монографии [13], изданной в 1962г. Однако позже выяснилось [19], что деление на линейные и нелинейные последовательности в достаточной степени условно, так как любая NLFFL последовательность над полем памяти N может быть, в конечном счете, сведена к линейной последовательности над полем памяти $1 \le N_1 < q^N - 1$. Более подробно этот вопрос обсуждается во 2-й главе. Широко распространенные двоичные линейные ПСП генерируются посредством линейных регистров сдвига с обратной связью, включающей сумматор по модулю два [13]. Важным достоинством таких последовательностей является относительная простота их генерации. К ним относятся m-последовательности, последовательности Голда и Касами и др. Нелинейные последовательности по сложности генерации значительно превосходят линейные, что долгое время являлось препятствием на пути их активного использования. Однако сегодня для большого числа ансамблей нелинейных последовательностей, а это, прежде всего бент-последовательности и последовательности GMW, получены достаточно простые методы их генерации. Для расширения спектра могут использоваться как бинарные, так и не бинарные последовательности. Не бинарные последовательности обычно имеют комплексные значения символов, имеющих одну и ту же амплитуду. Бинарные (2-х фазные) и четверичные (4-х фазные) последовательности более предпочтительны для систем с прямым расширением спектра, так как они хорошо сочетаются с BPSK, QPSK и O-QPSK методами модуляции, обычно используемых в DS-CDMA системах.

Последовательности для систем с CDMA могут быть также короткими и длинными. Период коротких последовательностей равен длительности бита данных, тогда как период

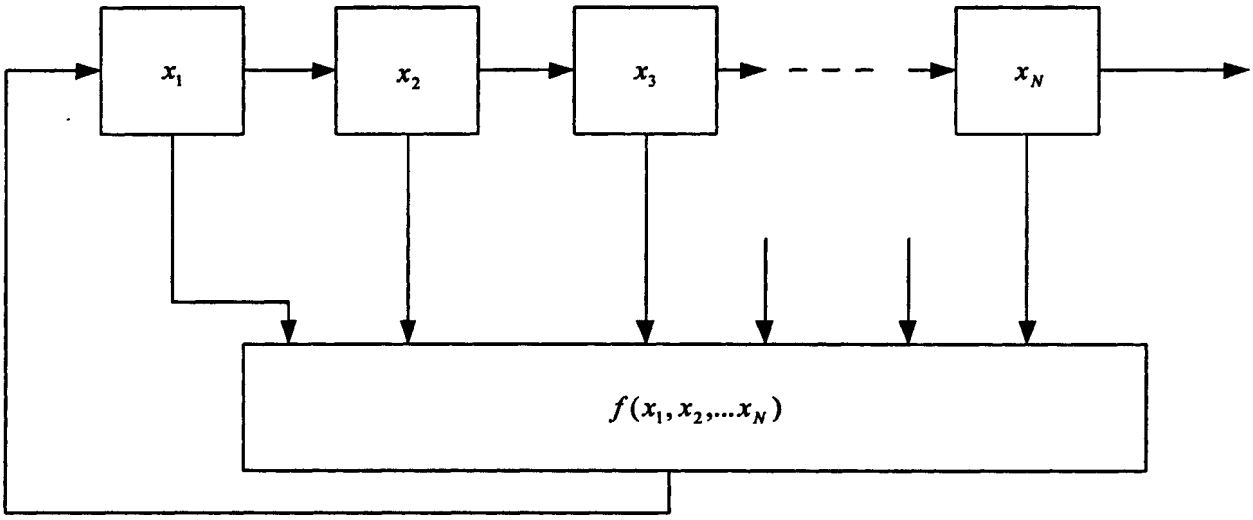

Рис. 1.1
Генератор линейной последовательности (LFSR)

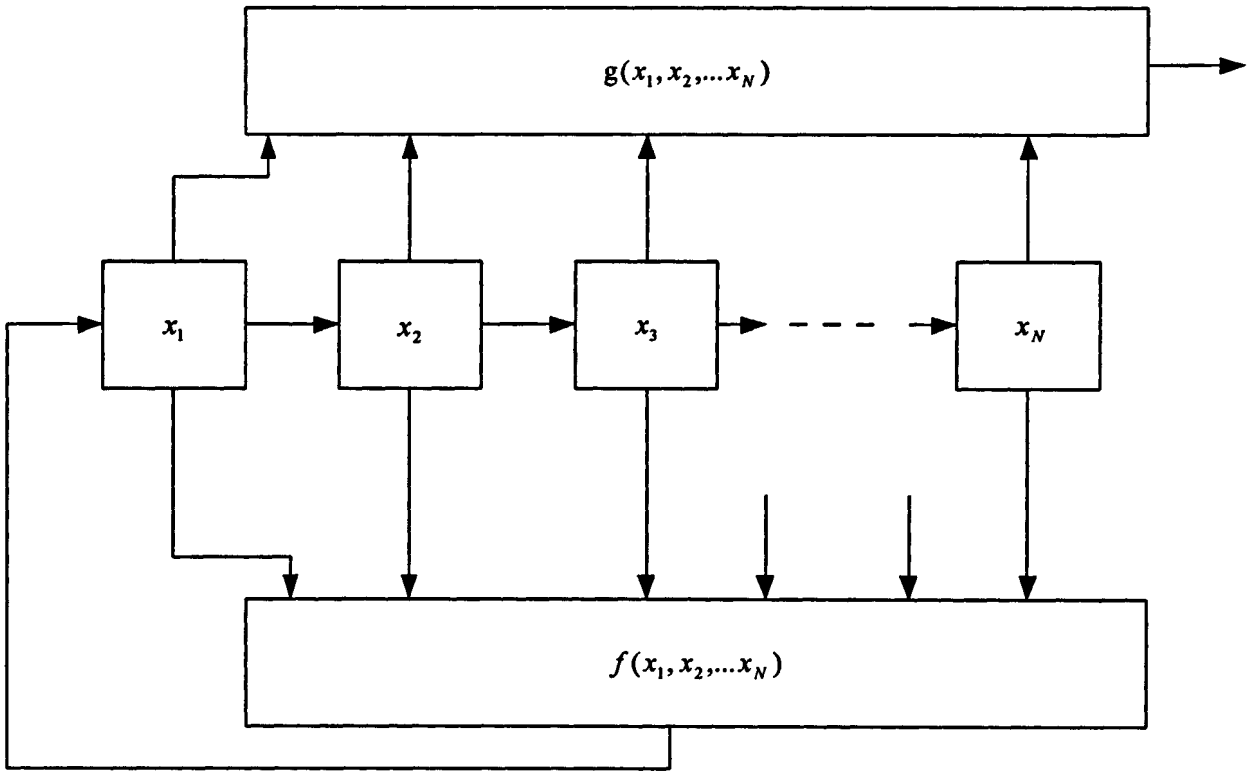

Рис. 1.2
Генератор нелинейной последовательности (NLFFL)

длинных последовательностей занимает несколько бит информации. Короткие последовательности преимущественно используются в случае необходимости выбора последовательностей с приемлемыми взаимно-корреляционными свойствами, а также для минимизации сложности реализации многопользовательского детектора. Длинные последовательности, как правило, применяются для рандомизации межканальных взаимодействий и в целях скремблирования. Основная проблема при использовании коротких последовательностей заключается в минимизации значений выбросов их взаимной корреляции.

Сами DS-CDMA системы подразделяются на синхронные и асинхронные. В синхронных системах время начала излучения последовательностей расширения спектра для каждого пользователя одно и то же, тогда как в асинхронных системах эти времена в общем случае различны. По этой причине в синхронных системах (например, в прямом канале систем сотовой связи) могут быть использованы короткие ортогональные последовательности. Заметим, что действие многолучевости неизбежно приводит к нарушению ортогональности и соответственно к снижению пропускной способности. Обратные каналы сотовых систем напротив, как правило, асинхронны, хотя в широкополосных системах CDMA (WCDMA) обратные каналы предполагают делать также синхронными. Заметим, что в асинхронных каналах для расширения спектра могут применяться как короткие, так и длинные последовательности. Примером могут служить обратные асинхронные каналы системы 2-го поколения cdmaone (стандарт IS-95), в которых для расширения спектра используются сдвиги m-последовательностей длины 2^{42}-1.

Исследованию псевдослучайных последовательностей посвящено достаточно большое количество работ [13], среди которых в первую очередь необходимо назвать фундаментальную статью М. Персли и Сарватера, опубликованную в 1980г. и посвященную m и родственным им семействам последовательностей: Голда, типа Голда и Касами [20]. Интересно, что в этом перечне отсутствует не менее "родственное" m-последовательностям

семейство последовательностей Гордона, Милза, Велча, по-видимому, неизвестное авторам. В это же время, т.е. к 80-му году, в СССР был уже опубликован целый ряд работ по данным последовательностям, а также получены патенты на их применение [14,21,22]. Из последних работ следует выделить обзорные статьи [9,11,12,23-26], в которых перечислены основные характеристики (длина, мощность, максимальное значение взаимной корреляции и линейная сложность) наиболее известных и недавно полученных двоичных псевдослучайных последовательностей. К ним в первую очередь относятся бент-последовательности [4], последовательности Ноу [27], последовательности Кердока [28], оптимальные перемежающиеся последовательности IM^{γ} [29], норм-следовые последовательности TN [30], ряд семейств последовательностей с идеальными автокорреляционными функциями [11,31] и т.д. К сожалению, из-за очень большого объема информации мы вынуждены ограничиться основными сравнительными характеристиками некоторых известных и новых двоичных последовательностей, представленными в таблице 1.1.

Таблица 1.1.

Характеристики известных и новых двоичных последовательностей.

Семейство	Период	Объем	Линейная Сложность	C_{max}	Примечание
Gold	2^r-1 r – не четно	2^r+1	2r	$1+2^{(r+1)/2}$	Оптимальное по Сидельникову
Gold	2^r-1 r – четно	2^r+1	2r	$1+2^{(r+2)/2}$	Оптимальное по Сидельникову
Касами малое	2^r-1 r – четно	$2^{r/2}$	3r/2	$1+2^{r/2}$	Оптимальное По Велчу
Касами большое	2^r-1 r – четно	$2^{r/2}(2^{r/2}+1)$	3r/2	$1+2^{(r+2/2)}$	Оптимальное по Сидельникову
Бент-последова-тельности	2^r-1 r : 4	$2^{r/2}$		$1+2^{r/2}$	Оптимальное По Велчу
Последователь-ности No	2^r-1 r : 4	$2^{r/2}$		$1+2^{r/2}$	Оптимальное По Велчу
M	2^r-1 r – не четно	2^r+1	r(r+1)/2	$1+2^{(r+1)/2}$	Оптимальное по Сидельникову

Продолжение таблицы 1.1.

Семейство	Период	Объем	Линейная Сложность	C_{max}	Примечание
M	2^r-1 r-четно	2^r+1	r(r+1)/2	$1+2^{(r+1)/2}$	Оптимальное по Сидельникову
IM^{γ} (γ=3)	$2(2^r-1)$ r – не четно	2^{r-1}+1	2r(r+3)/2	$2(1+2^{(r-1)/2})$	Оптимальное По Велчу (новое семейство)
IM^{γ} tr(γ=3)	$2(2^r-1)$ r – четно	2^{r-1}+1	2r(r+3)/2	$2(1+2^{r/2})$	Оптимальное по Сидельникову (новое семейство)
IM^{γ} tr(γ)=0	$2(2^r-1)$ r – не четно	2^{r-1}+1	2r(r+3)/2	$2(1+2^{(r+1)/2})$	Квази-Оптимальное по Сидельникову (новое семейство)
IM^{γ} tr(γ)=0	$2(2^r-1)$ r – четно	2^{r-1}+1	2r(r+3)/2	$2(1+2^{(r+1)/2})$	Квази-Оптимальное по Сидельникову (новое семейство)

Строгое математическое определение и физический смысл каждого из вышеперечисленных параметров подробно раскрывается в последующих главах настоящей диссертации. Здесь же лишь уместно напомнить, что под мощностью множества последовательностей понимается их общее количество, а под линейной сложностью последовательности некоторую меру степени непредсказуемости ее символов. Все вышеперечисленные параметры играют большую роль при выборе того или иного семейства последовательностей. Поэтому важнейшей задачей построения и анализа семейств последовательностей является оптимизация этих параметров с точки зрения требований CDMA. При этом необходимо подчеркнуть, что речь здесь идет не о случайных, а о псевдослучайных последовательностях, создаваемых в соответствии со строгой математической теорией. Действительно, как показывают исследования, короткие псевдослучайные последовательности обладают лучшими по сравнению со случайными последовательностями корреляционными свойствами. В случае же длинных последовательностей, несмотря на то, что корреляционные свойства случайных последовательностей статистически стремятся к оптимальным значениям, возникают значительные технические трудности, связанные с их реализацией.

Наряду с разделением последовательностей на линейные и не линейные существуют и другие виды типизации последовательностей в соответствии с их характерными свойствами. Одним из них является свойство идеальной автокорреляции, относящее семейства последовательностей с двух уровневой периодической АКФ (ПАКФ) к последовательностям типа Адамара [32].

Условно все последовательности типа Адамара могут быть разбиты на три временные группы: до 1976г., с 1976 по 1997гг. и с 1997.

К последовательностям, полученным до 1976г., относятся:

- m - последовательности длины 2^N-1 [13];
- последовательности квадратичных вычетов или последовательности Лежандра длины v=4t-1, где v- простое число [32];
- последовательности Холла длины $v=4x^2+27$, где v – простое [32];
- последовательности простых чисел-близнецов длины v=p(p+2), где p и p+2 – простые числа [32];
- последовательности Бомера-Фридриксена длины 127 [33].

К последовательностям, исследованным в период с 1976 по 1997гг. следует отнести последовательности Гордона, Милза и Велча длины 2^N-1, N=mk, m≥3, k≥2. Эти последовательности впервые были получены в 70гг. [21,22,44] и с этого времени на протяжении более 20 лет непрерывно переоткрывались под другими именами [34-36]. Самое близкое по форме и по содержанию к нашему названию – это "последовательности GMW" , которое в целях сокращения в основном и будет использоваться в диссертации. К этой не лишенной курьеза теме мы еще не раз вернемся в последующих главах диссертации, когда речь пойдет о классификации последовательностей Гордона, Милза и Велча.

И, наконец, к последовательностям, открытым после 1997г. относятся :

- последовательности No-Golomb-Gong-Lee-Gaal длины 2^N-1 , состоящие из [31]:
  - последовательностей Предположения 1 при N=2k+1 вида

$$b_1(t) = tr_1^N(\alpha^t) + tr_1^N(\alpha^{(2^k+1)t}) + tr_1^N(\alpha^{(2^k+2^{k-1}+1)t}) \quad ; (1.6)$$

- последовательностей Предположения 2 при N=3k-1 вида

$$b_2(t) = tr_1^N(\alpha^t) + tr_1^N(\alpha^{(2^k+1)t}) + tr_1^N(\alpha^{(2^{2k-1}+2^{k-1}+1)t}) + tr_1^N(\alpha^{(2^{2k-1}-2^{k-1}+1)t}) + \\ + tr_1^N(\alpha^{(2^{2k-1}+2^k-1)t}) \quad ; \quad (1.7)$$

- последовательностей Предположения 3 при N=3k-2 вида

$$b_3(t) = tr_1^N(\alpha^t) + tr_1^N(\alpha^{(2^{k-1}+1)t}) + tr_1^N(\alpha^{(2^{2k-2}+2^{k-1}+1)t}) + tr_1^N(\alpha^{(2^{2k-2}-2^{k-1}+1)t}) + \\ + tr_1^N(\alpha^{(2^{2k-1}-2^{k-1}+1)t}) \quad ; \quad (1.8)$$

- последовательностей Предположения 4 при N=3k-1 вида

$$b_4(t) = tr_1^N(g(\alpha^t + 1) + 1) \quad , \quad (1.9)$$

где g(x) для $x \in GF(2^N)$ удовлетворяет следующему уравнению

$$b_2(t) = tr_1^N(g(\alpha^t) \quad ; \quad (1.10)$$

- последовательностей Предположения 5 при N=3k-2 вида

$$b_5(t) = tr_1^N(g(\alpha^t + 1) + 1) \ , \quad (1.11)$$

где g(x) для $x \in GF(2^N)$ удовлетворяет следующему уравнению

$$b_3(t) = tr_1^N(g(\alpha^t) \quad . \quad (1.12)$$

- последовательности гипер-овальной конструкции Сегре и Глайна 1-го 2-го типов [37];

- последовательности степенных функций Касами [38].

Интересное обобщение, относящееся к последовательностям Сегре и Глайна, сделал Масчиетти [39]. В общем случае его конструкция сводится к следующему.

Пусть α есть примитивный элемент в $GF(2^n)$, $n \geq 3$ и пусть k удовлетворяет

$$\text{нод}(k,n) = \text{нод}(k-1,n) = 1$$

Рассмотрим отображение $f: GF(2^n) \rightarrow GF(2^n)$, где $f(x) = x^k + x$. Тогда последовательность

$$s(t) = \begin{cases} 0 & \alpha^t = x^k + x, \text{ для некоторых } x \in GF(2^n) \\ 1, & \text{в противном случае} \end{cases} \quad (1.13)$$

есть последовательность с идеальной автокорреляцией. При этом связь значений k с последовательностями Сегре и Глайна описывается следующей таблицей.

Таблица 1.2

Зависимость последовательностей Сегре-Глайна от параметра k

k	Семейство
6	Сегре
$k=2^{n+1/2}+2^r$, $r\in\{(n+1)/4,(3n+1)/4\}$	Глайна 1
$k=3*2^{n+1/2}+4$	Глайна 2

Значительный вклад в исследовании новых идеальных последовательностей был сделан Доббертином, который свел все 5 семейств последовательностей No-Golomb-Gong-Lee-Gaal к одному более общему выражению, доказательство которого им было найдено совместно с Дилоном [39].

Предположение Доббертина

Пусть α есть примитивный элемент в $GF(2^n)$ и $k<n$, нод(k, n)=1 и $d=2^{2k}-2^k+1$. Тогда

$$s(t)=\begin{cases}0 & \alpha^t=(x+1)^d+x^d+1\in GF(2^n)\\ 1, & \text{в противном случае}\end{cases} \qquad (1.14)$$

есть последовательность с идеальной автокорреляцией.

Все эти поистине революционные результаты в значительной мере обусловлены колоссальными финансовыми и материальными инвестициями в развитии современных средств и систем беспроводной, сотовой и спутниковой связи и особенно систем мобильной связи 3-го поколения на основе технологии DS-CDMA.

1.3. Критерии выбора ансамблей псевдослучайных последовательностей для систем с CDMA

Известно, что важнейшими критериями выбора ансамблей кодовых последовательностей в системах с CDMA являются [9]:

- корреляционные свойства;
- мощность ансамбля;
- степень непредсказуемости символов;
- сложность аппаратной реализации.

Корреляционные свойства кодовых последовательностей абонентов напрямую связаны с основными характеристиками системы и, прежде всего, с вероятностью ошибки на бит при заданном отношении сигнал-шум и поэтому должны быть оптимизированы. Наиболее подробно вопросы оптимизации кодовых последовательностей и критериев оценки корреляционных параметров исследованы Карлом Карккайненем в [40,41]. Исторически так сложилось, что разработчиками CDMA систем в основном применялся минимаксный критерий, минимизирующий максимальные (пиковые) значения четной (периодической) ВКФ. Это главным образом было обусловлено полученными аналитическими оценками максимума ПВКФ, с помощью которых было проще производить выбор необходимых подмножеств последовательностей. Однако реально для более полной характеристики ансамблей кодовых последовательностей необходимо также учитывать их нечетные корреляционные функции, влияние которых сказывается практически во всех действующих системах CDMA, так как они действуют в течение почти ½ всего времени передачи. Анализ этих функций достаточно нетривиальная задача, поскольку их пиковые значения в отличие от ПВКФ зависят от величины фазовых сдвигов последовательностей и плохо поддаются аналитическим методам оценки. Более того, Персли показал, что

среднее отношение сигнал-шум в асинхронных системах DS-CDMA, использующих BPSK модуляцию, полностью зависит от апериодических ВКФ сигнатурных кодовых последовательностей. Так, согласно [8] среднее отношение сигнал-шум SNR_j в случае аддитивно белого гаусского шума есть

$$SNR_j = \left\{ \frac{N_0}{2E_b} + \frac{1}{6v^3} \sum_{i=1, i\neq j}^{K} r_{ij} \right\}^{-1} . \qquad (1.15)$$

Здесь r_{ij} - есть средний интерференционный параметр (AIP), определяемый как

$$r_{ij}=2\mu_{ij}(0)+\mu_{ij}(1) \quad . \quad (1.16)$$

Для случая двоичных последовательностей $\mu_{ij}(n)$ находится по формуле

$$\mu_{ij}(n) = \sum_{m=1-v}^{v-1} C_{ij}(m) C_{ij}(m+n) \ , \ (1.17)$$

где $C_{ij}(m)$ – есть апериодическая функция взаимной корреляции i и j последовательностей.

Параметры SNR_j и r_{ij} широко используются в качестве критерия при сравнении различных кодовых последовательностей. Проведенные исследование показали [40], что для целого ряда семейств линейных кодовых последовательностей одинаковой длины с $v \geq 255$ среднее отношение сигнал-шум имеет приблизительно одно и то же значение. При этом соответствующие пиковые значения ВКФ семейств могут значительно различаться. Так согласно [40] для кодовых семейств последовательностей Голда, Касами и m-последовательностей средний интерференционный параметр r_{ij} в основном определяется суммой квадратов значений четных и нечетных взаимно-корреляционных функций, т.е. средним квадратом их взаимной корреляции при нормализации к длине последовательности. Кроме того, было показано, что оптимизация фазовых сдвигов при больших длинах последовательностей мало влияет на среднее значение SNR_j. Близость параметра r_{ij} для детерминированных (линейных и нелинейных), а также случайных последовательностей большой длины к значению $2v^2$ позволило даже предположить, что это есть проявление

некоторого закона природы [40]. Действительно, выборочная проверка ПСП GMW при N=8, 9, 10, 12, 14 показывает, что их AIP ведут аналогичным образом. При этих условиях в качестве основного критерия при выборе последовательностей Адамара целесообразно использовать минимаксный критерий. Поэтому в диссертации основное внимание будет уделено минимаксному критерию.

Некоторые авторы в целях преодоления практических и аналитических трудностей имеющих место при анализе детерминированных последовательностей предлагают использовать случайные последовательности, тем более что их средние корреляционные параметры мало отличаются от корреляционных параметров детерминированных последовательностей, особенно при больших периодах. Правда, при этом надо иметь в виду, что, во-первых, автокорреляционные функции случайных последовательностей, как правило, хуже, чем у детерминированных, и, во-вторых, а это самое главное, схемная реализация случайных последовательностей может оказаться во много раз сложнее по сравнению с детерминированными.

Исследования показали [23], что объем V ансамбля последовательностей периода v с фиксированным уровнем максимума корреляционного выброса для двоичных последовательностей ограничен величиной

$$V = \begin{cases} \dfrac{1-(]v\theta[_v^+)^2/v^2}{1-(]v\theta[_v^+)^2/v}, & 0 \le \theta^2 \le (v^2-2)/v^2 \\ \dfrac{v^2-(]v\theta[_v^+)^2}{3v-2-(]v\theta[_v^+)^2}, & (v-2)/v^2 \le \theta^2 \le (3v-8)/v^2 \end{cases} . \quad (1.18)$$

Здесь $]x[_v^+$ - ближайшее к x целое, не меньшее x и имеющее ту же четность, что и v, а $\theta=\{\theta_a, \theta_c\}$, т.е. максимум корреляционных выбросов ПАКФ и ПФКФ, взятых по всему ансамблю. Из формулы (1.18) следует, что чем жестче требования к корреляционному максимуму, тем меньше объем возможного ансамбля и соответственно число активных пользователей. Построение ансамблей оптимальных по минимаксному критерию, вообще

говоря, является достаточно сложной задачей. Поэтому на практике во многих случаях сначала строят ансамбль с минимально возможным значением θ_a, а затем выбирают из него подмножество последовательностей с требуемым уровнем взаимной корреляции. Более подробно этот вопрос рассматривается в главе 3.

Между показателем непредсказуемости символов последовательности – линейной сложностью и сложностью аппаратной ее реализации, измеряемой числом элементарных логических элементов (например, вентилей), также имеется определенная зависимость. Исследования последовательностей GMW показали, что при повышении их линейной сложности в некотором диапазоне аппаратная сложность этих последовательностей может оставаться неизменной, затем происходит ее скачкообразный рост [42].

Выводы

1. Рассмотрены особенности построения широкополосных систем связи на базе технологии CDMA и перспективы ее применения в сотовых системах радиосвязи.
2. Дан аналитический обзор семейств известных и новых двоичных последовательностей для систем связи с CDMA и приведены их основные сравнительные характеристики.
3. Рассмотрены современные критерии выбора ансамблей ПСП при проектировании систем связи по технологии DS-CDMA.

Глава 2. Математические основы построения классов ПСП GMW и их свойства

2.1. Разностные множества и последовательности с двухуровневой ПАКФ

Множество D, состоящее из k вычетов $d_1, d_2, \ldots, d_k$ по модулю v, называется (v, k, λ) – циклическим разностным множеством, если для каждого $d \neq 0 \bmod v$ существует точно λ упорядоченных пар (d_i, d_j), $d_i, d_j \in D$ таких, что $d_i - d_j \equiv d \bmod v$.

Легко проверить, что сложение по модулю v элементов разностного множества D с некоторой константой приводит к образованию нового разностного множества с теми же самыми параметрами. При этом разностное множество C называется сдвигом разностного множества $D=\{d_1, d_2, \ldots, d_k\}$, если $C=\{d_1+s, d_2+s, \ldots, d_k+s\} \bmod v$.

Параметры циклического разностного множества связаны следующим соотношением:

$$k(k-1)=\lambda(v-1).$$

Полином Холла разностного множества $D=\{d_1, d_2, \ldots, d_k\}$ есть

$$\theta(x)=\sum_{i=1}^{k} x^{d_i} \quad (2.1)$$

со свойством [43]

$$\theta(x)\,\theta(x^{-1}) \equiv k-\lambda + \lambda T_v(x) \bmod x^v - 1 \ , \quad (2.2)$$

где $T_v(x)=1+x+x^2+\ldots+x^{v-1}$.

Вектор инцидентности b разностного множества определяется следующим образом:

$$b_n = \begin{cases} 0, n \notin D \\ 1, n \in D \end{cases}.$$

Последовательность $\{b_n\}$, образованная повторением вектора инцидентности с периодом v, имеет двухуровневую периодическую автокорреляционную функцию (ПАКФ) $P_{bb}(\tau)$, задаваемую выражением:

$$P_{bb}(\tau)=\sum_{n=0}^{v-1} b_{n+\tau}b_n=\begin{cases}k, & \tau=0 \bmod v\\ \lambda, & \tau\neq 0 \bmod v\end{cases} .$$

И, наоборот, если задана периодическая двоичная последовательность $\{b_n\}$ с двухуровневой ПАКФ, то один период $\{b_n\}$ является вектором инцидентности разностного множества. Последовательность квадратных корней из единицы $\{\alpha_n\}$, основанная на разностном множестве D, определяется следующим выражением:

$$a_n=(-1)^{b_n}=1-2b_n \quad . \ (2.3)$$

ПАКФ $P_{aa}(\tau)$ последовательности $\{\alpha_n\}$ также двухуровневая с

$$\mathbf{P}_{aa}(\tau)=\sum_{n=0}^{v-1} a_{n+\tau}a_n=\begin{cases}v, & \tau\equiv 0 \bmod v\\ v-4k+4\lambda, & \tau\neq 0 \bmod v\end{cases} . \ (2.4)$$

Из выражения (2.4) следует, что любой двоичной последовательности с двухуровневой ПАКФ может быть поставлено в соответствие циклическое разностное множество. Иными словами методы построения циклических разностных множеств одновременно являются и методами построения последовательностей с двухуровневой ПАКФ и наоборот.

Два разностных множества $D=\{d_1, d_2, \ldots, d_k\}$ и $C=\{c_1, c_2, \ldots, c_k\}$ эквивалентны, т.е. D~C, если существуют такие взаимно простые целые s и t, что $\theta_D(x) \equiv x^s \theta_c(x^t) \bmod x^v - 1$.

Если существуют такие целые s и t, где (t, v)=1, что множества $\{td_1, td_2, \ldots, td_k\} \bmod v$ и $\{d_1+s, d_2+s, \ldots, d_k+s\} \bmod v$ совпадают в каком-либо порядке, т.е. выполняется сравнение $\theta_D(x)x^s \equiv \theta_D(x^t) \bmod x^v - 1$, то t называется множителем разностного множества $D=\{d_1, d_2, \ldots, d_k\}$. С алгебраической точки зрения множитель разностного множества t является автоморфизмом соответствующей циклической блок-схемы [43]. Множители образуют группу, называемую группой множителей блок-схемы. Если D ~ C

и D не является сдвигом C, то в соответствии с изоморфизмом блок-схем, D и C есть изоморфные разностные множества, а коэффициент t – немножитель разностного множества C. Все изоморфные друг другу разностные множества образуют класс разностных множеств, а множество всех неэквивалентных классов, имеющих сходную природу, - семейство разностных множеств. Из существующего разнообразия разностных множеств наибольший интерес представляют разностные множества типа Адамара, к числу которых относятся разностные множества Зингера (класс S) и Гордона, Милза, Велча (GMW) с параметрами [14,44]

$$v=2^N-1,\ k=2^{N-1}-1,\ \lambda=2^{N-2}-1\ ,\quad (2.5)$$

числовые разностные множества Лежандра (класс L), Холла (класс H) и Якоби (класс T) с параметрами $v=4t-1$, $k=2t-1$, $\lambda=t-1$ [10], а также целый ряд новых недавно открытых разностных множеств [39]. При этом последовательности, соответствующие зингеровским разностным множествам, оказываются хорошо известными m-последовательностями со значением бокового выброса ПАКФ, равным –1 [45]. Очевидно, что двоичные последовательности, соответствующие другим классам разностных множеств с параметрами (2.5), имеют точно такие же ПАКФ. В 1962г. Гордоном, Милзом и Велчем [44] на основе зингеровских разностных множеств были открыты и построены новые классы разностных множеств с параметрами (2.5), где $N=mk$, $m\geq 3$, $k\geq 2$. В литературе эти разностные множества получили название GMW разностных множеств [47]. За рубежом первое упоминание, касающееся прикладного аспекта этих разностных множеств, можно встретить в работе [10]. И то лишь косвенным образом в библиографии раздела, посвященного псевдослучайным последовательностям типа Адамара. Далее следует почти двадцатилетний период молчания, конец которому положила вызвавшая широкий отклик статья Велча и Шольца [46], посвященная последовательностям GMW. К сожалению, по не известным причинам авторы ограничились рассмотрением лишь некоторых классов GMW разностных множеств, определив при этом соответствующие этим классам последовательности как

последовательности GMW. Это внесло определенную путаницу при дефиниции последовательностей, получаемых на основе других, не рассмотренных в [46] классов GMW разностных множеств. В результате многие такие последовательности без должного на то основания получили название m-подобных, каскадных, расширенных, геометрических, новых последовательностей и т.д. [31,34,36,47,48]. Заметим, что десятилетием позже Шольц снял эту неоднозначность, определив все соответствующие GMW разностным множествам последовательности уже как последовательности GMW [46]. В нашей стране первые работы по исследованию последовательностей, на основе GMW разностных множеств появились в середине 70гг. [21,22]. Правда, в отличие от [46], они получили название последовательностей Гордона, Милза и Велча, и это название относилось к последовательностям, получаемым на основе всех GMW разностных множеств. Более подробно история этого вопроса изложена в [49,50]. Рассмотрим теперь математические аспекты построения этих новых классов последовательностей.

2.2. Алгебраическо-комбинаторные основания построения ПСП GMW

Выше было показано, что исследование свойств ПСП GMW может быть сведено к исследованию соответствующих свойств GMW разностных множеств, являющихся через свои векторы инцидентности алгебраическо-комбинаторными основаниями этих последовательностей. Теория GMW разностных множеств [44] состоит из ряда лемм и теорем, наиболее важные из которых приводятся ниже. Начнем с определения.

Определение.

Линейный функционал из поля E в подполе F есть отображение E→F, линейное над F.

Лемма 2.1[44].

Пусть F – конечное поле , E – конечное расширение поля F и L – не нулевой линейный функционал из E в F. Тогда каждый линейный функционал из E в F имеет вид L_μ , где $\mu \in E$ и $L_\mu(\omega)=L(\mu\omega)$ для $\forall\omega \in E$. Кроме того, если $\mu \neq \nu$, тогда $L_\mu \neq L_\nu$.

Согласно известной теореме Зингера о гиперплоскостях геометрии PG(N,q) [43] для любой степени простого числа $q=p^e$ и любого целого $N\geq 2$ существуют циклические разностные множества с параметрами:

$$v=q^N-1/q-1,\ k=q^{N-1}-1/q-1,\ ,\lambda=q^{N-1}-1/q-1\ . \qquad (2.6)$$

Впоследствии эти разностные множества получили название зингеровских. Приведем описание алгебраической конструкции этих разностных множеств.

Пусть α – есть примитивный элемент поля Галуа $GF(q^N)$, а L – ненулевой линейный функционал из $GF(q^N)$ в GF(2) такой, что L(1)=1. Тогда множество D_0 всех j таких, что $L(\alpha^j)=0$, образует зингеровское разностное множество [44] с параметрами (2.6). Дополнение зингеровского разностного множества D_0 есть разностное множество $D(L,\alpha)$ с параметрами:

$$v=q^N-1/q-1,\ k=q^{N-1},\quad \lambda=q^{N-1}(q-1)\ . \qquad (2.7)$$

При этом $j\in D(L,\alpha) \leftrightarrow L(\alpha^j)\neq 0$ для $0\leq j<v$.

Теорема 2.1 [44].

Пусть q есть степень простого числа p и пусть N есть целое, $N\geq 2$. Пусть L есть линейный функционал из конечного поля $GF(q^N)$ в подполе GF(q) такой, что L(1)=1. Пусть L_0 есть сужение L до подполя $GF(q^m)$, при этом m делит N. Пусть L_2 есть линейный функционал из $GF(q^N)$ в $GF(q^m)$ такой, что для $\forall x\in GF(q^N)$ элемент $L_2(x)$ из $GF(q^m)$ удовлетворяет соотношению $L_0(L_2(x)y)=L(xy)$ для $\forall y\in GF(q^m)$. Положим $v=q^N-1/q-1$, $w=q^m-1/q-1$ и $\xi=v/w$. Пусть α есть примитивный элемент $GF(q^N)$ и пусть $\beta=\alpha^\xi$. Пусть $\theta(x)$ и $\theta_0(y)$ есть полиномы Холла соответственно разностных множеств $D(L,\alpha)$ и $D(L_0,\beta)$. Пусть $y=x^\xi$. Тогда

$$\theta(x)\equiv\Omega(x)\theta_0(y) \pmod{x^v-1}\ , \quad (2.8)$$

где

$$\Omega(x)=\sum x^i y^{m_i}\ . \quad (2.9)$$

Суммирование здесь производится по всем i, для которых

$$L_2(\alpha^i)\neq 0, \quad 0\le i<\xi \quad \text{и} \quad L_2(\alpha^i)=\beta^{-m_i}\ .$$

Полином Холла $\theta_0(y)$ разностного множества $D(L_0,\beta)$ имеет следующие параметры:

$$w=q^m-1/q-1,\ l=q^{m-1},\quad \mu=q^{m-2}(q-1)\ . \quad (2.10)$$

Гордон, Милз и Велч показали, что если $\theta_0(y)$ в выражении (2.8) заменить полиномом Холла $\theta_b(y)$ произвольного разностного множества b с параметрами (2.10), тогда $\theta_B(x)\equiv\Omega(x)\theta_b(y) \pmod{x^v-1}$ есть полином Холла разностного множества B с параметрами (2.7). Построенные таким способом и отличные от зингеровских разностные множества получили в литературе название GMW-разностных множеств [45,46]. Из теоремы 2.1 вытекает следующее важное для построения ПСП GMW следствие [49].

Следствие 2.1.

Пусть L_1 - линейный функционал из $GF(2^N)$ в GF(2), L_0 - сужение L_1 до подполя $GF(2^m)$, а L_2 - линейный функционал из $GF(2^N)$ в $GF(2^m)$ такой, что $L_0(L_2(x)y)= L_1(xy)$ для $\forall x\in GF(2^N)$ и $\forall y\in GF(2^m)$. Пусть α и β примитивные элементы соответственно $GF(2^N)$ и $GF(2^m)$. Пусть $\{c_j\}$, где $0\le j<w$, есть двоичная ПСП, обладающая такой же автокорреляцией и балансностью, как m-последовательность $\{L_0(\beta^j)\}$, и при этом не совпадающая ни с каким ее сдвигом (в дальнейшем такие ПСП будем называть базисными). Тогда любая последовательность $\{b_n\}$ с элементами вида:

$$b_n = f(L_2(\alpha^n))\ , \quad (2.11)$$

где f: $GF(2^m)\to GF(2)$ - функционал, определяемый парой условий:

$$\begin{cases} f(\beta^j)=C_j \\ f(0)=0 \end{cases}\ , \quad (2.12)$$

является последовательностью GMW длины 2^N-1.

Теперь сформулируем условия, при которых два разностных множества B и C с параметрами (2.7), полученные этим способом, являются эквивалентными. Поставим в соответствие каждому (w, *l*, μ) разностному множеству b с полиномом Холла $\theta_b(y)$ некоторое (v, k, λ) – разностное множество B с полиномом Холла $\theta_B(x) \equiv \Omega(x)\theta_b(x^\xi)$.

Теорема 2.2 [44].

Пусть q есть степень простого числа p, и пусть N есть целое, N≥2. Пусть $m \mid N$, N>m≥2. Пусть v, k, λ, w, *l*, μ определены формулами (2.7) и (2.10) , $\xi = v/w$, и пусть Ω(x) есть полином, определяемый выражением (2.9). Пусть b и c есть (w, *l*, μ) разностные множества. Тогда (v, k, λ) разностные множества B и C эквивалентны тогда и только тогда, когда b является циклическим сдвигом c.

Заметим, что хотя данная теорема и включает случай m=2, GMW разностных множеств для m=2 не существует. В силу того, что предметом нашего исследования в основном являются двоичные ПСП, далее нас будут интересовать исключительно разностные множества с параметрами q=p=2.

На основе Теорем 2.1-2.2 может быть предложен следующий алгоритм построения GMW разностных множеств и связанных с ними последовательностей GMW. На первом шаге алгоритма строится комплиментарное (дополнительное) к зингеровскому разностное множество D(L,α) с параметрами

$$v=2^N-1,\ k=2^{N-1},\ \lambda=2^{N-2} \quad . (2.13)$$

Для этого из таблицы примитивных многочленов выбирается произвольный многочлен f(x) степени N над GF(2) и находится множество $D(L,\alpha)=\{n \mid L(\alpha^n)\neq 0, \text{ для } 0\le n<v\}$.

На втором шаге алгоритма строится таблица представителей элементов D(L,α) [45], которая получила еще название таблицы декомпозиции m-последовательности [14]. Эта

таблица состоит из $\xi=2^N-1/2^m-1$ строк и $w=2^m-1$ столбцов с элементами, определяемыми выражением $a_{ij}=\begin{cases}1, (i+\xi j)\in D(L,a) & 0\le j\le 2^m-2\\ 0, \text{ в противном случае} & 0\le i\le \xi-1\end{cases}$.

Заметим, что с помощью построенной таблицы производится вычисление полинома $\Omega(x)=\sum x^i y^{m_i} \pmod{x^v-1}$. Суммирование здесь ведется по всем ненулевым строкам таблицы, а m_i – есть число циклических сдвигов влево i – ой строки до ее совпадения с первой строкой этой таблицы.

На следующем шаге алгоритма производится выбор базисной последовательности длины $w=2^m-1$, не являющейся ни каким сдвигом, находящейся в первой строке ненулевой последовательности.

На четвертом шаге производится замещение ненулевых строк исходной таблицы представителей соответствующими сдвигами базисной последовательности таким образом, что на место i-й ненулевой строки записывается сдвинутая на m_i разрядов вправо базисная последовательность.

Обозначая элементы образованной таблицы через b_{ij} , в результате получаем разностное множество GMW, состоящее из всех различных вычетов $i+\xi j$, для которых $b_{ij}=1$. Соответственно последовательность с элементами $b_n=b_{ij}$ для всех $n=i+\xi j$ есть последовательность GMW с параметрами (2.13). Рассмотрим пример построения последовательности GMW длины 63. В соответствии с изложенным выше алгоритмом возьмем примитивный многочлен степени 6 над GF(2) вида $f(x)=x^6+x+1$. Пусть $\alpha^i=c_{i0}+c_{i1}\alpha+c_{i2}\alpha^2+\ldots+c_{i5}\alpha^5$ есть разложение α^i в базисе $1,\alpha, \alpha^2,\ldots\alpha^5$ с коэффициентами $(c_{i0},c_{i1},\ldots,c_{i5})$. Тогда имеем $L(\alpha^i)=c_{i0}$. Следовательно, $i\in D(L,\alpha)\Leftrightarrow L(\alpha^i)=\alpha_{i0}=1$. Отсюда имеем, что $D(L,\alpha)=\{0, 6, 11, 12, 16, 18, 21, 22, 23, 24, 26, 30, 31, 32, 35, 38, 40, 41, 45, 47, 48, 51, 52, 54, 56, 58, 59, 60, 61, 62\}$. Далее, так как $N=6=3*2$ и $m=3$, то $\xi=9$. Ниже приводится таблица 2.1 представителей элементов $D(L,\alpha)$, состоящая из 9 строк и 7 столбцов.

Таблица 2.1.

Представители элементов D(L,α) для N=6.

i/j	0	1	2	3	4	5	6	m_i
0	1	0	1	0	0	1	1	0
1	0	0	0	0	0	0	0	
2	0	1	0	0	1	1	1	6
3	0	1	1	1	0	1	0	3
4	0	0	1	1	1	0	1	4
5	0	0	1	1	1	0	1	4
6	1	0	1	0	0	1	1	0
7	0	1	0	0	1	1	1	6
8	0	0	1	1	1	0	1	4

Базисные разностные множества состоят из двух изоморфных (7,4,2) разностных множеств $b_1=\{0, 2, 5, 6\}$ и $b_2=\{0, 1, 2, 5\}$ с инцидентными последовательностями 1010011 и 1110010. Первому разностному множеству соответствует зингеровское разностное множество, а второе ведет к образованию нового (63, 32, 16) GMW разностного множества. Для его построения произведем замещение ненулевых строк таблицы 2.1 соответствующими сдвигами последовательности 1110010. В результате получаем следующую таблицу 2.2.

Таблица 2.2.

Декомпозия GMW разностного множества (63, 32,16).

i/j	0	1	2	3	4	5	6	m_i
0	1	1	1	0	0	1	0	0
1	0	0	0	0	0	0	0	
2	1	1	0	0	1	0	1	6

Продолжение таблицы 2.2

i/j	0	1	2	3	4	5	6	m_i
3	0	1	0	1	1	1	0	3
4	0	0	1	0	1	1	1	4
5	0	0	1	0	1	1	1	4
6	1	1	1	0	0	1	0	0
7	1	1	0	0	1	0	1	6
8	0	0	1	0	1	1	1	4

С помощью этой таблицы находим, что GMW разностное множество есть {0, 2, 6, 7, 9, 11, 12, 15, 16, 18, 22, 23, 24, 26, 30, 38, 39, 40, 41, 43, 44, 45, 48, 49, 50, 51, 53, 56, 58, 59, 61, 62}, а соответствующая ему последовательность GMW имеет вид:

10100011010110011010001110100010000000111101110011111010010110 11.

Нетрудно убедиться, что класс эквивалентности содержит 6 изоморфных друг другу разностных множеств. Все они образуются посредством умножения полученного разностного множества на числа 5, -5, 11, -11 и –1, являющимися немножителями разностного множества (63,32,16). Очевидно, столько же имеется и различных последовательностей GMW.

Теорема 2.3 [44].

Пусть D есть либо не тривиальное (v, k, λ) – разностное множество B из Теоремы 2.1, либо не тривиальное зингеровкое (v, k, λ) – разностное множество. Тогда множителями D являются исключительно степени p по mod v.

Очевидно, что применительно к случаю q=p=2 множители D являются степенями числа 2.

В заключение этого краткого экскурса в теорию GMW разностных множеств приведем формулировку основной теоремы Гордона, Милза и Велча.

Теорема 2.4 [44].

Пусть q есть степень простого числа p. Пусть m и k есть положительные целые числа, причем m≥3. Пусть k есть произведение r простых не равных единице множителей и N=mk. Тогда существуют, по меньшей мере, 2^r неэквивалентных разностных множеств с параметрами (2.7).

Заметим, что одно из этих разностных множеств в силу метода построения всегда является зингеровским, другие же являются GMW разностными множествами [44].

2.3. Мощность и общее число классов ПСП GMW

В соответствии с [45] под мощностью класса эквивалентности или просто класса разностных множеств будем понимать число всех различных изоморфных разностных множеств в этом классе. Тогда общее число различных с точностью до сдвига двоичных последовательностей, строящихся на основе GMW разностных множеств, равно сумме мощностей, взятых по всем неэквивалентным классам. Таким образом, задача нахождения общего числа ПСП GMW разбивается на построение всех неэквивалентных классов и определение мощности этих классов.

Теорема 2.5 [14].

Мощность класса эквивалентности любого GMW разностного множества с параметрами (2.13) равна:

$$M = \frac{\varphi(2^N - 1)}{N} \quad , \quad (2.14)$$

где N=mk, m≥3, k>1, а φ - функция Эйлера.

Доказательство.

Согласно Холлу [43] каждая степень числа 2 есть множитель GMW разностного множества с параметрами (2.13). С другой стороны, в соответствии с теоремой 2.3 каждый множитель GMW разностного множества есть степень 2 по mod v. Отсюда получаем, что все

множители GMW разностного множества образуют мультипликативную группу T по умножению порядка N. Тогда в соответствии с определением изоморфности разностных множеств мощность класса эквивалентности GMW разностного множества равна порядку факторгруппы G/T, где G – группа классов вычетов по mod v, взаимно простых с v. По теореме Лагранжа [51] порядок факторгруппы G/T равен отношению $\frac{|G|}{|T|}$, где |G| и |T| соответственно порядок групп G и T. Согласно [50] порядок группы G равен $\varphi(2^N-1)$. Отсюда получаем, что $M=|G/T|=\frac{|G|}{|T|}=M=\frac{\varphi(2^N-1)}{N}$.

Теорема доказана.

Переходим теперь к вопросу построения всех неэквивалентных GMW разностных множеств. Здесь мы докажем ряд теорем и лемм, с помощью которых будет получена формула для общего числа этих множеств. В начале сформулируем одно очевидное следствие, вытекающее из теорем Гордона, Милза, Велча.

Следствие 2.2.

Пусть q=p=2 и N=mk, m≥3, k>1. Тогда число различных неэквивалентных классов GMW разностных множеств с параметрами (2.13), построенных на основе (w, *l*, μ) - разностных множеств, равно числу всех (w, *l*, μ) - разностных множеств, не являющихся сдвигами друг друга.

Пусть $\theta(x)\equiv\Omega(x)\theta_0(y) \pmod{x^v-1}$ – полином Холла некоторого разностного множества с k≠λ , а ξ - произвольный корень бинома x^v-1. Очевидно, $\theta(\xi)\theta(\xi^{-1})=k-\lambda$. Отсюда в силу произвольности ξ получаем, что θ(x) и x^v-1 взаимно просты. Таким образом, доказана лемма 2.2

Лемма 2.2 [14].

Если θ(x) – полином Холла разностного множества, для которого k≠λ, тогда

$$(\theta(x),\ x^v-1)=1 \ . \ (2.15)$$

Пусть $N=km_1m_2$, k, $m_1,m_2\geq 2$ – целые числа. Положив $m=m_1m_2$, из теоремы 2.1 имеем $\theta(x)\equiv\Omega_N^{m_1m_2}(x)\,\theta_{m_1m_2}(y) \mod x^v-1$, где $\Omega_N^{m_1m_2}(x)$ определяется выражением (2.9), $y=x^{\xi}$, $\xi=\frac{v}{2^{m_1m_2}-1}$, $\theta_{m_1m_2}(y)$ - полином Холла разностного множества $D_1(L_{01},\beta)$. Здесь L_{01} – линейный функционал из $GF(2^m)$ в $GF(2)$, $\beta=\alpha^{\xi}$. Применяя теперь теорему 2.1 к $\theta_{m_1m_2}(y)$, получим:

$$\theta(x)\equiv\Omega_N^{m_1m_2}(x)\,\Omega_{m_1m_2}^{m_1}(x^{\xi})\;\theta_{m_1}(y_1) \mod x^v-1,$$

где $\theta_{m_1}(y_1)$ - полином Холла разностного множества $D_2(L_{02},\beta_2)$. Здесь L_{02} – линейный функционал из $GF(2^{m_1})$ в $GF(2)$, $y_1=x^{\xi_1}$, $\xi_1=\frac{v}{2^{m_1}-1}$. С другой стороны при $m=m_1$ имеем: $\theta(x)\equiv\Omega_N^{m_1}(x)\,\theta_{m_1}(y_1) \mod x^v-1$. Отсюда, по лемме 2.2 получаем:

$$\Omega_N^{m_1m_2}(x)\,\Omega_{m_1m_2}^{m_1}(x^{\xi}) = \Omega_N^{m_1}(x) \mod x^v-1.$$

Этот результат был сформулирован в виде следующей леммы.

Лемма 2.3 [14].

Пусть $N=km_1m_2$, k, $m_1,m_2\geq 2$ – целые числа. Тогда

$$\Omega_N^{m_1m_2}(x)\,\Omega_{m_1m_2}^{m_1}(x^{\xi}) = \Omega_N^{m_1}(x) \mod x^v-1 \quad .(2.16)$$

Пусть множество $\{GMW_N^m\}$ есть совокупность всех неэквивалентных GMW разностных множеств с параметрами (2.13), построенных на основе совокупности различных базисных (не являющихся сдвигами друг друга) разностных множеств с параметрами

$$w=2^m-1,\; l=2^{m-1},\; \mu=2^{m-2} \quad . \qquad (2.17)$$

Обозначим через $|GMW_N^m|$ мощность множества $\{GMW_N^m\}$. Тогда справедлива теорема.

Теорема 2.6 [14].

Пусть $N=km_1m_2$, где $k\geq 2$, $m_1\geq 2$, $m_2\geq 3$ – целые числа. Тогда

$$\{GMW_N^{m_1m_2}\} \supset \{GMW_N^{m_2}\} \text{ и } |GMW_N^{m_1m_2}| > |GMW_N^{m_2}| \quad . \quad (2.18)$$

Доказательство.

Пусть $\overline{A} \in \{GMW_N^{m_2}\}$. Тогда по теореме 2.1 полином Холла $\theta(x)$ разностного множества $\overline{A}$ есть $\theta(x) \equiv \Omega_N^{m_2}(x)\,\theta_{m_2}(y_2) \mod x^v-1$, где $y_2 = x^{\xi_2}$, $\xi_2 = \frac{v}{2^{m_2}-1}$. Согласно лемме 2.3 это выражение можно привести к виду:

$$\theta(x) \equiv \Omega_N^{m_1m_2}(x)\,\Omega_{m_1m_2}^{m_2}(x^{\xi})\ \theta_{m_2}(y_2) \mod x^v-1.$$

Обозначив $\theta_{m_1m_2}(x) \equiv \Omega_{m_1m_2}^{m_2}(x)\ \theta_{m_2}(x^{\xi/\xi_2}) \mod x^v-1$, получаем:

$$\theta(x) \equiv \Omega_N^{m_1m_2}(x)\ \ \theta_{m_1m_2}(x^{\xi}) \mod x^v-1.$$

Последнее означает, что любое разностное множество $\overline{A}$, построенное на основе (w, l, μ) базисного множества с $m=m_2$, может быть также образовано на основе (w, l, μ) базисного множества с $m= m_1m_2$. Таким образом, доказано, что $\overline{A} \in \{GMW_N^{m_1m_2}\}$ и , следовательно, $\{GMW_N^{m_1m_2}\} \supset \{GMW_N^{m_2}\}$. Далее, можно показать, что число базисных разностных множеств для $\{GMW_N^{m_1m_2}\}$, по меньшей мере, в $\varphi(2^{m_1m_2}-1)/m_1m_2$ раз превышает число базисных множеств для $\{GMW_N^{m_2}\}$. Действительно, все базисные разностные множества для $\{GMW_N^{m_2}\}$ являются также базисными и для $\{GMW_{m_1m_2}^{m_2}\}$. Последнее же в свою очередь является базисным для $\{GMW_N^{m_1m_2}\}$. При этом мощность любого класса $\{GMW_{m_1m_2}^{m_2}\}$ равна $\varphi(2^{m_1m_2}-1)/m_1m_2$. Теорема доказана.

Рассмотрим теперь разностное множество D(L,α) с полиномом Холла $\theta(x) \equiv \Omega_N^m(x)\,\theta_m(y) \mod x^v-1$ и параметрами (2.13). Предположим, что существует такой немножитель t разностного множества D(L,α), что выполняется сравнение

$$\Omega_N^m(x) \equiv x^{-s}\Omega_N^m(x^t) \mod x^v-1 \quad . \quad (2.19)$$

Разностное множество t D(L,α) с полиномом Холла $\theta(x^t)\equiv\Omega_N^m(x^t)\,\theta_m(y^t) \bmod x^v-1$ изоморфно D(L,α) по определению. Тогда с учетом (2.19) имеем:

$$\theta(x^t)\equiv\Omega_N^m(x)\,\theta_m(y^t)x^s \bmod x^v-1 \quad . \quad (2.20)$$

Возможны следующие два случая:

$$\theta_m(y^t)\equiv\theta_m(y)x^{s_1} \bmod x^v-1 \ , \qquad (2.21)$$

$$\theta_m(y^t)\neq\theta_m(y)x^{s_1} \bmod x^v-1 \ . \qquad (2.22)$$

Однако, в случае (2.21) в силу (2.20) получаем, что t D(L,α) является сдвигом D(L,α), что не возможно, так как t – немножитель D(L,α). В случае же (2.22) из Теоремы 2.2 и выражения (2.20) следует, что t D(L,α) и D(L,α) не эквивалентны, что также не возможно. Следовательно, наше предположение о существовании немножителя, для которого выполняется сравнение (2.19) не верно, и справедлива лемма 2.4.

Лемма 2.4 [14].

Пусть N=mk, m≥3, k>1 - целые числа, а t есть произвольный немножитель разностного множества D(L,α). Тогда

$$\Omega_N^m(x)\neq x^{-s}\Omega_N^m(x^t) \bmod x^v-1.$$

Теорема 2.7 [14].

Пусть $N=mk_1k_2$, m>1, $k_1\geq2$, $k_2\geq2$, $m_1=mk1$, $m_2=mk_2$. Пусть A и B - GMW разностные множества с параметрами (2.13) и полиномами Холла соответственно $\theta_A(x)\equiv\Omega_N^{m_1}(x)\,\theta_{m_1}(y_1) \bmod x^v-1$ и $\theta_B(x)\equiv\Omega_N^{m_2}(x)\,\theta_{m_2}(y_2) \bmod x^v-1$, где где $y_1=x^{\xi_1}$, $\xi_1=\frac{v}{2^{m_1}-1}$, $y_2=x^{\xi_2}$, $\xi_2=\frac{v}{2^{m_2}-1}$, а $\Omega_N^{m_1}(x)$ и $\Omega_N^{m_2}(x)$ такие, что $\theta_Z(x)\equiv\Omega_N^{m_1}(x)\,\theta_Z(y_1)\equiv\Omega_N^{m_2}(x)\,\theta_Z(y_2) \bmod x^v-1$ есть полином Холла зингеровского разностного множества. Тогда для эквивалентности разностных множеств A и B необходимо и достаточно, чтобы

$$\theta_A(x)\equiv x^s\theta_B(x) \bmod x^v-1 \ . (2.23)$$

Доказательство.

Достаточность теоремы очевидна. Для доказательства необходимости предположим, что выполняется:

$$\Omega_N^{m_1}(x)\,\theta_{m_1}(y_1) \equiv x^s \Omega_N^{m_2}(x^t)\,\theta_{m_2}(y_2^t) \bmod x^v-1 \ . \quad (2.24)$$

Умножим обе части этого сравнения на произведение полиномов Холла $\theta_Z(y_1)\theta_Z(y_2^t)$. В результате получаем:

$$\theta_Z(x)\ \theta_{m_1}(y_1)\ \theta_Z(y_2^t) \equiv x^s \theta_Z(x^t)\ \theta_{m_2}(y_2^t)\ \theta_Z(y_1) \bmod x^v-1 \ . (2.25)$$

Умножим левую и правую части сравнения (2.25) на произведение $T_1(y_1)T_2(y_2) \bmod x^v-1$, где $T_1(y_1)=1+y_1+y_1^2+\ldots+y_1^{m_1-1}$ и $T_2(y_2)=1+y_2+y_2^2+\ldots+y_2^{m_2-1}$

После упрощения, получаем:

$$\theta_Z(x)T_1(y_1)T_2(y_2) \equiv x^s \theta_Z(x^t)T_1(y_1)T_2(y_2) \bmod x^v-1 \ , \quad (2.26)$$

что, так как t - немножитель, не возможно. Теорема доказана.

Найдем условия, при которых выполняется сравнение (2.23). Пусть $N=p_1p_2$, где p_1, $p_2 \geq 3$ есть не равные друг другу простые числа. Рассмотрим два GMW разностных множеств A и B с параметрами (2.13) и полиномами Холла :

$$\theta_A(x) \equiv \Omega_N^{p_1}(x)\,\theta_{p_1}(y_1) \bmod x^v-1 \text{ и } \theta_B(x) \equiv \Omega_N^{p_2}(x)\,\theta_{p_2}(y_2) \bmod x^v-1.$$

Здесь $\theta_{p_1}(y_1)$ и $\theta_{p_2}(y_2)$ - полиномы Холла базисных разностных множеств. Предположим, что $A \sim B$, тогда согласно предыдущей теореме имеет место сравнение:

$$\Omega_N^{p_1}(x)\,\theta_{p_1}(y_1) \equiv x^s \Omega_N^{p_2}(x)\,\theta_{p_2}(y_2) \bmod x^v-1 \ . (2.27)$$

Умножим обе части этого сравнения на произведение полиномов Холла $\theta_{p_1}^z(y_1)\,\theta_{p_2}^z(y_2)$ зингеровских разностных множеств таких, что

$$\theta_z(x) \equiv \Omega_N^{p_1}(x)\,\theta_{p_1}^z(y_1) \equiv x^s \Omega_N^{p_2}(x)\,\theta_{p_2}^z(y_2) \bmod x^v-1 \ . (2.28)$$

В результате сравнение (2.27) преобразуется в эквивалентное сравнение:

$$\theta_{p_2}^z(y_2)\ \theta_{p_1}(y_1) \equiv\equiv x^s \theta_{p_1}^z(y_1)\ \theta_{p_2}(y_2) \bmod x^v-1 \ .$$

Отсюда, так как $y_2 = y_1^{\xi_2/\xi_1} = y_1^{\xi_3}$, где $\xi_3=\xi_2/\xi_1=2^{p_1}-1/2^{p_2}-1$, в итоге получаем:

$$\theta^z_{p_2}(y_1^{\xi_3})\ \theta_{p_1}(y_1) \equiv x^s \theta^z_{p_1}(y_1)\ \theta_{p_2}(y_1^{\xi_3}) \mod x^v-1 . \quad (2.29)$$

Так как $(p_1,p_2)=1$, то можно показать, что $(2^{p_1}-1, 2^{p_2}-1)=1$. Кроме того степени полиномов $\theta^z_{p_2}(y_1^{\xi_3})$ и $\theta_{p_2}(y_1^{\xi_3})$ меньше $2^{p_2}-1$. Следовательно, полиномы $\theta^z_{p_2}(y_1^{\xi_3})$ и $\theta_{p_2}(y_1^{\xi_3})$ не содержат членов с целыми степенями y_1. Независимо от значения s для выполнения сравнения (2.29) необходимо выполнение сравнения: $\theta_{p_1}(y_1) \equiv x^{s_1}\theta^z_{p_1}(y_1)$ mod x^v-1. Отсюда следует, что A – зингеровское разностное множество. Поэтому в силу эквивалентности множеств A и B множество B также должно быть зингеровское.

Итак, доказано, что совокупности всех неэквивалентных GMW разностных множеств $\{GMW_N^{p_1}\}$ и $\{GMW_N^{p_2}\}$ не содержат общих элементов, т.е. не пересекаются.

Рассмотрим теперь более сложный случай $N=p_1p_2p_3$. Здесь так же, как в предыдущем случае, $p_1 \geq 3$, $p_2 \geq 3$ и $p_3 \geq 3$ есть не равные друг другу простые числа. По предыдущей теореме $\{GMW_N^{p_ip_j}\} \supset \{GMW_N^{p_i}\} \cup \{GMW_N^{p_j}\}$ для i, j=1,2,3 и i≠j.

Рассмотрим следующие две совокупности GMW разностных множеств $GMW_N^{p_1p_2}$ и $GMW_N^{p_1p_3}$ и выясним, что представляет собой их пересечение. Очевидно, что оно не пусто, так как каждое из них содержит одно и то же зингеровское разностное множество. Предположим, что существует некоторое разностное множество C, отличное от зингеровского и принадлежащее этому пересечению $\overline{C}$. Тогда должно выполняться следующее сравнение:

$$\Omega_N^{p_1p_2}(x)\,\theta_{p_1p_2}(y_1) \equiv \Omega_N^{p_1p_3}(x)\,\theta_{p_1p_3}(y_2) \mod x^v-1 ,$$

которое, в свою очередь, эквивалентно сравнению:

$$\theta_{p_1p_2}(y_1)\theta^z_{p_1p_3}(y_2) \equiv \theta^z_{p_1p_2}(y_1)\theta_{p_1p_3}(y_2) \mod x^v-1 . \quad (2.30)$$

Здесь $\theta_{p_1p_2}(x_1)$ и $\theta_{p_1p_3}(x_2)$ - полиномы Холла базисных разностных множеств с параметрами (2.13), соответственно при $m_1=p_1p_2$ и $m_2=p_1p_3$, $y_1=x^{\xi_1}$, $\xi_1=\frac{v}{2^{m_1}-1}$, $y_2=x^{\xi_2}$, $\xi_2=\frac{v}{2^{m_2}-1}$, а $\theta^z_{p_1p_2}(x)$ и $\theta^z_{p_1p_3}(x)$ - полиномы Холла зингеровских разностных множеств таких, что

$$\theta^z_{p_1p_2}(x) \equiv \Omega^{p_1}_{p_1p_2}(x)\,\theta^z_{p_1}(y_3) \bmod x^{2^{m_1}-1}-1 \quad \text{и} \quad \theta^z_{p_1p_3}(x) \equiv \Omega^{p_1}_{p_1p_3}(x)\,\theta^z_{p_1}(y_4) \bmod x^{2^{m_2}-1}-1,$$

где $y_3 = x^{2^{m_1}-1/2^{p_1}-1}=x^{\xi_3}$, и $y_4 = x^{2^{m_2}-1/2^{p_1}-1}=x^{\xi_4}$. С учетом этого (2.30) принимает вид

$$\theta_{p_1p_2}(y_1)\ \Omega^{p_1}_{p_1p_3}(y_1^{\xi_0}) \equiv \theta_{p_1p_3}(y_1^{\xi_0})\ \Omega^{p_1}_{p_1p_2}(y_1) \mod y_1^{2^{m_1}-1}-1, \text{ где } \xi_0=\xi_2/\xi_1.$$

Замечаем, что в левой части полученного сравнения только первый сомножитель содержит целые степени y_1. Поэтому для выполнения этого сравнения необходимо, чтобы полином Холла $\theta_{p_1p_3}(y_1^{\xi_0})$ из его правой части раскладывался на следующие множители:

$$\theta_{p_1p_3}(y_1^{\xi_0}) \equiv \Omega^{p_1}_{p_1p_3}(y_1^{\xi_0 t})\ \theta_{p_1}(y_1^{\xi_3}).$$

Приравнивая сомножители с целыми степенями y_1, в итоге получаем: $\theta_{p_1p_2}(y_1) \equiv \Omega^{p_1}_{p_1p_2}(y_1)\ \theta_{p_1}(y_1^{\xi_0}) \mod x^v-1$. После сокращений, находим, что $\Omega^{p_1}_{p_1p_3}(y_1^{\xi_0 t}) \equiv \Omega^{p_1}_{p_1p_3}(y_1^{\xi_0})$. Отсюда, без нарушения общности положим $t=1$. Таким образом, установлено, что если GMW разностное множество принадлежит $\overline{C}$, то его полином Холла имеет вид:

$$\theta_c \equiv \Omega^{p_1p_2}_N(x)\,\Omega^{p_1}_{p_1p_2}(y_1)\ \theta_{p_1}(y_1^{\xi_3}) \equiv \Omega^{p_1p_3}_N(x)\,\Omega^{p_1}_{p_1p_3}(y_2)\ \theta_{p_1}(y_2^{\xi_4}) \mod x^v-1,$$

где $\xi_1\xi_3=\xi_2\xi_4$ и $\theta_{p_1}(y_1^{\xi_3}) \equiv \theta_{p_1}(y_2^{\xi_4}) \bmod x^v-1$.

Итак, получен следующий результат:

$$\overline{C} = \{GMW_N^{p_1p_2}\} \cap \{GMW_N^{p_1p_3}\} = \{GMW_N^{p_1}\} \quad . \quad (2.31)$$

Аналогично доказывается, что

$$\{GMW_N^{p_1p_2}\} \cap \{GMW_N^{p_2p_3}\} = \{GMW_N^{p_2}\}, \quad (2.32)$$

$$\{GMW_N^{p_1p_3}\} \cap \{GMW_N^{p_2p_3}\} = \{GMW_N^{p_3}\}. \quad (2.33)$$

Теперь положим $N=p_1p_2^2$, т.е. $p_1=p_2$. Учитывая, что при получении предыдущего результата условие строго неравенства p_1 и $p2$ нигде не использовалось, находим:

$$\{GMW_N^{p_1p_2}\}\cap\{GMW_N^{p_2^2}\}=\{GMW_N^{p_2}\}. \quad (2.34)$$

Далее, пусть $N=p_1^{\alpha_1}p_2^{\alpha_2}...p_s^{\alpha_s}$, где $p_1, p_2...p_s$ есть простые отличные от единицы числа, а $\alpha_1,\alpha_1...,\alpha_s$ – целочисленные, положительные показатели. Тогда индукцией по s, используя предыдущее, получим:

$$\{GMW_N^{N_1}\}\cap\{GMW_N^{N_2}\}=\{GMW_N^{(N_1,N_2)}\}, \quad (2.35)$$

где N_1, N_2 – некоторые делители N. Этот результат крайне важен для получения аналитического выражения числа GMW разностных множеств и поэтому сформулируем его в виде самостоятельной теоремы.

Теорема 2.8 [14].

Пусть $N\,|\,N_i$ и $N\,|\,N_j$ и $(N_i,N_j)\geq 3$. Тогда

$$\{GMW_N^{N_i}\}\cap\{GMW_N^{N_j}\}=\{GMW_N^{(N_i,N_j)}\}. \quad (2.36)$$

Введем следующие обозначения. Пусть $N_{i_1}=N/p_{i_1}$, $i_1=\overline{1,s}$, $N_{i_1i_2}=(N_{i_1},N_{i_2})=N/p_{i_1}p_{i_2}$, $i_1<i_2$; i_1, $i_2\in\overline{1,s}$. Пусть $N_{i_1i_2...i_k}=(N_{i_1},N_{i_2}...,N_{i_k})=N/p_{i_1}p_{i_2}...p_{i_k}$, $i_1<i_2<...<i_k$, i_1, $i_2...i_k\in\overline{1,s}$ и $N_{12...s}=(N_1,N_2...,N_s)=N/p_1p_2...p_s$. Тогда $\{GMW_N^{N_{i_1}}\}$ есть совокупность неэквивалентных GMW разностных множеств с параметрами (2.13), построенных на основе базисных разностных множеств с параметрами (2.17) при $m=N_{i_1}$. Аналогично $\{GMW_N^{N_{i_1i_2...i_k}}\}$ есть совокупность неэквивалентных GMW разностных множеств, строящихся на основе базисных разностных множеств с параметрами (2.17) и $m=N_{i_1i_2...i_k}$, а $\{GMW_N^{N_{12...s}}\}$ есть совокупность неэквивалентных GMW разностных множеств, строящихся на основе базисных разностных множеств с параметрами (2.17) и $n=N_{12...s}$.

Обозначим через $|GMW_N^{N_{i_1i_2\dots i_k}}|$ мощность множества $\{GMW_N^{N_{i_1i_2\dots i_k}}\}$, а через $M_{N_{i_1i_2\dots i_k}}$ соответственно мощность класса зингеровских разностных множеств с параметрами (2.13) при $N=N_{i_1i_2\dots i_k}$.

Пусть $N_{i_1i_2\dots i_k}\geq 6$ и не простое число. Тогда согласно следствию 2.1 и теореме 2.5 имеем:

$$|GMW_N^{N_{i_1i_2\dots i_k}}|=(|GMW_{N_{i_1i_2\dots i_k}}|+1)M_{N_{i_1i_2\dots i_k}}-1. \quad (2.37)$$

Действительно, множество $\{GMW_N^{N_{i_1i_2\dots i_k}}\}$ строится на основе базисных разностных множеств с параметрами (2.17) при $m=N_{i_1i_2\dots i_k}$. Число всех базисных множеств при $m=N_{i_1i_2\dots i_k}$ равно произведению суммы числа неэквивалентных друг другу классов GMW и зингеровского разностного множества на мощность этих классов $M_{N_{i_1i_2\dots i_k}}$. Отсюда, учитывая, что одно из базисных множеств соответствует зингеровскому разностному множеству с параметрами (2.13), приходим к формуле (2.37). Рассмотрим случай, когда $N_{i_1i_2\dots i_k}$ есть простое число. Тогда

$$|GMW_N^{N_{i_1i_2\dots i_k}}|=|B_{N_{i_1i_2\dots i_k}}|-1, \quad (2.38)$$

где $|B_{N_{i_1i_2\dots i_k}}|$ - мощность соответствующих базисных разностных множеств с параметрами (2.17) при $m=N_{i_1i_2\dots i_k}$. Очевидно, $B_1=B_2=1$. Обобщая (2.37) и (2.38), получаем:

$$|GMW_N^{N_{i_1i_2\dots i_k}}|=(|GMW_{N_{i_1i_2\dots i_k}}|+1)A_{N_{i_1i_2\dots i_k}}-1, \quad (2.39)$$

где $$A_{N_{i_1i_2\dots i_k}}=\begin{cases} M_{N_{i_1i_2\dots i_k}}, \text{ если } |GMW_{N_{i_1i_2\dots i_k}}|\neq 0 \\ |B_{N_{i_1i_2\dots i_k}}| - \text{в противном случае} \end{cases}.$$

Для определения числа неэквивалентных GMW разностных множеств с параметрами (2.13) и $N=p_1^{\alpha_1}p_2^{\alpha_2}\dots p_s^{\alpha_s}$ воспользуемся известным из комбинаторного анализа принципом включения и исключения [43]. В соответствии с ним множество $\{GMW_N\}$

рассматривается как некоторое множество элементов со свойствами $\{P_{i_1}\}$, $i_1=\overline{1,s}$, где элемент $g\in\{GMW_N\}$ обладает свойством P_{i_1}, если $g\in\{GMW_N^{N_{i_1}}\}$. Применив теорему 2.8, получаем, что g обладает свойствами $P_{i_1}, P_{i_2}\ldots, P_{i_k}$, $i_1<i_2<\ldots<i_k$, $i_1,i_2,\ldots i_k\in\overline{1,s}$, если $g\in\{GMW_N^{N_{i_1i_2\ldots i_k}}\}$.

Отсюда следует, что $|GMW_N^{N_{i_1i_2\ldots i_k}}|$ есть число элементов со свойствами $P_{i_1}, P_{i_2}\ldots, P_{i_k}$. Применяя принцип включения и исключения, в результате получаем

$$|GMW_N| = \sum_{i_1}\left|GMW_N^{N_{i_1}}\right| - \sum_{i_1<i_2}\left|GMW_N^{N_{i_1i_2}}\right| + \ldots + (-1)^{k-1}\sum_{i_1<i_2\ldots<i_k}\left|GMW_N^{N_{i_1i_2\ldots i_k}}\right| + \ldots + (-1)^{s-1}|GMW_N^{N_{12\ldots s}}|. \quad (2.40)$$

Подставляя в формулу (2.40) выражение для $|GMW_N^{N_{i_1i_2\ldots i_k}}|$ из (2.39) и учитывая, что $0=(1-1)^s=1-C_s^1+C_s^2+\ldots+(-1)^s$, получаем следующую рекуррентную формулу:

$$|GMW_N| = \sum_{i_1}\left(\left|GMW_{N_{i_1}}\right|+1\right)A_{N_{i_1}} - \sum_{i_1<i_2}\left(\left|GMW_{N_{i_1i_2}}\right|+1\right)A_{N_{i_1i_2}} + \ldots +$$

$$+(-1)^{k-1}\sum_{i_1<i_2\ldots<i_k}\left(\left|GMW_{N_{i_1i_2\ldots i_k}}\right|+1\right)A_{N_{i_1i_2\ldots i_k}} + \ldots + (-1)^{s-1}\left(\left|GMW_{N_{12\ldots s}}\right|+1\right)A_{N_{12\ldots s}} - 1 \quad . (2.41)$$

Тогда число P_N различных ПСП GMW для всех возможных значений N может быть вычислено по формуле:

$$P_N = |GMW_N| M_N \quad . \quad (2.42)$$

На основе полученных выражений для $N\le 18$ в [14] были рассчитаны:

- число $|GMW_N^m|$ неэквивалентных классов ПСП GMW длины 2^N-1, строящихся на основе базисных последовательностей длины $w=2^m-1$;
- число $|GMW_N|$ всех неэквивалентных классов ПСП GMW длины 2^N-1;
- мощность M_N классов;
- общее число P_N ПСП GMW.

Результаты вычислений приведены в таблицах 2.3 и 2.4. При этом в качестве базисных разностных множеств наряду с зингеровскими использовались разностные множества Лежандра, Холла, Бомера-Фридриксена [45], а также GMW. Более подробно свойства последовательностей, полученных на основе разностных множеств Лежандра, Холла и Бомера-Фридриксена будут рассмотрены в 3-й главе настоящей диссертации. Впервые эти результаты были опубликованы в 1979г в работе [14]. К сожалению, полученные в этой работе результаты остались не замеченными ни в нашей стране, ни за рубежом. Всплеск интереса к последовательностям GMW в 90-х гг. привлек внимание к проблеме нахождения их численности ведущих ученых мира и, прежде всего, С. Голомба и др. В общем виде эта задача для q-ичных каскадных ПСП GMW зингеровской природы была решена в работе [52]. Следует отметить, что ее результаты в случае двоичных ПСП GMW полностью совпадают с результатами [14].

Таблица 2.3.

Число неэквивалентных классов ПСП GMW в зависимости от m.

N	Число неэквивалентных классов						
	3	4	5	6	7	8	9
6	1	—	—	—	—	—	—
8	—	1	—	—	—	—	—
9	1	—	—	—	—	—	—
10	—	—	7	—	—	—	—
12	1	1	—	11	—	—	—
14	—	—	—	—	79	—	—
15	1	—	—	—	—	—	—
16	—	1	—	—	—	31	—
18	1	—	—	11	—	—	95

Таблица 2.4.

Общее число ПСП GMW для N≤18.

N	GMW_N	M_N	P_N
6	1	6	6
8	1	16	16
9	1	48	48
10	7	60	420
12	12	144	1728
14	79	756	59724
15	8	1800	14400
16	31	2048	63488
18	105	7776	816460

Теперь настало время сделать одно важное замечание. Формулы (2.39) и (2.41) были получены исходя из предположения, что для не простых N существуют только два типа разностных множеств: зингеровские и GMW. Однако недавно опубликованные работы [11,31] показывают, что для таких N могут существовать и другие типы разностных множеств. Краткий обзор получаемых на их основе последовательностей приведен в разделе 1.2. Отсюда следует, что для вычисления общего количества последовательностей GMW можно воспользоваться только формулой (2.40). Формулы же (2.39) и (2.41) в силу последних результатов оказываются не полными, поскольку не отражают все возможные базисные последовательности. Исходя из этого обозначим через $\{B_{N_{i_1 i_2 \dots i_k}}\}$ и $|B_{N_{i_1 i_2 \dots i_k}}|$ множество и соответственно мощность всех базисных последовательностей длины $2^{N_{i_1 i_2 \dots i_k}}-1$.

Тогда по-прежнему $|GMW_N^{N_{i_1 i_2 \dots i_k}}| = |B_{N_{i_1 i_2 \dots i_k}}| - 1$

С учетом этого выражение (2.40) преобразуется к следующему

$$|GMW_N| = \sum_{i_1} \left|B_{N_{i_1}}\right| - \sum_{i_1<i_2} \left|B_{N_{i_1 i_2}}\right| + \dots + (-1)^{s-1} \left|B_{N_{i_2 \dots s}}\right| - 1 \quad . (2.42)$$

В таблице 2.5 для всех N≤20 представлены скорректированные результаты расчета значений параметров $|GMW_N|$ и P_N. При этом в качестве базисных наряду с известными последовательностями использовались недавно полученное семейство последовательностей No-Golomb-Gong-Lee-Gaal, а также два класса последовательностей длины 511, найденные Дрейером [31]. В результате число базисных последовательностей для m=8, m=9 и m=10 увеличивается с 31, 95 и 479 до 63, 143 и 599 соответственно.

Таблица 2.5.

Скорректированые значения параметров $|GMW_N|$ и P_N.

N	m	B_m-1	$\|GMW_N\|$	M_N	P_N
6	3	1	1	6	6
8	4	1	1	16	16
9	3	1	1	48	48
10	5	7	7	60	420
12	3 4 6	1 1 11	12	144	1728
14	7	79	79	756	59724
15	3 5	1 7	8	1800	14400
16	8	63	63	2048	129024
18	3 6 9	1 11 239	249	7776	1936224
20	4 10	1 599	600	24000	14400000

В заключение следует отметить, что экспериментальная проверка правильности выведенных расчетных формул довольно сложна, а при больших значениях N просто не возможна. И все же для одного частного случая N=12 такая проверка была проведена. С помощью имитационного моделирования на компьютере для m=3, m=4 и m=6 были построены ПСП, являющиеся векторами инцидентности всех GMW разностных множеств с параметрами (4095, 2048, 1024). При этом использовался новый метод генерации [49]. В

результате сравнения этих ПСП, было установлено, что $GMW_{12}^3 \subset GMW_{12}^6$, тогда как $GMW_{12}^4 \not\subset GMW_{12}^6$. При этом $|GMW_{12}^4| = 1$, а $|GMW_{12}^6| = 11$. Таким образом, $GMW_{12} = |GMW_{12}^4| + |GMW_{12}^6| = 1+11=12$. Заметим, что аналогичные результаты были получены при нахождении общего числа последовательностей GMW каскадного типа [52].

2.4. Статистические свойства

Анализ статистических свойств последовательностей GMW будем проводить в сравнении с соответствующими статистическими свойствами порождающих их m-последовательностей. Согласно широко известной аксиоматики псевдослучайных последовательностей [13] последние в идеале должны удовлетворять следующим критериям случайности:

критерий R1 (свойство сбалансированности): в каждом периоде последовательности число 1 отличается от числа -1 не более чем на единицу, т.е.

$$\left|\sum_{n=1}^{v} a_n\right| \le 1;$$

критерий R2 (свойство серий): в течение периода последовательности половина серий 1 и -1 имеет длину 1, одна четверть – 2, одна восьмая – 3 и т.д.;

критерий R3 (свойство корреляции): если последовательность почленно сравнивать с любым ее циклическим сдвигом на длине периода этой последовательности, то число совпадений отличается от числа несовпадений не более, чем на единицу. Фактически это означает, что $\left|C(\tau) = \sum_{n=1}^{v} a_n a_{n+\tau}\right| \le 1$ для всех $0<\tau<v$.

Всем этим критериям в точности удовлетворяют m-последовательности, причем для них строго выполняются равенства $\sum_{n=1}^{v} a_n = -1$ и $C(\tau) = \sum_{n=1}^{v} a_n a_{n+\tau} = -1$, т.е. автокорреляционная функция является двухуровневой со значениями 2^N-1 и –1. Кроме того, m-последовательности обладают важным для практического применения аддитивно-циклическим свойством, состоящим в том, что сумма по модулю два двух любых сдвигов m-последовательности также является ее некоторым сдвигом.

Что же касается нелинейных последовательностей GMW, то, как было показано в разделе 2.1, они обладают точно такими же свойствами R1 и R3, что и родственные им m-последовательности. Однако в отличие от m-последовательностей свойство R2 выполняется лишь для серий длины равной или меньшей k=N/m. Это устанавливается следующей теоремой [4].

Теорема 2.9.

Пусть $\{b_n\}$ есть последовательность GMW периода 2^N-1, N=mk. Тогда число N_a позиций внутри периода $\{b_n\}$, на которых встречается J-серия $a_1\, a_2 \ldots a_J$ определяется выражением

$$N_a = \begin{cases} 2^{N-J}, \text{ для } a \neq 0, & 1 \le J \le k \\ 2^{N-J} - 1, \text{ для } a = 0, & 1 \le J \le k \end{cases} . \quad (2.43)$$

Так, например, для N=10=5*2, одиночные серии (1) и (0) встречаются на периоде соответственно 512 и 511 раз, двойные серии (01), (10), (11) – 256 раз, а (00) -соответственно 255 раз. В процессе математического моделирования последовательностей GMW разной длины было установлено, что в частоте появлении более длинных серий нет регулярного порядка как случае m-последовательностей, число их случайно, а вероятность серий длины более N+3, состоящих из одних 1 или нулей равна нулю.

Нетрудно проверить, что последовательности GMW в общем случае не обладают и свойством аддитивно-циклического сдвига. Для последовательностей GMW на основе нелинейных базисных последовательностей это утверждение очевидно. В случае же

базисных m-последовательностей это верно лишь частично, поскольку аддитивно-циклическим свойством обладает лишь подмножество, состоящее из равномерно сдвинутых на ξ разрядов копий одной и той же последовательности GMW, которые образуют подгруппу относительно операции сложения по модулю два порядка 2^m-1. Причем всего таких подгрупп ровно ξ.

2.5. Структурные свойства

Говоря о структурных свойствах псевдослучайных последовательностей, будем подразумевать, прежде всего, различные типы отношений, связывающих их элементы, а также сами эти последовательности между собой. Структурные свойства последовательностей GMW, равно как и m-последовательностей основываются на рассмотренных в разделах 2.1-2.2 свойствах порождающих их разностных множеств.

Исследования структур этих и им подобным математических объектов началось более трех десятилетий назад. Так в начале 70гг. Венгом была сформулирована и доказана следующая замечательная теорема о разложении или декомпозиции m-последовательностей [53].

Теорема 2.10.

Пусть $\{m_n\}$ есть двоичная m-последовательность длины $2^N-1=n_1 \times n_2$, а $M_{n_1 n_2}$ есть матрица порядка $n_1 \times n_2$ с элементами $a_{ij}=m_n$, $n=0, 1, 2,\ldots, 2^N-2$, где $i=n-n_1\left[\frac{n}{n_1}\right]$, $j=n-n_2\left[\frac{n}{n_2}\right]$ целые числа, начиная от нуля, и пусть $n_2=2^m-1$. Тогда каждая строка матрицы $M_{n_1 n_2}$ есть либо m-последовательность длины 2^m-1, либо последовательность из 2^m-1 нулей. Причем число таких нулевых строк в точности равно $2^N-1/2^m-1-2^{N-m}$.

Отметим, что полученную теорему Венг применил исключительно к исследованию m-последовательностей, хотя у него и имеется ссылка на известную работу [44]. Почти

тогда же Бомер в своей монографии [45], посвященной циклическим разностным множествам, интерпретируя Теорему 2.1, также представил m-последовательность в виде таблицы размером 2^m-1×ξ, назвав ее таблицей представителей элементов m-последовательности (об этом уже говорилось в разделе 2.2). Декомпозиции по Венгу и Бомеру, хотя и обладают одинаковыми с точностью до транспонирования структурными свойствами, вместе с тем являются различными формами представления одной и той же m-последовательности. Заметим, что в силу теоремы 2.1 точно таким же свойством декомпозиции должны обладать и родственные m-последовательностям последовательности GMW. Табличное представление последовательностей по Бомеру, без всякого сомнения, можно считать фундаментальным, поскольку большинство полученных в диссертации результатов в той или иной степени основываются на этом представлении. Более подробно на этом мы остановимся при рассмотрении вопросов взаимной корреляции (Глава 3) и генерации (Глава 4).

Следующее структурное свойство последовательностей GMW связано с понятием децимации, введенным Голомбом [13], и обозначающим замещение последовательности $\{\alpha_n\}$ последовательностью $\{\alpha_{tn}\}$, образованной элементами последовательности $\{\alpha_n\}$ с номерами tn (mod v). В общем случае с учетом существующей связи между разностными множествами и соответствующими им векторами инцидентности имеет место следующая теорема.

Теорема 2.11.

Пусть $\{\alpha_n\}$ есть последовательность, соответствующая разностным множествам с параметрами (2.13), т.е. разностным множествам типа Адамара. Тогда последовательность $\{\alpha_{tn}\}$, где t – есть множитель разностного множества, является сдвигом исходной последовательности $\{\alpha_n\}$. Если же t есть немножитель разностного множества, тогда последовательность $\{\alpha_{tn}\}$ есть изоморфная $\{\alpha_n\}$ последовательность того же периода.

Во 2-й главе было показано, что множители GMW разностных множеств при q=2 являются исключительно степенями числа два и образуют мультипликативную группу t=1, 2, ..., 2^{N-1} порядка N. Очевидно, что децимации с этими числами последовательности GMW приводят с точностью до сдвига к той же самой последовательности. Причем согласно теореме Манна-Джонса [43] существует единственный циклический сдвиг последовательности GMW, фиксируемый каждым ее множителем. Подобный сдвиг в литературе получил название характеристического сдвига [18]. Заметим, что сказанное в равной степени относится и к семейству m-последовательностей.

2.6. Линейная сложность

Мощность класса *m* - последовательностей во многих случаях оказывается вполне достаточной, чтобы на их основе путем соответствующего отбора сформировать нужное подмножество последовательностей с малыми значениями пиков взаимной корреляции [20, 54, 55]. С другой стороны, будучи линейными, *m* - последовательности характеризуются малыми значениями параметра линейной сложности L, составляющей для *m* - последовательности длины 2^N -1 величину, равную N. Напомним, что параметр линейной сложности, введенный для оценки степени непредсказуемости символов последовательности, численно равен длине эквивалентного регистра сдвига с линейной обратной связью, посредством которого может быть сформирована данная псевдослучайная последовательность, что в свою очередь совпадает с линейным размахом этой последовательности [4]. В соответствие с общепринятой точкой зрения параметр линейной сложности в значительной мере характеризует степень раскрываемости последовательности [18]. Действительно, несанкционированный "взлом" закона формирования ПСП в условиях отсутствия каких-либо априорных сведениях и невозможности достоверного поэлементного приема сигнала, по существу, сводится к комбинаторному перебору вариантов кодовой

последовательности и проверке сходства каждой из них с кодом реально принятой последовательности. Очевидно, что число перебираемых последовательностей растет как степень длины последовательности по основанию два, что делает задачу перебора практически не разрешимой уже при длинах порядка нескольких сотен. Если стратегия раскрытия ориентируется на линейные способы формирования последовательностей, то передающая сторона будет иметь тем большую криптозащищенность, чем большую линейную сложность имеет применяемая в ней ПСП. Нетрудно убедиться, что линейная сложность L произвольной последовательности длины 2^N-1 лежит в диапазоне $N \le L \le 2^N-1$.

Математический анализ линейной сложности нелинейных двоичных последовательностей впервые был проведен Э. Кейем в работе [19]. В основном им исследовались последовательности, получаемые в результате произведения двух и более разрядов одного и того же генератора с линейными обратными связями (LFSR), а также комбинации LFSR генераторов различной длины. Проведенный анализ основывался на представлении элементов этих последовательностей в виде суммы степеней примитивного элемента поля $\alpha \in GF(q^N)$ с коэффициентами из $GF(q^N)$, как это имеет место в случае m-последовательности, для элементов которой справедливо следующее равенство:

$$b_n = tr_1^N(\alpha^n) = \sum_{i=0}^{N-1} \alpha^{n2^i}.$$

Очевидно, что линейная сложность L такой последовательности численно совпадает со степенью ее характеристического полинома и связана с последовательностью степеней α следующей теоремой [4].

Теорема 2.12.

Пусть $\{b_n\}$ есть последовательность с элементами над GF(q), и пусть α есть примитивный элемент поля $GF(q^N)$. Пусть $\{b_n\}$ имеет вид

$$b_n = \sum_{\delta \in \Delta} \alpha_\delta \alpha^{\delta n} \quad . (2.44)$$

для всех n, где Δ есть множество индексов при не нулевых коэффициентах в этом расширении. Тогда линейная сложность (размах) L последовательности $\{b_n\}$ равен числу элементов в представлении (2.44), т.е.

$$L= \Delta \quad . (2.45)$$

Не смотря на то, что данная теорема непосредственно не содержит способа получения искомого представления, она имеет большое значение для нахождения линейной сложности последовательностей различной природы и в частности ПСП GMW длины 2^N-1 сложной конфигурации, обладающих существенно более высокой по сравнению с m - последовательностями линейной сложностью. Поэтому эти ПСП могут быть использованы в помехозащищенных широкополосных системах связи, где требуются последовательности, обладающие высокой непредсказуемостью символов и одновременно хорошими корреляционными свойствами.

Как уже отмечалось выше, базисными могут являться последовательности следующих типов: Зингера, Лежандра, Холла, Бомера-Фридриксена, No-Golomb-Gong-Lee-Gaal, GMW. Последние в свою очередь также могут иметь в качестве базисных все выше перечисленные типы последовательностей. Процесс итеративного разложения базисных ПСП GMW может быть продолжен до тех пор, пока в качестве наименьшей базисной последовательности не окажется последовательность любого типа, кроме GMW. Важно подчеркнуть, что чисто линейными среди них являются только m-последовательности. Рассмотрим далее различные методы вычисления линейной сложности ПСП GMW в зависимости от их классификации и способа генерации.

В широко известной работе [46] Шольцем и Велчем предложен механизм генерации некоторых классов ПСП GMW, общий член которых определяется как

$$b_n = tr_1^m([tr_m^N(\alpha^n)]^r) \ , (2.46)$$

где $0<r<2^m-1$, где $(r, 2^m-1)=1$. Очевидно, данная формула является частным случаем выражения более общего вида, в котором в качестве функционала f выбирается след tr_1^m. В соответствие с доказанной в [46] теоремой линейный размах ПСП GMW вида (2.46) равен:

$$L=m(N/m)^w \quad , \quad (2.47)$$

где w- есть число единиц в двоичном представлении r.

В общем, случае с помощью индукции для $N=m_1 \bullet m_2 \ldots\ldots m_l$, где $m_1 \geq 3$, $m_2 \geq 2, \ldots\ldots, m_l \geq 2$, получаем ПСП GMW с элементами:

$$b_n = tr_1^{e_1}\left(\left[tr_{e_1}^{e_2}\left(\left[\ldots\left[tr_{e_i}^{e_{i+1}}\left(\ldots\left[tr_{e_{l-1}}^{N}\left(\alpha^n\right)\right]^{r_{l-1}}\right)\ldots\right]^{r_i}\ldots\right]^{r_2}\right)\ldots\right]^{r_1}\right), \quad (2.48)$$

где $e_i = m_1 m_2 \ldots\ldots m_l$, а $1 \leq r_i < 2^{e_i} - 1$ взаимно простые с $2^{e_i} - 1$.

Из анализа (2.46) и (2.48) следует, что ПСП GMW с элементами (2.46) являются подмножеством множества ПСП GMW с элементами (2.48).

В данном месте нельзя не вступить в полемику с точкой зрения некоторых авторов [40], относящих ПСП вида (2.48) к новым, т.е. ранее (до 1993г.) не известным классам последовательностей GMW и названных ими каскадными последовательностями GMW. Не имея ничего против данного названия, хорошо отражающего структурные свойства этих последовательностей, новыми все же их можно назвать с большим трудом. В этой связи уже упоминались пионерские работы [14, 21,22] отечественных авторов, в которых были получены и исследовались все возможные классы ПСП GMW, составной частью которых являются и так называемые "новые" классы последовательностей GMW. При вычислении линейной сложности ПСП GMW каскадного типа ограничимся рассмотрением случая $l=3$.

Введем следующие обозначения: $m=m_1$, $J=m_1m_2$ и $K=N/m_1m_2$. Тогда по аналогии с (2.46), можно показать, что элементы последовательности GMW имеют вид:

$$b_n = tr_1^m([tr_m^J([tr_J^N(\alpha^n)]^{r_2})]^{r_1}) \quad , \quad (2.49)$$

где $0<r_1<2^m-1$, $0<r_2<2^J-1$ и $(r_1,2^m-1)=1$, $(r_2,2^J-1)=1$.

В соответствии с известным из [4,19] методом для вычисления линейной сложности последовательности $\{b_n\}$ достаточно представить ее в виде (2.44). Тогда линейная сложность L последовательности $\{b_n\}$ равна числу различных членов в этом представлении, то есть $L=|\Delta|$. Исходя из этого, преобразуем последовательность (2.49) к последовательности вида (2.44). Пусть $r_2=\sum_{i_2=1}^{w_2}2^{j_{i_2}}$, а $r_1=\sum_{i_1=1}^{w_1}2^{m_{i_1}}$, где j_{i_2} и m_{i_1} соответственно - различные целые числа такие, что $0\le j_{i_2}<J$, а $0\le m_{i_1}<m$.

Тогда подставив r_2 в (2.49), получаем:

$$b_n=tr_1^m([tr_m^J(\prod_{i_2}^{w_2}[tr_J^N(\alpha^n)]^{2^{j_{i_2}}})]^{r_1}) \quad . \quad (2.50)$$

После раскрытия внутреннего следа tr_N^J имеем:

$$b_n=tr_1^m\left(\left[tr_m^J\left(\prod_{i_2=1}^{w_2}\sum_{\kappa=0}^{K-1}\alpha^{n2^{J\kappa+j_{i_2}}}\right)\right]^{r_1}\right)=tr_1^m\left(\prod_{i_1=1}^{w_1}\left[tr_m^J\left(\sum_{\kappa_1=0}^{K-1}\dots\sum_{\kappa_{\omega_2}=0}^{K-1}\alpha^{nc(\kappa,r_2)}\right)\right]^{2^{m_{i_1}}}\right), \quad (2.51)$$

где

$$c(k,r_2)=\sum_{i_2=1}^{w_2}2^{Jk_{i_2}+j_{i_2}} \quad . \quad (2.52)$$

Из анализа (2.52) следует, что на всех наборах $k=(k_1\ k_2,\dots,k_{\omega_2})$ значения $c(\kappa, r_2)$ всегда меньше 2^N-1 и различны. Поэтому различными будут и все члены ω_2 кратной суммы в выражении (2.52). После раскрытия внутреннего следа tr_m^J и возведения в степень, получаем

$$b_n=tr_1^m(\prod_{i_1=1}^{w_1}\sum_{t=0}^{T-1}(\sum_{k_1=0}^{K-1}\dots\sum_{k_1=0}^{K-1}\alpha^{nc(k,r_2)})^{2^{mt+m_{i_1}}}) \quad . \quad (2.53)$$

Обозначим аргумент следовой функции tr_1^m в выражении (2.53) через $g_n^{(m)}$. Очевидно, что $\{g_n^{(m)}\}$ есть последовательность длины 2^N-1 с элементами из $GF(2^m)$. Можно показать, что линейная сложность последовательности $\{b_n\}$ в этом случае оказывается

равной: L=m l, где l- есть число различных степеней α^{ni} в представлении $g_n^{(m)}$. Поэтому основная задача при вычислении L заключается в нахождении величины l. Очевидно, что при r_1=1, $l = m_2 K^{\omega_2}$, а $L = m_1 m_2 K^{\omega_2} = JK^{\omega_2}$, что совпадает с формулой Велча-Шольца [46]. К сожалению, в общем случае при r_1>1, не удается отыскать компактную и простую формулу для преставления l. Поэтому для нахождения l в каждом конкретном случае надо выполнить достаточно большой объем вычислений. С помощью компьютера Pentium-120 и системы MATLAB, предназначенной для выполнения инженерных и научных расчетов, были проведены расчеты линейной сложности ПСП GMW для случаев N=12,16,18,20 и 24. Результаты расчетов для N=12 и 16 приведены соответственно в таблицах 2.6 и 2.7. Кроме того, в этих таблицах для сравнения приведены значения L для классов ПСП GMW, получаемых на основе метода [46]. Из таблиц видно, что в среднем значения L для ПСП GMW на основе не зингеровского класса базисных последовательностей, несколько выше. Кроме того, имеются классы ПСП, у которых линейная сложность превышает максимально возможные значения L для ПСП GMW на основе базисных m - последовательностей. Для N=12 и N=16 это соответственно 216 и 1472. И хотя получаемый здесь выигрыш в линейной сложности не значителен, достигается он, а это главное, на одном и том же генераторном оборудовании. Дальнейшие расчеты для случаев N=18, 20 и 24 (таблица 2.8) свидетельствуют о тенденции к росту относительного выигрыша в линейной сложности с увеличение N.

Наряду с описанным выше методом нахождения линейной сложности для строящихся каскадно последовательностей GMW, требующим большого объема вычислений, Клаппером, Чаном и Горецким для некоторых классов таких последовательностей были найдены довольно простые аналитические выражения для представления их линейной сложности [36]. С учетом выше сделанных обозначений приведем формулировку одной из доказанных ими теорем.

Таблица 2.6.

Линейная сложность ПСП GMW для N=12.

	ПСП GMW (2.46)				ПСП GMW (2.49)					
Число классов	1	2	1	1	1	1	1	1	1	1
L	24	48	92	192	48	72	108	144	192	216

Таблица 2.7.

Линейная сложность ПСП GMW для N=12.

	ПСП GMW (2.46)				ПСП GMW (2.49)									
Кл	5	4	5	1	1	1	2	2	2	2	1	1	2	2
L	64	128	256	1024	256	384	464	512	656	704	768	1024	1280	1472

Таблица 2.8.

Максимальная линейная сложность ПСП GMW для случаев N=18, 20, 24.

N	L_{max}	
	ПСП GMW (4)	ПСП GMW (5)
18	2304	3456
20	5120	8000
24	25576	≥44160

Теорема 2.12 [34].

Пусть $N=m_1 \bullet m_2 \ldots\ldots m_l$, $q_0=2$, $q_i=q_{i-1}^{m_i}$ для любого i, $1 \le i \le l$ и пусть $r_i=q_{i-1}^{s_i}+q_{i-1}^{t_i}$ (т.е. k_i имеет q_{i-1} – адический вес 2) с $1 \le s_i < t_i < m_i$ и m_i/нод(m_i, t_i-s_i) нечетно. Тогда линейная сложность каскадных последовательностей GMW выражается формулой

$$L = m_1 m_2^2 m_3^3 \ldots m_l^{2^{l-1}} . \qquad (2.54)$$

Из этой формулы следует, что линейная сложность каскадных последовательностей GMW при больших N может во много раз превышать линейную сложность последовательностей GMW с общим членом (2.46).

В качестве примера рассмотрим приложение этой теоремы к случаю N=12 с m_1=3, m_2=2 и m_3=2. Тогда $q_1 = 2^3$=8 и $q_2 = 8^2$=64. Выберем параметры r_1 и r_2 так, чтобы они удовлетворяли условиям данной теоремы. Такие параметры существуют и равны $r_1 = 2^1 + 2^2$ =6, а $r_2 = 8^0 + 8^2$=2 mod 63. Нетрудно проверить, что последовательность GMW с этими параметрами вырождается в последовательность GMW с параметрами m_1=6 и m_2=2. При этом значения L, вычисленные по формулам (2.54), (2.53) совпадают и равны 192. Можно показать, что найденные параметры единственные, т.е. других классов последовательностей GMW, для которых может быть применима теорема 2.9, не существует. В этом случае остается применить более сложную расчетную формулу (2.53). Результаты расчета представлены в таблице 2.6.

Рассмотрим теперь задачу нахождения верхней границы линейной сложности последовательностей GMW . Для этого воспользуемся следующим результатом, полученным Брайниэлсоном [34].

Предложение 2.1.

Пусть $q = 2^m$ и N=mk, где m≥3, k>1. Предположим, что последовательность S определяется выражением $S_n = f(tr_m^N(\alpha_n))$ с функцией обратной связи вида

$f: GF(2^m) \rightarrow GF(2)$. Пусть f имеет полиномиальное представление

$$f = \sum_{i=0}^{q-1} A_i x^i \qquad (2.55)$$

с коэффициентами $A_i \in GF(q)$. Тогда GF(q) – линейная сложность последовательности S равна

$$L = \sum_{A_i \neq 0} k^{\|i\|} \quad , \quad (2.56)$$

где $||i||$ - диадическое представление целого i (т.е. число единиц в двоичном представлении числа i).

Оценим теперь линейную сложность последовательности S. Для этого заметим, что максимальное число членов одной и той же степени k^u, где $0 \le u \le m$, в правой части выражения (2.56) равно C_m^u, а максимальное число всех членов равно 2^m. Тогда согласно биному Ньютона имеем $(k+1)^m = \sum_{i=0}^{m} C_m^i k^i$. Отсюда следует, что выражение (2.56) может быть ограничено сверху величиной, равной $(k+1)^m$. Применительно к последовательностям GMW $f(0)=0$. Следовательно, $A_0=0$. По этой же причине оказывается равным нулю и коэффициент при степени $x^{q-1}=1$. В результате получаем следующую верхнюю границу для линейной сложности последовательностей GMW.

Теорема 2.13.

Линейная сложность L последовательностей GMW удовлетворяет неравенству:

$$L \le (k+1)^m - (2^m+1) \ . \quad (2.57)$$

Применяя полученную оценку к случаю N=14 с m=7 и k=2, находим $L \le 3^7 - 2^7 - 1 = 2058$. Таким образом, потенциально возможная линейная сложность любой из 59724 последовательностей GMW не превышает числа 2058. Для этого случая на компьютере Pentium 2 с помощью системы автоматизации математических и научно-технических расчетов MATLAB 5.3 были проведены расчеты линейной сложности последовательностей GMW, строящихся на основе всех известных 62-х нелинейных последовательностей длины 127, к которым относятся последовательности Лежандра, Холла и Бомера-Фридриксена (классы A, B, C). Все выше перечисленные последовательности 127 подробно исследуются в главе 3. При проведении расчетов использовался интегрированный пакет инструментария связи Communications, позволяющий вести разработку, анализ и тестирование моделей цифровых систем передачи информации. В том числе пакет содержит все средства, необходимые для проведения расчетов в полях Галуа и, в частности, функцию

GFLINEQ, предназначенную для решения системы линейных уравнений над GF(2). Результаты расчета линейной сложности последовательностей GMW на основе нелинейных базисных последовательностей 127 приведены в таблице 2.9.

Таблица 2.9.

Линейная сложность ПСП GMW для N=14.

тип базисного семейства	Линейная сложность
L	826, 1232
H_6	140, 196, 294, 392, 448, 588
A	252, 266, 378, 378, 392, 420, 448, 448, 462, 574, 588, 644, 644, 756, 840, 924, 924, 952
B	252, 266, 266, 280, 448, 476, 518, 532, 630, 630, 644, 672, 672, 672, 700, 728, 952, 952
C	98, 154, 168, 182, 224, 252, 252, 252, 280, 308, 336, 336, 336, 364, 504, 616, 728, 784

Как видно из таблицы 2.9, максимальной линейной сложностью обладают последовательностей GMW на основе последовательности Лежандра. Заметим, что именно они обладают наибольшей линейной сложностью из всех последовательностей Адамара длины 127, которая равна 63.

Аналогично были проведены расчеты линейной сложности для случаев M=15, m=5, k=3 и M=20, m=5, k=3 с последовательностями Лежандра 31 в качестве базисных. Результаты расчета представлены в таблице 2.10.

Таблица 2.10.

Линейная сложность ПСП GMW на основе последовательностей Лежандра.

N	**M**	**k**	**L**	**Верхняя граница**
15	**5**	**3**	**195, 585**	**780**
20	**5**	**4**	**420, 1680**	**2100**

К сожалению, ограничения, связанные с производительностью использованных вычислительных средств, не позволили с помощью этого метода отыскать линейную сложность классов последовательностей GMW 2^{21}-1 на основе нелинейных последовательностей 127. Заметим, что максимально возможная линейная сложность последовательностей GMW 2^{21}-1 на основе m-последовательностей согласно формуле (2.47) составляет 5103, тогда как ее верхняя граница равна 14196. Поэтому имеются веские основания полагать, что существуют классы последовательностей с большим, чем 5103, значением линейной сложности и, очень вероятно, в качестве базисной используется одна из последовательностей Лежандра. Для точного расчета линейной сложности в этом случае можно воспользоваться аналитическим методом, предложенным работе [56]. Основу этого метода составляет найденное недавно представление последовательностей Лежандра длины 2^N-1 в виде суммы $\varphi(2^N-1)/N$ различных m-последовательностей. В качестве примера в [56] для N=14 и одной из двух базисных последовательностей Лежандра была рассчитана линейная сложность соответствующей ПСП GMW длины 16383. Она оказалась равной 826, что совпадает с результатом таблицы 2.9. Очевидно, в ближайшем будущем следует ожидать появления новых интересных результатов по расчету линейной сложности ПСП GMW на основе нелинейных базисных последовательностей.

Выводы

1. В соответствие с предложенным определением последовательностей GMW проведена их классификация и доказан ряд теорем о разбиении этих последовательностей на неэквивалентные классы. Получено аналитическое выражение для подсчета общего числа последовательностей GMW при любых возможных значениях N. Приведенные результаты расчетов для всех $N \leq 20$ полностью совпадают с результатами Голомба-Гонга-Дейя для двоичного случая.
2. Предложен метод расчета линейной сложности последовательностей GMW каскадного типа, дополняющий другие известные аналитические методы расчета.

3. Доказано, что все принадлежащие одному и тому же классу последовательности GMW обладают одинаковой линейной сложностью.
4. Найдена верхняя граница линейной сложности последовательностей GMW.
5. Приведенные результаты расчета линейной сложности последовательностей GMW каскадного типа для N=12, 16, 18, 20 и 24 показывают, что последовательности данного типа обладают в среднем большей линейной сложностью по сравнению с последовательностей GMW на основе m-последовательностей. Причем этот разрыв с ростом N все более увеличивается.
6. Впервые сделан полный расчет линейной сложности для всех классов последовательностей GMW длины 16383.

Глава 3. Исследование взаимной корреляции двоичных последовательностей на основе разностных множеств типа Адамара

В этой главе рассматриваются периодические взаимно-корреляционные функции двоичных последовательностей на основе Адамаровых разностных множеств и их свойства. Основным содержанием главы являются:

- основные корреляционные свойства и тождества;
- метод ускоренного расчета ПВКФ последовательностей с помощью изоморфных коэффициентов;
- получение наибольших аналитических нижних границ для их корреляционных максимумов и их использование для отбора и формирования множеств последовательностей с требуемыми корреляционными параметрами;
- примеры численного расчета взаимной корреляции последовательностей на основе Адамаровых разностных множеств, включая классы m и GMW последовательностей, последовательностей Холла, Лежандра, а также последовательностей Бомера-Фридриксена длины 127.

3.1. Основные взаимно-корреляционные свойства и тождества

В этом параграфе будут рассмотрены основные определения взаимной корреляции двоичных последовательностей, а также их свойства и тождества в том виде как они представлены в работе [20]. Пусть $\mathbf{x}=(x_0, x_1,\ldots,x_{v-1})$ и $\mathbf{y}=(y_0, y_1,\ldots,y_{v-1})$ есть векторы в v размерном векторном пространстве над GF(2), а $(\mathbf{x},\mathbf{y})=x_0y_0+x_1y_1+\ldots+x_{v-1}y_{v-1}$ есть скалярное произведение векторов **x и y.** Пусть T есть оператор циклического сдвига вектора **x** на одну позицию влево, т.е. $T\mathbf{x}=(x_1, x_2,\ldots,x_{v-1}, x_0)$. Результат k-кратного применения оператора T к **x** обозначим $T^k\mathbf{x}$. Очевидно, $T^k\mathbf{x}=(x_k, x_{k+1},\ldots,x_{v-1}, x_0,\ldots,x_{k-1})$, а $T^v\mathbf{x}=\mathbf{x}$. Кроме того, $T^k\mathbf{x}=T^i\mathbf{x}$, где

$k \equiv i \bmod v$. Аналогичным образом вводится оператор T^{-1} циклического сдвига на одну позицию вправо. Ясно, что $T^{-k}\mathbf{x}=T^{v-k}\mathbf{x}$ при $0 \le k < v$, а $T^{-v}\mathbf{x}=\mathbf{x}$. Неограниченно повторяя вектор $\mathbf{x}$, построим бесконечную в обе стороны последовательность $x=\ldots, x_{-2}, x_{-1}, x_0, x_1, x_2, \ldots, x_{-v-1}, x_v, \ldots$, где $x_{mv+i}=x_i$ для всех m и $0 \le i \le v-1$. Оператор T левого циклического сдвига очевидным образом распространяется и на эти последовательности. Период последовательности определяется как наименьшее целое положительное число v, для которого $x_i=x_{i+v}$. Последовательности вида $x, Tx, \ldots, T^{v-1}x$ еще иначе называются сдвиговыми последовательностями или просто сдвигами.

В большинстве практических приложений двоичные последовательности преобразуются в последовательность биполярных импульсов единичной амплитуды, которые получаются заменой каждой 1 импульсом с амплитудой –1, а каждого 0 – импульсом с амплитудой +1. Последовательности биполярных импульсов часто называют бинарными последовательностями. Следуя [13], введем функцию $\chi(\alpha)=(-1)^{\alpha}$, где $\alpha \in \{0,1\}$: $\chi(0)=+1$, $\chi(1)=-1$.

Для каждой пары v-векторов $\mathbf{x}$ и $\mathbf{y}$ определена периодическая взаимно-корреляционная функция

$$\theta_{x,y}(l)=(\mathbf{x},T^{l}\mathbf{y}),\ l \in \mathbf{Z} \quad , (3.1)$$

где $\mathbf{Z}$ – множество целых чисел.

Если x и y – бинарные последовательности, порожденные векторами $\mathbf{x}$ и $\mathbf{y}$, то (3.1) эквивалентно следующему определению

$$\theta_{x,y}(l)=\sum_{i=0}^{v-1} x_i y_{i+l},\ l \in \mathbf{Z} \ . (3.2)$$

Очевидно, что при всех $l \in \mathbf{Z}$

$$\theta_{x,y}(l)=\theta_{x,y}(l+v) \quad \text{и} \quad \theta_{x,y}(-l)=\theta_{y,x}(l) \ . (3.3)$$

Нетрудно также показать, что для бинарных последовательностей справедливо следующее равенство:

$$\sum_{i=0}^{v-1}\theta_{x,y}(l)=(\sum x)(\sum y).$$

В случае последовательностей типа Адамара оно преобразуется к виду:

$$\sum_{i=0}^{v-1}\theta_{x,y}(l)=1 \quad . (3.4)$$

Таким образом, при больших значениях v среднее значение $\theta_{x,y}(l)$ близко к нулю. Рассмотрим еще несколько полезных и имеющих широкое применение тождеств. Пусть **x, y** $\in \mathbf{C}^{v}$, где **C** – множество комплексных чисел, есть произвольные векторы, а x и y соответствующие им последовательности. Тогда

$$\sum_{i=0}^{v-1}\theta_{x,y}(l)\theta_{x,y}(l+n)^{*}=\sum_{i=0}^{v-1}\theta_{x}(l)\theta_{y}(l+n)^{*} \quad . (3.5)$$

Положив в (3.5) n=0 , получим

$$\sum_{i=0}^{v-1}\left|\theta_{x,y}(l)\right|^{2}=\sum_{i=0}^{v-1}\theta_{x,}(l)[\theta_{y}(l)]^{*} \quad . \qquad (3.6)$$

Это соотношение впервые было приведено в работах Голда и Столдера и Кана, опубликованных в середине 60-х годов. Очень важны и интересны приложения этих тождеств. Так с их помощью был найден ряд нижних границ, кроме того, они приводят к полезным алгоритмам и методам построения последовательностей. Обратимся к тождеству (3.5). Оно означает, что автокорреляционная функция последовательности $\theta_{x,y}$ совпадает с взаимно-корреляционной функцией последовательностей θ_x и θ_y. Пусть x и y – последовательности длины v с двухуровневой автокорреляцией. Тогда последовательность $\theta_{x,y}$ также имеет длину v и обладает двухуровневой автокорреляционной функцией.

Далее из соотношения (3.5) следует, что для всех последовательностей типа Адамара должно выполняться следующее корреляционное тождество

$$\sum_{i=0}^{v-1}\left|\theta_{x,y}(l)\right|^{2}=v^{2}+v-1 \quad . \qquad (3.7)$$

Из (3.7) следует, что для m и GMW последовательностей среднеквадратичное значение $\theta_{x,y}(\ )$ близко к 2^N и что, по меньшей мере, для одного значения l выполняется $\theta_{x,y}(l) > 2^{N/2}-1$. К сожалению, эта оценка оказывается довольно слабой. К этому вопросу мы еще не раз вернемся при исследовании корреляционных пиков последовательностей типа Адамара.

3.2. Метод изоморфных коэффициентов

Для оценки взаимокорреляционных свойств последовательностей часто используют пиковые значения их периодических (четных) взаимно-корреляционных функций (ПВКФ) и меандро-инвертированных (нечетных) взаимно-корреляционных функций (МИВКФ). В работе [57] предложен метод исследования корреляционных функций периодических двоичных последовательностей, строящихся на основе разностных множеств, который позволяет существенно ускорить расчет этих функций на компьютере. Этот метод основывается на возможности применения ко всем классам таких последовательностей понятий изоморфизма и немножителей, введенных первоначально для разностных множеств. Поскольку немножители называют еще изоморфными коэффициентами [58], данный метод исследования ПВКФ получил наименование метода изоморфных коэффициентов.

Пусть $\alpha=(\alpha_1, \alpha_2,\ldots,\alpha_v)$ и $b=(b_1, b_2,\ldots,b_v)$ есть последовательности длины $v= 2^N-1$, принадлежащие одному классу, и пусть t есть некоторое положительное целое, взаимно простое с v. Так как t по определению есть немножитель, то последовательности $a^t = (a_{i_1}, a_{i_2},\ldots, a_{i_v})$ и $b^t = (b_{i_1}, b_{i_2},\ldots, b_{i_v})$, где $i_k=(t(l-1)+1) \bmod v$ для всех $l = \overline{1,v}$, также будут принадлежать этому классу. Очевидно, что изоморфизм $t : \alpha \rightarrow \alpha^t$ является унитарным оператором в евклидовом пространстве R^v. В силу свойств этого оператора имеем:

$$(\alpha, b)=(\alpha^t, b^t) \ . \quad (3.8)$$

Обозначим спектр взаимной корреляции последовательностей α и b через S(α, b). Тогда согласно (3.8)

$$S(\alpha,\ b)=S(\alpha^t,\ b^t)\ .\ (3.9)$$

и, следовательно, имеет место равенство их корреляционных максимумов, т.е.

$$\max S(\alpha,\ b)=\max S(\alpha^t,\ b^t)\ .\ (3.10)$$

Применяя соотношение (3.10) к вычислению ПВКФ последовательностей из одного класса эквивалентности, получаем, что достаточно исследовать ПВКФ одной произвольно взятой последовательности со всеми оставшимися. Более того, используя результаты теории чисел [59], можно показать, что множество изоморфных коэффициентов, состоящее из представителей смежных классов приведенной группы T вычетов по модулю v по ее мультипликативной подгруппе H автоморфных коэффициентов (множителей), также является группой относительно операции умножения. Поэтому для любого немножителя t всегда найдется такой немножитель l, что $t \cdot l \equiv 1 \bmod v$. Отсюда получаем

$$\max\ S(\alpha, \alpha^t)=\max S(\alpha,\alpha^l)\ .\ (3.11)$$

Последнее означает, что число исследуемых пар последовательностей может быть уменьшено почти вдвое. Найденное свойство позволяет также значительно упростить процесс вычисления матрицы максимальных значений выбросов ПФКФ. Как следует из (3.9), строки этой корреляционной матрицы являются некоторыми различными подстановками любой произвольно выбранной строки. Однако в общем случае нельзя непосредственно по одной строке матрицы восстановить вид всей матрицы, так как для этого необходимо провести довольно трудоемкую работу по определению соответствия элементов исходной строки элементам остальных строк. Кроме того, возникают неудобства с запоминанием такой матрицы ввиду ее громоздкости. Тем не менее, все эти трудности можно избежать благодаря преобразованию корреляционной матрицы к одному из следующих видов:

1) когда каждая последующая строка этой матрицы является циклическим сдвигом предыдущей;
2) когда сама матрица состоит из циклических сдвигов некоторой совокупности u квадратных матриц порядка p<M, где up=M, а M – число всех изоморфных кодовых последовательностей, т.е. мощность. При этом строки образующих матриц также обладают циклическими свойствами.

При таком представлении, зная только первые строки образующих матриц и порядок их следования, можно довольно просто восстановить любую из строк корреляционной матрицы. Для доказательства этого среди множества различных изоморфных коэффициентов выберем коэффициент с максимально возможным порядком. Напомним, что под порядком изоморфного коэффициента t понимается наименьший, отличный от нуля, показатель степени l, для которого $t^l \bmod v$ является множителем. Не нарушая общности рассуждений, всегда можно выбрать t таким, что $t^l \equiv 1 \bmod v$.

Рассмотрим две возможные ситуации: l=M и l<M. В первом случае l совпадает с мощностью ансамбля. Поэтому на основе одной какой-нибудь произвольно выбранной последовательности с помощью изоморфных коэффициентов t, t^2,...t^{l-1} строим систему остальных последовательностей этого класса, присваивая каждой полученной последовательности порядковый номер i, где $1 \le i \le l$. Затем, расположив последовательности в порядке возрастания их номеров, вычислим первую строку корреляционной матрицы. В силу того, что $t^{l/2+i}\, t^{l/2-i} \equiv 1 \bmod v$, достаточно найти только первые $l/2+1$ ее значений. Рассмотрим теперь вторую строку корреляционной матрицы, состоящей из максимальных значений выбросов ПВКФ пар последовательностей: $(t,1), (t,t^2), \ldots,(t,t^{l-1})$. Нетрудно проверить, что данные пары последовательностей изоморфны следующим парам:
$(1, t^{l-1}), (1, 1), (1, t),\ldots,(1, t^{l-2})$. Последнее означает, что вторая строка является циклическим сдвигом вправо первой строки. Аналогично показывается, что третья строка является сдвигом второй строки и т.д. Ч.Т.Д.

Перейдем теперь к рассмотрению второго, более сложного и чаще встречающегося случая, когда максимальный порядок, взятый по всему множеству изоморфных коэффициентов, меньше M. Аналогично предыдущему также строим мультипликативную группу изоморфного коэффициента t_1 максимального порядка l_1. . Предположим, что существует такая мультипликативная группа изоморфного коэффициента t_2, не принадлежащего группе $\{t_1^i\}$ порядка l_2, что $l_1 l_2$=M. Тогда поступаем следующим образом. Присваиваем номер 1 любой произвольно выбранной кодовой последовательности класса и на ее основе с помощью изоморфных коэффициентов вида $t_1^k t_2^i$, где $0 \le k \le l_1-1$, $0 \le i \le l_2-1$, строим l_2 различных множеств, состоящих из l_1 упорядоченных последовательностей. Расположив упорядоченные таким образом последовательности по строкам и столбцам, получаем корреляционную матрицу K вида:

$$K=\begin{bmatrix} A_1 & A_{t_2} & A_{t_2^2}\dots & A_{t_2^{l_2-1}} \\ A_{t_2^{l_2-1}} & A_1 & A_{t_2} & A_{t_2^{l_2-2}} \\ \cdot & \cdot & \cdot & \cdot \\ A_{t_2} & A_{t_2^2} & \cdot & A_1 \end{bmatrix},$$

где $A_{t_2^i}$, $0 \le i \le l_2-1$, есть корреляционная матрица порядка $l_1 \times l_2$, столбцы которой соответствуют последовательностям вида t_1^k, а строки – последовательностям $t_1^k t_2^l$. При этом в силу построения строки матриц $A_{t_2^i}$ также обладают циклическими свойствами.

Заметим, что для случаев, когда M есть произведение большего числа сомножителей, построение производится аналогичным образом. Таким образом, получена простая процедура построения корреляционной матрицы по ее первой строке, позволяющая в M-1 раз ускорить расчет корреляционных параметров на компьютере.

В качестве иллюстрации сказанного рассмотрим построения корреляционной матрицы для последовательностей GMW длины v=63 и v=255. Эти последовательности (по одной из каждого ансамбля) приведены ниже.

Последовательность длины 63:

101000110101100110100011101000100000001111011100111101001011011.

Последовательность длины 255:

100001000010111110001011001000110101010110000101011101101111111100010011001111010111000100101100100011011100111000010001100010001111100111110111101010111110100100011101001000000110111110001100101110000101100100100110100100100000001010011011100001111011.

Для случая v=63 (M=6) выбираем изоморфный коэффициент t=5 порядка l=6. По исходной последовательности и множеству $\{5^i\}$, $1 \le i \le 5$, строим другие пять последовательностей ансамбля, которым присваиваем номера с 2-го по 6-ой. Так как l=M=6, то в соответствии с вышеизложенным корреляционная матрица K определяется ее первой строкой и имеет вид:

$$K=\begin{bmatrix} 63 & 15 & 23 & 15 & 23 & 15 \\ 15 & 63 & 15 & 23 & 15 & 23 \\ 23 & 15 & 63 & 15 & 23 & 15 \\ 15 & 23 & 15 & 63 & 15 & 23 \\ 23 & 15 & 23 & 15 & 63 & 15 \\ 15 & 23 & 15 & 23 & 15 & 63 \end{bmatrix}.$$

Легко проверить, что эта матрица полностью совпадает с корреляционной матрицей, полученной в результате вычислений обычным способом.

Для случая v=255 (M=16) в качестве изоморфного коэффициента, имеющего максимально возможный порядок, выбираем t_1=7 *с* l_1=8. Тогда t_2=-1 , а l_2=2, т.е. имеет место случай M= l_1 l_2. Поэтому для построения корреляционной матрицы K достаточно найти лишь первые строки двух матриц A_1 и A_{-1}. В результате расчетов получаем, что матрица $K=\begin{bmatrix} A_1 & A_{-1} \\ A_{-1} & A \end{bmatrix}$ имеет вид:

$$\begin{bmatrix}
255 & 47 & 47 & 63 & 63 & 63 & 47 & 47 & 31 & 31 & 63 & 63 & 95 & 63 & 63 & 31 \\
47 & 255 & 47 & 47 & 63 & 63 & 63 & 47 & 31 & 31 & 31 & 63 & 63 & 95 & 63 & 63 \\
47 & 47 & 255 & 47 & 47 & 63 & 63 & 63 & 63 & 31 & 31 & 31 & 63 & 63 & 95 & 63 \\
63 & 47 & 47 & 255 & 47 & 47 & 63 & 63 & 63 & 63 & 31 & 31 & 31 & 63 & 63 & 95 \\
63 & 63 & 47 & 47 & 255 & 47 & 47 & 63 & 95 & 63 & 63 & 31 & 31 & 31 & 63 & 63 \\
63 & 63 & 63 & 47 & 47 & 255 & 47 & 47 & 63 & 95 & 63 & 63 & 31 & 31 & 31 & 63 \\
47 & 63 & 63 & 63 & 47 & 47 & 255 & 47 & 63 & 63 & 95 & 63 & 63 & 31 & 31 & 31 \\
47 & 47 & 63 & 63 & 63 & 47 & 47 & 255 & 31 & 63 & 63 & 95 & 63 & 63 & 31 & 31 \\
31 & 31 & 63 & 63 & 95 & 63 & 63 & 31 & 255 & 47 & 47 & 63 & 63 & 63 & 47 & 47 \\
31 & 31 & 31 & 63 & 63 & 95 & 63 & 63 & 47 & 255 & 47 & 47 & 63 & 63 & 63 & 47 \\
63 & 31 & 31 & 31 & 63 & 63 & 95 & 63 & 47 & 47 & 255 & 47 & 47 & 63 & 63 & 63 \\
63 & 63 & 31 & 31 & 31 & 63 & 63 & 95 & 63 & 47 & 47 & 255 & 47 & 47 & 63 & 63 \\
95 & 63 & 63 & 31 & 31 & 31 & 63 & 63 & 63 & 63 & 47 & 47 & 255 & 47 & 47 & 63 \\
63 & 95 & 63 & 63 & 31 & 31 & 31 & 63 & 63 & 63 & 63 & 47 & 47 & 255 & 47 & 47 \\
63 & 63 & 95 & 63 & 63 & 31 & 31 & 31 & 47 & 63 & 63 & 63 & 47 & 47 & 255 & 47 \\
31 & 63 & 63 & 95 & 63 & 63 & 31 & 31 & 47 & 47 & 63 & 63 & 63 & 47 & 47 & 255
\end{bmatrix}$$

Во многих случаях множители разностных множеств и образованных на их основе последовательностей образуют мультипликативнью группу по модулю v. Это справедливо для многих классов последовательностей, в том числе для последовательностей Лежандра, Холла, а также m и GMW последовательностей. Покажем, что число целочисленных точек, в которых необходимо вычислить значения ПВКФ таких последовательностей может быть уменьшено с v до v_1, где v_1 есть число смежных эквивалентных классов, получаемых при разбиении полной системы вычетов по модулю v по мультипликативной группе H множителей разностного множества. Для доказательства этого утверждения воспользуемся теоремой Манна-Джонса о фиксирующем множителе разностного множества. Применительно к последовательностям на основе разностных множеств эта теорема утверждает существование такого циклического сдвига последовательности, который фиксируется каждым ее множителем. Обозначим этот сдвиг α. Тогда $\alpha^h=\alpha$, где $h\in H$. Очевидно, что если $b=\alpha^t$, то $b=b^h$. Можно показать, что для любого r взаимно простого с v справедливо равенство:

$$(\alpha_\tau\, b) = ((\alpha^r)_{\tau_1}\, b^r) \qquad , (3.12)$$

где $\tau\equiv\tau_1 r \bmod v$.

Отсюда следует, что $(\alpha_\tau\ b) = (\alpha_{\tau_1}\ b)$ для всех $\tau_1 \equiv \tau h \bmod v$ и $\forall h \in H$. Таким образом, мы доказали, что значения ПВКФ достаточно вычислять не во всех точках (сдвигах), а только в тех, которые являются представителями классов смежности, полученных при разбиении полной системы вычетов по модулю v по мультипликативной группе H.

В качестве примера рассмотрим вычисление ПВКФ последовательностей символов Лежандра. Эти последовательности существуют для всех простых чисел вида v=4t-1 и имеют M=2. Из свойств последовательностей Лежандра следует, что их множители совпадают с множеством квадратичных вычетов по модулю v, при этом порядок группы H равен (v-1)/2. Поэтому, разбив числа от 0 до v-1 на смежные классы по множеству H, в итоге получим три смежных класса, представителями которых являются элементы {0}, {1} и {-1}. В результате число точек, в которых достаточно вычислять значения ПВКФ, может быть уменьшено с v до 3. Ниже будет показано, что спектр взаимной корреляции последовательностей Лежандра может быть найден аналитически. Аналогичным образом можно показать, что число точек, необходимых для расчета ПВКФ последовательностей Холла, равно 7. Это, безусловно, не означает, что число различных значений в корреляционном спектре в точности равно числу классов смежности. Оно может быть и меньшим как, например, в случае трехуровневых m-последовательностей.

3.3. Взаимно-корреляционные пики m-последовательностей

Численные исследования показали, что в целом ансамбль m-последовательностей обладает плохими ПВКФ [20]. Это связано с существованием пар, пиковые значения взаимной корреляции которых достаточно велики и могут достигать одной трети от ее длины. На практике для улучшения взаимной корреляции обычно производится просеивание "плохих" пар, в результате чего получается меньшее множество последовательностей с приемлемыми ПВКФ. Наряду с численными методами расчета ПВКФ, в настоящее время

большое распространение получили также и аналитические, основанные на связи m-последовательностей с конечными полями Галуа. В общем случае эта связь выражается формулой:

$$b_j=L(\alpha^j) \quad , \quad (3.13)$$

где L - линейный функционал из $GF(2^N)$ в GF(2), $0\leq j<2^N-1$, а α - примитивный элемент $GF(2^N)$. В качестве линейного функционала наиболее часто используется след элемента $z\in GF(2^N)$ в GF(2),определяемый выражением [4]:

$$tr_2^{2^N}(z)=\sum_{i=0}^{N-1} z^{2^i} \quad . \quad (3.14)$$

По теореме, обобщенная формулировка которой приведена в [20], ПВКФ m-последовательностей, связанных между собой либо децимацией 2^t+1, либо $2^{2t}-2^t+1$, взаимно простыми с 2^N-1, где N не есть степень 2, а $1<t<N/2$ и e=(N,t) такие, что N/e - нечетно, является трехуровневой с максимальным абсолютным значением взаимной корреляции

$$P_{max}=2^{(N+e)/2}+1 \quad . \quad (3.15)$$

В случае же $N\equiv \bmod 4$ и децимации $2^{(N+2)/2}-1$ максимальное значение взаимной корреляции составляет

$$P_{max}=2^{(N+2)/2}-1 \quad . \quad (3.16)$$

На практике широко используются так называемые предпочтительные пары m-последовательностей с e=1 для нечетных N и e=2 для четных N, образующие ПСП Голда. Заметим, что на практике широко используются так называемые предпочтительные пары m-последовательностей с e=1 для нечетных N и e=2 для четных N, образующие ПСП Голда.

В 1976г. норвежский математик Т. Хелесев опубликовал статью [60], в которой доказал, что в случае $N \equiv 0 \bmod 2$ ПВКФ m-последовательностей, связанных децимациями $d=(2^N-1)/3+2^i$, где i равно 0 или 1, является 6-ти уровневой с максимальным значением

а) $P_{max}=(2^N+2^{N/2})/3$, если N кратно 3 и не кратно 4;

б) $P_{max}=(2^N+2^{N/2+2})/3$, если N не кратно 3 и 4; . (3.17)

в) $P_{max}=(2^N+2^{N/2+1})/3$, если N кратно 4;

Выражение (3.17) можно принять в качестве аналитической нижней границы максимума взаимной корреляции класса m-последовательностей (другой вопрос насколько эта граница наибольшая).

Как показывает практика, для подавляющего числа приложений требуются не пары, а большие подмножества m-последовательностей, отобранные по результатам компьютерного расчета их ВКФ. Свое дальнейшее развитие эта задача получила в работе А. Тиркеля [61], где на основе конечных полей и статистических свойств m-последовательностей предложена концепция, устанавливающая зависимость между пиковыми значениями взаимной корреляции m-последовательностей и их децимациями. Согласно этой концепции сверхбольшими пиками взаимной корреляции обладают пары, связанные децимациями вида:

$$d_r = \frac{r(2^N-1)+p_i}{p_i} \quad , \quad (3.18)$$

где $0 < r < p_i$, $0 < i \le q$, а $2^N - 1 = \prod_{i=1}^{q} p_i$ - есть факторизация 2^N-1. Кроме того, должно выполняться $(2^N-1, d_r)=1$. Нетрудно убедиться, что децимации вида (3.18) обладают свойством оставлять на месте ровно $2^N-1/p_i$ элементов исходной последовательности. На этом основании с учетом статистических свойств m-последовательностей в [61] делается вывод, что, во-первых, наибольшее пиковое значение ПВКФ, взятое по всему ансамблю m-

последовательностей по знаку всегда положительно, а, во-вторых, оно может быть оценено величиной

$$\Theta_b = 2^N - 1/p_u \quad , \quad (3.19)$$

где $p_u = \min\{p_i\}$, со среднеквадратичным отклонением от нее $[(2^N-1)(p_u-1)/p_u]^{1/2}$. Заметим, что оценка (3.19) применима не ко всем m-последовательностям, а только к тем, у которых длина есть составное число. В [61] приведена также таблица с результатами компьютерного расчета пиков ПВКФ m-последовательностей для $3 \le N \le 17$. Предпринятая нами с целью устранения возможных неточностей компьютерная проверка этих результатов полная для $3 \le N \le 15$ и выборочная для N=16 выявила ошибки в пиковых значениях для случаев N=4 и N=15 (отметим, что в последующей работе А. Тиркеля эти ошибки были исправлены). В таблице 3.1 приведены скорректированные значения этих пиков, а также Θ_b для $3 \le N \le 17$. И хотя приведенные в таблице 3.1 значения пиков в целом согласуются с предсказанной оценкой (3.19), нельзя не заметить и случаев, когда это не так. Во-первых, при N=11 имеется более чем трехкратное превышение реальным пиком его ожидаемого значения. Во-вторых, при n=9 пиковое значение, взятое со знаком, равно -113 и обнаруживается при децимациях отличных от (3.18). И если случай N=11 еще может быть объяснен значительной статистической флуктуацией, то наличие пика с отрицательным знаком при децимации отличной от (3.18) противоречит сделанному в [61] предположению о положительном знаке пика. Выход из этого может состоять в отказе от утверждения об обязательно положительном знаке корреляционного пика, а все отклонения от оценки (3.19) считать результатом действия статистических флуктуаций. Ни в какой мере не умаляя значения оценки (3.19), остановимся на некоторых ее принципиальных недостатках, обусловленных особенностями статистического подхода. Первое, на что следует обратить внимание, статистическая оценка не может полностью исключить возможность флуктуаций, в результате которой на месте предсказуемого пика обнаружится пик с совершенно иным

значением, а то и вовсе его отсутствие, как это имеет место при N=9. Другими словами, полученная оценка имеет вероятностный характер и не может считаться полностью достоверной. Поэтому принять ее в качестве новой нижней границы максимума взаимных корреляций для всего класса m-последовательностей, строго говоря, нельзя. Во-вторых, будучи инвариантной к любым случайным последовательностям, оценка (3.19) не учитывает структурной специфики псевдослучайных последовательностей, которые по своей природе, как известно, являются строго детерминированными последовательностями. Напротив, выражение (3.17), полученное в результате представления m-последовательностей посредством следов в полях Галуа, эту специфику учитывает. Однако, как следует из [60], это выражение справедливо только для случая четных N и p_i=3. В качестве альтернативы в настоящей работе предлагается подход, основанный на структурных свойствах m-последовательностей, связанных децимацией (3.18). В соответствие со свойством декомпозиции [45] m-последовательность с N=mk, m≥2, k≥2 может быть представлена в виде двумерной таблицы из $w=2^m-1$ столбцов и $\varepsilon=2^N-1/w$ строк. При этом каждая строка является либо некоторым сдвигом более короткой m-последовательности длины 2^m-1 либо строкой из одних нулей. Нетрудно подсчитать, что число нулевых строк всегда равно $\varepsilon-2^{N-m}$. Пусть $2^N-1=\prod_{i=1}^{q} p_i$ есть факторизация 2^N-1, а $p_u=\min_i\{p_i\}$. Пусть $l=\max_j\{l_j\}$, где $1<l_j<N$, $l_j|N$ и $p_u\left|(2^N-1)/(2^{l_j}-1)\right.$. Рассмотрим декомпозиции m-последовательностей $\{a_i\}$ и $\{b_i\}$, связанных децимацией (3.18), где $1\le r<N$ при условии $m=l$. Тогда $\varepsilon=2^N-1/2^l-1$ и, следовательно, $p_u|\varepsilon$. Очевидно, что при децимации (3.18) ε/p_u строк последовательности $\{a_i\}$ с номерами $0,p_u,2p_u,\ldots,\varepsilon-p_u$ останутся на своих местах. А так как за счет выбора соответствующего сдвига последовательности $\{a_i\}$ строку с номером 0 всегда можно сделать ненулевой, то все ненулевые строки в декомпозиции $\{b_i\}$ окажутся сдвигами этой строки. Полагая далее остальные $\varepsilon(p_u-1)/p_u$ строк не совпадающими, находим, что смещение пика ПВКФ от его

среднего значения $(2^N-1)/p_u$ влево не может быть более чем на $\varepsilon(p_u-1)/p_u$. Таким образом, мы доказали следующую теорему [62].

Теорема 3.1.

Пусть $2^N-1=\prod_{i=1}^{q} p_i$ есть факторизация 2^N-1. Пусть $l=\max_j\{l_j\}$, где $1<l_j<N$, $l_j|N$ и $p_i|(2^N-1)/(2^{l_j}-1)$. Пусть $\Theta_c(m)$ есть пиковое значение ПВКФ класса m-последовательностей. Тогда

$$\Theta_c(m)\geq\hat{\Theta}_c \quad , \quad (3.20)$$

где $$\hat{\Theta}_c=\frac{2^N-1}{p_i}-\frac{(2^N-1)}{(2^l-1)}\frac{(p_i-1)}{p_i} \quad . \quad (3.21)$$

Очевидно, что оценку (3.21) можно использовать только при $(2^l-1)/p_i > 2$.Анализ показывает, что при $p_u=\min\{p_i\}$ $\hat{\Theta}_c$ имеет наибольшее значение и для нечетных N является наибольшей нижней границей максимального значения корреляционного пика, взятого по всему классу m-последовательностей. Можно показать, что когда N четно и не кратно 3, то $p_u=3$, а 2^N-1 не кратно 9. В этом случае d_r принимает единственное значение: $(2^N-1)/3+1$ или $2(2^N-1)/3+1$. В результате получаем следующее полезное для практических приложений следствие.

Следствие 3.1.

Пусть N четно, не кратно 3 и удовлетворяет условиям Теоремы 3.1. Тогда все множество m-последовательностей может быть разбито на два не пересекающихся равномощных подмножества, связанных между собой децимацией (3.18) .

Проиллюстрируем данное следствие на примере m-последовательностей значности 2^{14}-1=16383. В этом случае мощность M=756, d_r=5461 и $\Theta_c(m)$=5631. Разделим пары, связанные децимацией 5461 (а таких ровно 378), на два подмножества. В результате каждое

будет содержать по 378 последовательностей с пиковым значением 897. Это всего лишь в 3,5 раза превышает аналогичное значение для последовательностей Голда, обладающих худшими автокорреляционными функциями. Расчеты показывают, что при $p_i > p_u$ также могут существовать пары последовательностей со сверхвысокими пиками взаимной корреляции. Например, при N=12, m=6 и p_i =5 все пары последовательностей с децимациями 1639, 2458 и 3277 имеют корреляционный пик $\Theta_c \geq \hat{\Theta}_c = 769$; при N=18, m=9, p_i=19 и d_r=13798 $\Theta_c \geq \hat{\Theta}_c$ =13311; при N=20, m=10, p_i=5 и d_r=209716 $\Theta_c \geq \hat{\Theta}_c = 209919$.

Выражение (3.21) было получено в предположении минимального вклада в корреляционный пик строк с некратными p_u номерами. Очевидно, что это крайний, граничный случай. Если же исходить из равновероятности сдвигов в ненулевых строках декомпозиции, то реально пиковое значение будет больше. Более того, по меньшей мере, p_u сдвигов между последовательностями $\{a_i\}$ и $\{b_i\}$ приводят к совпадению ε/p_u строк их декомпозиций. А по Теореме 3.1 каждый такой пик должен быть не менее $\hat{\Theta}_c$. Следовательно, Теорема 3.1 гарантирует существование, по меньшей мере, p_u пиков со значениями $\geq \hat{\Theta}_c$. В таблице 3.1 приведены полученные в соответствие с формулой (3.21) значения $\hat{\Theta}_c$ для N=6, 10, 12, 14, 15. Кроме того, в таблице приведены значения корреляционных пиков последовательностей с децимациями (5) для N=18 (p_u=3) и N=21 (p_u=7). И хотя $\hat{\Theta}_c$ оказывается дальше от истинного значения пика, чем Θ_b, тем не менее, это совершенно достоверное значение. Причем для случаев N=6, 10, 14 граница $\hat{\Theta}_c$ даже совпадает со значениями некоторых вычисленных на компьютере сверхвысоких пиков. К сожалению, предлагаемый структурный метод неприменим для случаев $N=p^t$, где p-простое, а $t \geq 1$-целое число, так как не выполняются условия Теоремы 3.1.

3.4. Взаимно-корреляционные пики последовательностей GMW

Как уже отмечалось выше, в качестве базисных последовательностей при построении ПСП GMW, кроме m-последовательностей, могут быть также выбраны любые другие идеальные ПСП, в том числе ПСП Холла, Лежандра, ПСП GMW меньшей значности, последовательности Бомера-Фридриксена [14] и др. Очевидно, что описанный выше структурный подход может быть распространен также и на классы ПСП GMW. Согласно [21,22,63] для построения ПСП GMW в декомпозиции m-последовательности с параметрами $w=2^m-1$ и $\varepsilon=2^N-1/w$, где $N=mk$ и $m\geq 3$, $k\geq 2$, необходимо все нулевые строки, являющиеся сдвигами некоторой более короткой m-последовательности длины w, заместить на строки с теми самыми сдвигами, но уже другой базисной последовательности. Причем эта базисная последовательность должна удовлетворять следующим двум условиям:

- обладать двухуровневой ПАКФ;
- не являться никаким сдвигом замещаемой короткой m-последовательности.

Строки же, состоящие из одних нулей, остаются без изменения. И хотя данный метод в силу его сложности на практике не применяется, он оказывается весьма эффективным при анализе ПВКФ последовательностей с описанной выше структурой. Действительно, из алгоритма построения ПСП GMW следует, что для всех N_s удовлетворяющим условиям теоремы 3.1 при $m=l_j$, $\Theta_{d_r}(g)=\Theta_{d_r}(m)$, где $\Theta_{d_r}(g)$ и $\Theta_{d_r}(m)$ соответственно значения пиков ПВКФ пар ПСП GMW и m-последовательностей при децимации (3.18). Этот результат может быть сформулирован в виде следующей теоремы [62].

Теорема 3.2.

Пусть $N\geq 6$ составное число, удовлетворяющее условиям Теоремы 3.1, а $\Theta_c(g)$ есть пиковое значение ПВКФ класса ПСП GMW с параметрами $w=2^{l_j}-1$ и $\varepsilon=2^N-1/w$. Тогда

$$\Theta_c(g)\geq\hat{\Theta}_c \quad , \quad (3.22)$$

где $\hat{\Theta}_c$ определяется выражением (8) и $\Theta_{d_r}(g)=\Theta_{d_r}(m)$.

Следствие 3.2.

Пусть N четно, не кратно 3 и удовлетворяет условиям теоремы 3.1. Тогда любой класс ПСП GMW можно разбить на два не пересекающихся равномощных подмножества, связанных между собой децимацией (3.18) при $p_i=3$.

На компьютере были исследованы ПВКФ ПСП GMW для всех $6\le N\le 15$ и некоторые для N=16. Результаты этих вычислений приведены в таблице 3.2. При этом рассматривались все возможные классы ПСП GMW [14], а пары последовательностей выбирались только в пределах одного и того же класса. Исследования показывают, что для N=6, 8,10, 12, 14 и 15 имеет место равенство $\Theta_c(g)=\Theta_{d_r}(g)$, т.е. пиковое значение всецело определяется децимацией d_r. Очень вероятно, что это может быть справедливо и при больших значениях N. При рассмотрении Таблицы 3.2 особо следует выделить случай N=12 с m=3, 4, 6, для которых $\Theta_c(g)$ имеет одно и то же значение, равное 1407. То, что это так, когда m=3 или 4, следует непосредственно из Теоремы 2. Для случая m=6 условия Теоремы 3.2 не выполняются. Однако вследствие того, что сами строки в декомпозициях последовательностей $\{a_i\}$ и $\{b_i\}$ в свою очередь представимы в виде декомпозиций с параметрами w=7 и ε=9 на базе одной и той же последовательности длины 7, результат оказывается таким же, как для m=3. Неприменима также Теорема 3.2 и для случаев N=8, 9 и 16, хотя то, что при N=8, 16 имеет место $\Theta_{d_r}(g)=\Theta_{d_r}(m)$, вряд ли можно считать результатом простого совпадения. Другим итогом проделанных расчетов является вывод, что пики ПВКФ ПСП GMW при других децимациях ведут примерно так же, как в случае m-последовательностей. В качестве иллюстрации рассмотрим класс ПСП GMW значности $2^{14}-1=16383$, представителем которого является последовательность, сформированная на

основе характеристического полинома $x^{14}+x^{13}+x^{11}+x^{9}+1$ и базисной последовательности класса Бомера-Фридриксена длины 127 [64,65] вида:

“01111010110111010000101101001000000111101000110010001110101011111111100100110100111101100100101010110011110001100001100010001000”.

Исследования показывают, что этот класс может быть разбит на 6 подмножеств из 126 последовательностей, имеющих одни и те же взаимно-корреляционные матрицы с $\Theta_c(g)$=815, тогда как равномощный класс m-последовательностей при аналогичном разбиении содержит подмножества с $\Theta_c(m)$=897.

Декомпозиционный метод может оказаться также весьма полезным и при анализе межклассовых ПВКФ ПСП GMW. Очевидно, что в этом случае нижняя граница максимума взаимной корреляции будет определяться как числом совпадающих нулевых строк, так и корреляционными параметрами самих базисных последовательностей, подставляемых в одну и ту же декомпозицию исходной m-последовательности.

Сформулируем теперь следующие важные утверждения, касающиеся спектров взаимной корреляции рассматриваемых последовательностей при децимации (3.18) [66].

Утверждение 3.1.

Спектры взаимной корреляции m-последовательностей с децимацией (3.18) при N, удовлетворяющих условиям Теоремы 3.1, совпадают со спектрами взаимной корреляции последовательностей GMW с той же децимацией.

Доказательство этого утверждения основывается на следующем:

- совпадении ПВКФ пар m-последовательностей с децимацией (3.18) с ПВКФ пар последовательностей GMW, образованных на основе тех же самых примитивных многочленов, что и эти m-последовательности;
- равенстве спектров взаимной корреляции любых пар m-последовательностей (последовательностей GMW) с одной и той же децимацией.

Утверждение 3.2.

Значения взаимной корреляции $\theta_{x,y}(i)$ m-последовательностей (последовательностей GMW) x и y, связанных децимацией (3.18) при всех N, удовлетворяющих условиям Теоремы 3.1, определяются выражением:

$$\theta_{x,y}(i)=u_i 2^m - (2^N-1)/(2^m-1) \quad , (3.23)$$

где u_i - положительное целое или нуль.

Для доказательства рассмотрим декомпозиции последовательностей x и y. В силу построения ненулевые строки их декомпозиций являются сдвигами друг друга. Предположим, что при i-ом сдвиге у этих последовательностей совпадает u_i строк. Тогда число несовпадающих строк равно $(2^N-1)/(2^m-1)- u_i$. Отсюда, имеем:

$\theta_{x,y}(i)=u_i (2^m-1)- (2^N-1)/(2^m-1)- u_i = u_i 2^m - (2^N-1)/(2^m-1)$. Ч.Т.Д.

Согласно теоремам 3.1 и 3.2 при i=0, по меньшей мере, $(2^N-1)/p_i(2^m-1)$ строк их декомпозиций должны совпадать. Обозначим через v_0 число дополнительных совпадений. Тогда $\theta_{x,y}(0)= [(2^N-1)/p_i(2^m-1) +v_0] 2^m - (2^N-1)/(2^m-1)$. Нетрудно убедиться, что существуют еще pi-1 сдвигов вида $j (2^N-1)/p_i$, где $0<j<p_i$, при которых также имеет место совпадение $(2^N-1)/p_i(2^m-1)$ строк. Таким образом, мы доказали следующее утверждение.

Утверждение 3.3.

Для пар m-последовательностей и последовательностей GMW, связанных децимациями (3.18) при N, удовлетворяющих условиям Теоремы 3.1, существует p_u взаимно-корреляционных пиков вида

$$\theta_{x,y}(j (2^N-1)/p_i)= [(2^N-1)/p_i(2^m-1) +v_j] 2^m - (2^N-1)/(2^m-1) \quad , (3.24)$$

равно отстоящих один от другого на $(2^N-1)/p_i$ сдвигов. Здесь $0\leq j<p_i$, а v_j - положительное целое или нуль.

Проиллюстрируем сказанное на примерах. При этом будем рассматривать случаи, когда $p_i=p_u$. Пусть N=10 и $p_i=3$. Тогда в силу (3.23) и (3.24) имеем: $\theta_{x,y}(i)=32u_i - 33$ и

$\theta_{x,y}(343j)=319 + 32v_j$, где $0<j<3$. С другой стороны, согласно численным расчетам $\theta_{x,y}(i)$ имееет 6-ти уровневый спектр взаимной корреляции со значениями –33, -1, 31, 63, 319 и 383 и распределением пиков взаимной корреляции: $\theta_{x,y}(0)=319$, $\theta_{x,y}(341)=383$ и $\theta_{x,y}(682)=319$.

Пусть N=14 и $p_i=3$. Тогда $\theta_{x,y}(i)=128u_i - 129$ и $\theta_{x,y}(5461j)=5375 + 128v_j$, где $0<j<3$.

Расчеты показывают, что и в этом случае спектр взаимной корреляции будет 6-ти уровневый со значениями: –129, -1, 127, 255, 5375 и 5631. Причем корреляционные пики принимают значения: $\theta_{x,y}(0)=5375$, $\theta_{x,y}(5461)=5375$ и $\theta_{x,y}(10922)=5631$.

Рассмотренные примеры демонстрируют хорошую согласованность теоретических и практических результатов. Отметим, что корреляционные спектры m-последовательностей для четных N и $p_i=3$ получены Т. Хеллесофом в работе [60].

В заключении сделаем одно важное замечание, касающееся поиска пиковых значений взаимной корреляции. Исследования показали, что при $p_i>p_u$ также могут существовать пары последовательностей со сверхвысокими пиками взаимной корреляции, правда, меньшими, чем при p_u. Соответствующие децимации и оценки находятся подстановкой в формулы (3.18) и (3.21) значения p_i вместо p_u . Так, например, для N=20 такие пики имеют место при $p_u=3$, 5, 11 и 41. Сответственно их значения будут больше или равны: 326975, 208895, 64575 и 24575.

3.5. Взаимная корреляция последовательностей Холла и Лежандра

Класс ПСП Холла имеет следующие параметры [43]:

$$p=4m^2+27,\ w=2m^2+13,\ d_x=2m^2+14,\ \rho=-1,\ M=6 \quad ,(3.25)$$

где p-значность ПСП(p-простое число),w-вес ПСП, d_x-хэммингово расстояние ПСП от ее циклических копий, ρ - неглавное значение ненормированной ПАКФ. При этом мощность класса ПСП Холла не зависит от p и всегда равна шести. Для определения наибольшей аналитической нижней границы максимума ПВКФ множества ПСП Холла воспользуемся найденным в [62] расстоянием по Хэммингу между этими ПСП:

$$d_{ПВКФ}=d_{ЭЛЕМ}(2m^2+13)/3 \quad , \quad (3.26)$$

где $d_{ЭЛЕМ}$ - расстояние по Хэммингу между ПСП в пределах каждой элементарной группы из шести чисел с последовательно возрастающими степенями первообразного корня g. Наименьшее $d_{ЭЛЕМ}=2$ (см. таблицу 2 работы [67]) дает наибольшую нижнюю границу $\hat{\Theta}_c(H)$ для максимума ПВКФ ПСП Холла. В итоге получаем

$$\hat{\Theta}_c(H)=p-2d_{ПВКФ}=4m^2+27-4(2m^2+13)/3=(4m^2+29)/3=p/3+2/3 \; . \; (3.27)$$

В таблице 3.3 представлены параметры класса ПСП Холла вместе со значениями $\hat{\Theta}_c(H)$. Сравнение Таблицы 3.1 с таблицей 3.3 показывает полное совпадение значений $\hat{\Theta}_c(H)$ с $\Theta_c(m)$ при p=31, что не удивительно, так как в этом случае m-последовательности и ПСП Холла совпадают. В результате проведенных расчетов было установлено, что при p=31,43 и 127 реальные пики ПВКФ совпадает со значением $\hat{\Theta}_c(H)$, т.е. найденная нижняя граница для этих случаев является также и верхней. Но если при значности 127 в классе m-последовательностей можно выделить так называемое максимально связанное подмножество из 6 последовательностей с $\Theta_c(m)=17$, то в классе ПСП Холла нет ни одной пары со значением пика меньшим 41. Еще меньшую мощность (равную двум) имеет класс ПСП Лежандра значности p, где p=4m-1 простое число. Известно [43], что символы ПСП Лежандра, за исключением нулевого, связаны между собой равенством

$$\left(\frac{i}{p}\right)=-\left(\frac{p-i}{p}\right), \text{ где}$$

$$\left(\frac{i}{p}\right)=\begin{cases} 1, \text{если i есть квадратичный вычет по mod p} \\ -1, \text{если i есть квадратичный невычет по mod p} \; . \end{cases}$$

Это равенство устанавливает зеркально-инверсную симметрию символов этих двух последовательностей. С помощью его получаем следующее точное выражение для пика ПВКФ ПСП Лежандра [62]:

$$\Theta_c(L)=2\text{-}p \quad , \qquad (3.28)$$

справедливое при всех возможных значениях p. Используя свойство зеркально-инверсной симметрии можно также доказать, что кроме одиночного пика 2-р ПВКФ может принимать еще только два значения +3 и -1, являясь, таким образом, трехуровневой. Это полностью подтверждается расчетами ПВКФ, выполненными для всех p≤127. Очевидно, что наличие сверхвысокого пика является существенным препятствием для совместного использования этих последовательностей.

Таблица 3.1.

Значения пиков взаимной корреляции m-последовательностей.

N	2^N-1	Множители	M	p_i	$\Theta_c(m)$	Θ_b	$\hat{\Theta}_c$
3	7	—	2	—	-5	—	—
4	15	3*5	2	3	+7	5	—
5	31	—	6	—	+11	—	—
6	63	$3^2$7	6	3	+23	21	15
7	127	—	18	—	+41	—	—
8	255	3*5*17	16	—	+95	85	—
9	511	7*73	48	—	-113	73	—
10	1023	3*11*31	60		+383	341	319
11	2047	23*89	176	—	+287	89	—
12	4095	3^2*5*7*13	144	3	+1407	1365	1183
13	8191	—	630	—	+703	—	—
14	16383	3*43*129	756	3	+5631	5461	5375
15	32767	7*31*151	1800	7	+4927	4681	3775
16	65535	3*5*17*257	2048	—	+22015	21845	—
17	131071	—	7710	—	+5951	—	—
18	262143	3^3*7*19*73	7776	3	≥87551	87039	87039
21	2097151	7*127*2359	84672	7	≥ 300159	299593	285439

2^N-1 - значность m-последовательностей;

M - Мощность класса m-последовательностей;

$\Theta_c(m)$ - пиковое значение ПВКФ со знаком ;

Θ_b - статистическая оценка (3.19);

$\hat{\Theta}_c$ - нижняя граница максимума ПВКФ.

Таблица 3.2.

Значения пиков взаимной корреляции последовательностей GMW.

N	m	K	M	P(m,k)	$\Theta_c(g)$	$\hat{\Theta}_c$
6	3	2	6	1	+23	15
8	4	2	16	1	+95	85
9	3	3	48	1	+149	—
10	5	2	60	7	+383	319
12	3	4	144	1	+1407	1183
12	4	3	144	1	+1407	1183
12	6	2	144	11	+1407	—
14	7	2	756	79	+5631	5375
15	5	3	1800	7	+4927	3775
15	3	5	1800	1	+4927	—
16	8	2	2048	63	≥ 22015	—
18	9	2	7776	239	≥87551	87039
21	7	3	84672	79	≥ 300159	285439

P(m,k) - число различных классов при заданных m и k;

$\Theta_c(g)$ - пиковое значение ПВКФ ПСП GMW.

Таблица 3.3.

Значения пиков взаимной корреляции последовательностей Холла.

m	P	$\hat{\Theta}_c$ (H)
1	$2^5-1=31$	11
2	43	15
5	$2^7-1=127$	43
7	223	75
8	283	95
14	811	271
16	1051	351
19	1471	491
20	1627	543
23	2143	715
26	2731	911
28	3163	1055
29	3391	1131
34	4651	1551
37	5503	1835
181	$2^{17}-1=131071$	43691

p - значность ПСП Холла;

$\hat{\Theta}_c$ (H) - нижняя граница максимума ПВКФ ПСП Холла.

3.6. Последовательности значности 127

Для систем связи с многостанционным доступом с кодовым разделением каналов (CDMA) требуется, чтобы используемые в них кодовые последовательности имели малые значения автокорреляционных и взаимно-корреляционных функций. Среди двоичных псевдослучайных последовательностей значности 127 наиболее известны m-последовательности и ПСП Голда, корреляционные свойства которых достаточно подробно исследованы в [20]. Однако при значности N=127 существует еще много других классов ПСП [64,65], имеющих такие же близкие к идеальным ПАКФ, что и m-последовательности. К ним относятся ПСП на основе различных классов совершенных разностных множеств с параметрами v=127, k=63, λ=31 [45,64,65], для которых все неглавные значения ПАКФ равны $\theta = v - 4(k-\lambda) = -1$.

Компактная запись совершенных разностных множеств с параметрами v=127, k=63, λ=31 приведена в таблице 3.4. Здесь буквами A, B, C обозначены классы разностных множеств Бомера-Фридриксена [33], а буквами S, L, H соответственно разностные множества Зингера, Лежандра и Холла.

Единицами в соответствующей строке отмечены те вычеты α_j в первой строке таблицы, которые участвуют в образовании соответствующего данной строке множества по правилу $\alpha_j\ 2^i$, $0 \le i \le 6 \bmod 127$. Коэффициентов α_j всегда 9 для любого множества и они образуют $k=9\cdot 7=63$ вычета. Все 18 изоморфных множеств каждого эквивалентного класса образуются последовательным умножением на первообразный корень 3 mod 127 по правилу $\{\alpha_j\}3^k$, $1 \le k \le 18$, кроме множества Холла, которое имеет только 6 изоморфных множеств $\{\alpha_j\}3^k$, $1 \le k \le 6$. Множество Лежандра образуется по простому правилу $\alpha_j \equiv 9^i$, $0 \le i \le 62 \bmod 127$ и имеет только два изоморфных множества – прямое и обратное.

Таблица 3.4.

Разностные множества (127,63,31).

	ВЫЧЕТЫ α_j														
	5	7	9	11	13	15	19	21	23	27	29	43	47	55	63
S		1			1	1	1	1	1				1	1	1
H	1		1	1				1		1	1	1		1	1
	5	7	9	11	13	15	19	21	23	27	29	43	47	55	63
A			1	1	1		1	1		1	1		1		1
B				1	1	1	1	1	1		1			1	1
C			1		1	1		1	1		1	1		1	1

Таким образом, существуют 2 изоморфных разностных множеств Лежандра, 6 изоморфных разностных множеств Холла и по 18 изоморфных разностных множеств в каждом из классов Зингера, A, B и C, т.е. всего 80 множеств. Псевдослучайные последовательности двоичных символов "1" и "0" образуются записью символов "0" на позициях, соответствующих по номеру вычетам разностных множеств, и записью символов "1" на всех остальных (127-63)=64 позициях. Образованные таким способом ПСП классов A, B, C известны еще как последовательности Бомера-Фридриксена. При этом m-последовательности являются последовательностями класса Зингера.

Интересно, что в отличие от класса S ПСП классов L, H, A, B и C не линейны и имеют линейную сложность, превышающую линейную сложность m-последовательностей значности 127, для которых она равна 7. Поэтому довольно привлекательным может быть использование этих ПСП в качестве базисных для генерации ПСП GMW. Действительно, линейная сложность у образуемых на их основе ПСП GMW, как показано в разделе 2.6, в

целом оказывается больше, чем у ПСП GMW на основе базисных m-последовательностей. К тому же применение ПСП классов L, H, A, B, C в качестве базисных для генерации ПСП GMW длины 2^{7J}-1, где J≥2, приводит к существенному увеличению общего числа ПСП GMW.

ПСП символов Лежандра – ПСП L

ПСП L образуют самый маломощный класс ПСП с двухуровневой ПАКФ из двух ПСП (прямой и обратной), символы которых обладают свойством зеркально-инверсной симметрии. С помощью этого свойства было получено следующее точное выражение для пикового значения ПВКФ ПСП L

$$\theta_c = \text{v-2} \quad , \qquad (3.29)$$

где v – значность ПСП.

Так, например, для v=127, θ_c=125. Отсюда приходим к выводу о нежелательности совместного использования этих двух ПСП в системах CDMA. С другой стороны, компьютерный анализ показал, что среди всех известных 80-ти ПСП с двухуровневыми ПАКФ ПСП L обладают наилучшими корреляционными параметрами автооптимальности (АО), в смысле [8].

Действительно, для них существует такой АО-сдвиг, при котором пиковое значение нечетной (меандро-инвертированной) АКФ равно $\hat{\theta}_{AO} = 13$, а энергия боковых лепестков S [8] равна 1491. Другой не менее важной по значимости особенностью ПСП L является их ВКФ с ПСП S. На компьютере были получены результаты, по которым пиковые значения ПВКФ ПСП L с m-последовательностями (класс ПСП S) для одной половины ПСП S составляет 17, а для другой - соответственно 19. Это обстоятельство делает возможным сформировать множество из семи последовательностей, состоящее из 6-ти ПСП S максимального связного множества и одной ПСП L с пиковым значением θ_c=19, причем в

85% случаях это значение равно 17. Здесь уместно заметить, что произвольное множество ПСП S периода 127 из 7-ми и более ПСП характеризуется сравнительно большим пиковым значением взаимной корреляции θ_c=41. Аналогичные расчеты были также проведены для нечетных ПВКФ m-последовательностей с ПСП L. При этом пиковые значения нечетных ПВКФ для АО-сдвигов ПСП, входящих в 7-ми элементное множество с θ_c=19, не превышают 33.

Таким образом, за счет объединения ПСП S с ПСП L могут быть образованы два непересекающихся подмножества из 7-ми ПСП с θ_c=19 и $\hat{\theta}_c = 33$. Дальнейшие исследования показали, что объединение ПСП S со всеми остальными классами ПСП приводят к существенному ухудшению их ВКФ.

ПСП классов A, B, C

Внутри каждого класса ПСП введем нумерацию, при которой ПСП с номером k будет соответствовать изоморфный коэффициент $3^k \bmod 127$. В соответствие с результатами раздела 3.2 матрица пиковых значений P_{ij} ПВКФ для каждого такого класса будет обладать следующим замечательным свойством. Каждая последующая строка корреляционной матрицы P_{ij} является циклическим сдвигом вправо ее предыдущей строки. Таким образом, все строки матрицы, начиная с первой, могут быть получены из нулевой строки, при этом достаточно вычислить только первые ее 9 элементов, не считая первого. В таблице 3.5 приведены нулевые строки матрицы P_{ij} для каждого класса A, B, C, а также для класса ПСП S, имеющего тот же самый набор изоморфных коэффициентов. Из анализа этой таблицы следует, что при выборе подмножеств из 9 ПСП класс A оказывается более предпочтительным, так как можно получить θ_c=27, тогда как для классов B, C и S θ_c=41.

Проведенные на компьютере расчеты пиковых значений ПВКФ пар ПСП, взятых из различных классов, приводят к следующему выводу.

Таблица 3.5.

Пиковые значения ПВКФ ПСП классов A, B, C, S.

j	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
P_{0j}^{A}	127	23	23	23	23	41	27	41	23	25	23	41	27	41	23	23	23	23
P_{0j}^{B}	127	23	29	21	25	25	41	31	27	27	27	31	41	25	25	21	29	23
j	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
P_{0j}^{C}	127	41	41	25	23	19	17	23	41	43	41	23	17	19	23	25	41	41
P_{0j}^{S}	127	17	17	17	17	17	41	41	41	21	41	41	41	17	17	17	17	17

Комбинации ПСП из различных классов A, B, C, S образуют множества ПСП с большими значениями θ_c, чем у ПСП исходных классов. При этом множество из 36-ти ПСП классов C и S имеет параметр θ_c=43, в то время как множества ПСП, образованные соответственно из классов $A \cap B$, $A \cap C$, $B \cap C$, $A \cap S$, $B \cap S$ обладают сравнительно худшими параметрами θ_c, достигающими значений 69÷71. Интересно отметить, что взаимокорреляционный параметр θ_c ПСП L с ПСП классов A, B, C составляет соответственно 43, 29 и 27.

Для более полного представления корреляционных свойств ПСП классов A, B, C целесообразно рассмотреть их нечетные ПВКФ. Известно, что нечетные ВКФ так же как и нечетные АКФ зависят от выбора сдвигов коррелируемых ПСП. Для нахождения оптимальных сдвигов, минимизирующих значение $\hat{\theta}_c$ была использована квазиоптимальная процедура поиска. В таблице 3.6 (верхняя часть от диагонали) приведены значения пиков

нечетной ВКФ для последовательностей класса А при оптимальных сдвигах, минимизирующих эти значения. Соответственно, в таблице 3.6 (нижняя часть от диагонали) приведены значения пиков нечетной ВКФ для автооптимальных сдвигах этих последовательностей. Из таблицы 3.6 видно, что существует подмножество из 14 последовательностей класса А со значением корреляционного параметра $\hat{\theta}_c$=33. Для сравнения при АО сдвигах для этого же подмножества ПСП $\hat{\theta}_c$=43. В целом же для ПСП класса А этот параметр при оптимальных и автооптимальных сдвигах соответственно равен 35 и 47. Заметим, что ПСП классов В, С и S при АО-сдвигах обладают примерно такими же значениями ВКФ, что и класс А.

Таблица 3.6.

Пики нечетных ВКФ последовательностей класса А при автооптимальных и оптимальных сдвигах .

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
0	25/21	31	29	31	29	33	31	29	31	29	29	33	33	31	31	31	33	31
1	33	19/17	33	31	23	33	33	27	31	27	27	29	31	33	33	27	29	27
2	27	25	21/19	29	33	27	31	29	31	33	29	27	29	31	27	33	31	29
3	39	33	37	17/17	31	31	33	29	31	31	33	31	31	35	27	31	33	29
4	27	25	39	31	21/21	33	29	29	29	31	31	29	27	33	31	27	29	27
5	31	29	29	27	35	21/19	25	29	29	27	31	31	31	35	35	25	33	29
6	37	41	31	31	39	35	21/19	29	29	31	33	35	35	31	29	29	31	31
7	27	27	35	27	25	43	27	23/19	31	27	31	31	35	35	29	31	29	31
8	27	29	27	39	29	29	31	37	21/17	31	27	27	33	31	31	27	29	25
9	41	29	31	35	37	35	35	35	31	23/21	29	27	27	29	33	33	31	27
10	29	41	29	29	31	33	29	27	31	33	29/17	35	35	29	27	31	31	31
11	31	29	47	29	27	39	35	27	35	27	25	23/19	29	27	35	31	35	29
12	35	29	29	43	25	31	27	31	31	39	33	37	25/17	29	35	33	29	27
13	37	31	27	25	43	31	33	25	33	27	25	39	31	25/21	23	31	33	33
14	35	33	39	31	31	43	27	35	27	31	29	29	27	35	33/19	33	33	33
15	35	29	35	27	33	27	43	29	31	37	41	31	31	39	35	23/19	33	29
16	35	27	27	31	25	35	29	47	31	27	27	35	27	25	43	27	31/19	29
17	31	31	35	31	33	27	31	31	37	27	29	27	39	29	29	31	37	21/17

Последовательности Холла

Как и ранее, строки корреляционной матрицы значений ПВКФ для ПСП Н могут быть получены из нулевой строки посредством ее циклических сдвигов вправо. Эта строка имеет вид:

0	1	2	3	4	5
127	41	41	43	41	41

В соответствии с (3.27) наибольшая нижняя граница максимума ПВКФ ПСП Холла длины 127 равна $\hat{\theta}=(v+2)/3=41$, что согласуется с приведенными выше результатами расчета. Дополнительно к этому были также исследованы ПВКФ ПСП H с ПСП остальных классов. В результате было установлено, что наиболее предпочтительными являются сочетания ПСП H с ПСП классов B и S, для которых параметр θ_c не превышает значения 41, тогда как сочетание с классами A и C дают θ_c=69. Кроме того, для ПСП H были также исследованы нечетные ВКФ при автооптимальных и оптимальных сдвигах. Оказалось, что в первом случае $\hat{\theta}_c = 47$, а во втором - 29.

Линейная сложность ПСП классов S, L, H, A,B, C

В недавно опубликованной работе [31] было показано, что последовательности A, B, C являются частным случаем при n=7 трех новых семейств последовательностей, получивших соответственно условные названия: Предложение 3, Предложение 5 и Предложение1. Причем последовательности всех этих семейств выражаются в виде сумм следовых функций. В соответствии с этим для ПСП классов A, B, C имеем:

$$a(t) = tr_1^7(a^t) + tr_1^7(a^{5t}) + tr_1^7(a^{21t}) + tr_1^7(a^{13t}) + tr_1^7(a^{29t}) \quad , \quad (3.30)$$

$$b(t) = tr_1^7(a^t) + tr_1^7(a^{5t}) + tr_1^7(a^{21t}) + tr_1^7(a^{13t}) + tr_1^7(a^{29t}) \quad , \quad (3.31)$$

$$c(t) = tr_1^7(a^t) + tr_1^7(a^{9t}) + tr_1^7(a^{13t}) \quad . \quad (3.32)$$

Аналогичные представления также были найдены для ПСП H и L значности 127 [35]:

$$h(t) = tr_1^7(a^t) + tr_1^7(a^{25t}) + tr_1^7(a^{47t}) \quad , \quad (3.33)$$

$$l(t) = \sum_{i=0}^{8} tr_i^7(a^{3^{2i}t}) \quad . \qquad (3.34)$$

Из выражений (3.30)-(3.34) легко вычисляется линейная сложность этих последовательностей, значения которой представлены в таблице 3.7.

Таблица 3.7.

Линейная сложность последовательностей длины 127.

тип последовательности	линейная сложность
Зингер (S)	7
Лежандр (L)	63
Холл (H)	21
A	35
B	35
C	21

Проведенные исследования показали (см. таблицу 2.9), что на основе нелинейных последовательностей классов L, H, A, B и C могут быть построены ПСП GMW с линейной сложностью, превышающей линейную сложность ПСП GMW на основе m-последовательностей 127. В частности, было установлено, что линейная сложность ПСП GMW 2^{14}-1 на основе одной из ПСП Лежандра равна 1232, когда как максимальная линейная сложность ПСП GMW на основе m-последовательностей составляет 448.

Выводы.

1. Предложенный метод изоморфных коэффициентов является эффективным средством исследования взаимно-корреляционных свойств последовательностей, построенных на основе разностных множеств типа Адамара. Этот метод позволяет существенно ускорить расчет на компьютере их ПВКФ, а, следовательно, и построение систем ФМ сигналов с заданными корреляционными свойствами.

2. Природа сверхвысоких пиков ПВКФ m-последовательностей, родственных им ПСП GMW, а также ПСП Холла и Лежандра носит строго детерминированный характер, обусловленный структурной спецификой данных последовательностей.
3. Наибольшая аналитическая нижняя граница максимума ПВКФ класса m-последовательностей совпадает с аналогичной нижней границей для большинства классов ПСП GMW, при этом сверхвысокими пиковыми значениями будут обладать пары, связанные децимациями d_r. Полученные результаты могут быть использованы в системах с CDMA при отборе последовательностей с небольшими пиками взаимной корреляции.
4. Проведенные полные расчеты ПВКФ ПСП GMW для $6 \le N \le 15$ показывают, что эти ПСП обладают примерно такими же корреляционными параметрами, что и m-последовательности. Поэтому с учетом их высокой линейной сложности они могут составить серьезную конкуренцию более распространенным в широкополосной связи m-последовательностям.
5. Классы ПСП Холла и Лежандра характеризуются большими пиковыми значениями ПВКФ и малой мощностью, что существенно ограничивает их практическое применение.
6. ПСП классов L, H, A, B и C значности 127, построенные на основе разностных множеств с параметрами $v=127$, $k=63$, $\lambda=31$, образуют в совокупности мощное множество из 62-х последовательностей с близкими к идеальным значениями ПАКФ. Использование этих ПСП наряду с m-последовательностями в системах связи с CDMA позволяет значительно расширить возможность выбора множеств ПСП с приемлемыми корреляционными параметрами. ПСП класса A, B, C и H целесообразно также использовать в тех случаях, когда требуются последовательности с более высокими, чем у m-последовательностей значениями линейной сложности.

7. Другой не менее важной областью применения последовательностей классов L, H, A, B и C может стать их использование в качестве базисных для генерации новых классов ПСП GMW, что приводит к существенному увеличению общего числа этих последовательностей. Кроме того, в силу нелинейности последовательностей классов L, H, A, B и C можно предположить, что образованные на их основе ПСП GMW будут обладать большими значениями линейной сложности.

Глава 4. Генераторы последовательностей GMW

4.1 Краткая историческая справка

Первые схемы генераторов последовательностей GMW были построены и описаны еще в 70гг. [21,22,63]. Их принцип работы основывался на декомпозиционном свойстве последовательностей GMW. По этой причине все эти генераторы получили название декомпозиционных. Основное различие между ними состоит в количестве генерируемых форм. Так генератор [22] позволяет получить все возможные последовательности GMW, однако за такой универсализм приходится расплачиваться сверхвысокой аппаратной сложностью его реализации. Напротив, генератор [21] относительно проще, правда и число генерируемых им форм намного меньше. Необходимо отметить, что все эти генераторы характеризуются экспоненциальным ростом сложности в зависимости от N и поэтому большого практического распространения они не получили. Вместе с тем несомненная полезность декомпозиционных генераторов проявилась в том, что они послужили прототипом при создании наиболее простого с точки зрения реализации на сегодняшний день генератора [49].

В 1984г. Велчем и Шолцем был предложен метод генерации некоторых классов последовательностей GMW, основанный на генерации q-ичной m-последовательности [46]. Эта публикация явилась началом триумфального распространения последовательностей GMW и одновременно дало мощный импульс для их дальнейшего исследования. В последствии было показано, что данный метод может быть распространен на все классы этих последовательностей [49]. К сожалению, в силу различных причин пионерские работы [21,22,63] остались не известными для большинства отечественных и зарубежных исследователей. История последовательностей GMW за рубежом не избежала и некоторых курьёзов. Так, в 1985г. Прасадом и Квином [47] было объявлено о построении нового класса

последовательностей с хорошими авто и взаимно-корреляционными свойствами, названными ими m-подобными шифрованными последовательностями. Однако последующие исследования показали их полную эквивалентность последовательностям GMW. При этом схема предложенного ими генератора во многом совпадает со схемой генератора [63]. Последующее десятилетие не привнесли ничего кардинального в технику генерации последовательностей GMW. Существенный прорыв произошел только в 1997г., когда на Научно-технической конференции МТУСИ был предложен новый метод генерации двоичных последовательностей GMW, существенным образом упрощающий разработку генераторов (подробное описание этого метода опубликовано в 5-ом номере журнала "Радиотехника" за 1998г.). Простота данного метода в отличие от метода Велча-Шольца заключается в использовании сдвинутых копий двоичной m-последовательности и, как следствие, чисто двоичной логики. Поэтому есть основания ожидать, что с появлением данного генератора число разработчиков систем связи, использующих последовательности GMW увеличится.

Переходим теперь к подробному рассмотрению в хронологическом порядке известных методов и схем генерации последовательностей GMW.

4.2. Декомпозиционные генераторы последовательностей GMW

В 1977г. было получено авторское свидетельство на устройство для генерации псевдослучайных последовательностей двоичных сигналов [21], соответствующих всем изоморфным в своих классах эквивалентности GMW разностным множествам с параметрами (2.13), строящихся на основе зингеровского класса базисных разностных множеств с параметрами (2.17). В основе построения генераторов декомпозиционного типа лежит идея воссоздания декомпозиционной таблицы в порядке следования в ней элементов последовательности GMW. Для этой цели предварительно вычисляются значения 2^{N-m}

сдвигов ненулевых строк декомпозиционной таблицы соответствующей m-последовательности относительно первой строки с их порядковыми номерами, а также расположение ε-2^{N-m} ее нулевых строк. Полученная информация составляет основу программного устройства, с помощью которого выполняется построение декомпозициоиой таблицы последовательности GMW. При этом по определенной циклической программе производится автоматическое. изменение задержки генерируемой базисной m-последовательности длины 2^m-1. Согласно этой программе первые ε двоичные символы генерируемой последовательности GMW определяются первыми двоичными символами формируемой совокупности из сдвинутых копий базисной последовательности и нулевых последовательностей длины 2^m-1.Следующие ε двоичных символов определяются всеми вторыми двоичными символами этой совокупности и т.д. В результате в генераторе формируются все 2^N-1 символов последовательности GMW.

На рис.4.1 представлена функциональная схема устройства для генерации двоичных последовательностей GMW, на основе базисных m-последовательностей. Устройство содержит генератор 1 тактовых импульсов, делитель 2 с коэффициентом деления ε, генератор 3 m-последовательности в виде m-разрядного регистра сдвига с линейной обратной связью через сумматор по модулю два, m-входовый сумматор 4 по модулю два, m схем совпадения 5 и программное устройство 6, состоящего из m ε-разрядных циклических регистров сдвига 7. Генератор 1 тактовых импульсов подключен к входу делителя 2 и к m входам цепей продвигающих импульсов циклических регистров сдвига 7-1, ..., 7- m. Выходы циклических регистров сдвига 7 соединены с первыми входами схем совпадения 5, вторые входы этих схем подключены к выходам соответствующих разрядов формирующего регистра генератора m-последовательности. Тактовые импульсы сдвига генератора 3 снимаются с выхода делителя 2. Все m выходов схем совпадения 5 подключены к m входам сумматора по модулю два 4. Устройство работает следующим образом. Вырабатываемые генератором 1 тактовые импульсы частоты f_T осуществляют последовательное продвижение

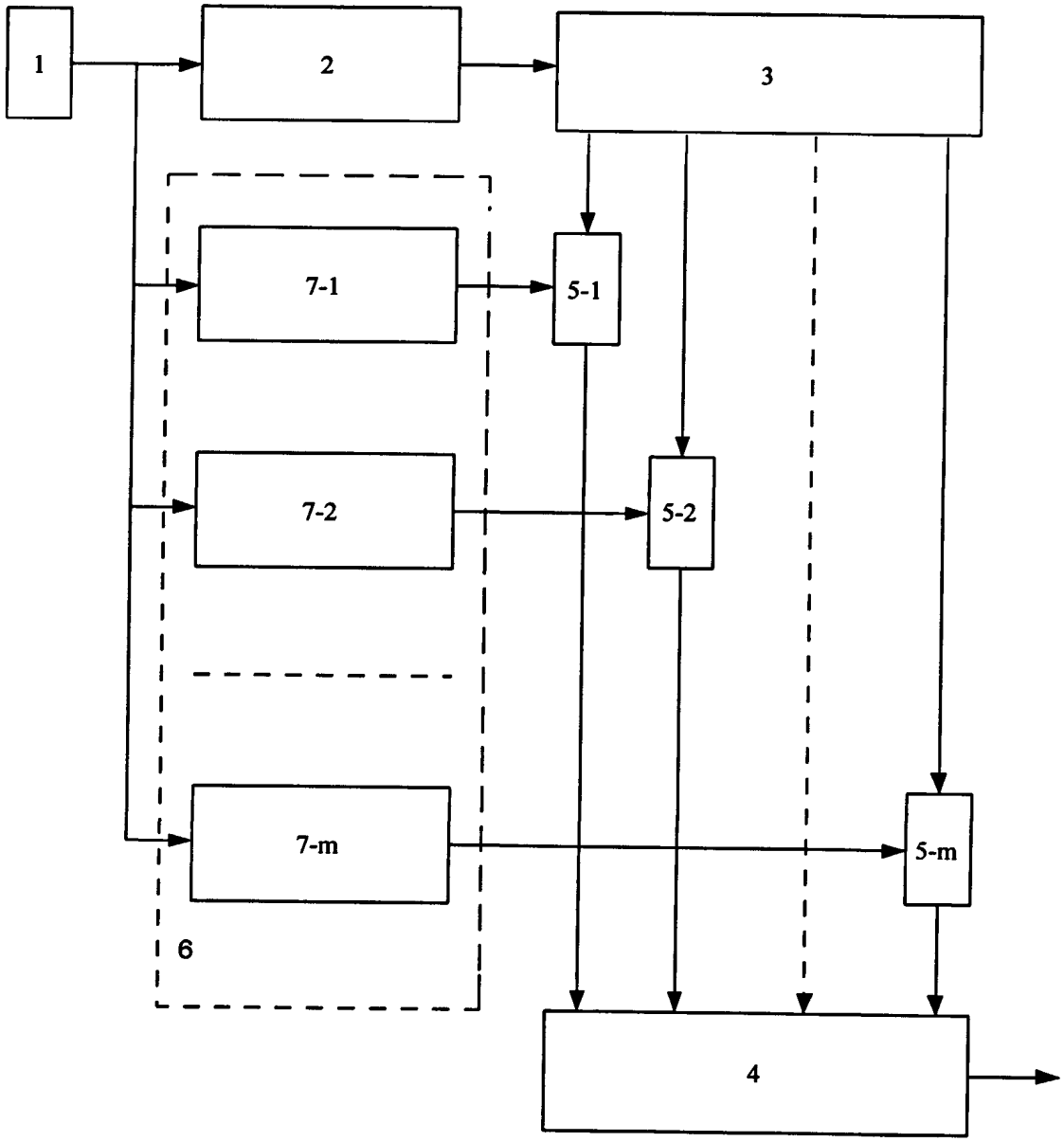

Рис. 4.1
Генератор ПСП GMW на основе базисных m-последовательностей

записанной в циклических регистрах сдвига 7 двоичной информации, при этом каждое m-разрядное двоичное число, находящееся в течение периода $\tau=1/f_T$ генератора 1 в m выходных разрядов этого регистра, определяет величину сдвига m-последовательности генератора 3. Схемы совпадения в зависимости от состояний выходов циклических регистров сдвига 7 открыты или закрыты и в соответствии с этим пропускают или не пропускают двоичные сигналы разрядов регистра сдвига генератора 3 m-последовательности на входы сумматора 4. В результате на выходе сумматора 4 появляются двоичные сигналы формируемой последовательности GMW. Импульсы с выхода делителя 2 с частотой следования f_T/ε поступают на тактовый вход регистра сдвига генератора 3 , изменяя состояние разрядов этого регистра в соответствии с уравнением обратной связи. Таким образом, за длительность периода m-последовательности генератора 3 на выходе сумматора 4 появятся сигналы всех 2^N-1 двоичных символов генерируемой последовательности GMW.

Для лучшего понимания работы устройства рассмотрим генерацию класса последовательностей GMW длины 63. В этом случае N=6, m=3, k=2 и ε=9. В силу этого коэффициент деления делителя 2 равен 9. Генератор базисной m-последовательности состоит из 3-х разрядного регистра сдвига с обратными связями, описываемыми уравнениями $D^0y=Dy+D^3y$ и $D^0y=Dy+D^3y$, где D – оператор сдвига, соответствующими примитивным полиномам степени 3 над GF(2) $f_1(x)=x^3+x+1$ и $f_2(x)=x^3+x^2+1$. Программное устройство 6 состоит из 3-х 9-ти разрядных циклических регистров сдвига 7. Необходимые для его загрузки данные находятся с помощью декомпозиции исходной m-последовательности. Отметим, что теоретически данный генератор позволяет также формировать и шесть m-последовательностей длины 63, хотя, конечно, на практике это делать не следует.

Почти одновременно с данным генератором было предложено устройство для генерации всех последовательностей GMW, строящихся на основе всех возможных базисных последовательностей [22]. На Рис.4.2 представлена функциональная схема этого устройства.

Оно состоит из генератора 1 тактовых импульсов, делителя 2 с коэффициентом деления ε, генератора 3 базисной последовательности на 2^m-1-разрядном регистре циклическом регистре сдвига, элемента ИЛИ 4 на 2^m-1 входов, 2^m-1 схем совпадения 5, программного устройства 6, состоящего в свою очередь из m ε-разрядных циклических регистров сдвига 7 и дешифратора 8. Генератор 1 тактовых импульсов подключен к входу делителя 2 и к m входам цепей продвигающих импульсов регистров 7-1, 7-2,...7-m.

В соответствии с алгоритмом построения программное устройство задает необходимую для генерации последовательности GMW совокупность из ε m-разрядных двоичных чисел, ненулевые значения которых соответствуют сдвигам базисной последовательности, а нули - нулевым последовательностям. Устройство работает следующим образом. Тактовые импульсы генератора 1 осуществляют последовательное продвижение записанной в циклических регистрах сдвига 7 двоичной информации, при этом каждое m-разрядное двоичное число, находящееся в течение периода генератора 1 в выходных разрядах этих регистров, является двоичным кодом номера соответствующего разряда регистра генератора 3 базисной ПСП и, следовательно, определяет величину сдвига базисной ПСП. Появляющийся на одном из выходов дешифратора соответствующий этому коду сигнал открывает одну из схем совпадения 5 и пропускает двоичный сигнал с выхода соответствующего разряда регистра генератора 3 на вход элемента ИЛИ 4. В результате циклических сдвигов информации в программном устройстве 6 на выходе элемента ИЛИ 4 появляются ε двоичных сигналов формируемой ПСП.

Импульсы с выхода делителя 2, поступая с частотой f_T/ε на тактовый вход генератора 3, осуществляют циклический сдвиг базисной ПСП. Поэтому за 2^m-1 сдвигов последовательности в генераторе 3 на выходе элемента ИЛИ 4 появятся сигналы всех 2^N-1 двоичных символов генерируемой последовательности.

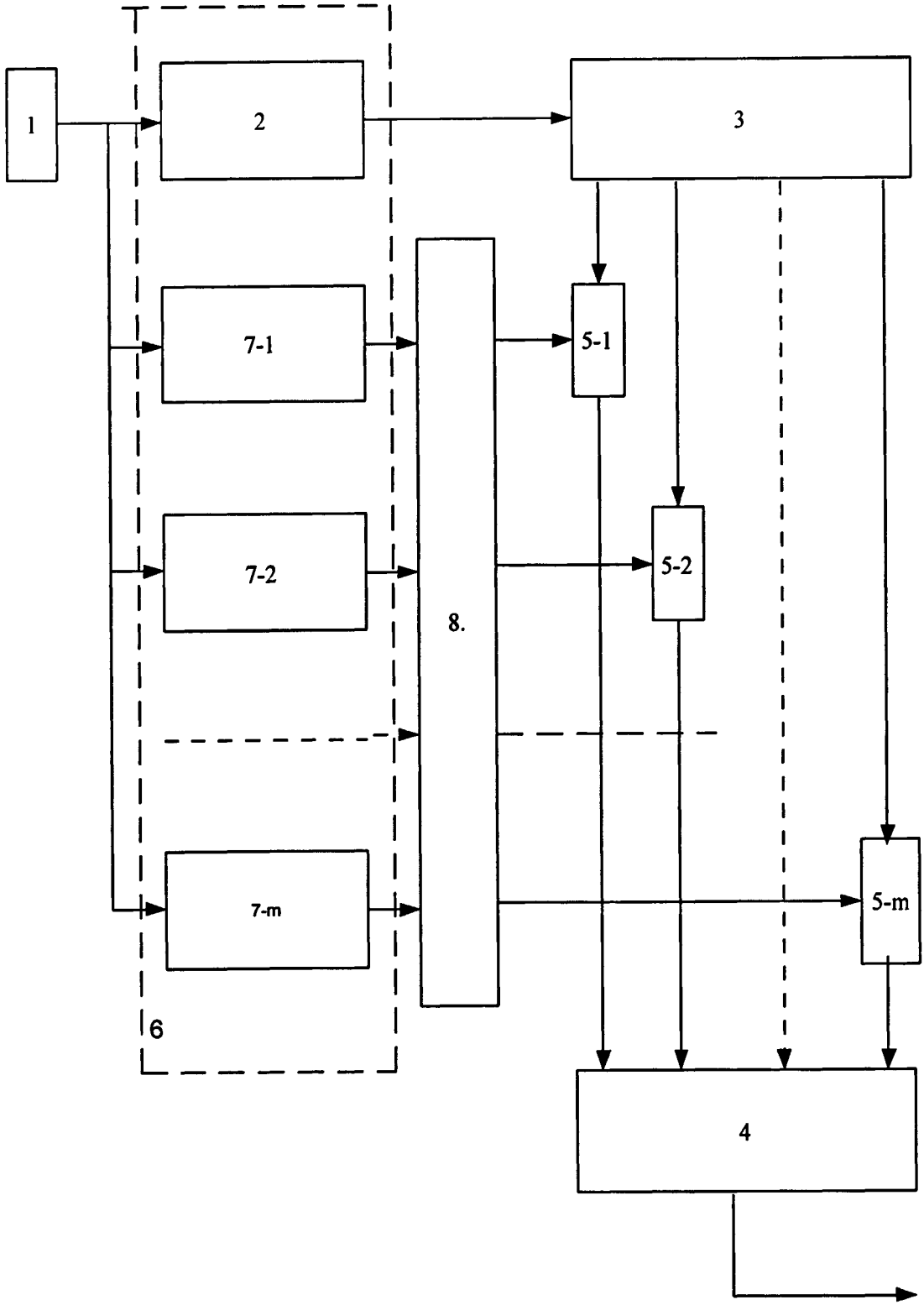

Рис. 4.2
Генератор ПСП GMW на основе всех базисных последовательностей

При этом так называемая нулевая последовательность кодируется в программном устройстве 6 в виде двоичного числа из одних нулей, а дешифратор декодирует все числа от 1 до 2^m-1. Поэтому при появлении кода нулевой последовательности в последних разрядах регистров 7 на всех выходах дешифратора появятся сигналы логического нуля, которые, закрывая схемы совпадения 5, создадут нулевой сигнал на выходе элемента ИЛИ 4.

Проведенный анализ показывает, что устройство целесообразно использовать для генерации последовательностей Гордона, Милза, Велча, начиная с N=10. Так, например, в случае N=14=7×2 предлагаемое устройство позволяет генерировать 59724 новых псевдослучайных последовательностей вместо 12852 генерируемых предыдущим устройством. В случаях N<10 те же самые последовательности GMW могут быть получены с помощью генератора [21], обладающего несколько меньшей сложностью. Однако, когда нет необходимости в генерации всех существующих форм ПСП GMW и можно остановиться на одной или нескольких из них, выбранных в соответствии с определенными критериями (например, по минимаксному), использования схем [21,22] в силу их функциональной избыточности и сложности становится не целесообразным.

Рассматриваемое ниже устройство формирования двоичных ПСП GMW позволяет получить одну или несколько форм ПСП при значительно меньших технических затратах, что можно рассматривать, как своего рода компенсацию за проигрыш в числе генерируемых форм [63].

На рис.4.3 представлена структурная схема предлагаемого устройства для генерации псевдослучайных последовательностей. Поступающие с генератора 1 тактовые импульсы с частотой $f_т$ продвигают записанную в регистре распределителя 2 "единицу", которая, проходя через ту или иную схему ИЛИ коммутатора 6, открывает связанную с ней схему совпадения 5, тем самым, пропуская двоичный сигнал с выхода соответствующего разряда регистра генератора 3 базисной последовательности на вход ИЛИ 4. Выходные импульсы распределителя 2 с частотой $f_т/\epsilon$ поступают на тактовый вход регистра сдвига

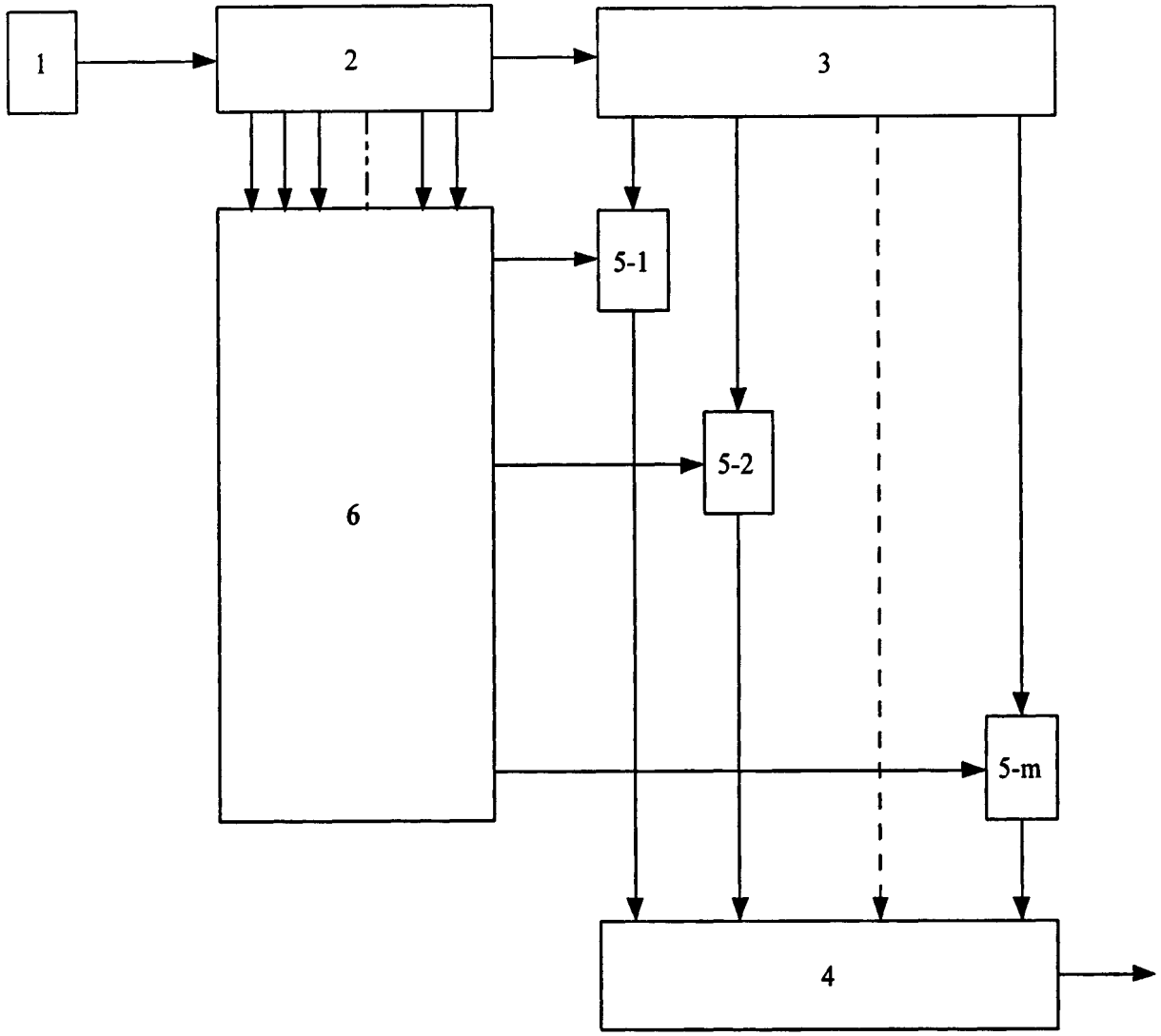

Рис.4.3
Блок-схема генератора нескольких форм ПСП GMW

генератора 3, осуществляя циклический сдвиг информации в этом регистре. Таким образом, за длительность периода базисной последовательности на выходе элемента ИЛИ 4 появятся сигналы всех 2^N-1 двоичных символов генерируемой устройством последовательности.

При этом в соответствии с особенностями структуры ПСП GMW коммутатор 6 производит разбиение выходов разрядов регистра распределителя на определенные группы, соответствующие различным разрядам регистра генератора базисной последовательности, а, следовательно, и различным сдвигам базисной последовательности, что обеспечивает формирование совокупности из ε последовательностей из сдвигов базисной и нулевой.

Первые ε двоичных символов генерируемой последовательности совпадают со всеми первыми двоичными символами сформированной совокупности. Следующие ε двоичных символов - со всеми вторыми двоичными символами той же совокупности и т. д. В результате такой циклической процедуры в устройстве формируются все 2^N-1=εω двоичных символов ПСП GMW.

Чтобы понять работу устройства, рассмотрим генерацию ПСП GMW значности 63 [63]. Эта последовательность имеет вид:

1010001101011001101000111010001000000011110111001111010010011011 и соответствует GMW разностному множеству с параметрами ν=63, κ=32, λ=16 и образующим полиномом $\Omega(x) \equiv 1+x^2y^6+x^3y^3+x^4y^4+x^5y^4+x^6+x^7y^6+x^8y^4 \bmod x^{63}-1$, где $y=x^9$. В общем случае члены полинома Ω(x) содержат всю информацию о структуре коммутатора 6 устройства, а именно:

1) члены с разными степенями y соответствуют разным элементам ИЛИ коммутатора 6;

2) члены с одинаковыми степенями y соответствуют входам одного элемента ИЛИ коммутатора 6;

3) выход определенного разряда распределителя 2 соединяется с определенным входом одного из элементов ИЛИ коммутатора 6 таким образом, что выход разряда с

номером, на единицу большим показателя степени **x**, соединяется с входом элемента ИЛИ, соответствующего степени **y** в члене, содержащем эту степень **x**;

4) выход каждого элемента ИЛИ подключается к входу схемы совпадения с номером, на единицу большим величины показателя соответствующей степени **y**.

При этом следует иметь в виду, что одновходовые элементы ИЛИ, предполагаемые данным описанием коммутатора 6, на самом деле отсутствуют. Поэтому разряды распределителя 2, соответствующие этим одновходовым элементам ИЛИ, подключаются непосредственно к входам схем совпадения 5. Каждая схема совпадения (а число таких схем, как следует из описания коммутатора, может быть меньше ω) соединяется по входу с выходом одноименного разряда регистра сдвига генератора 3 базисной последовательности.

В соответствии с этим устройство для генерации ПСП ГМВ значности 63 (рис.4.4) содержит генератор тактовых импульсов 1, коммутатор 6, состоящий из трех элементов ИЛИ: двух двухвходовых (7-1,7-2) и одного трехвходового (7-3), распределитель 2 импульсов на 9-разрядном циклическом регистре сдвига, генератор 3 базисной последовательности на 7-разрядном циклическом регистре сдвига, четыре схемы совпадения 5-1, 5-2, 5-3, 5-4, четырехвходовой элемент ИЛИ 4.

Рассматриваемый генератор содержит один ε-разрядный циклический регистр сдвига, выполняющий функции делителя тактовых импульсов и распределителя импульсов для коммутатора, в то время как генератор, описываемый в работе [22], содержит m циклических регистров сдвига разряда ε, входящих в состав его программного устройства.

Сложность обоих генераторов при больших значениях N определяется числом регистров, поэтому технико-экономический эффект, получаемый в результате применения предложенного в данной статье, равен приблизительно m.

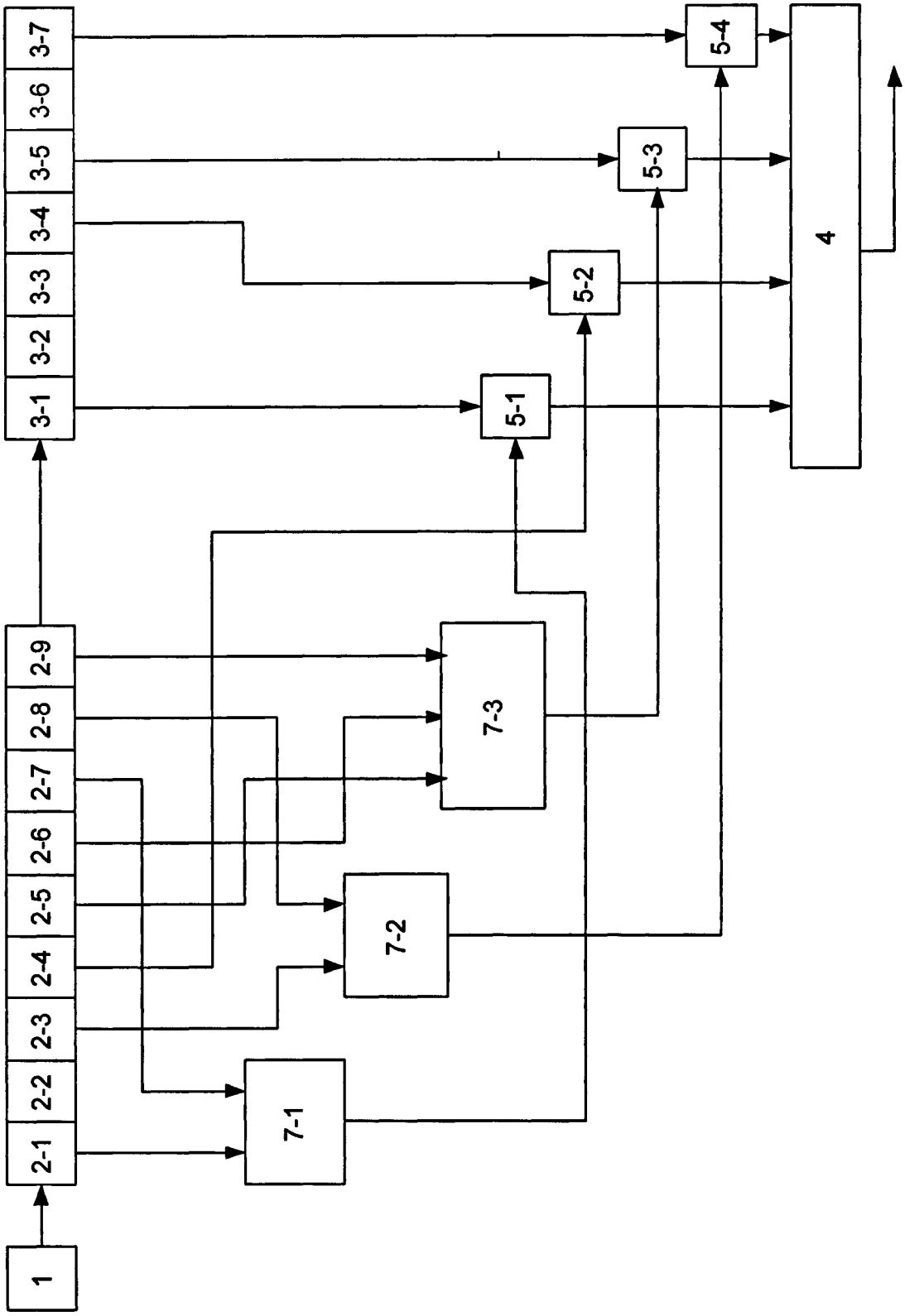

Рис.4.4
Функциональная схема генератора ПСП GMW длины 63

Общее число генерируемых этим устройством ПСП равно числу существующих базисных последовательностей, причем эти последовательности принадлежат различным классам ПСП GMW. Так, например, для N=14 устройство генерирует 80 ПСП из различных классов.

Описанный генератор имеет следующую особенность: если регистры распределителя импульсов и генератора базисной последовательности формирователя сделать реверсивными, то число генерируемых ПСП может быть увеличено вдвое. При этом если сдвиг информации в указанных регистрах происходит вправо, устройство генерирует одни псевдослучайные последовательности, а при сдвиге влево генерирует другие ПСП, "обратные" к первым.

Возможность генерации "обратных" копий ПСП GMW без какого-то либо изменения в информации, находящейся в регистрах этого устройства, обусловлена свойством ПСП, строящихся на основе разностных множеств. В соответствие с этим свойством преобразование, меняющее порядок следования всех элементов исходной ПСП, кроме первого, на противоположный, приводит к образованию ПСП из того же класса, но отличной от исходной. Таким образом, для рассматриваемого выше случая N=14 реверс регистров приводит к получению дополнительно еще 80 форм последовательностей.

4.3. Генератор последовательностей GMW на основе следов полей Галуа

В 1984г. в майском номере журнала IEEE Transactions on Information Theory появилась знаменитая статья Шольца и Велча, посвященная исследованию последовательностей GMW [46] (впервые эти результаты были доложены на международном симпозиуме по теории информации в 1983г. в Канаде). Более точно предметом исследования в [46] были последовательности GMW, строящиеся на основе m-последовательностей. При этом для

построения последовательностей GMW использовалось представление линейных функционалов в виде следовых функций. Общий вид элементов этих последовательностей имеет вид:

$$b_n = tr([tr_m^N(\alpha^n)]^r) \ , \ (4.1)$$

где $0<r<2^m-1$, $(r, 2^m-1)=1$, а α примитивный элемент из $GF(2^N)$. Очевидно, что когда r=1 данная формула является следовым представлением m-последовательности 2^N-1. В соответствии с тем, что внутренняя функция в этом выражении является m-последовательностью над $GF(2^m)$ длины 2^N-1, авторами была предложена следующая очевидная конструкция генератора последовательностей GMW, блок-схема которой представлена на Рис.4.5. Данный генератор состоит из последовательно соединенных генератора m-последовательности над $GF(2^m)$ и ПЗУ объемом 2^m , задающим закон отображения элементов $GF(2^m)$ в GF(2). В [46] приведен пример реализации генератора для последовательности GMW длины 63. Уже на основе данного примера видно, что математически это достаточно непростая задача. Причем основная проблема состоит в построении q-ичной m-последовательности, которая при больших N переходит в разряд трудно решаемых задач. Возможно поэтому, касаясь вопроса генерации ПСП GMW, большинство авторов ограничиваются общими рассуждениями о простоте и компактности схемы генератора, явно уходя в сторону от вопроса его инженерной реализации. Дальнейшие исследования показали, что число последовательностей с идеальными ПАКФ, формируемых с помощью данного генератора, может быть существенным образом увеличено за счет использования в качестве базисных других семейств идеальных последовательностей. Правда, при этом, как уже отмечалось выше, все такие новые последовательности получали совершенно другие названия, не имеющие ничего общего с "последовательностями GMW". И это несмотря на то, что все они соответствовали классам GMW-разностных множеств. Впервые на это было обращено внимание в работе [49], в которой на основании теории GMW разностных множеств было получено общее

выражение для представления всех соответствующих этим разностным множествам последовательностей.

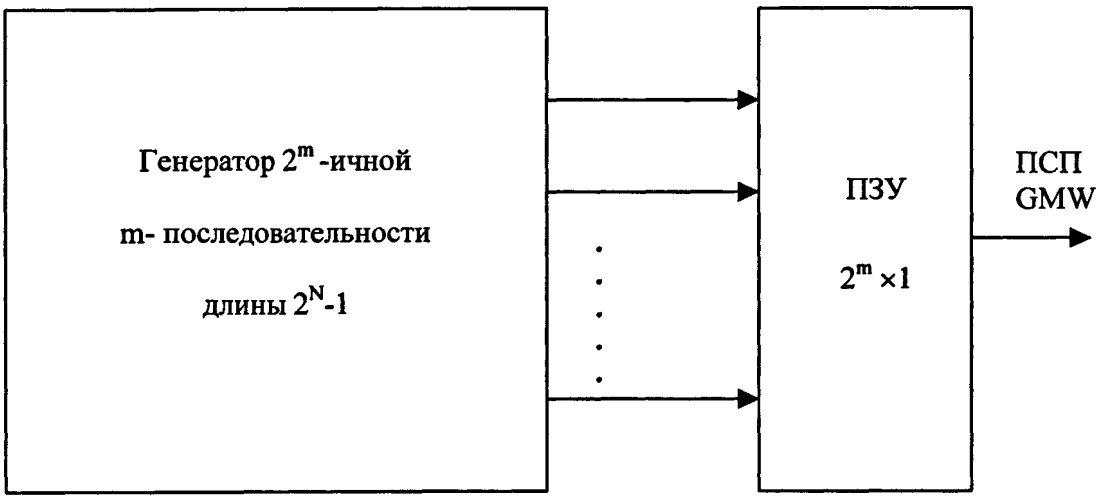

Рис. 4.5

Генератор ПСП GMW по схеме Шольца-Велча

4.4. Генератор последовательностей GMW на основе сдвигов m-последовательностей.

Касаясь практической реализации генератора [46], надо отметить, что, несмотря на свою достаточно простую и компактную структуру, его разработчику предстоит решить целый ряд далеко не тривиальных задач, обусловленных особенностями данного метода.

Остановимся на этом вопросе более подробно. Первая задача, которую необходимо решить, связана непосредственно с выбором примитивного полинома степени k над GF(2^m). Ведь

возможна ситуация, когда в существующих таблицах полинома с такими параметрами может не оказаться. Заметим, что синтез примитивного полинома является достаточно непростой математической задачей, которая обычно выполняется на компьютере с помощью специально составленных алгоритмов.

Следующая задача связана с построением самого генератора q-ичной m-последовательности по имеющемуся примитивному полиному. Возникающие здесь трудности обусловлены необходимостью использования нетривиальных арифметических операций над GF(q). Очевидно, что и в этом случае также не обойтись без написания специальных компьютерных программ.

И, наконец, последняя по порядку, но не по сложности задача связана с разработкой ПЗУ генератора. Дело в том, что в силу метода построения структура ПЗУ полностью определяется элементами подполя $GF(2^m)$ поля $GF(2^N)$, представленного в базисе 1, β, β^2,..., β^{m-1}, где β - примитивный элемент подполя $GF(2^m)$. Трудности, возникающие в связи с решением перечисленных задач, в значительной мере ограничивают практическое использование последовательностей GMW в технике связи. Поэтому вполне своевременным представляется нахождение такого метода генерации, который бы способствовал более широкому их практическому применению. Предлагаемый новый, более простой метод генерации последовательностей GMW основан на формировании сдвинутых копий двоичной m-последовательности значности v. При рассмотрении этого метода будем опираться на известные свойства линейных функционалов над полями Галуа [45].

Пусть L-линейный функционал из $GF(2^N)$ в GF(2) такой, что L(1)=1. Соответственно, пусть L_0-сужение L до подполя $GF(2^m)$, а L_2-линейный функционал из $GF(2^N)$ в $GF(2^m)$ такой, что для $\forall x \in GF(2^N)$ выполняется условие:

$$L_0(L_2(x)\beta)=L(x\beta) \text{ для } \forall \beta \in GF(2^m). \quad (4.2)$$

Обозначим через $\{c_j\}$, $0 \le j < 2^m-1$, базисную последовательность длины 2^m-1, образованную на основе некоторого разностного множества с параметрами (2.17). Тогда, используя результаты [14], можно показать, что любая последовательность GMW с точностью до сдвига может быть представлена в следующем виде:

$$b_n = f(L_2(\alpha^n)) \ , \ (4.3)$$

где α - примитивный элемент $GF(2^N)$, $0 \le n < 2^N-1$, а f: $GF(2^m) \to GF(2)$ - функционал, определяемый условиями:

$$f(\beta^j) = C_j \text{ для всех } 0 \le j < 2^m-1 \text{ и } f(0)=0 \ . \ (4.4)$$

Заметим, что при $f=L_0$ последовательность $\{C_j\}$ уже сама определяется условиями (4.4), при этом последовательности $\{b_n\}$ и $\{C_j\}$ являются m-последовательностями со значностями соответственно v и w. Рассмотрим теперь последовательность $\{m_n\}$, определяемую условием: $m_n = L_2(\alpha^n)$, $0 \le n < 2^N-1$.

Согласно [4,13] последовательность $\{m_n\}$ является q-ичной m-последовательностью злачности 2^N-1. Представим последовательность $\{m_n\}$ в виде двумерной таблицы размерности $\varepsilon \times w$, в которой каждый элемент m_n стоит на пересечении i-ой строки и j-го столбца, где $0 \le i < \varepsilon$ и $0 \le j < w$ связаны с n соотношением вида: $n = i + j\varepsilon$. Можно показать, что полученная таблица состоит из $\varepsilon \cdot 2^{N-m}$ строк, содержащих единственный элемент 0 из $GF(2^m)$, тогда как остальные 2^{N-m} строки представляют собой последовательности из ненулевых элементов $GF(2^m)$ и имеют вид:

$$\{\beta^{S_i+j}\} \ , (4.5)$$

где $0 \le i < \varepsilon$, $0 \le j < w$, $0 \le S_i < w$ и $L_2 = (\alpha^i) = \beta^{S_i}$.

Нетрудно убедиться, что все такие ненулевые строки являются циклическими сдвигами друг друга и могут быть получены из первой строки с i=0 вида $\{\beta^j\}$, $0 \le j < 2^m-1$. То, что эта

строка ненулевая следует из условия L(1)=1. Образуем на основе последовательности $\{\beta^j\}$ двоичную последовательность $\{d_j\}$ значности 2^m-1, имеющую вид:

$$d_j=L_0(\beta^j) \text{для всех } 0\le j<2^m-1 \ . \quad (4.6)$$

Согласно построению последовательность $\{d_j\}$ есть m-последовательность значности 2^m-1. Введем теперь функционал L_1: $GF(2^m) \rightarrow GF(2^m)$, определяемый из следующих условий:

$$L_1(\beta^j)=d_j + d_{j+1}\beta +... + d_{j+m-1}\beta^{m-1} \text{ и } L_1(0)=0 \ . (4.7)$$

Покажем, что L_1 есть взаимно однозначное отображение $GF(2^m) \rightarrow GF(2^m)$. Воспользуемся для этого известным свойством m-последовательности, иногда называемым свойством окна. Согласно этому свойству любой ненулевой набор из m последовательных символов m-последовательности значности 2^m-1, встречается на ее периоде ровно один раз, причем число различных таких наборов равно 2^m-1. А поскольку коэффициенты при степенях β в правой части выражения (4.7) образуют именно такие наборы, то L_1 - взаимно однозначное отображение.

Обозначим через g: $GF(2^m) \rightarrow GF(2)$ функционал, определяемый следующими условиями:

$$g(L_1(\beta^j))=C_j \text{ и } g(0)=0 \ .$$

Тогда в силу построения последовательность $\{b_n'\}$ вида:

$$b_n'=g(L_1(L_2(\alpha^n))) \ . \quad (4.8)$$

оказывается эквивалентной последовательности $\{b_n\}$, определяемой (4.3). Подставляям (4.7) в (4.8) с учетом (4.2), (4.5) и (4.6), в итоге получаем:

$$b_n'=g(L(\alpha^n)+ L(\alpha^{n+\varepsilon})\beta+...+ L(\alpha^{n+\varepsilon(m-1)})\beta^{m-1}) \ . (4.9)$$

Из анализа (4.9) видно, что коэффициенты $L(\alpha^n)$, $L(\alpha^{n+\varepsilon})$,... $L(\alpha^{n+\varepsilon(m-1)})$ представляют собой сдвинутые на ε чипов копии m-последовательности $\{L(\alpha^n)\}$. С другой стороны эти коэффициенты могут быть интерпретированы как m-разрядные адреса, по которым в ПЗУ записаны символы последовательности $\{c_j\}$, причем по нулевому адресу в ПЗУ всегда должен находиться символ "0". В результате построенный в соответствии с (4.9) генератор

последовательностей GMW будет состоять из последовательно включенных генератора сдвинутых копий m-последовательности злачности v и ПЗУ базисной ПСП, состоящего из 2^m однобитных слов. Функциональная схема этого генератора представлена на Рис.4.6.

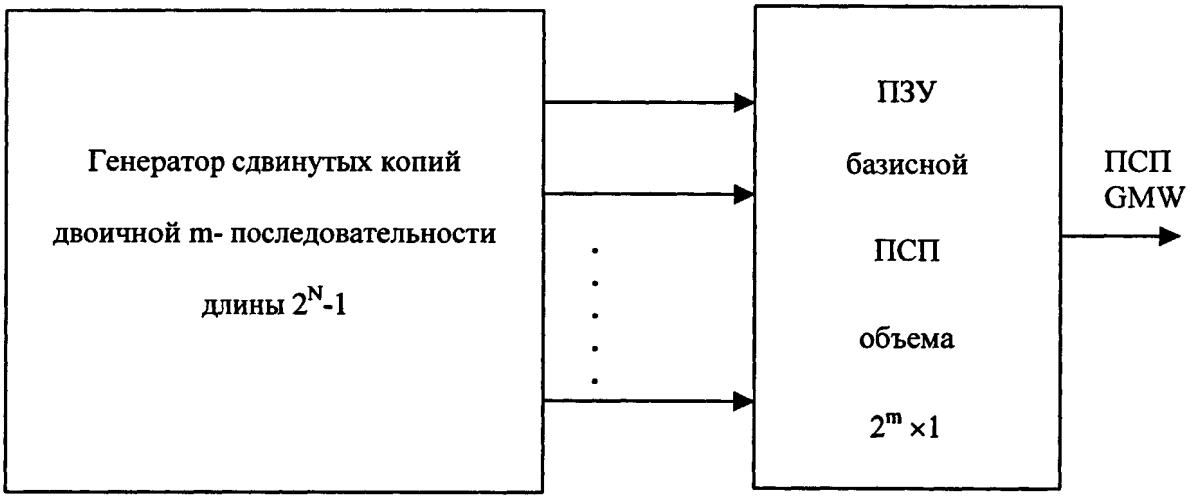

Рис. 4.6.

Генератор ПСП GMW по схеме Кренгеля-Мешковского.

Сопоставление нового генератора с генератором [46] показывает, что, несмотря на почти одинаковую элементную сложность, новый генератор оказывается более предпочтительным в виду явно очевидной простоты его реализации. Главным неоспоримым преимуществом предлагаемого генератора является то, что все арифметические операции выполняются в нем исключительно по правилам двоичной логики над GF(2). Это, очевидно, значительно упрощает его разработку по сравнению с генератором [46], в котором используется более сложная арифметика над GF(q). В отношении генерации сдвинутых копий двоичной m-последовательности следует сказать, что этот вопрос в литературе [24] освещен достаточно подробно и никаких трудностей здесь не возникает. Предлагаемый метод может быть также эффективен и в случае его программной реализации. Особенно это относится к генерации

сверхдлинных последовательностей, применяемых для защиты передаваемых по каналам связи данных. Следует отметить, что область применения этого метода не ограничивается только последовательностями GMW. Данный метод может быть также использован для генерации и других двоичных последовательностей, образованных на основе 2^m-ичной m-последовательности и разностных множеств [18].

В заключении в качестве примера рассмотрим генерацию последовательности GMW значности $v=2^{12}-1=4095$,где N=12 и m=3. Пусть примитивный элемент α поля $GF(2^{12})$ является корнем неприводимого примитивного полинома [68]:

$$X^{12}+X^{11}+X^8+X^6+1\ . \quad (4.10)$$

Тогда генератор сдвинутых копий m-последовательности должен формировать m=3 сдвинутых последовательностей b_n, b_{n+585}, b_{n+1170} , где $b_n=L(\alpha^n)$. Нетрудно убедиться, что последовательности b_{n+585} и b_{n+1170} являются задержанными соответственно на 3510 и 2925 чипов копиями m-последовательности b_n. Формирование задержанных копий m-последовательности наиболее просто осуществить суммированием по модулю два соответствующих разрядных выходов регистра сдвига генератора m-последовательности b_n, выполненного по схеме с вынесенными сумматорами. Однако вид обратной связи при этом будет уже определяться полиномом:

$$X^{12}+X^6+X^4+X+1 \quad , (4.11)$$

двойственным к полиному (4.10). Пусть γ корень примитивного полинома (4.11), а b_n, b_{n-1}, ...,$b_{n-(N-1)}$ - последовательности, образующиеся на разрядных выходах регистра сдвига генератора m-последовательности. Тогда последовательность b_{n-l} для всех $0\le l<v$ может быть представлена в следующем виде:

$$b_{n-l}=l_0b_n+l_1b_{n-1},...,+l_{N-1}b_{n-(N-1)},$$

где вектор двоичных коэффициентов (координат) $l_0, l_1,..., l_{N-1}$ из GF(2) численно совпадает с соответствующими коэффициентами в разложении элемента γ^l по базису 1, γ, $\gamma^2,...,\gamma^{N-1}$. В результате для $b_{n+585}=b_{n-3510}$ и $b_{n+1170}=b_{n-2925}$ с помощью компьютера находим, что:

$$b_{n+585}=b_n+b_{n-1}+b_{n-2}+b_{n-3}+b_{n-5}+b_{n-7}+b_{n-10}\text{, а}$$

$$b_{n+1170}=b_{n-1}+b_{n-2}+b_{n-8}+b_{n-9}+b_{n-10}.$$

Образуем теперь 7-ми элементную ненулевую последовательность $\{d_j\}$, где в соответствии с (4.6) $d_j=b_{585j}$, $0\le j<7$. Это всегда можно сделать путем соответствующего выбора начального состояния генератора последовательности b_n . Тогда при начальном состоянии $S_0=1$ последовательность $\{d_j\}$ имеет вид: $\{d_j\}=1101001$. Для построения ПЗУ в соответствии с (4.7) образуем таблицу 4.1, в которой каждому 3-х элементному набору символов последовательности $\{d_j\}$ ставится в соответствие его порядковый номер j, а наборы при этом рассматриваются как двоичные адреса.

Таблица 4.1.

Взаимосвязь адреса и j.

АДРЕС			J
1	**1**	**0**	**0**
1	**0**	**1**	**1**
0	**1**	**0**	**2**
1	**0**	**0**	**3**
0	**0**	**1**	**4**
0	**1**	**1**	**5**
1	**1**	**1**	**6**

Для генерации последовательности GMW выберем теперь в качестве базисной последовательность $\{c_j\}=1001011$, обратную к $\{d_j\}$. Заметим, что для рассматриваемого

случая существует всего только одна базисная последовательность. Затем поместим символы последовательности $\{c_j\}$ по адресам Таблицы 4.1 в соответствие со значениями индекса j. Тогда, учитывая, что по нулевому адресу всегда находится символ 0, после упорядочения таблицы по возрастанию адресного параметра получаем таблицу 4.2, полностью определяющую структуру ПЗУ генератора.

Таблица 4.2 .

Структура ПЗУ генератора ПСП GMW длины 4095.

АДРЕС			СИМВОЛ
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	1
1	0	1	0
1	1	0	1
1	1	1	1

После этого не представит особого труда построить и сам генератор, функциональная схема которого изображена на Рис.4.7.

В Приложении 2 представлены тексты программ вычисления координат векторов сдвигов, используемых для построения генераторов ПСП GMW для N=12, 14, 15, 16, 20, 32, 48 и 63. Здесь же приведены тексты программ, моделирующие его работу.

Выводы

1. Проведен сравнительный анализ известных схем генераторов последовательностей GMW .

2. Предложен новый простой метод генерации двоичных последовательностей GMW, на основе генерации сдвинутых копий двоичной m-последовательности той же длины. Показано преимущество данного метода по сравнению с известным методом Велча-Шольца, основанного на генерации q-ичной m-последовательности.

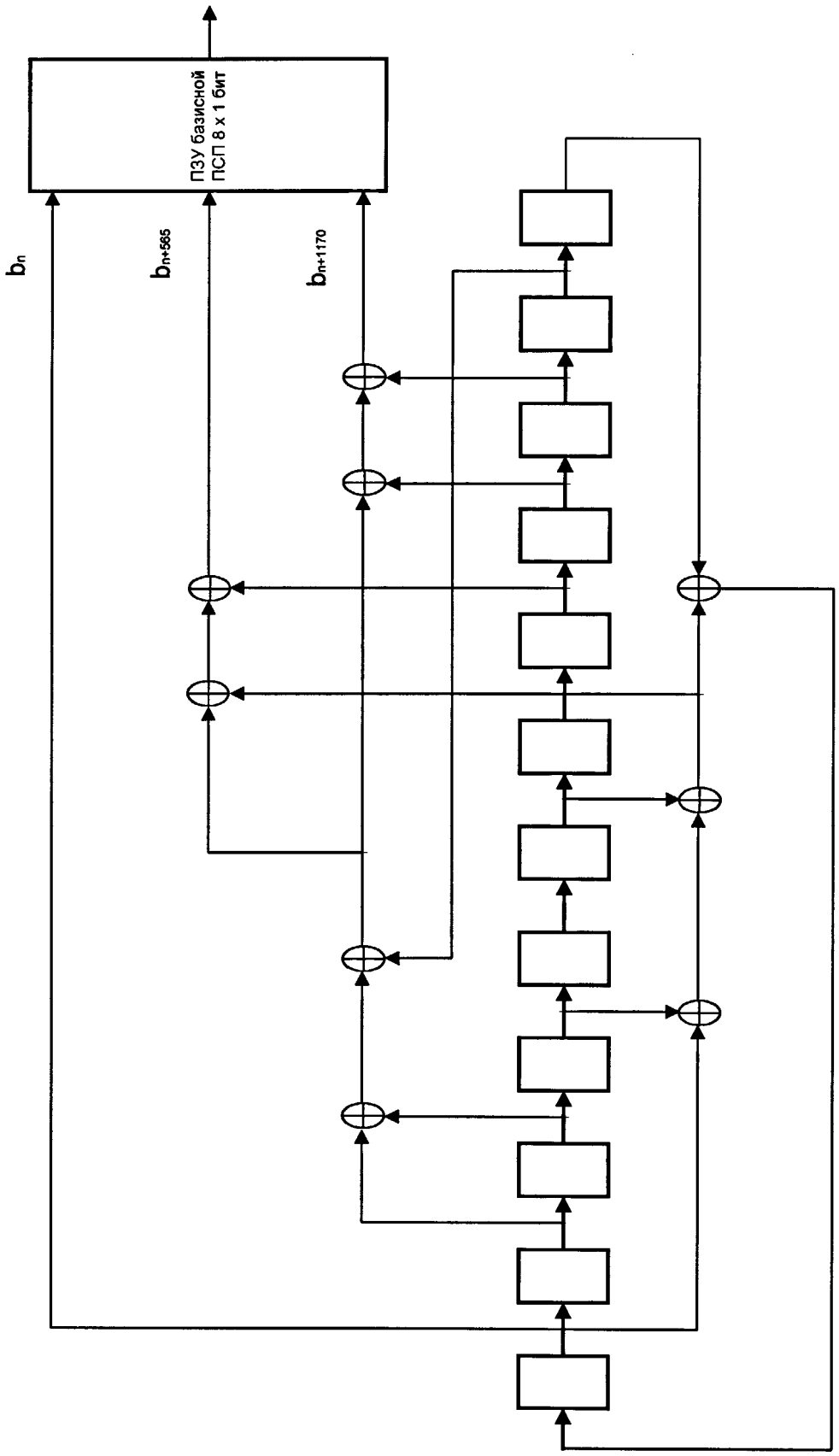

Рис.4.7
Генератор ПСП GMW длины 4095

Глава 5. Применение новых классов ПСП в системах связи с CDMA

5.1. Ортогональные производные системы сигналов на основе ПСП GMW

Современный период развития широкополосных систем связи, базирующихся на технологии CDMA, сопровождается бурным ростом числа работ, посвященных поиску новых систем ортогональных сигналов, используемых в этих системах для расширения спектра и каналообразования [17]. Системы ортогональных сигналов строятся на основе ансамблей ортогональных кодовых псевдослучайных последовательностей, основными требованиями к которым являются [24]:

1) большой ансамбль последовательностей, формируемых посредством единого алгоритма;
2) хорошие корреляционные свойства последовательностей ансамбля;
3) сбалансированность структуры;
4) большая линейная сложность или непредсказуемость символов последовательностей.

В настоящее время в системах связи с CDMA широкое распространение получили ортогональные системы сигналов на основе циркулянтных матриц Адамара и системы функций Уолша, являющимися матрицами Адамара порядка 2^n. Известно [20], что системы ортогональных сигналов на основе матриц Адамара в целом характеризуются плохими АКФ и ВКФ, что приводит к росту межканальных интерференционных помех в приемнике. Поэтому на практике с целью уменьшения уровня интерференционных помех более целесообразно использовать производные ортогональные системы сигналов [69], имеющие относительно лучшие взаимно-корреляционные характеристики. Напомним, что производный сигнал получается в результате посимвольного перемножения двух сигналов. Соответственно система, составленная из множества производных сигналов, называется производной. Среди производных систем сигналов большое распространение получили системы, строящиеся следующим образом. В качестве первого сомножителя берется некоторая ортогональная система сигналов, последовательности которой не удовлетворяют

требованиям на корреляцию, однако обладают определенными преимуществами с точки зрения простоты их формирования и обработки. Это так называемая исходная система сигналов. Затем в качестве второго сомножителя выбирается широкополосный производящий сигнал с относительно малыми боковыми пиками АКФ. Как показано в [69], корреляционные свойства такой производной системы оказываются лучше, чем у исходной. Обычно в качестве исходной системы используют функции Уолша или циркулянтные матрицы Адамара, образованные всеми сдвигами m-последовательностей, а в качестве производящих сигналов m-последовательности. В этом случае сбалансированность последовательностей производной системы будет тем лучше, чем меньше пиковое значение взаимной корреляции исходной и производящей последовательностей. Анализ показывает, что, в основном удовлетворяя трем первым критериям отбора, все вышеописанные производные системы сигналов обладают незначительной линейной сложностью. Поэтому актуальной задачей является построение новых ортогональных производных систем сигналов большой линейной сложности с приемлемыми корреляционными свойствами и сбалансированностью.

Для решения этой задачи были исследованы производные системы сигналов, в которых исходные системы строятся на основе циклических сдвигов m-последовательностей, а в качестве производящих последовательностей выбраны нелинейные последовательности GMW. Оценка линейной сложности такой производной системы производится с помощью следующей теоремы [70].

Теорема 5.1.

Линейная сложность производной системы сигналов $L_{пр.с}$ с исходной m-последовательностью длины 2^N-1 и производящей последовательностью GMW такой же длины и линейной сложностью L_{GMW} заключена в границах

$$L_{GMW}-N \le L_{пр.с} \le L_{GMW}+N \quad . \quad (5.1)$$

Доказательство.

Согласно формуле (2.44) любая последовательности $\{b_n\}$ длины 2^N-1 с элементами над GF(2) может быть представлена в виде $b_n = \sum_{\delta \in \Delta} \alpha_\delta \alpha^{\delta n}$, где α есть примитивный элемент поля $GF(q^N)$, а Δ есть множество индексов при ненулевых коэффициентах α_δ в этом расширении. Линейная сложность последовательности $\{b_n\}$ численно равна количеству элементов в этой сумме. Известно [4], что m-последовательность может быть представлена в виде суммы вида

$$m_n = tr_1^N(\alpha^n) = \sum_{i=0}^{N-1} \alpha^{n2^i}$$

с числом членов равным N. А так как последовательности производной системы получаются в результате поэлементного суммирования по модулю два последовательности GMW со сдвигами m-последовательности, то в силу предыдущего их линейная сложность оказывается ограниченной снизу величиной L_{GMW} - N, а сверху L_{GMW}+N. Теорема доказана.

В качестве примера рассмотрим случаи N=10 и N=14. Учитывая, что для N=10 максимальная линейная сложность последовательности GMW равна 140 [71], а для N=14 соответственно 1232 , имеем:

для N=10 $\quad 140-10=130 \le L_{пр.с} \le 140+10=150,$

для N=14 $\quad 1232-14=1218 \le L_{пр.с} \le 1232+14=1246.$

Отсюда видно, линейная сложность производных систем на основе нелинейных последовательностей GMW и m-последовательностей определяется в основном линейной сложностью последовательностей GMW и может во много раз превышать линейную сложность m-последовательностей. Для рассмотренных случаев на основе последовательностей GMW был построен ряд ортогональных производных систем и проведен расчет их периодических АКФ и ВКФ. Анализ показывает, что для некоторых из них абсолютные пиковые значения АКФ и ВКФ, взятые по всем последовательностям

системы, не превышают величины $6\sqrt{v}$. Это всего в 3 раза хуже по сравнению с ортогональной производной системой на основе последовательностей Голда, которая имеет наилучшие корреляционные свойства, но небольшую линейную сложность, равную 2N. Что же касается сбалансированности последовательностей рассматриваемых систем, то, очевидно, она полностью определяется значением пика взаимной корреляции исходной и производящей последовательностей и, как показывают численные расчеты, в лучшем случае может быть соизмерима с последовательностями Голда. Оценим теперь общее число образованных таким способом ортогональных производных систем. В соответствие с [14] их число может быть найдено по формуле

$$(\varphi(2^N-1)/N)^2 \cdot |GMW| . \quad (5.2)$$

Здесь φ - есть функция Эйлера, а $|GMW|$ - число различных неэквивалентных классов последовательностей GMW длины 2^N-1. В соответствии с этим находим, что для случаев N=10 и N=14 общее число таких систем составляет соответственно 25200 и 45151344. Касаясь вопроса сложности аппаратной или программной реализации предлагаемых систем сигналов, необходимо отметить, что возникающие при этом трудности связаны в основном с генерацией последовательностей GMW. Эти вопросы достаточно подробно исследованы в 4-й главе настоящей диссертации. Наиболее предпочтительным в силу своей простоты является метод [49], использующий исключительно двоичную арифметику, тогда остальные или требуют применения q-ичной арифметики [46] или обладают большой аппаратной сложностью [21,22].

Выводы

Предложенный метод построения ортогональных производных систем сигналов позволяет получить системы, последовательности которых удачно совмещают большую линейную сложность с удовлетворительными корреляционными параметрами. Данные

системы могут быть успешно использованы в системах связи с CDMA, требующих повышенную имито и криптозащиту.

5.2. Применение последовательностей GMW для повышения безопасности CDMA систем на основе стандарта IS-95

В настоящее время технология CDMA с кодовым разделением каналов на основе шумоподобных сигналов прочно утвердилась в качестве одного из перспективных методов радиодоступа. Наряду с другими стандартами особенно широкое распространение получил стандарт IS-95 на систему сотовой подвижной связи с CDMA, разработанный корпорацией Qualcomm [17,19,72]. В целях обеспечения скрытности и безопасности стандарт IS-95 предусматривает скремблирование кодированных данных, передаваемых в прямом CDMA канале, длинным кодом на основе m-последовательности длины 2^{42}-1. Одновременно, что сдвиги той же самой m-последовательности используются для расширения спектра обратных CDMA каналов. Величина сдвига для каждого пользователя выбирается уникальной и определяется кодом маски пользователя, вычисляемого в соответствии с секретным алгоритмом на базовых и мобильных станциях. Используемая схема скремблирования имеет принципиальный недостаток, обусловленный тем, что наложение m-последовательности на серии из более 42-х подряд идущих нулей или единиц может привести к быстрому раскрытию кода маски пользователя на приемном конце. Подобная ситуация особенно возможна в случае передачи данных неречевых источников, что, безусловно, является недостатком существующего стандарта IS-95.

Одним из распространенных методов повышения безопасности передачи данных является метод, в котором в качестве скремблера используются нелинейные последовательности, обладающие значительно более высокой по сравнению с m-последовательностью степенью непредсказуемости символов. Основными требованиями,

предъявляемыми к таким последовательностям помимо их высокой линейной сложности, являются хорошие статистические свойства, а также закон формирования, совместимый с законом формирования m-последовательности. Последнее должно сохранить неизменным существующую в IS-95 систему синхронизации длинных кодов базисных и абонентских станций, реализуемую посредством передачи абонентским станциям состояний генераторов длинного кода базовых станций.

Анализ показывает, что в наибольшей степени всем этим требованиям удовлетворяют классы последовательностей GMW и бент-последовательности длины 2^N-1 [4,14]. Однако бент-последовательности существуют только при N кратных 4, тогда как последовательности GMW существуют при всех N=mk, m≥3, k≥2 и, следовательно, при N=42. Эти последовательности имеют высокую линейную сложность и, самое главное, как было показано в [49], закон их формирования легко совместим с законом формирования двоичных m-последовательностей. В работе [73] описан метод, в котором в качестве скремблера используется последовательность GMW на основе базисной m-последовательности. Согласно [73] наибольшей линейной сложностью последовательности GMW длины 2^{42}-1 обладают при m=14 и k=3. В этом случае она равна 22320522, что требует ПЗУ объемом 16384. Поэтому более целесообразно использовать последовательности GMW с параметрами m=7 и k=6, при которых объем ПЗУ равен 128, а линейная сложность достигает 326592, что в 7776 раз превышает линейную сложность синхронизирующей m-последовательности [73]. Заметим, что в качестве базисных могут использоваться также последовательности из других классов, например последовательности Бомера-Фридриксена длины 127. Правда остается не выясненным вопрос, какая в этом случае будет достигнута линейная сложность. При разработке генератора ПСП GMW необходимо решить две основные задачи. Найти координаты векторов сдвигов, определяющие схемотехнику блока сумматоров и сформировать базисную последовательность длины 127, необходимую для построения ПЗУ. Решение первой задачи подробно описано в [73] и всецело определяется

примитивным полиномом, на основе которого формируется m-последовательность длины 2^{42}-1 генератора длинного кода. Этот полином имеет следующий вид:

$$f(x)=1+x+x^2+x^3+x^5+x^6+x^7+x^{10}+x^{16}+x^{17}+x^{18}+x^{19}+x^{21}+x^{22}+x^{25}+x^{26}+x^{27}+x^{31}+x^{33}+x^{35}+x^{42} . \quad (5.3)$$

Как известно [4], на основе примитивного полинома могут быть построены два типа генераторов одной и той же m-последовательности: генератор типа Галуа со встроенными сумматорами по модулю два и генератор типа Фибоначчи с вынесенными сумматорами. Пусть γ есть примитивный корень полинома, двойственного к полиному (5.3), а b_n, b_{n-1}, b_{n-2},..., b_{n-41} есть последовательности на выходах разрядов регистра сдвига генератора m-последовательности по типу Фибоначчи. Тогда последовательность b_{n-l} для всех $0 \le l < v$ может быть представлена в следующем виде:

$$b_{n-l}=l_0 b_n+l_1 b_{n-1},...,+l_{41} b_{n-41} \quad , (5.4)$$

где вектор двоичных коэффициентов l_0, l_1,..., l_{41} из GF(2) совпадает с соответствующими коэффициентами в разложении элемента γ^l по базису $1, \gamma, \gamma^2,..., \gamma^{41}$.

Далее замечаем, что согласно (4.9) коэффициенты $L(\alpha^n)$, $L(\alpha^{n+\varepsilon})$, ..., $L(\alpha^{n+6\varepsilon})$ есть b_n, $b_{n+\varepsilon}$,..., $b_{n+6\varepsilon}$, для которых справедливы следующие соотношения:

$$b_{n+\varepsilon}=b_{n-126\varepsilon}, \; b_{n+2\varepsilon}=b_{n-125\varepsilon}, \; b_{n+3\varepsilon}=b_{n-124\varepsilon}, \; b_{n+4\varepsilon}=b_{n-123\varepsilon}, \; b_{n+5\varepsilon}=b_{n-122\varepsilon}, \; b_{n+6\varepsilon}= b_{n-121\varepsilon} \quad , (5.5)$$

где $\varepsilon=(2^{42}-1)/127$.

Отсюда следует, что координаты сдвигов могут быть найдены посредством разложения элементов поля Галуа $1, \gamma^{-\varepsilon}, \gamma^{-2\varepsilon}, \gamma^{-3\varepsilon},..., \gamma^{-6\varepsilon}$ в базисе $1, \gamma, \gamma^2,... , \gamma^{41}$. Результаты вычислений в 16-ричном виде представлены в таблице 5.1.

ТАБЛИЦА 5.1.

i	0	1	2	3	4	5
$\gamma^{-i\varepsilon}$	1	19766AA628	3F90529375E	38D71A4907	2587443EA36	4E2B3E113C
i	6					
$\gamma^{-i\varepsilon}$	2D2507FEC06					

Вторая задача может быть решена следующим образом. Сначала строится 127-ми значная m-последовательность вида $\{L(\alpha^{j\varepsilon})\}$, $0 \le j < 2^m-1$. Затем на ее основе строится зеркально сопряженная к ней m-последовательность вида $\{L(\alpha^{-j\varepsilon})\}$, при которой линейная сложность достигает максимального значения 326592. Для построения ПЗУ согласно описанному в параграфе 4.4 методу генерации каждому 7-ми элементному набору символов последовательности $\{L(\alpha^{j\varepsilon})\}$ ставится в соответствие с его порядковым номером символ последовательности $\{L(\alpha^{-j\varepsilon})\}$. Рассматривая эти наборы, как двоичные адреса, и учитывая, что по нулевому адресу всегда находится символ 0, после упорядочения в порядке возрастания адресов получаем таблицу 5.2, полностью определяющую структуру ПЗУ генератора.

ТАБЛИЦА 5.2.

Структура генератора ПСП GMW длины $2^{42}-1$.

АДРЕС	БИТ	АДРЕС	БИТ	АДРЕС	БИТ
0000000	0	0000001	1	0000010	0
0000011	0	0000100	0	0000101	1
0000110	1	0000111	0	0001000	0
0001001	1	0001010	0	0001011	0
0001100	1	0001101	1	0001110	1
0001111	0	0010000	1	0010001	0

Продолжение таблицы 5.2.

АДРЕС	БИТ	АДРЕС	БИТ	АДРЕС	БИТ
0010010	1	0010011	1	0010100	1
0010101	1	0010110	1	0010111	0
0011000	1	0011001	1	0011010	1
0011011	0	0011100	1	0011101	1
0011110	0	0011111	1	0100000	1
0100001	1	0100010	0	0100011	0
0100100	0	0100101	1	0100110	0
0100111	0	0101000	1	0101001	0
0101010	0	0101011	0	0101100	1
0101101	1	0101110	0	0101111	1
0110000	1	0110001	0	0110010	1
0110011	1	0110100	0	0110101	1
0110110	1	0110111	1	0111000	1
0111001	0	0111010	0	0111011	0
0111100	1	0111101	0	0111110	0
0111111	0	1000000	0	1000001	1
1000010	1	1000011	1	1000100	1
1000101	1	1000110	0	1000111	0
1001000	1	1001001	0	1001010	1
1001011	1	1001100	1	1001101	1

Продолжение таблицы 5.2.

АДРЕС	БИТ	АДРЕС	БИТ	АДРЕС	БИТ
1001110	0	1001111	1	1010000	0
1010001	0	1010010	0	1010011	0
1010100	1	1010101	1	1010110	1
1010111	1	1011000	0	1011001	1
1011010	1	1011011	0	1011100	1
1011101	0	1011110	0	1011111	0
1100000	0	1100001	0	1100010	0
1100011	0	1100100	0	1100101	1
1100110	1	1100111	0	1101000	1
1101001	0	1101010	0	1101011	0
1101100	0	1101101	1	1101110	0
1101111	1	1110000	0	1110001	0
1110010	1	1110011	0	1110100	1
1110101	0	1110110	0	1110111	0
1111000	0	1111001	1	1111010	0
1111011	0	1111100	0	1111101	0
1111110	1	1111111	1		

Ниже на Рис.5.1 изображена блок схема генератора длинного кода на основе последовательности GMW 2^{42}-1. Пунктиром выделен генератор длинного кода на основе m-последовательности 2^{42}-1, являющийся частью стандарта TIA/EIA/IS-95.

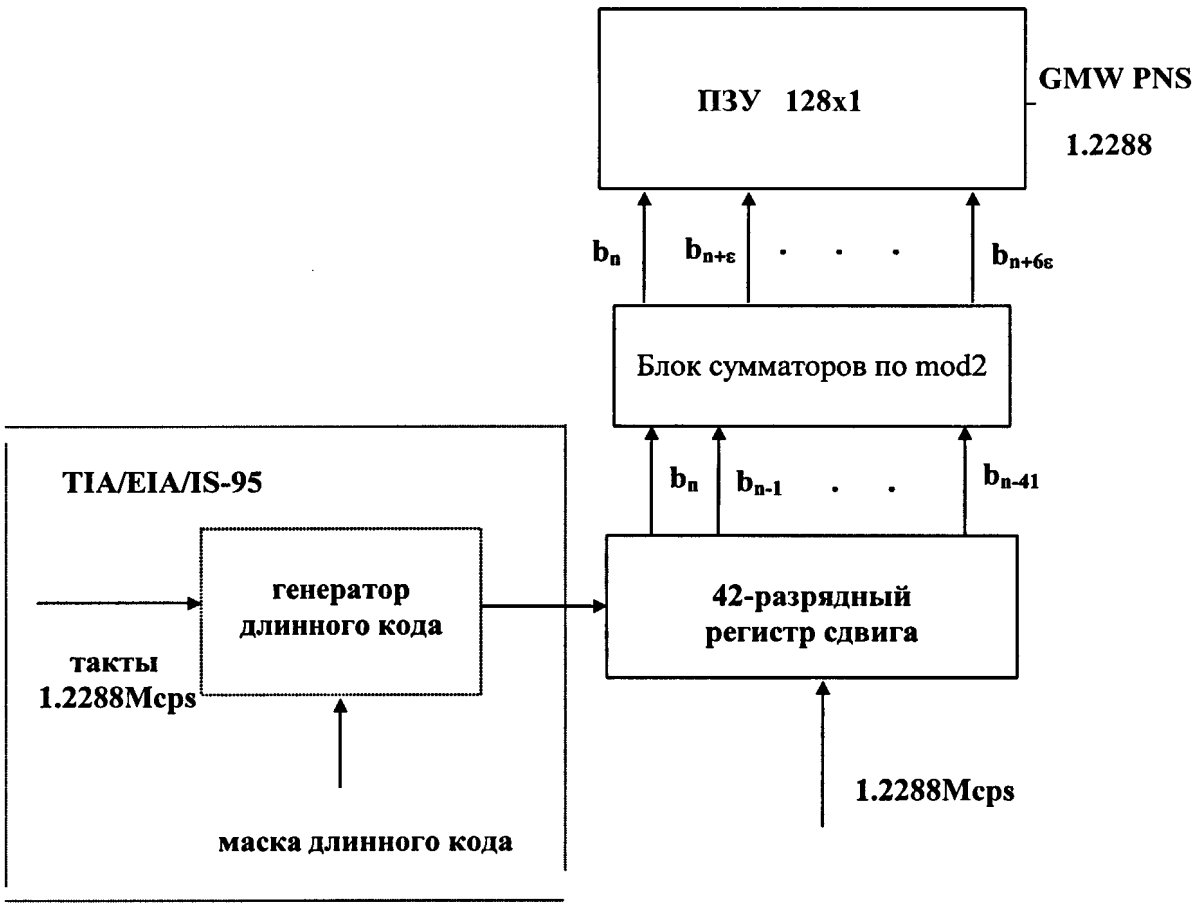

Рис. 5.1.

Генератор длинного кода 2^{42}-1 с большой линейной сложностью.

Остановимся теперь на другом важном аспекте использования последовательностей GMW 2^{42}-1 в стандарте IS-95. Очевидно, что непосредственное конструирование индивидуальных генераторов ПСП GMW для каждого из абонентских каналов приводит к значительному удорожанию стоимости аппаратуры, связанной с невозможностью получению сдвинутых копий этих последовательностей также просто как для случая m-последовательностей. Возникшую здесь коллизию между требованиями достижения высокой линейной сложности и одновременно приемлемой сложностью аппаратной реализации можно успешно разрешить на основе результатов, полученных Геймсом при

исследовании взаимно-корреляционных свойств m-последовательности и ПСП GMW, образованных из одного и того же примитивного многочлена [74]. Приведем формулировку теоремы, доказанной Геймсом.

Теорема 5.2.

Пусть N, m и r есть целые числа, при этом m делит N , $(r,2^m-1)=1$ и $\varepsilon=(2^N-1)/(2^m-1)$. Пусть s есть m-последовательность (GMW последовательность), а g есть GMW последовательность длины 2^N-1, полученные на основе одного и того же примитивного многочлена степени N. Пусть u есть m-последовательность длины 2^m-1, соответствующая не нулевой строке декомпозиционного разложения последовательности s, а v есть последовательность, полученная в результате децимации r последовательности u, т.е. $v=u_r$. Тогда

$$\theta_{sg}(i)=\begin{cases}2^{N-m}(\theta_{uv}(j)+1)-1, \text{если } i=j\varepsilon \\ -1, \quad \text{в противном случае}\end{cases} . \quad (5.6)$$

Можно показать, что условие $v=u_r$ в этой теореме является излишним. Для ее справедливости достаточно лишь выполнения одного условия: формировать s и g на основе одного и того же примитивного многочлена. Построим теперь производную систему сигналов, используя в качестве исходной последовательности s, а производящей соответственно g. Тогда из теоремы Геймса следует, что почти все за исключением 2^m-1 последовательностей этой производной системы окажутся сбалансированы. Кроме того, согласно теореме 5.1 их линейная сложность будет определяться линейной сложностью производящей последовательности GMW. На Рис.5.2 представлена укрупненная блок схема генератора скремблирующих последовательностей на основе m и GMW последовательностей. Настоящий генератор рекомендуется использовать как в прямых, так и в обратных каналах систем мобильной и фиксированной связи, разрабатываемых на основе стандарта IS-95 или его последующих модернизациях.

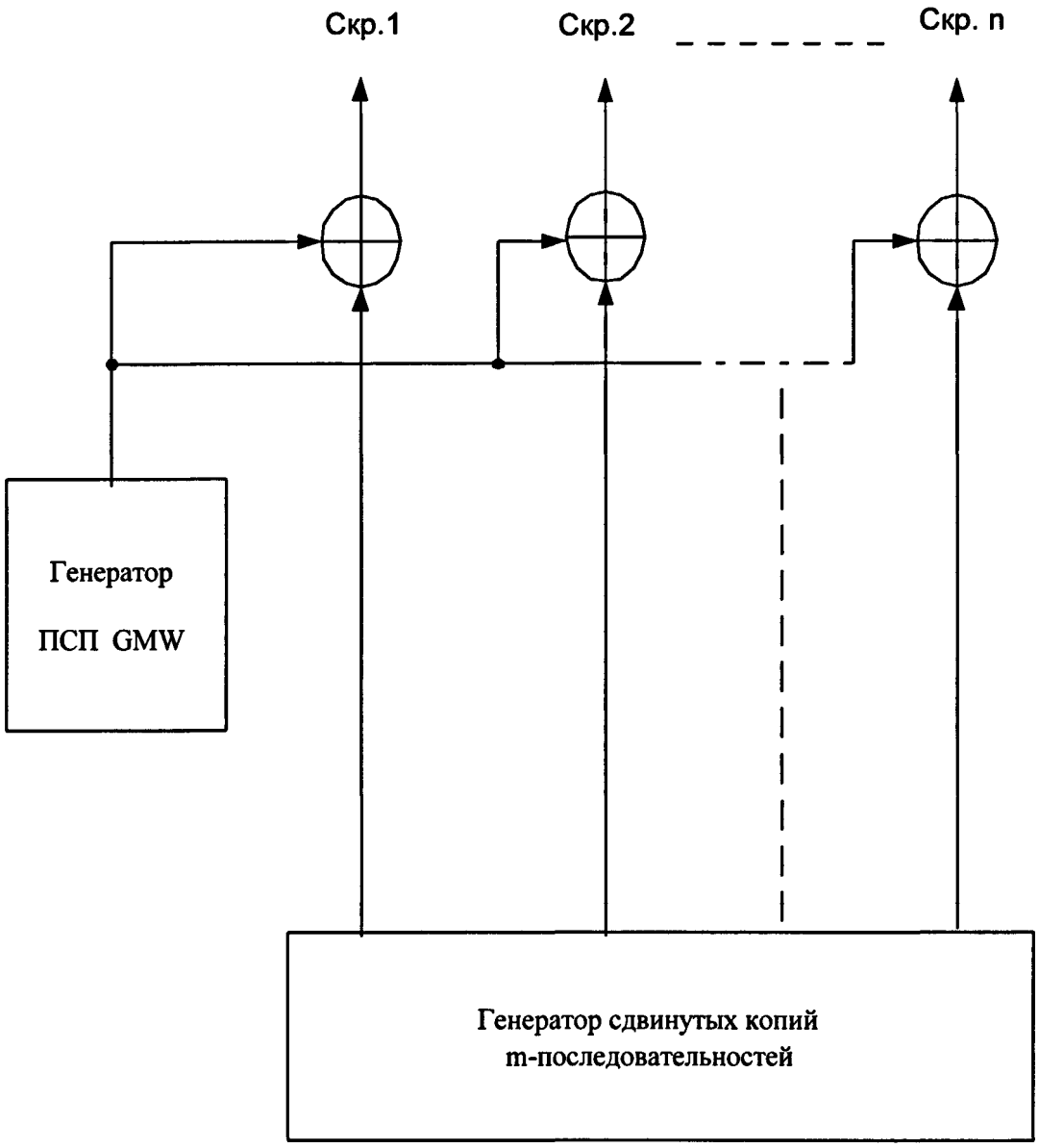

Рис.5.2
Генератор последовательностей скремблера
большой линейной сложности

5.3. Формирование максимальных по объему подмножеств оптимальных последовательностей

При разработке систем CDMA актуальна задача формирования максимальных по объему подмножеств последовательностей типа Адамара, оптимальных в смысле выбранного критерия. От способности решить эту задачу напрямую зависит реальное увеличение числа активных абонентов, т.е. эффективность работы системы. В первой главе были рассмотрены два основных критерия, использующихся при выборе последовательностей: минимаксный, минимизирующий максимальные значения выбросов ВКФ, и минимизации средней вероятности ошибки (критерий AIP). В качестве критерия оптимальности последовательностей выберем минимаксный критерий, поскольку, как было показано ранее, средняя вероятность ошибки в системе DS-CDMA при использовании последовательностей типа Адамара длины 255 и выше мало зависит от выбора этих последовательностей и их начальных фаз. Очевидно, что для таких систем средняя вероятность ошибки будет определяться только числом активных пользователей, а не выбором сигнатурных последовательностей. Выбор же последовательностей скажется на распределении ошибок по времени и на характеристиках подсистем поиска и слежения. В 3-й главе при рассмотрении вопроса формирования подмножеств оптимальных последовательностей типа Адамара длины 127 было показано, что расширение исходной базы для их отбора позволяет увеличить число последовательностей с заданным уровнем взаимной корреляции. Например, можно сформировать множество из семи последовательностей (шести 6-ти m-последовательностей и одной последовательности Лежандра) с пиковым значением θ_c=19, причем в 85% случаях это значение равно 17, тогда как для произвольного подмножества из 7-ми и более m-последовательностей θ_c=41. Далее, для θ_c=27 существуют всего два подмножества из 9 последовательностей класса А, для которых это справедливо. Заметим, что для любого равномощного подмножества

последовательностей из классов S, B и C θ_c=41. Таким образом, чем больше исходное число последовательностей, среди которых производится отбор, тем больше объем подмножества сигнатурных последовательностей с приемлемым уровнем взаимной корреляции. С другой стороны если задаться средней вероятностью ошибки, то максимальное число пользователей K может быть найдено по формуле (1.4). Рассмотрим пример. Пусть в качестве сигнатурных последовательностей используются последовательности типа Адамара длины 1023. Пусть $(E_b/N_0)_{треб}$=10dB, G_p=1023, α=0.5. Тогда K≈204. Согласно таблице 2.5 мощность классов m и GMW последовательностей M=60, а их общее число равно 480. Поэтому требуемое число сигнатурных последовательностей можно получить только при совместном использовании последовательностей этих классов. Отбор последовательностей можно производить исходя из требований на величину максимального выброса ВКФ.

В соответствии с традиционным способом формирования подмножеств последовательностей с приемлемой для систем с CDMA взаимной корреляцией из всего класса m-последовательностей или последовательностей GMW исключают все пары последовательностей, связанных децимациями d_r. В результате этого оставшееся множество последовательностей будет в два или более число раз меньше исходного. Применив такого рода процедуру к оставшимся последовательностям, в конечном итоге можно получить требуемое подмножество. Некоторые авторы, касаясь проблемы выбора псевдослучайных последовательностей для систем связи с DS-CDMA, не без основания полагают, что при длине последовательностей, составляющей величину порядка несколько тысяч и выше, большие значения взаимно-корреляционных пиков могут быть преодолены за счет соответствующей расстановки начальныз фаз этих последовательностей. Действительно в соответстви с известной теоремой Парсеваля уровень остальных выбросов взаимной корреляции у таких последовательностей будет достаточно мал. Вместе с тем проведенные исследования позволяют коренным образом изменить точку зрения на использование пар со

сверхвысокими пиками взаимной корреляции. Действительно из Утверждения 3 раздела 3.3 следует, что за счет выбора соответствующих сдвигов между такими последовательностями они также могут быть использованы в квазисинхронных системах CDMA. На этапе поиска сигнала знание периода появления сверхвысоких пиков взаимной корреляции может быть использовано для уменьшения вероятности ложного захвата за любой из этих пиков.

В качестве примера рассмотрим m-последовательности с N=14. Для этого случая мощность класса M=756, а θ_c=5631. Можно показать, что для каждой такой m-последовательности существует единственная децимация вида (3.18), ведущая к образованию пары со сверхвысокими пиками взаимной корреляции. Поэтому после надлежащей расстановки сдвигов во всех 376 парах m-последовательностей фактическая взаимная корреляция по ансамблю снижается до величины 897. Точно такую же процедуру можно применить и к любому из классов последовательностей GMW. Сходная картина наблюдается при совместном использовании разных классов ПСП GMW или класса m-последовательностей и класса GMW. Заметим, что в этом случае дополнительно появляются пары последовательностей со сверхвысокими пиками взаимной корреляции, принадлежащие различным классам.

К сожалению, для большинства других случаев существуют несколько различных децимаций вида (3.18), при которых выполняются Теоремы 3.1 и 3.2, что делает процедуру расстановки сдвигов несколько более сложной. Кроме того, как следует из (3.18), свехвысокие пики взаимной корреляции могут иметь место и для значений p, отличных от p_u, например 5 или 7 для N=12. Можно показать, что для этих пиков также будет справедлива оценка (3.20) с подстановкой значений p_i вместо p_u.

5.4. m-подобные последовательности над $GF(2^m)$ и их применение в широкополосных системах связи

На сегодняшний день существует достаточно хорошо развитая теория и практика как двоичных, так и q-ичных m-последовательностей. Бесспорно, двоичные m-последовательности являются наиболее простыми с точки зрения генерации, так как в отличие от q-ичных используют обычную булевую логику. Вместе с тем в достаточно большом числе приложений, связанных с кодированием, модуляцией по закону прыгающей частоты и др., применяются q-ичные m-последовательности. Известны исследования, в которых генерация q-ичных m-последовательностей сводится к генерации двоичных [75,76]. Из них наибольший интерес представляет работа [76], касающаяся выявления связей между m-последовательностями над $GF(q^m)$ и GF(q). Согласно [76] любой элемент m-последовательности над $GF(q^m)$ длины q^{nm}-1 может быть представлен в виде линейной комбинации элементов m-последовательности над GF(q) в базисе $GF(q^m)$. Недостатком работы [76] является то, что, доказывая существование такого представления, она в то же время не содержат явного указания на то, как следует выбирать эти q-ичные m-последовательности. Действительно, в [76] в начале строится m-последовательность над $GF(q^m)$, а уже потом с ее помощью строится m-последовательности над GF(q). В настоящей диссертации предпринята попытка обойти эту трудность за счет построения нового класса q-ичных последовательностей длины 2^N-1, где $q=2^m$, $N=mk$, $m\geq 2$, $k\geq 2$, обладающих статистическими свойствами класса m-последовательностей над $GF(2^m)$ и формирующихся на основе сдвинутых копий двоичных m-последовательностей той же длины.

Пусть L есть линейный функционал из $GF(2^N)$ в GF(2) такой, что L(1)=1. Соответственно пусть L_0 есть сужение L до подполя $GF(2^m)$, а L_2 есть линейный

функционал из $GF(2^N)$ в $GF(2^m)$ такой, что для $\forall x \in GF(2^N)$ справедливо $L_0(L_2(x)y)=L(xy)$ для $\forall y \in GF(2^m)$. Тогда согласно [45] последовательность $\{b_n\}$ с элементами вида:

$$b_n = L_2(\alpha^n) \quad , \qquad (5.7)$$

где α есть примитивный элемент $GF(2^N)$ и $0 \le n < 2^N-1$, есть m-последовательность над $GF(2^m)$ длины 2^N-1, а последовательность $\{c_n\}$ с элементами:

$$c_n = L(\alpha^n) \qquad (5.8)$$

есть двоичная m-последовательности длины 2^N-1.

Пусть $\beta=\alpha^\varepsilon$, где $\varepsilon=2^N-1/2^m-1$. Тогда β есть примитивный элемент поля $GF(2^m)$. Пусть $\{d_n\}$ последовательность над $GF(2^m)$ с элементами вида:

$$d_n=L(\alpha^n)+\beta L(\alpha^{n+\varepsilon})+\beta^2 L(\alpha^{n+2\varepsilon})+....+\beta^{m-1}L(\alpha^{n+\varepsilon(m-1)}) \quad . \qquad (5.9)$$

Покажем, что последовательность $\{d_n\}$ имеет период 2^N-1 и не совпадает с классом m-последовательностей $GF(2^m)$. Первое утверждение тривиально и следует из того, что период последовательностей $\{L(\alpha^n)\},....,\{L(\alpha^{n+(m-1)\varepsilon})\}$ есть 2^N-1. Для доказательства второго утверждения представим последовательности $\{b_n\}$, $\{c_n\}$, $\{d_n\}$ в виде двумерных таблиц T_b, T_c, T_d размерности $\varepsilon \times w$, в которых каждый n-ый элемент последовательности стоит на пересечении i строки и j столбца, где $0 \le i < \varepsilon$, $0 \le j < w$, $n=i+j\varepsilon$. Согласно [4] таблица T_b содержит $\varepsilon-2^{N-m}$ нулевых строк, т.е. строк из w $\mathbf{0} \in GF(2^m)$, тогда как остальные строки являются циклическими сдвигами строки с номером i=0 вида 1, β, β^2,...,β^{w-1}. Таблица T_c также содержит $\varepsilon-2^{N-m}$ нулевых строк, однако уже из GF(2). Соответственно остальные являются циклическими сдвигами m-последовательности над GF(2) длины w вида $\{L(\alpha^{j\varepsilon})\}$, $0 \le j < w$.

Далее замечаем, что в силу построения последовательности $\{d_n\}$ нулевые строки таблицы T_d оказываются расположенными на тех же местах, что и в таблицах T_b и T_c. Кроме того, в силу свойства «окна» m-последовательности любые ненулевые строки таблицы T_d будут состоять из w различных ненулевых элементов $GF(2^m)$ и являться сдвигами друг друга.

Предположим теперь, что для некоторого i-ого элемента последовательности $\{d_n\}$ $d_i=1$. Тогда $L(\alpha^i)=1$, $L(\alpha^{i+\varepsilon})=L(\alpha^{i+2\varepsilon})=....L(\alpha^{i+\varepsilon(m-1)})=0$. Рассмотрим строку таблицы T_d, содержащую элемент d_i. В соответствие с (5.9) следующим элементом в этой строке будет

$$d_{i+\varepsilon}=L(\alpha^{i+\varepsilon})+\beta L(\alpha^{i+2\varepsilon})+\beta^2 L(\alpha^{i+3\varepsilon})+....+\beta^{m-1}L(\alpha^{i+\varepsilon m})=\beta^{m-1}L(\alpha^{i+\varepsilon m}).$$

Данная строка не содержит нулевых элементов, поэтому $L(\alpha^{i+\varepsilon m})=1$ и $d_{i+\varepsilon}=\beta^{m-1}$. Таким образом, установлено, что в ненулевой строке T_d за элементом поля **1** всегда следует элемент β^{m-1}. Отсюда следует, что последовательности $\{b_n\}$ и $\{d_n\}$ суть различные последовательности, не являющиеся сдвигами друг друга. Рассуждая аналогично, можно показать, что последовательность $\{d_n\}$ не совпадает также ни с одной другой q-ичной m-последовательностью той же длины. Данное утверждение справедливо применительно к любой другой последовательности $\{d_n'\}$, элементы которой определяются выражением

$$d_n'=L(\gamma^n)+\lambda L(\gamma^{n+\varepsilon})+\lambda^2 L(\gamma^{n+2\varepsilon})+....+\lambda^{m-1}L(\gamma^{n+\varepsilon(m-1)}) \quad , \quad (5.10)$$

где $\gamma=\alpha^t$, t-целое, взаимно простое с 2^N-1, $\lambda=\alpha^{t\varepsilon}=\beta^t$.

Число различных последовательностей $\{d_n\}$ совпадает с числом m-последовательностей степени N над GF(2) , равным $\varphi(2^N-1)/N$, что меньше общего числа m-последовательностей степени N над $GF(2^m)$ в k раз.

Согласно [4,13] псевдослучайный характер последовательностей целиком определяется ее статистическими свойствами. При исследовании статистических свойств последовательностей $\{d_n\}$ будем опираться на известные статистические свойства m-последовательностей $\{b_n\}$ в том виде, как они даны в [4].

Свойство 1(балансное).

Число N_b появления ненулевого символа b на периоде m-последовательности $\{b_n\}$ на 1 превышает число N_0 появления символа **0** на этом периоде, т.е. $N_b=N_0+1$.

Свойство 2.

Число N_a позиций внутри периода последовательности, на которых встречается J-строка $\mathbf{a}=a_1a_2...a_J$, определяется выражением

$$N_a=\begin{cases}2^{N-mJ}, & \text{для } a\neq 0,\quad 1\le J\le k\\ 2^{N-mJ}-1, & \text{для } a=0,\ 1\le J\le k\\ 0 \text{ или } 1, & k<J\end{cases}.$$

Свойство 3 (аддитивно-циклическое).

Разность между m-последовательностью $\{b_n\}$ и ее τ-сдвигом $\{b_{n+\tau}\}$ есть другой ν-сдвиг $\{b_{n+\nu}\}$ той же самой m-последовательности. При этом выполняется

$$b_{n+\nu}=b_{n+\tau}-b_n \quad \text{для всех n.}$$

Свойство 4.

Пусть $\{i_n\}$ есть последовательность целых чисел таких, что

$$i_n=\sum_{j=0}^{J-1} b_{n+j}2^{mj},$$

где $(b_n, b_{n+1},..., b_{n+J-1})$ есть J-строка m-последовательности $\{b_n\}$, а $1\le J\le k$

Пусть $\mathbf{i}_s$ есть последовательность длины 2^N-1, образованная из элементов $\{i_n\}$, начиная с s-го. Тогда для $\tau\neq 0 \bmod(2^N-1)$ расстояние по Хэммингу между $\mathbf{i}_1$ и $\mathbf{i}_{1+\tau}$ вычисляется по формуле

$$H(\mathbf{i}_1,\mathbf{i}_{1+\tau})=2^N(1-2^{-mJ}).$$

Здесь $H(x,y)=\sum_{i=1}^{\nu} h(x_i,y_i)$ есть метрика Хэмминга, где $h(x_i,y_i)$ есть 0,если $x_i=y_i$ и 1 в противном случае.

Теперь покажем, что свойствами 1-4 обладают также построенные выше последовательности $\{d_n\}$. Действительно, выполнение свойств 1-2 для $\{d_n\}$ следует из взаимной однозначности элементов строк таблиц T_d и T_b. Справедливость свойства 3 вытекает из справедливости этого свойства для компонент $L(\alpha^n)\},....,\{L(\alpha^{n+(m-1)\varepsilon})$ элемента d_n. Доказательство свойства 4 для последовательности $\{d_n\}$ вытекает из свойств 2 и

3. Заметим, что одновременно этим доказывается и псевдослучайность последовательности $\{d_n\}$.

Таким образом, последовательности $\{d_n\}$, обладая всеми свойствами m-последовательностей, по-существу, являются m-подобными последовательностями меньшей мощности. Поэтому в дальнейшем последовательности $\{d_n\}$ будем называть m-подобными. Можно построить и другие классы m-подобных последовательностей, получаемых, например, перестановкой компонент в символах $\{d_n\}$ или $\{b_n\}$. Очевидно, такие последовательности также будут обладать свойствами 1-4.

В соответствие с (5.9) генератор m-подобных последовательностей может быть представлен в виде формирователя m сдвинутых друг относительно друга на ε разрядов копий двоичной m-последовательности. Генератор сдвинутых копий достаточно подробно рассмотрен во многих работах, например, в [24]. Он состоит из последовательно соединенных генератора двоичной m-последовательности и блока сумматоров по модулю два (Рис.5.3). Можно указать на две возможные области применения m-подобных последовательностей.

Это широкополосные системы многостанционного доступа с модуляцией прямыми последовательностями (DS-CDMA) и широкополосные системы многостанционного доступа с модуляцией прыгающей частотой (FH-CDMA). Применение m-подобных последовательностей в DS-CDMA носит косвенный характер, выражающийся в том, что основу генератора ПСП GMW (Рис.4.6.) составляет генератор m-подобных последовательностей длины 2^N-1. Кроме того, генератор m-подобных последовательностей может быть использован для получения других семейств нелинейных последовательностей, строящихся на основе m-последовательностей над $GF(2^m)$ и разностных множеств [18].

m-подобные последовательности могут найти применение и в системах с кодовым разделением и модуляцией с прыгающей частотой, закон изменения которой определяется

m-последовательностью над $GF(2^m)$ [4]. Очевидно, в этом случае генераторы m-последовательностей также можно безболезненно заменить более простыми генераторами m-подобных последовательностей. Однако, как справедливо отмечено в [4], недостатком этих последовательностей является их малая линейная сложность, численно равная k. Поэтому в тех случаях, когда требуется большая линейная сложность, используются довольно сложные конструкции, например, обобщенные бент-последовательности [77]. Ниже будет показано, как на основе m-подобных последовательностей за счет незначительного усложнения конструкции могут быть получены последовательности с большей линейной сложностью. Для этого рассмотрим последовательность $\{z_n\}$ длины 2^N-1 с элементами вида

$$z_n=[L_2(\alpha^n)]^t \quad , \quad (5.11)$$

где $1<t<w$-целое число и $(t, 2^N-1)=1$.

Пусть T_z - двумерная (ε,w)-таблица последовательности $\{z_n\}$. Тогда в силу того, что отображение $\beta^j \rightarrow \beta^{jt}$, где $0 \le j < w$, есть изоморфизм поля Галуа $GF(2^m)$, заключаем, что между элементами соответствующих строк таблиц T_b и T_z имеется взаимно однозначное соответствие. С учетом этого нетрудно убедиться, что для последовательностей $\{z_n\}$ справедливы статистические свойства 1,2,4 и не справедливо 3. В соответствие с [4] находим, что линейная сложность L_z последовательности $\{z_n\}$ определяется следующим выражением:

$$L_z=k^u \quad , \quad (5.12)$$

где u-число единиц в двоичном представлении числа t.

При этом максимальное значение $L_z=k^{m-1}$ достигается при $t=(2^{m-1}-1)2^s \bmod (2^N-1)$, где $0 \le s < m$. Аналогично предыдущему заменим m-последовательность $L_2(\alpha^n)$ в выражении (5.11) соответствующей m-подобной последовательностью $\{d_n\}$. В результате генератор последовательности $\{z_n\}$ будет состоять из последовательно соединенных генератора m-подобных последовательностей и ПЗУ объемом $2^m \times m$, по соответствующим адресам

которого хранятся двоичные представления всех элементов поля $GF(2^m)$. В целях упрощения генерации последовательностей с максимальной линейной сложностью выберем t=-1 и рассмотрим отображение L_3: $GF(2^m) \rightarrow GF(2^m)$, удовлетворяющее следующим условиям :

$$(\beta^j)^{-1} \rightarrow \mathbf{L}(\alpha^{\varepsilon(2^m-2-j)}) + \beta^{-1}L(\alpha^{\varepsilon(2^m-3-j)}) + \ldots + \beta^{-(m-1)}L(\alpha^{\varepsilon(2^m-m-1-j)}) \quad \text{и} \quad \mathbf{0 \rightarrow 0} \quad , (5.13)$$

где $0 \le j < 2^m-1$.

Это отображение взаимно однозначное, так как $\{\mathbf{L}(\alpha^{\varepsilon(2^m-2-i)})\}$, где $0 \le j < 2^m-1$, есть m-последовательность длины 2^m-1 и, следовательно, любой ненулевой набор из m последовательных ее символов встречается на ее периоде ровно один раз, причем число различных таких наборов равно 2^m-1. Если теперь в ПЗУ по тем же самым адресам вместо элементов $(\beta^j)^{-1}$ разместить соответствующие им согласно (5.13) элементы, то в результате на выходе такого генератора образуется последовательность с элементами $z_n' = L_3([L_2(\alpha^n)]^{-1})$, которая имеет такие же статистические свойства и линейную сложность, что и последовательность $\{[L_2(a^n)]^{-1}\}$. Нетрудно заметить, что элементы последовательности $\{z_n'\}$ обладают следующим замечательным свойством. Согласно (5.10), (511) двоичные координаты ее элементов в рассмотренном базисе $GF(2^m)$ представляют собой сдвинутые на ε разрядов копии последовательности GMW с базисной m–последовательностью $\{L(\alpha^{-\varepsilon j})\}$, т.е. $z_n' = (gmw_n, gmw_{n+\varepsilon}, \ldots, gmw_{n+\varepsilon(m-1)})$. Основное преимущества данного генератора перед генератором последовательности $\{[L_2(\alpha^n)]^{-1}\}$ состоит в том, что для построения его ПЗУ необходимо лишь знать обратную к $\{L(\alpha^{\varepsilon j})\}$, где $0 \le j < 2^m-1$, последовательность $\{L(\alpha^{-\varepsilon j})\}$, для получения которой достаточно использовать двоичную арифметику над GF(2).

Для построения псевдослучайного генератора для FHMA поступим следующим образом. Пусть $\mathbf{z_n'}$ J-строка последовательных элементов из $\{z_n'\}$. Кроме того, пусть $\mathbf{s(x)}$ произвольное взаимно однозначное отображение $\mathbf{z_n'}$ в множество 2^{Jm} различных частот. Рассмотрим последовательность $f_n = \mathbf{s}(\mathbf{z_n'})$. Тогда для всех $\tau \neq 0$ будет выполняться равенство $H(f_n, f_{n+\tau}) = 2^N - 2^{N-Jm}$. Это следует из свойства (5.10) и взаимно однозначности отображения **s**.

На Рис.5.4. изображена блок-схема такого псевдослучайного генератора для случая J=1. В качестве примера рассмотрим генерацию 2^3-ичной последовательности $\{L_3([L_2(\alpha^n)]^{-1})\}$ длины 4095 на основе генератора m-подобной последовательности с параметрами N=12, m=3 и J=1. Пусть примитивный элемент α поля $GF(2^{12})$ является корнем неприводимого примитивного полинома :

$$X^{12}+X^{11}+X^8+X^6+1 \ . \qquad (5.14)$$

Тогда в соответствие с [49] генератор m-подобной последовательности должен формировать m=3 сдвинутых последовательностей $\{c_n\}$, $\{c_{n+585}\}$, $\{c_{n+1170}\}$, где $c_n=L(\alpha^n)$. Очевидно, последовательности c_{n+585} и c_{n+1170} являются задержанными соответственно на 3510 и 2925 чипов копиями m-последовательности c_n. Формирование задержанных копий m-последовательности наиболее просто осуществить с помощью суммирования по модулю два соответствующих разрядных выходов регистра сдвига генератора m-последовательности по схеме Фибоначчи. Пусть $c_n,c_{n-1},\ldots,c_{n-(N-1)}$ - последовательности, образующиеся на выходах разрядов регистра сдвига этого генератора. Тогда для $c_{n+585}=c_{n-3510}$ и $c_{n+1170}=c_{n-2925}$ с помощью компьютера находим, что:

$$c_{n+585}=c_n+c_{n-1}+c_{n-2}+c_{n-3}+c_{n-5}+c_{n-7}+c_{n-10} \text{ и } c_{n+1170}=c_{n-1}+c_{n-2}+c_{n-8}+c_{n-9}+c_{n-10}\,.$$

Образуем 7-ми элементную ненулевую последовательность $\{e_j\}$, где $e_j=L(a^{585j})$. Это всегда можно сделать путем соответствующего выбора начального состояния генератора последовательности c_n. При L(1)=1 эта последовательность имеет вид: 1101001. Тогда обратная к ней последовательность есть 1001011. Для построения ПЗУ образуем таблицу 5.3, в которой наборам из 3-х подряд идущих символов последовательности $\{e_j\}$, рассматриваемым как двоичные адреса, ставятся в соответствие 3-х разрядные элементы $L_3(\beta^{-j})$.

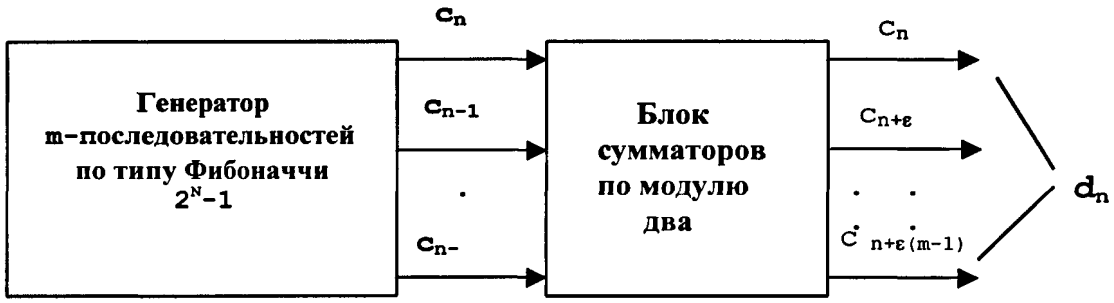

Рис.5.3.

Генератор m-подобной последовательности над $GF(2^m)$.

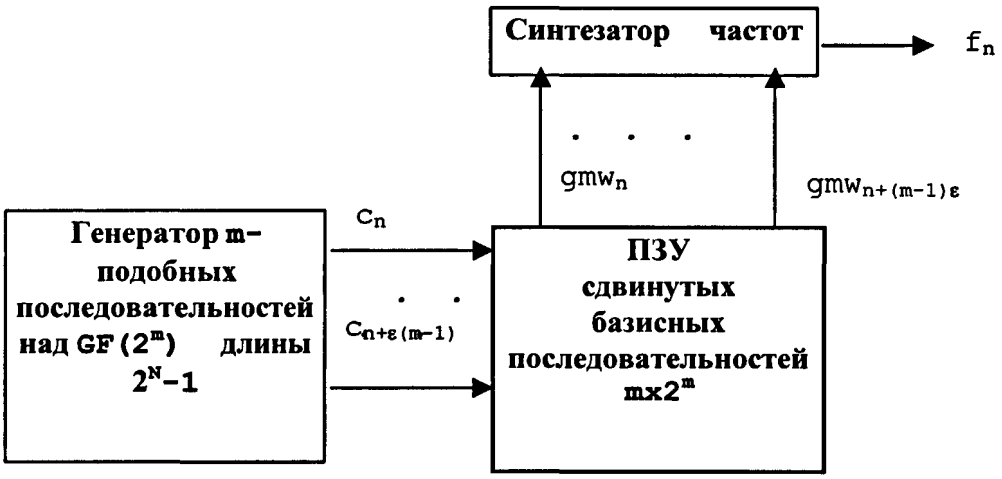

Рис.5.4.

Генератор 2^m -ичной псевдослучайной последовательности повышенной линейной сложности для FHMA .

С учетом того, что по нулевому адресу всегда находится символ 0, после упорядочения таблицы по возрастанию адресного параметра в результате получаем таблицу 5.4, полностью определяющую структуру ПЗУ генератора. Функциональная схема генератора представлена на Рис.5.5. Формируемая последовательность имеет параметры: L=16 и H=3584. Однако, задержав z_n' всего на один разряд и переходя к случаю J=2, можно существенно улучшить параметр H до 4032. При этом число различных частот составит 64. Отметим, что такой же результат можно получить посредством генератора с параметрами N=12, m=6, k=2 и J=1.

К сожалению, генератор на основе последовательности $\{z_n'\}$ позволяет получать только сдвинутые копии последовательности $\{f_n\}$. В то же время описанный в [4] псевдослучайный генератор FH на основе 2^m-ичной m-последовательности обеспечивает генерацию целого семейства последовательностей с элементами $f_n^{\nu}=s(x+\nu)$, где ν - произвольная J-строка, с хорошими Хэмминговыми расстояниями. Анализ показывает, что на основе последовательности (5.11) с помощью преобразования $s(x+\nu)$ также могут быть получены последовательности с такими же Хэмминговыми расстояниями, но значительно большей линейной сложностью.

Таблица 5.3.

Адреса элементов $L_3(\beta^{-j})$.

АДРЕС			$L_3(\beta^{-j})$
1	1	0	100
1	0	1	001
0	1	0	010
1	0	0	101
0	0	1	011
0	1	1	111
1	1	1	110

Таблица 5.4.

Структура ПЗУ генератора m-подобной последовательности над GF(8).

АДРЕС			СИМВОЛ $GF(2^3)$
0	0	0	000
0	0	1	011
0	1	0	010
0	1	1	111
1	0	0	101
1	0	1	001
1	1	0	100
1	1	1	110

Выводы

1. Построенные на основе m-последовательностей и последовательностей GMW ортогональные производные системы сигналов характеризуются большой линейной сложностью и удовлетворительными корреляционными параметрами и могут быть использованы в системах связи с CDMA, требующих повышенную имито и криптозащиту.
2. Предложенный генератор длинного кода на основе последовательности GMW длины 2^{42}-1 позволяет существенным образом повысить безопасность CDMA систем по технологии IS-95 и cdma2000.
3. Найденные закономерности взаимно-корреляционных спектров пар последовательностей со сверхвысокими пиками взаимной корреляции позволяют производить отбор последовательностей для систем связи с CDMA среди всего класса последовательностей, увеличивая тем самым число последовательностей с

приемлемыми корреляционными свойствами. Причем на этапе поиска сигнала знание периода появления сверхвысоких пиков взаимной корреляции может быть использовано для уменьшения вероятности ложного захвата за любой из этих пиков.

4. Построенные новые семейства m-подобных последовательностей высокой линейной сложности могут найти применение в широкополосных системах многостанционного доступа с прыгающей частотой (FHMA).

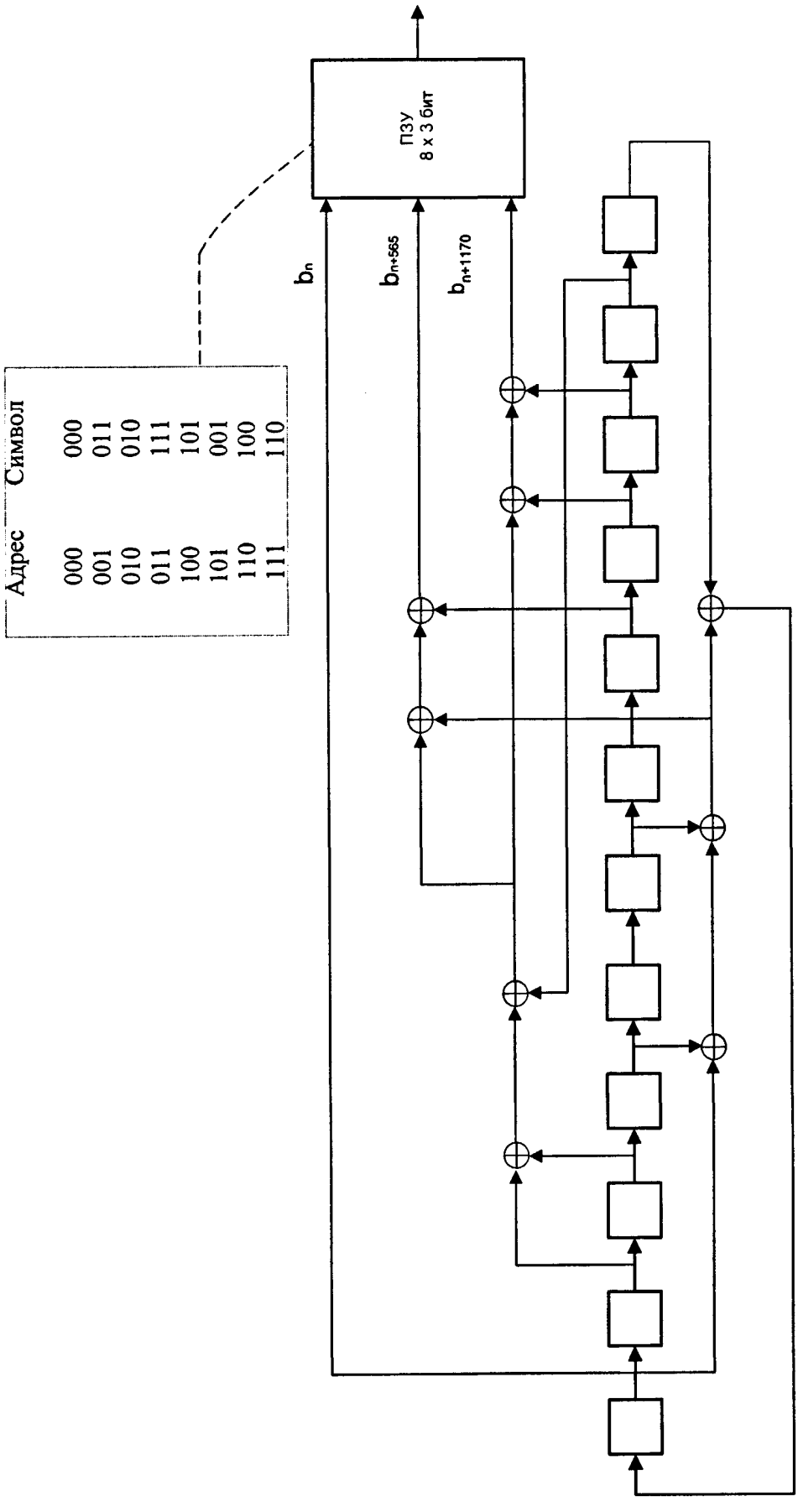

Рис.5.5
Генератор последовательности
над GF(8) длины 4095

Глава 6. Экспериментальная проверка новых классов ПСП в сетях фиксированной связи по технологии CDMA

6.1. Кодовые последовательности для расширения спектра в радиосистеме многостанционного доступа "СТС-ИСТОК CDMA РРК 3/5.0"

В 2000г. российским государственным предприятием СИЛИКОН ТЕЛЕКОМ СОФТ (СТС) были проведены успешные испытания опытного образца цифровой стационарной радиосимстемы многостанционного доступа "СТС-ИСТОК CDMA РРК 3/5.0". Данная система предназначена для построения фиксированной радиосвязи по принципу "точка-точка" и "звезда". Система включает базовую станцию (БС), соединенную по интерфейсу Е1 с местной АТС, и абонентские станции (АС), соединенные по интерфейсу Е1 с учрежденческой АТС или локальными сетями. Связь БС с АС осуществляется по радиоканалу в диапазоне 3,4-3,6 ГГц. В системе СТС-ИСТОК CDMA РРК 3/5.0 реализуются принципы МДКР, цифровой коммутации равнодоступных каналов, предоставляемых по запросу, управления и контроля с помощью микропроцессоров и программ. Каждая станция состоит из цифрового модема, реализованного на цифровых сигнальных процессорах типа ADSP-21061 SHARC, программируемых логических схемах типа FPGA XCS40XL-4 и микросхем СТ812, интерфейсов Е1 для связи с АТС, радиочастотного блока и антенного устройства.

Основные технические параметры радиосистемы СТС-ИСТОК CDMA РРК 3/5.0 следующие:

- полоса частот широкополосного сигнала – 5 МГц;
- мощность передатчика: 0,25; 0,35 Вт;

- максимальное число АС на одну БС при односекторной антенне и использовании одной несущей – 2;
- общая скорость в радиоканале 4,096Мбит/с;
- максимальное число предоставляемых на БС стандартных каналов со скоростью 64 Кбит/с – 60;
- максимальное число абонентских линий, подключаемых к одной АС – от 30 до 60;
- модуляция данных осуществляется методом квадратурной фазовой модуляции (QPSK) для каждого отдельного канала, групповой сигнал соответствует модуляции QAM;
- вероятность ошибки на бит передаваемой информации при передаче речевых сообщений и данных в отсутствии многолучевости составляет не более 10^{-6} и 10^{-7} соответственно;
- для расширения спектра и кодового разделения каналов в прямом и обратном направлениях используются ансамбли ортогональных ПСП длины 128.

Синхронизация осуществляется в обоих направлениях посредством пилот сигналов, образованных на основе последовательностей данного ансамбля и ортогональных сигналам информационных каналов. Применение пилот сигнала позволяет упростить поиск и поддерживать синхронизм во времени между принимаемыми и опорными сигналами в приемнике, облегчить выделение когерентного напряжения в блоке ФАПЧ для когерентного детектирования сигналов синфазной и квадратурной составляющих, задать цикловую синхронизацию всем АС для декодирования помехоустойчивого кода. При этом в качестве последовательностей пилот сигналов выбираются последовательности с наилучшими авто и взаимно-корреляционными свойствами. Для того, чтобы ортогональность сохранялась и на входе приемника БС в системе осуществляется жесткая временная синхронизация всех АС по пилот сигналу БС и вычисление всех временных задержек прохождения радиосигнала от БС к каждой АС с высокой точностью с последующей компенсацией этих задержек. Поэтому

данная система радиодоступа является полностью ортогональной в прямом и обратном направлениях, т.е. OCDMA системой. Наряду с выравниванием задержек в системе также реализуется и алгоритм выравнивания мощностей АС. Для борьбы с многолучевостью применяется когерентный RAKE-приемник, работающий по трем лучам. Модульное построение системы позволяет оптимизировать ее по числу пространственных секторов и числу несущих частот в зависимости от числа и расположения абонентов в зоне обслуживания.

Рассмотрим более подробно принципы построение системы ортогональных сигналов, используемых в радиосистеме СТС-ИСТОК CDMA РРК 3/5.0

Как известно, системы ортогональных сигналов на основе циркулянтных матриц Адамара обладают плохими ВКФ. Это приводит к росту межканальных интерференционных помех, обусловленных действием многолучевости. Поэтому на практике с целью уменьшения уровня интерференционных помех более целесообразно использовать производные ортогональные системы сигналов, имеющие относительно лучшие взаимно-корреляционные характеристики.

В этой связи были исследованы производные системы сигналов, полученные в результате наложения сверху на строки циркулянтной матрицы Адамара порядка 128 одной и той же производящей кодовой последовательности. В качестве производящей кодовой последовательности была взята m-последовательность вида: 00010111000010000110100000111110110000001010110111111100110110101010001001001100 11110001110111010111101001011001010011100100011 0 с характеристическим полиномом $x^7+x^6+x^5+x^2+1$. Такой выбор обусловлен следующими обстоятельствами:

- минимальным среди всех возможных других последовательностей значением бокового выброса, равным 12, ее четной и не четной АКФ;

- исходя из минимизации взаимно-корреляционных пиков последовательностей во вновь образованных производных системах;
- исходя из максимизации численности сбалансированных ортогональных последовательностей.

Эта последовательность в силу ее хороших корреляционных свойств была использована в качестве пилот сигнала прямого канала. Ниже она обозначена через m1.

В качестве исходных последовательностей при построении матриц Адамара 128 использовались 79 ПСП типа Адамара длины 127 из семейств:

- m-последовательностей $(m2 \div m18)$;
- последовательностей Лежандра $(l1 \div l2)$;
- последовательностей Холла $(h1 \div h6)$;
- последовательностей А типа $(A1 \div A18)$;
- последовательностей В типа $(B1 \div B18)$;
- последовательностей С типа $(C1 \div C18)$.

Все вышеперечисленные последовательности вместе с последовательностью пилот сигнала m1 представлены в Приложении 2. Построенная таким способом производная система сигналов 128 будет состоять из 127-ми последовательностей вида $r_i = m1 + T^i u$, где $0 \le i \le 126$, $m1$ – производящая последовательность, u – исходная последовательность, T^i - оператор сдвига на i разрядов, и самой последовательности *m1*.

Основными критериями при выборе систем сигналов были следующие:

- минимальный уровень боковых лепестков АКФ;
- минимальный уровень выбросов ВКФ;

- максимальное число сбалансированных последовательностей.

Заметим, что для низкоскоростных систем абонентского доступа максимальное число индивидуальных абонентов определяется максимальным числом сбалансированных последовательностей в выбранном ансамбле. Это вызвано тем, что для последовательностей пилот сигналов лучше всего использовать последовательности с равным количеством нулей и единиц. Поэтому при анализе ортогональных систем последовательностей учитывалось также и число имеющихся сбалансированных последовательностей.

При проведении математического моделирования вышеперечисленных производных систем сигналов с помощью системы MATLAB 5.3 на компьютере Pentium 2 были выполнены расчеты их корреляционных характеристик, представленные в таблице 6.1. Сравнительный анализ корреляционных характеристик систем сигналов на основе перечисленных в Приложении 2 исходных последовательностей позволяет сделать следующие выводы.

1. С точки зрения первых двух критериев выбора производные системы m3, m6, m14, и m16 являются наилучшими.
2. Системы сигналов на основе m-последовательностей, образующих с производящей последовательностью m1 последовательности Голда, содержат ровно 64 сбалансированные последовательности. Всего имеется 10 таких систем.
3. Максимальным числом сбалансированных последовательностей, равным 84, обладают производные системы на основе последовательностей типа A и C (последовательности A14, C5 и C14).
4. Системы, образованные на основе голдовских пар m-последовательностей обладают наименьшими выбросами ВКФ при сдвигах на ± 20 чипов относительно нулевого сдвига (точки ортогональности) по сравнению с другими системами.

5. При минимальных значениях обобщенных параметров θ_a=40 и θ_c=48 наилучшей с точки зрения выбора пилот сигналов является система сигналов m14. При этом максимум бокового выброса автокорреляции, взятый по всему множеству последовательностей пилот сигналов, равен 36.

6. Указанное в пункте 5 значение может быть уменьшено до 32 в случае системы C14, имеющей 84 сбалансированных последовательностей, что в целом улучшает выбор множества пилот сигнальных последовательностей. Заметим, что при дальнейшем уменьшении этого параметра до 28, количество возможных пилот сигналов в системах m14 и C14 составляет соответственно 52 и 61. Более того, система C14 содержит 11 сбалансированных последовательностей с θ_a=20 против 5 аналогичных последовательностей в m14.

7. Все системы сигналов на основе последовательностей семейств h,*l*,A,B,C являются нелинейными, что существенным образом повышает их криптостойкость по сравнению с системами на основе m- последовательностей.

При проведении испытания аппаратуры СТС-ИСТОК CDMA РРК 3/5.0 использовались две системы сигналов: не оптимальная m2 и оптимальная m14. При этом испытания на реальных радиолиниях проводились в отсутствие многолучевости, а работа в режиме многолучевости проверялась посредством ее имитации в лабораторных условиях. Испытания на реальных трассах показали возможность обеспечения почти полной ортогонализации сигналов АС на входе приемника БС за счет выравнивания их задержек. Кроме того, была продемонстрирована инвариантность выбранных ортогональных систем сигналов в случае отсутствия действия помех, вызванных многолучевостью. В этом случае измеренная вероятность ошибки при полной загрузке системы, т.е. при 60-ти работающих информационных каналов, оказалась не хуже 10^{-7}. При имитации многолучевости использовались два луча с задержкой соответственно 2 и 5 чипов и такой же мощности, что

и основной сигнал. Результаты эксперимента показывают, что при небольших задержках рассматриваемые ортогональные системы m2 и m14 примерно одинаковы. Такое совпадение обусловлено поведением их корреляционных характеристик, которые при сдвигах менее 20 чипов мало отличаются друг от друга.

Таблица 6.1.

Обобщенные корреляционные параметры производных ортогональных систем сигналов.

Тип системы	$N_{сбал}$	θ_a	θ_c
m2	64	56	52
m3	-//-	40	48
m4	-//-	48	48
m5	-//-	48	48
m6	-//-	40	48
m14	-//-	40	48
m15	-//-	48	48
m16	-//-	40	48
m17	-//-	48	56
m18	-//-	48	48
A4	-//-	44	56
A5	-//-	48	52
A7	-//-	44	56
A14	84	52	56
B2	-//-	44	56
B9	-//-	48	56
B14	-//-	44	52
C5	84	44	52
C7	-//-	48	56
C8	-//-	44	52
C10	-//-	40	56
C11	-//-	40	52
C12	-//-	48	56
C14	84	48	48
$h1$	64	40	52
$l1$	22	44	52

$N_{сбал}$ - число сбалансированных последовательностей;

θ_a - максимальный уровень боковых лепестков АКФ;

θ_c - максимальный уровень выбросов ВКФ.

Выводы

1. Экпериментальные исследования продемонстрировали возможность достижения почти полной ортогонализации сигналов АС на входе приемника БС за счет выравнивания их задержек. При этом число одновременно работающих информационных каналов с BER=10^{-7} составило 60.
2. Испытания показали правильность выбора в качестве последовательности пилот сигнала производящей m-последовательности значности 127 типа m1.

Заключение

Настоящая диссертация является результатом многолетней работы по поиску и исследованию ансамблей псевдослучайных последовательностей с хорошими корреляционными свойствами для широкополосных систем связи с кодовым разделением каналов. Основная задача, решаемая в диссертации, заключается в конструировании новых классов ПСП с хорошими корреляционными свойствами, строящихся на основе совершенных разностных множеств типа Адамара, и исследовании их свойств, а также разработке сравнительно простых методов и устройств их генерации для систем с кодовым разделением каналов и многостанционным доступом. Проведенные исследования позволяют сформулировать следующие результаты диссертации:

1. На основе предложенной классификации двоичных последовательностей GMW сформулированы и доказаны условия их эквивалентности, а также найдена формула для расчета общего числа этих последовательностей. Данная формула более универсальна по сравнению с формулой Голомба-Гонга-Дейя, область применения которой ограничена классами ПСП GMW каскадного типа на основе m-последовательностей.
2. Разработаны новые методы расчета линейной сложности двоичных последовательностей GMW, для которых не могут быть использованы известные аналитические методы, а также получены оригинальные результаты расчета их сложности на компьютере для $N \leq 24$. Показано, что линейная сложность большинства классов ПСП GMW на основе нелинейных базисных последовательностей выше, чем у ПСП GMW на основе m-последовательностей и

этот выигрыш с ростом N увеличивается. Получена формула для оценки линейной сложности ПСП GMW.

3. Разработан новый метод исследования взаимно-корреляционных функций двоичных последовательностей типа Адамара на основе разбиения их изоморфных коэффициентов на смежные классы по подгруппе максимального порядка. Данный метод позволяет в M-1 раз сократить объем вычислений ВКФ, производимых на компьютере
4. Найдены новые оценки нижних границ максимума взаимной корреляции семейств m-последовательностей, последовательностей GMW, последовательностей Холла и Лежандра. Показано, что полученные оценки могут быть использованы для эффективного отбора последовательностей с заданными корреляционными свойствами при проектировании систем с CDMA.
5. На основе найденных новых свойств пар m и GMW последовательностей со сверхбольшими значениями выбросов взаимной корреляции обоснована возможность их совместного использования наряду с другими последовательностями в CDMA системах.
6. Проведено исследование основных параметров (мощности, корреляционных свойств и линейной сложности) всех известных последовательностей типа Адамара длины 127. Показана возможность расширения подмножеств последовательностей с хорошими корреляционными параметрами за счет включения последовательностей из разных семейств.
7. Разработан новый более простой по сравнению с методом Шольца - Велча метод генерации двоичных последовательностей GMW на основе сдвинутых копий двоичной m-последовательности той же длины и его схемное решение. Использование данного метода позволит перевести рассмотрение

последовательностей GMW из абстрактно-теоретической области в практическую плоскость.

8. Получены новые ансамбли ортогональных сигналов большой линейной сложности на основе систем производных последовательностей, в которых исходной является m-последовательность, а производящей соответственно последовательность GMW. Данные ансамбли могут успешно использоваться в системах CDMA, требующих повышенную защиту информации без существенных аппаратных затрат.
9. Разработан новый метод повышения безопасности передачи данных в системах связи с CDMA на основе стандартов IS-95 и cdma2000, в котором в качестве скремблирующей последовательности вместо m-последовательности предлагается использовать последовательность GMW той же длины, но значительно большей линейной сложности. Разработаны оригинальные схемотехнические решения, позволяющие совместить высокую степень защиты передаваемой информации с приемлемой сложностью аппаратной реализации.
10. На основе нового метода генерации ПСП GMW получены новые ансамбли q-ичных последовательностей большой линейной сложности для систем с FH-CDMA и схемы их генерации, основанные на генераторе ПСП GMW.
11. Получены экспериментальные доказательства возможности использования разработанных на базе последовательностей типа Адамара длины 127 новых ортогональных систем сигналов для действующей радиосистемы многостанционного доступа "СТС-ИСТОК CDMA РРК 3/5.0", подтверждающие результаты математического моделирования.

Основные результаты работы докладывались на НТК профессорско-преподавательского состава МТУСИ в 1996-2001гг., на третьей международной научно-технической конференции "Микроэлектроника и информатика" (г. Москва, Зеленоград) в 1997г., на второй и третьей международных конференциях "Цифровая обработка сигналов и

ее применение" (г. Москва) в 1999-2000гг., на шестой и седьмой научно-технических конференциях "Радиолокация, навигация, связь" (г.Воронеж) в 20000-2001гг. Перечисленные публикации включают основные научные результаты и выводы, полученные в настоящей диссертации.

Результаты диссертации внедрены в разрабатываемые на государственном предприятии ЦКТ "Силикон-Телеком-Софт" системы фиксированной связи абонентского доступа по технологии DS-CDMA. В дальнейшем хорошие перспективы для широкополосной связи могут иметь исследования как новых семейств последовательностей No-Golomb-Gong-Lee-Gaal и Сегре-Глайна, так и новых классов последовательностей GMW, строящихся на их основе. Значительное увеличение числа последовательностей с идеальной автокорреляцией ставит перед их исследователями другую не менее важную для практики задачу: нахождение аналитических методов формирования из них необходимого числа последовательностей с заданным уровнем взаимной корреляции. Определенная попытка ее решения была предпринята в настоящей диссертационной работе. При этом основу предлагаемого метода формирования составляют найденные аналитические оценки нижних границ максимума взаимной корреляции ансамблей m и GMW последовательностей. Подобного рода исследования проводятся и во многих других странах мира, и, судя по предварительным результатам, есть основания полагать, что в будущем эта проблема будет успешна решена.

Библиографический список использованной литературы

1. Окинавская хартия глобального информационного общества, принятая 22 июля 2000г. лидерами стран G8 - //http//www.ibo.ru/online/legal-deal/akt/6027.
2. Невдяев Л.М. Мобильная связь 3-го поколения //под редакцией Ю.М. Горностаева.- М.: Связь и Бизнес, 2000.
3. Громаков Ю.А. 3-е поколение – динамика развития. – Мобильные системы, №3, 2000.
4. M.K. Simon, J.K. Omura, R.A. Scholtz, B.K. Levit. Spread spectrum communications handbook. – McGraw-Hill,Inc., 1994.
5. Варакин Л.Е., Анфилофьев С.А. Технология CDMA в современных системах радиосвязи. – Мобильные системы, Спецвыпуск по стандарту CDMA, 1998.
6. Трофимов Ю.К. Перспективы использования технологии CDMA в сетях подвижной связи третьего поколения. - Мобильные системы, Спецвыпуск по стандарту CDMA, 1998.
7. Golomb S.W. Shift-register sequences and spread-spectrum communications. – Third International Symposium on Spread Spectrum Techniques and Application, Oulu, Finland, July, 1994.
8. M. B. Pursley and H.F. Roefs. – Numerical evalution of correlation parameters for optimal phases of binary shift-register sequences. – IEEE Trans. Commun., vol.COM-27, 1979.
9. Стельмашенко Б.Г., Тараненко П.Г. Нелинейные псевдослучайные последовательности в широкополосных системах передачи информациии. – Зарубежная радиоэлектроника, №9, 1988.

10. Цифровые методы в космической связи // под ред. С. Голомба. – Изд-во Связь, Москва, 1969.

11. P.V Kumar. Recent results on sequences with low autocorrelation. – 1999 IEEE ITW, Kruger National Park, South Africa, June, 1999.

12. Архипкин В.Я., Кренгель Е.И., Соколов А.Г. Псевдослучайные последовательности для систем связи CDMA. – 7-ая Международная научно-техническая конференция " Радиолокация, навигация и связь", г.Воронеж, апрель, 2001.

13. Golomb S.W. Shift register sequences.- AEGEAN PARK PRESS, Laguna Hills, California, 1982.

14. Кренгель Е.И. О числе псевдослучайных последовательностей Гордона, Милза, Велча. - Техника средств связи, Сер. ТРС, вып. 3,1979.

15. J.S. Lee, L.E. Miller. CDMA systems engineering handbook. - Artech House, Boston-London, 1998.

16. Агеев Д.В. Основы теории линейной селекции. – Научно-технический сборник ЛЭИС, №10, 1935г.

17. T. Ojanpera, R. Prasad. Wideband CDMA for third generation mobile communications. – Artech House, Boston-London, 1998.

18. Ипатов В.П. Периодические дискретные сигналы с оптимальными корреляционными свойствами. – М.: Радио и связь, 1992.

19. I. L. Key. Analysis of the structure and complexity of non-linear binary sequence. - IEEE Trans. on Inform. Theory, vol. IT-22, №6, 1976.

20. Сарватер Д.В., Персли М.Б. Взаимно-корреляционные свойства псевдослучайных и родственных последовательностей. – ТИИЭР, N5, 1980.

21. А. с. N 632067, кл.H03 K/84 с приоритетом от 03.05.1977. Генератор псевдослучайных последовательностей двоичных сигналов / К.А. Мешковский, Е.И Кренгель.

22. А. с. N 674204, кл.H03 K/84 с приоритетом от 05.07.1977. Генератор псевдослучайных последовательностей двоичных сигналов / К.А. Мешковский, Е.И Кренгель.

23. Ипатов В.П., Камалетдинов Б.Ж., Самойлов И.М. Дискретные последовательности с хорошими корреляционными свойствами. – Зарубежная радиоэлектроника, N9, 1989.

24. Бессарабова А.П. Журавлев В.И. Псевдослучайные последовательности сигналов и их применение в технике связи. – Итоги науки и техники. Сер. Связь, Москва, ВИНИТИ, №7, 1991.

25. P.Udaya and M.U. Siddiqi. Optimal biphase sequences with large linear complexity derived from sequences over Z4. - IEEE Trans. Inform. Theory, vol.42, No.1, 1996.

26. G.Gong. New designs for signal sets with low cross-correlation, balance property and large linear span: GP(2) case. – CACR, University of Waterloo, 1999.

27. J.S. No and V.P. Kumur. A new family of binary pseudo-random sequences having optimal periodic correlation properties and large linear span. – IEEE Trans. Inform. Theory, vol.35, no.2, March, 1989.

28. P.V. Kumar, D.J. Shin, K. Shum. On sequence design for CDMA. – IEEE ISSSTA96, September, Mainz, Germany.

29. G. Gong. Theory and applications of q-ary interleaved sequences. – IEEE. Trans. Inform. Theory, vol.41, No.2, March, 1995.

30. A. M. Klapper. D-form sequences: families of sequences with low correlation values and large linear spans. – IEEE. Trans. Inform. Theory, vol.41, No.2, March, 1995.

31. J.S. No, S. Golomb, G. Gong, H. K. Lee, P. Gaal. Binary pseudorandom sequences of period 2^n-1 with ideal autocorrelation. - IEEE. Trans. Inform. Theory, vol.44, No.2, March, 1998.

32. Цифровые методы в космической связи /под ред. С. Голомба. – Изд-во Связь, Москва, 1969.

33. L.D. Baumert and Fredrickson. The cyclotomic numbers of order 18 with application to difference sets.- Math. Comp., vol.21, 1967.

34. A. Klapper, A.H. Chan, M. Goresky. Cascaded GMW sequences.- IEEE Transactions on Information Theory, vol.39, No.1,1993.

35. J.-S No, K.Yang, H.Chung and H.-Y. Song, "On the construction of binary sequences with ideal autocorrelation property",- in Proc. IEEE ISITA'96, pp. 837-840, Sept. 1996.

36. S.Bychenkov, "New GMW-sequences with analytically estimated values of cross-correlation maximums", in Proc. ITC-CSCC, vol.2, 1996.

37. J.S.No, H. Chung and M.S. Yin. Binary pseudorandom sequences of period 2^m-1 with ideal autocorrelation generated by polynomial $z^d+(z+1)^d$. - IEEE. Trans. Inform. Theory, vol.44, No.3, 1998.

38. Q. Xiang. On balanced binary sequences with two-level autocorrelation functions. - IEEE. Trans. Inform. Theory, vol.44, No.7, 1998.

39. P.V Kumar. Recent results on sequences with low autocorrelation. – 1999 IEEE ITW, Kruger National Park, South Africa, June, 1999.

40. K. H. Karkkainen. Mean-square cross-correlation as a performance for spreading code families. – IEEE Second International Symposium on Spread Spectrum Techniques and Application, Yokohama, Japan, December,1992.

41. K. H. Karkkainen, M.J. Laukkanen and H.K. Tarnanen. Perfomance of asynchronous DS-CDMA system with long and short spreading codes – Electronics letters, vol.30, No.13, 23rd June, 1994.

42. Кренгель Е. И., Мешковский К.А. О линейной сложности псевдослучайных последовательностей GMW. // Повышение эффективности цифровых и аналоговых средств радиосвязи / Моск. техн. ун-т связи и информатики. – М., 1998.-Библиограф.: 7 назв.- Рус. –Деп. в ЦНТИ "Информсвязь", №2125 от 5.05.98.

43. М.Холл. Комбинаторика. – М., Мир, 1970.

44. Gordon B., Mills W.,Welch L. Some new difference sets.- Canad.Jornal Math., 14(1962).

45. L.D. Baumert. Cyclic difference sets. – Berlin, Springer-Verlag, 1971.

46. R.A.Scholtz, L.R.Welch. GMW sequences.- IEEE Trans. Inform. Theory, vol. IT-30, №9, 1984.

47. L.C.Quynh, S.Prasad. Class of binary ciper sequences with best possible autocorrelation function. - IEE Proc., vol.132-F, N7, 1985.

48. A.Klapper, A.Chan, M.Goresky, "Cross-correlation of linearly and quadratically related geometric sequences and GMW sequences", Discrete Applied Mathematics, vol.46, N1,1993.

49. Мешковский К.А., Кренгель Е. И.Генерация псевдослучайных последовательностей Гордона, Милза, Велча. – Радиотехника, N5, 1998.

50. Мешковский К.А., Кренгель Е. И. Классификация последовательностей Гордона, Милза, Велча. – Радиотехника, N12, 2001.

51. Ван-дер-Варден Б.Л. Современная алгебра. – изд-во "Наука", 1975.

52. Gong G., Dai Z.D., Golomb S.W. Enumeration and criteria for cyclically shift-distinct GMW sequences. - IEEE Trans. Inform. Theory, vol. 46, No.2, 2000.

53. Weng L.J. Decomposition of m-sequences and its applications. – IEEE Trans. Inform. Theory, vol. IT-17, No.4, 1971.

54. Смирнов Н.И. Применение М-последовательностей в асинхронных радиотехнических системах. – Электросвязь, №7, 1970.

55. Шумоподобные сигналы в системах передачи информации. // Под ред. проф. В. Б. Пестрякова. – М.: "Сов. Радио", 1973.

56. Chung H. and J.S. No. Linear span of extended sequences and cascaded GMW sequences. - Trans. Inform. Theory, vol.45, No.6, 1999.

57. Кренгель Е, И. Метод исследования корреляционных функций периодических последовательностей.- Техника средств связи, сер.ТРС, вып.3, 1980.

58. Свердлик М.Б. Оптимальные дискретные сигналы. – М.: Советское радио, 1975.

59. Виноградов И. М. Основы теории чисел. – М.: Наука, 1972.

60. T. Helleseth. Some results about cross-correlation function between two maximal linear sequences. – Discrete Mathematics, Vol.16, 1976.

61. A.Z.Tirkel. Cross-correlation of m-sequences-Some unusual coincidences.-1996 IEEE 4 th International Simposium on Spread Spectrum Techniques and Applications Proceedings, September 22-25,Mainz,Germany.

62. Мешковский К.А, Кренгель Е.И. Взаимная корреляция некоторых классов псевдослучайных последовательностей. – Радиотехника, N6, 2000.

63. Мешковский К.А, Кренгель Е.И. Генератор псевдослучайных последовательностей Гордона, Милза, Велча. - Техника средств связи, сер.ТРС, вып.3, 1979.

64. Миллер Ф.,Мешковский К.А., Кренгель Е.И., Архипкин В.Я., Соколов А.Г. Псевдослучайные последовательности значности 127 для систем связи с CDMA - Сб. тез.

докл. 3-я международная НТК "Микроэлектроника и информатика", Москва,1997 - С.80-83.

65. Миллер Ф., Мешковский К.А., Кренгель Е.И., Архипкин В.Я., Соколов А.Г. Кодовое разделение каналов на основе псевдослучайных последовательностей значности 127. – Сборник докладов 3-ей Международной Конференции DSPA2000, Vol.3, Москва, 2000г.

66. Архипкин В.Я., Кренгель Е.И., Соколов А.Г. m-последовательности и последовательности GMW с сверхвысокими пиками взаимной корреляции и их применение в системах с CDMA. - 6-ая Международная научно-техническая конференция " Радиолокация, навигация и связь", г.Воронеж, апрель, 2000.

67. Мешковский К.А. Новый класс псевдослучайных последовательностей двоичных сигналов. - Проблемы передачи информации,Том IX,Вып.3,1973.

68. Питерсон У. Коды, исправляющие ошибки. – М.:, Мир, 1964.

69. Варакин Л.Е. Теория систем сигналов. — М.: Советское радио, 1978.

70. Кренгель Е. И., Мешковский К.А. Ортогональные производные системы сигналов большой линейной сложности. // Повышение эффективности цифровых и аналоговых средств радиосвязи / Моск. техн. ун-т связи и информатики. – М., 2000.-Библиограф.: 7 назв.- Рус. –Деп. в ЦНТИ "Информсвязь", №21174 Св. 2000 от 20.04. 2000.

71. Конопелько В.К., Юрцевич Д.М., Юрцевич М.М. М-подобные нелинейные последовательности с идеальными автокорреляционными свойствами. // Труды 1-ой международной конференции "Цифровая обработка сигналов и ее применение" — DSPA'98, 1998, Москва.

72. V.K. Garg, K. Smolik, J.Wilkes. Applications of CDMA in wireless/ personal communications. – Prentice Hall PTR, 1997.

73. Кренгель Е.И. Повышение безопасности систем передачи данных на основе стандарта IS-95. - Сборник докладов 2-й Международной Конференции DSPA'99, Vol.2, Москва, 1999- С.463-465.

74. Games A.R. Cross-correlation of m-sequences and GMW-sequences with the same primitive polynomial. – Journal Discrete applied mathematics, 12, 1985.

75. Krone S. M., Sarwate D.V. Quadriphase sequences for spread-spectrum multiple access communication. – IEEE Trans. Inform. Theory, vol. 30, No. 5, 1984.

76. Park W.J., Komo J.J. Relationships between m-sequences over GF(q) and GF(q^m). - IEEE Trans. Inform. Theory, vol. 35, No. 1, 1989.

77. P.V Kumar. Frequency-hopping code sequence designs having linear span. - IEEE Trans. Inform. Theory, vol. 34, No. 1, 1988.

Приложения

Приложение 1

Тексты программ расчета координат векторов сдвигов генераторов ПСП GMW

Программа расчета координат сдвигов для N=8 и m=4.

```
#include <stdio.h>
#include <memory.h>
static unsigned int sqw[8];
  static unsigned int bas[18];
  void multi_xa(int);
  void multi_uv( unsigned int, unsigned int, unsigned int *);
  void qdr( unsigned int *);
  static   unsigned int x=1,vr=2,ur,zr=2,vt;
  main( )
  {  int i,j,n;
    sqw[0]=1;
    for(i=1;i<15;i++)
     { multi_xa(&x);
     printf("%x\n\r",x);
     if(!(i%2)) sqw[i/2]=x;
     }
   for(i=0;i<17;i++)   printf("%x\n\r",sqw[i]);
    for(n=0;n<1;n++)
        { for(i=0;i<4;i++) {
          qdr(&vr);  printf("%x\n\r",vr);      }
          vt=vr;
          ur=zr;
          multi_uv(ur,vr,&zr);
          printf("%x %x\n\r",vt,zr);
          vr=vt;
         }
        vr=zr;
        vt=vr;
        bas[0]=1;
        bas[1]=zr;
        for(i=2;i<17;i++)
         { ur=zr;
           multi_uv(ur,vr,&zr);
           bas[i]=zr;
           vr=vt;
          }
   for(i=0;i<17;i++)   printf("%x\n\r",bas[i]);
    }
```

```
void qdr(unsigned int *w)
 { int i,j;
  unsigned int rez=0,mask1=1,mask2=1;
  for(i=0;i<8;i++)
  {  if(*w & mask1) rez=rez^sqw[i];
       mask1<<=1;
  }
  *w=rez;
  }

void multi_xa(unsigned int *px)
 { if( *px & 0x0080)
       { *px<<=1;
        *px^=0x001d;
        }
       else *px<<=1 ;
   *px&=0x00ff;
 }

 void multi_uv( unsigned int u, unsigned int v, unsigned int *z)
  { int i;
   *z=0;
   for(i=0;i<8;i++)
   { if(v & 0x0001) *z^=u;  *z &=0x00ff;
        multi_xa(&u) ;
        v>>=1;  v&=0x00ff;
       }
   }
```

Программа расчета координат сдвигов для N=9 и m=3.

```
#include <stdio.h>
#include <memory.h>
static unsigned int sqw[9];
  static unsigned int bas[14];
  void multi_xa(int);
  void multi_uv( unsigned int, unsigned int, unsigned int *);
  void qdr( unsigned int *);
  static  unsigned int x=1,vr=2,ur,zr=2,vt;
  main( )
  {  int i,j,n;

    sqw[0]=1;
    for(i=1;i<17;i++)
     { multi_xa(&x);
     printf("%x\n\r",x);
```

```
   if(!(i%2)) sqw[i/2]=x;
   }
  for(i=0;i<10;i++)   printf("%x\n\r",sqw[i]);

   for(n=0;n<2;n++)
      { for(i=0;i<3;i++) {
       qdr(&vr);  printf("%x\n\r",vr);      }
       vt=vr;
       ur=zr;
       multi_uv(ur,vr,&zr);
       printf("%x %x\n\r",vt,zr);
       vr=vt;
      }
      vr=zr;
      vt=vr;
      bas[0]=1;
      bas[1]=zr;
      for(i=2;i<33;i++)
       { ur=zr;
         multi_uv(ur,vr,&zr);
         bas[i]=zr;
         vr=vt;
       }

  for(i=0;i<12;i++)   printf("%x\n\r",bas[i]);

   }


void qdr(unsigned int *w)
 { int i,j;
  unsigned int rez=0,mask1=1,mask2=1;
  for(i=0;i<9;i++)
  {  if(*w & mask1) rez=rez^sqw[i];
       mask1<<=1;
  }
  *w=rez;
  }


void multi_xa(unsigned int *px)
 { if( *px & 0x0100)
       { *px<<=1;
         *px^=0x0011;
        }
       else *px<<=1 ;
   *px&=0x01ff;
```

```
}

void multi_uv( unsigned int u, unsigned int v, unsigned int *z)
 { int i;
  *z=0;
  for(i=0;i<9;i++)
  { if(v & 0x0001) *z^=u;  *z &=0x01ff;
       multi_xa(&u) ;
       v>>=1;  v&=0x01ff;
      }
  }
```

Программа расчета координат сдвигов для N=10 и m=5.

```
#include <stdio.h>
#include <memory.h>
static unsigned int sqw[10];
  static unsigned int bas[34];
  void multi_xa(int);
  void multi_uv( unsigned int, unsigned int, unsigned int *);
  void qdr( unsigned int *);
  static  unsigned int x=1,vr=2,ur,zr=2,vt;
  main( )
  {  int i,j,n;
    sqw[0]=1;
    for(i=1;i<19;i++)
     { multi_xa(&x);
     printf("%x\n\r",x);
     if(!(i%2)) sqw[i/2]=x;
     }
   for(i=0;i<10;i++)   printf("%x\n\r",sqw[i]);
     for(n=0;n<1;n++)
        { for(i=0;i<5;i++) {
          qdr(&vr);  printf("%x\n\r",vr);      }
          vt=vr;
          ur=zr;
          multi_uv(ur,vr,&zr);
          printf("%x %x\n\r",vt,zr);
          vr=vt;
         }
        vr=zr;
        vt=vr;
        bas[0]=1;
        bas[1]=zr;
        for(i=2;i<33;i++)
```

```
        { ur=zr;
          multi_uv(ur,vr,&zr);
          bas[i]=zr;
          vr=vt;
         }
  for(i=0;i<33;i++)   printf("%x\n\r",bas[i]);
   }

void qdr(unsigned int *w)
 { int i,j;
  unsigned int rez=0,mask1=1,mask2=1;
  for(i=0;i<10;i++)
  {  if(*w & mask1) rez=rez^sqw[i];
       mask1<<=1;
  }
  *w=rez;
  }

void multi_xa(unsigned int *px)
 { if( *px & 0x0200)
       { *px<<=1;
         *px^=0x0003;
        }
       else *px<<=1 ;
    *px&=0x03ff;
 }

 void multi_uv( unsigned int u, unsigned int v, unsigned int *z)
  { int i;
   *z=0;
   for(i=0;i<10;i++)
   { if(v & 0x0001) *z^=u;  *z &=0x03ff;
        multi_xa(&u) ;
        v>>=1;  v&=0x03ff;
       }
   }
```

Программа расчета координат сдвигов для N=12 и m=4.

```
#include <stdio.h>
#include <memory.h>
static unsigned int sqw[12];
  static unsigned int bas[20];
  void multi_xa(int);
  void multi_uv( unsigned int, unsigned int, unsigned int *);
  void qdr( unsigned int *);
  static   unsigned int x=1,vr=2,ur,zr=2,vt;
```

```
main( )
{  int i,j,n;

   sqw[0]=1;
   for(i=1;i<23;i++)
    { multi_xa(&x);
    printf("%x\n\r",x);
    if(!(i%2)) sqw[i/2]=x;
    }
  for(i=0;i<12;i++)   printf("%x\n\r",sqw[i]);

    for(n=0;n<3;n++)
       { for(i=0;i<3;i++) {
         qdr(&vr);  printf("%x\n\r",vr);      }
         vt=vr;
         ur=zr;
         multi_uv(ur,vr,&zr);
         printf("%x %x\n\r",vt,zr);
         vr=vt;
        }
       vr=zr;
       vt=vr;
       bas[0]=1;
       bas[1]=zr;
       for(i=2;i<19;i++)
        { ur=zr;
          multi_uv(ur,vr,&zr);
          bas[i]=zr;
          vr=vt;
         }

  for(i=0;i<19;i++)   printf("%x\n\r",bas[i]);

    }

void qdr(unsigned int *w)
 { int i,j;
  unsigned int rez=0,mask1=1,mask2=1;
  for(i=0;i<12;i++)
  {  if(*w & mask1) rez=rez^sqw[i];
       mask1<<=1;
  }
  *w=rez;
  }

void multi_xa(unsigned int *px)
 { if( *px & 0x0800)
       { *px<<=1;
```

```
        *px^=0x0053;
        }
       else *px<<=1 ;
   *px&=0x0fff;
 }

 void multi_uv( unsigned int u, unsigned int v, unsigned int *z)
  { int i;
   *z=0;
   for(i=0;i<12;i++)
   { if(v & 0x0001) *z^=u;  *z &=0x0fff;
        multi_xa(&u) ;
        v>>=1;  v&=0x0fff;
       }
   }
```

Программа расчета координат сдвигов для N=14 и m=7.

```
#include <stdio.h>
#include <memory.h>
static unsigned int sqw[14];
  static unsigned int bas[150];
  void multi_xa(int);
  void multi_uv( unsigned int, unsigned int, unsigned int *);
  void qdr( unsigned int *);
  static   unsigned int x=1,vr=2,ur,zr=2,vt;
  main( )
  {  int i,j,n;
    sqw[0]=1;
    for(i=1;i<27;i++)
     { multi_xa(&x);
     printf("%x\n\r",x);
     if(!(i%2)) sqw[i/2]=x;
     }
   for(i=0;i<14;i++)   printf("%x\n\r",sqw[i]);

     for(n=0;n<1;n++)
        { for(i=0;i<7;i++) {
         qdr(&vr);  printf("%x\n\r",vr);      }
         vt=vr;
         ur=zr;
         multi_uv(ur,vr,&zr);
         printf("%x %x\n\r",vt,zr);
         vr=vt;
         }
        vr=zr;
        vt=vr;
```

```
        bas[0]=1;
        bas[1]=zr;
        for(i=2;i<129;i++)
         { ur=zr;
           multi_uv(ur,vr,&zr);
           bas[i]=zr;
           vr=vt;
          }

   for(i=0;i<129;i++)   printf("%x   ",bas[i]);
    }

void qdr(unsigned int *w)
 { int i,j;
   unsigned int rez=0,mask1=1,mask2=1;
   for(i=0;i<14;i++)
   {  if(*w & mask1) rez=rez^sqw[i];
        mask1<<=1;
   }
   *w=rez;
   }

void multi_xa(unsigned int *px)
 { if( *px & 0x2000)
        { *px<<=1;
          *px^=0x1803;
         }
        else *px<<=1 ;
    *px&=0x3fff;
  }

 void multi_uv( unsigned int u, unsigned int v, unsigned int *z)
   { int i;
     *z=0;
     for(i=0;i<14;i++)
     { if(v & 0x0001) *z^=u;  *z &=0x3fff;
          multi_xa(&u) ;
          v>>=1;  v&=0x3fff;
        }
    }
```

Программа расчета координат сдвигов для N=15 и m=3.

```
#include <stdio.h>
#include <memory.h>
static unsigned int sqw[15];
  static unsigned int bas[20];
```

```
void multi_xa(int);
void multi_uv( unsigned int, unsigned int, unsigned int *);
void qdr( unsigned int *);
static  unsigned int x=1,vr=2,ur,zr=2,vt;
main( )
{  int i,j,n;
   sqw[0]=1;
   for(i=1;i<29;i++)
    { multi_xa(&x);
    printf("%x\n\r",x);
    if(!(i%2)) sqw[i/2]=x;
    }
  for(i=0;i<15;i++)   printf("%x\n\r",sqw[i]);

    for(n=0;n<4;n++)
        { for(i=0;i<3;i++) {
          qdr(&vr);  printf("%x\n\r",vr);     }
          vt=vr;
          ur=zr;
          multi_uv(ur,vr,&zr);
          printf("%x %x\n\r",vt,zr);
          vr=vt;
         }
        vr=zr;
        vt=vr;
        bas[0]=1;
        bas[1]=zr;
        for(i=2;i<19;i++)
         { ur=zr;
           multi_uv(ur,vr,&zr);
           bas[i]=zr;
           vr=vt;
          }
  for(i=0;i<19;i++)   printf("%x   ",bas[i]);

    }

void qdr(unsigned int *w)
 { int i,j;
   unsigned int rez=0,mask1=1,mask2=1;
   for(i=0;i<15;i++)
   {  if(*w & mask1) rez=rez^sqw[i];
        mask1<<=1;
   }
   *w=rez;
   }

void multi_xa(unsigned int *px)
```

```
{ if( *px & 0x4000)
      { *px<<=1;
       *px^=0x0003;
       }
      else *px<<=1 ;
  *px&=0x7fff;
 }

void multi_uv( unsigned int u, unsigned int v, unsigned int *z)
 { int i;
  *z=0;
  for(i=0;i<15;i++)
  { if(v & 0x0001) *z^=u;  *z &=0x7fff;
       multi_xa(&u) ;
       v>>=1;  v&=0x7fff;
      }
  }
```

Программа расчета координат сдвигов для N=16 и m=4.

```
#include <stdio.h>
#include <memory.h>
static unsigned int sqw[16];
  static unsigned int bas[20];
  void multi_xa(int);
  void multi_uv( unsigned int, unsigned int, unsigned int *);
  void qdr( unsigned int *);
  static   unsigned int x=1,vr=2,ur,zr=2,vt;
  main( )
  {  int i,j,n;
    sqw[0]=1;
    for(i=1;i<31;i++)
     { multi_xa(&x);
     printf("%x\n\r",x);
     if(!(i%2)) sqw[i/2]=x;
     }
   for(i=0;i<16;i++)   printf("%x\n\r",sqw[i]);

    for(n=0;n<3;n++)
       { for(i=0;i<4;i++) {
        qdr(&vr);  printf("%x\n\r",vr);      }
        vt=vr;
        ur=zr;
        multi_uv(ur,vr,&zr);
        printf("%x %x\n\r",vt,zr);
        vr=vt;
       }
```

```
        vr=zr;
        vt=vr;
        bas[0]=1;
        bas[1]=zr;
        for(i=2;i<19;i++)
         { ur=zr;
           multi_uv(ur,vr,&zr);
           bas[i]=zr;
           vr=vt;
          }
  for(i=0;i<19;i++)   printf("%x   ",bas[i]);
    }

void qdr(unsigned int *w)
 { int i,j;
  unsigned int rez=0,mask1=1,mask2=1;
  for(i=0;i<16;i++)
  {  if(*w & mask1) rez=rez^sqw[i];
       mask1<<=1;
  }
  *w=rez;
  }

void multi_xa(unsigned int *px)
 { if( *px & 0x8000)
       { *px<<=1;
         *px^=0x002d;
        }
       else *px<<=1 ;
    *px&=0xffff;
 }

 void multi_uv( unsigned int u, unsigned int v, unsigned int *z)
  { int i;
    *z=0;
    for(i=0;i<16;i++)
    { if(v & 0x0001) *z^=u;  *z &=0xffff;
        multi_xa(&u) ;
        v>>=1;  v&=0xffff;
       }
    }
```

Программа расчета координат сдвигов для N=16 и m=8.

```
#include <stdio.h>
#include <memory.h>
static unsigned int sqw[16];
```

```
static unsigned int bas[260];
void multi_xa(int);
void multi_uv( unsigned int, unsigned int, unsigned int *);
void qdr( unsigned int *);
static  unsigned int x=1,vr=2,ur,zr=2,vt;
main( )
{  int i,j,n;
   sqw[0]=1;
   for(i=1;i<31;i++)
    { multi_xa(&x);
    printf("%x\n\r",x);
    if(!(i%2)) sqw[i/2]=x;
    }
  for(i=0;i<16;i++)   printf("%x\n\r",sqw[i]);
    for(n=0;n<1;n++)
        { for(i=0;i<8;i++) {
          qdr(&vr);  printf("%x\n\r",vr);      }
          vt=vr;
          ur=zr;
          multi_uv(ur,vr,&zr);
          printf("%x %x\n\r",vt,zr);
          vr=vt;
         }
        vr=zr;
        vt=vr;
        bas[0]=1;
        bas[1]=zr;
        for(i=2;i<257;i++)
         { ur=zr;
           multi_uv(ur,vr,&zr);
           bas[i]=zr;
           vr=vt;
          }
  for(i=0;i<257;i++)   printf("%x   ",bas[i]);
    }

void qdr(unsigned int *w)
 { int i,j;
   unsigned int rez=0,mask1=1,mask2=1;
   for(i=0;i<16;i++)
   {  if(*w & mask1) rez=rez^sqw[i];
        mask1<<=1;
   }
   *w=rez;
   }

void multi_xa(unsigned int *px)
 { if( *px & 0x8000)
```

```
        { *px<<=1;
          *px^=0x002d;
         }
        else *px<<=1 ;
     *px&=0xffff;
   }

  void multi_uv( unsigned int u, unsigned int v, unsigned int *z)
   { int i;
    *z=0;
    for(i=0;i<16;i++)
    { if(v & 0x0001) *z^=u;  *z &=0xffff;
         multi_xa(&u) ;
         v>>=1;  v&=0xffff;
        }
    }
```

Программа расчета координат сдвигов для N=20 и m=5.

```
#include <stdio.h>
#include <memory.h>
static unsigned long sqw[20];
  static unsigned long bas[65];
  void multi_xa(long);
  void multi_uv( unsigned long, unsigned long, unsigned long *);
  void qdr( unsigned long *);
  static   unsigned long x=1,vr=2,ur,zr=2,vt;
  main( )
  {  int i,j,n;
    sqw[0]=1;
    for(i=1;i<39;i++)
     { multi_xa(&x);
     printf("%lx\n\r",x);
     if(!(i%2)) sqw[i/2]=x;
     }
    for(i=0;i<16;i++)   printf("%lx\n\r",sqw[i]);
     for(n=0;n<3;n++)
        { for(i=0;i<5;i++) {
          qdr(&vr);  printf("%lx\n\r",vr);       }
          vt=vr;
          ur=zr;
          multi_uv(ur,vr,&zr);
          printf("%lx %lx\n\r",vt,zr);
          vr=vt;
         }
        vr=zr;
        vt=vr;
```

```
        bas[0]=1;
        bas[1]=zr;
        for(i=2;i<36;i++)
         { ur=zr;
           multi_uv(ur,vr,&zr);
           bas[i]=zr;
           vr=vt;
          }
   for(i=0;i<35;i++)   printf("%lx  ",bas[i]);
    }

 void qdr(unsigned long *w)
  { int i,j;
   unsigned long rez=0,mask1=1,mask2=1;
   for(i=0;i<20;i++)
   {  if(*w & mask1) rez=rez^sqw[i];
        mask1<<=1;
   }
   *w=rez;
   }

 void multi_xa(unsigned long *px)
  { if( *px & 0x00080000L)
        { *px<<=1;
          *px^=0x00000009L;
         }
        else *px<<=1 ; *px&=0x000fffff;
  }

  void multi_uv( unsigned long u, unsigned long v, unsigned long *z)
   { int i;
     *z=0;
     for(i=0;i<20;i++)
     { if(v & 0x00000001L) *z^=u;
          multi_xa(&u) ;
          v>>=1;  v&=0x000fffff;
        }
    }
```

Программа расчета координат сдвигов для N=24 и m=4.

```
#include <stdio.h>
#include <memory.h>
static unsigned long sqw[24];
  static unsigned long bas[65];
  void multi_xa(long);
  void multi_uv( unsigned long, unsigned long, unsigned long *);
```

```
void qdr( unsigned long *);
static  unsigned long x=1,vr=2,ur,zr=2,vt;
main( )
{  int i,j,n;
   sqw[0]=1;
   for(i=1;i<47;i++)
    { multi_xa(&x);
    printf("%lx\n\r",x);
    if(!(i%2)) sqw[i/2]=x;
    }
  for(i=0;i<16;i++)   printf("%lx\n\r",sqw[i]);
    for(n=0;n<5;n++)
       { for(i=0;i<4;i++) {
         qdr(&vr);  printf("%lx\n\r",vr);      }
         vt=vr;
         ur=zr;
         multi_uv(ur,vr,&zr);
         printf("%lx %lx\n\r",vt,zr);
         vr=vt;
        }
       vr=zr;
       vt=vr;
       bas[0]=1;
       bas[1]=zr;
       for(i=2;i<36;i++)
        { ur=zr;
          multi_uv(ur,vr,&zr);
          bas[i]=zr;
          vr=vt;
         }
  for(i=0;i<35;i++)   printf("%lx  ",bas[i]);

    }

void qdr(unsigned long *w)
 { int i,j;
  unsigned long rez=0,mask1=1,mask2=1;
  for(i=0;i<24;i++)
  {  if(*w & mask1) rez=rez^sqw[i];
       mask1<<=1;
  }
  *w=rez;
  }

void multi_xa(unsigned long *px)
 { if( *px & 0x00800000L)
       { *px<<=1;
         *px^=0x0000001bL;
```

```
        }
       else *px<<=1 ; *px&=0x00ffffff;
}


void multi_uv( unsigned long u, unsigned long v, unsigned long *z)
 { int i;
  *z=0;
  for(i=0;i<24;i++)
  { if(v & 0x00000001L) *z^=u;
       multi_xa(&u) ;
       v>>=1;  v&=0x00ffffff;
      }
 }
```

Программа расчета координат сдвигов для N=32 и m=4.

```
#include <stdio.h>
#include <memory.h>
static unsigned long sqw[32];
  static unsigned long bas[30];
  void multi_xa(long);
  void multi_uv( unsigned long, unsigned long, unsigned long *);
  void qdr( unsigned long *);
  static   unsigned long x=1,vr=2,ur,zr=2,vt;
  main( )
  {  int i,j,n;
    sqw[0]=1;
    for(i=1;i<63;i++)
     { multi_xa(&x);
     printf("%lx\n\r",x);
     if(!(i%2)) sqw[i/2]=x;
     }
   for(i=0;i<16;i++)   printf("%lx\n\r",sqw[i]);
    for(n=0;n<7;n++)
        { for(i=0;i<4;i++) {
          qdr(&vr);  printf("%lx\n\r",vr);       }
          vt=vr;
          ur=zr;
          multi_uv(ur,vr,&zr);
          printf("%lx %lx\n\r",vt,zr);
          vr=vt;
         }
        vr=zr;
        vt=vr;
        bas[0]=1;
        bas[1]=zr;
```

```
        for(i=2;i<19;i++)
         { ur=zr;
           multi_uv(ur,vr,&zr);
           bas[i]=zr;
           vr=vt;
          }
   for(i=0;i<19;i++)   printf("%lx\n\r",bas[i]);
    }

void qdr(unsigned long *w)
 { int i,j;
  unsigned long rez=0,mask1=1,mask2=1;
  for(i=0;i<32;i++)
  {  if(*w & mask1) rez=rez^sqw[i];
       mask1<<=1;
  }
  *w=rez;
  }

void multi_xa(unsigned long *px)
 { if( *px & 0x80000000L)
       { *px<<=1;
         *px^=0x00400007L;
        }
       else *px<<=1 ;
 }

 void multi_uv( unsigned long u, unsigned long v, unsigned long *z)
  { int i;
    *z=0;
    for(i=0;i<32;i++)
    { if(v & 0x00000001L) *z^=u;
        multi_xa(&u) ;
        v>>=1;
       }
   }
```

Программа расчета координат сдвигов для N=42 и m=3.

```
#include <stdio.h>
#include <memory.h>
typedef struct data
 { unsigned long xl;
  unsigned int xh;
 } REG ;
void multi_xa(unsigned long *,unsigned *);
void multi_uv( REG, REG, REG *) ;
```

```
void qdr(REG *);
static REG sqw[42];
static REG bas[16];
unsigned long mask1=1;
unsigned mask2=1;
  main( )
  {  int i,j,n;
     unsigned  long l=1;
     unsigned int h=0 ;
     REG vr,ur,zr,vt;
     sqw[0].xl=1; sqw[0].xh=0;
     for(i=1;i<83;i++)
      { multi_xa(&l,&h);
/*      printf("%lx\n\r",x);*/
     if(!(i%2)) {sqw[i/2].xl=l; sqw[i/2].xh=h ; }
      }
    for(i=0;i<30;i++)   printf("%x\n\r",sqw[i].xh);
     vr.xl=2; vr.xh=0;
     zr.xl=2; zr.xh=0;
     for(n=0;n<13;n++)
         { for(i=0;i<3;i++) {
           qdr(&vr);/*  printf("%lx\n\r",vr); */     }
           vt=vr;
           ur=zr;
           multi_uv(ur,vr,&zr);
   /*      printf("%lx %lx\n\r",vt,zr);*/
           vr=vt;
          }
         vr=zr;
         vt=vr;
         bas[0].xl=1; bas[0].xh=0;
         bas[1].xl=zr.xl; bas[1].xh=zr.xh;
         for(i=2;i<16;i++)
          { ur=zr;
            multi_uv(ur,vr,&zr);
            bas[i].xl=zr.xl;   bas[i].xh=zr.xh;
            vr=vt;
           }

    for(i=0;i<16;i++)   printf("%x   %lx  \n\r",bas[i].xh,bas[i].xl);
     }

 void qdr(REG *w)
 { int i,j;
   REG rez;
   mask1=1;
   mask2=1;
   rez.xl=0;
```

```
 rez.xh=0;
 for(i=0;i<32;i++)
 {  if(w->xl & mask1)
  { rez.xl^=sqw[i].xl;
      rez.xh^=sqw[i].xh;
     }
      mask1<<=1;
 }
 for(i=0;i<10;i++)
 {  if(w->xh & mask2)
  { rez.xl^=sqw[i+32].xl;
      rez.xh^=sqw[i+32].xh;
     }
      mask2<<=1;
 }
  w->xl=rez.xl;
  w->xh=rez.xh;
}

void multi_xa(unsigned long *pxl,unsigned int *pxh)
{ if(*pxh & 0x0200)
  { *pxh<<=1;  *pxh &=0x03ff;
     if(*pxl & 0x80000000L) *pxh^=0x000b; else *pxh^=0x000a;
     *pxl<<=1;
     *pxl^=0x8e6f04efL;
  }
  else
  { *pxh<<=1;  *pxh &=0x03ff ;
     if(*pxl & 0x80000000L) *pxh^=0x0001;
     *pxl<<=1;
     }
}

void multi_uv( REG u, REG v, REG *z)
 { int i;
  z->xh=0; z->xl=0;
  for(i=0;i<32;i++)
  { if(v.xl & 0x00000001L) { z->xh^=u.xh;  z->xl^=u.xl; }
     multi_xa(&u.xl,&u.xh) ;
     v.xl>>=1;
    }
  for(i=0;i<10;i++)
  { if(v.xh & 0x0001) { z->xh^=u.xh;  z->xl^=u.xl; }
     multi_xa(&u.xl,&u.xh) ;
     v.xh>>=1;
    }
 }
```

Программа расчета координат сдвигов для N=48 и m=8.

```
#include <stdio.h>
#include <memory.h>
typedef struct data
 { unsigned long xl;
  unsigned int xh;
 } REG ;
void multi_xa(unsigned long *,unsigned *);
void multi_uv( REG, REG, REG *) ;
void qdr(REG *);
static REG sqw[48];
static REG bas[270];
unsigned long mask1=1;
unsigned mask2=1;
 char   mas[510], str[9];
  main( )
  {  int i,j,n;
     unsigned  long l=1;
      FILE *fp;
     unsigned int h=0 ;
     REG vr,ur,zr,vt;
     sqw[0].xl=1; sqw[0].xh=0;
    fp=fopen("gn48_8p1.txt","a");
     for(i=1;i<95;i++)
      { multi_xa(&l,&h);
/*      printf("%lx\n\r",x);*/
     if(!(i%2)) {sqw[i/2].xl=l; sqw[i/2].xh=h ; }
      }
    for(i=0;i<30;i++)   printf("%x\n\r",sqw[i].xh);
     vr.xl=2; vr.xh=0;
     zr.xl=2; zr.xh=0;
     for(n=0;n<5;n++)
        { for(i=0;i<8;i++) {
          qdr(&vr);/*  printf("%lx\n\r",vr); */     }
          vt=vr;
          ur=zr;
          multi_uv(ur,vr,&zr);
   /*     printf("%lx %lx\n\r",vt,zr);*/
          vr=vt;
         }
        vr=zr;
        vt=vr;
        bas[0].xl=1; bas[0].xh=0;
        bas[1].xl=zr.xl; bas[1].xh=zr.xh;
        for(i=2;i<270;i++)
         { ur=zr;
           multi_uv(ur,vr,&zr);
```

```
            bas[i].xl=zr.xl;  bas[i].xh=zr.xh;
            vr=vt;
           }
    for(i=0;i<260;i++)
    { fprintf(fp,"\n\r");
      fprintf(fp,"i=%-3d     %4x  %8lx  ",i,bas[i].xh,bas[i].xl);
    }
       fprintf(fp,"\n\r");
    for(i=0;i<255;i++) { if(bas[i].xl & 0x0001){ mas[i]='1'; mas[i+255]='1';} else { mas[i]='0';
mas[i+255]='0';}}
    for(i=0;i<255;i++) { memcpy(str,mas+i,8); str[8]='\0';
              fprintf(fp,"     %s  %c \n\r ",str,mas[254-i]);
                   }
     }

 void qdr(REG *w)
  { int i,j;
    REG rez;
    mask1=1;
    mask2=1;
    rez.xl=0;
    rez.xh=0;
    for(i=0;i<32;i++)
    {  if(w->xl & mask1)
     { rez.xl^=sqw[i].xl;
         rez.xh^=sqw[i].xh;
        }
         mask1<<=1;
    }
    for(i=0;i<16;i++)
    {  if(w->xh & mask2)
     { rez.xl^=sqw[i+32].xl;
         rez.xh^=sqw[i+32].xh;
        }
         mask2<<=1;
    }
     w->xl=rez.xl;
     w->xh=rez.xh;
    }

 void multi_xa(unsigned long *pxl,unsigned int *pxh)
  { if(*pxh & 0x8000)
     { *pxh<<=1;  *pxh &=0xffff;
         if(*pxl & 0x80000000L) *pxh^=0x0001; else *pxh^=0x0000;
         *pxl<<=1;
         *pxl^=0x18000003L;
      }
     else
```

```
    { *pxh<<=1;  *pxh &=0xffff ;
        if(*pxl & 0x80000000L) *pxh^=0x0001;
        *pxl<<=1;
       }
  }

  void multi_uv( REG u, REG v, REG *z)
   { int i;
    z->xh=0; z->xl=0;
    for(i=0;i<32;i++)
    { if(v.xl & 0x00000001L) { z->xh^=u.xh;  z->xl^=u.xl; }
        multi_xa(&u.xl,&u.xh) ;
        v.xl>>=1;
       }
    for(i=0;i<16;i++)
    { if(v.xh & 0x0001) { z->xh^=u.xh;  z->xl^=u.xl; }
        multi_xa(&u.xl,&u.xh) ;
        v.xh>>=1;
       }
    }
```

Программа расчета координат сдвигов для N=63 и m=3.

```
#include <stdio.h>
#include <memory.h>
typedef struct data
 { unsigned long xl;
  unsigned long xh;
 } REG ;
void multi_xa(unsigned long *,unsigned long *);
void multi_uv( REG, REG, REG *) ;
void qdr(REG *);
static REG sqw[63];
static REG bas[16];
unsigned long mask1=1;
unsigned long mask2=1;
  main( )
  {  int i,j,n;
    unsigned  long l=1;
    unsigned long  h=0 ;
    REG vr,ur,zr,vt;
    sqw[0].xl=1; sqw[0].xh=0;
    for(i=1;i<125;i++)
     { multi_xa(&l,&h);
/*     printf("%lx\n\r",x);*/
     if(!(i%2)) {sqw[i/2].xl=l; sqw[i/2].xh=h ; }
     }
```

```
 for(i=0;i<30;i++)   printf("%x\n\r",sqw[i].xh);
  vr.xl=2; vr.xh=0;
  zr.xl=2; zr.xh=0;
  for(n=0;n<20;n++)
     { for(i=0;i<3;i++) {
       qdr(&vr);/*  printf("%lx\n\r",vr); */     }
       vt=vr;
       ur=zr;
       multi_uv(ur,vr,&zr);
/*     printf("%-lx %-lx\n\r",vt,zr);*/
       vr=vt;
      }
     vr=zr;
     vt=vr;
     bas[0].xl=0x00000001L; bas[0].xh=0x00000000L;
     bas[1].xl=zr.xl; bas[1].xh=zr.xh;
     for(i=2;i<16;i++)
      { ur=zr;
        multi_uv(ur,vr,&zr);
        bas[i].xl=zr.xl;   bas[i].xh=zr.xh;
        vr=vt;
       }
 for(i=0;i<16;i++)   printf("%8.lx          %8.lx  \n\r",bas[i].xh,bas[i].xl);
  }

void qdr(REG *w)
 { int i,j;
  REG rez;
  mask1=1;
  mask2=1;
  rez.xl=0;
  rez.xh=0;
  for(i=0;i<32;i++)
  {  if(w->xl & mask1)
    { rez.xl^=sqw[i].xl;
       rez.xh^=sqw[i].xh;
      }
       mask1<<=1;
  }
  for(i=0;i<31;i++)
  {  if(w->xh & mask2)
    { rez.xl^=sqw[i+32].xl;
       rez.xh^=sqw[i+32].xh;
      }
       mask2<<=1;
  }
   w->xl=rez.xl;
   w->xh=rez.xh;
```

```
 }

void multi_xa(unsigned long *pxl,unsigned long *pxh)
 { if(*pxh & 0x40000000L)
   { *pxh<<=1;  *pxh &=0x7fffffffL;
       if(*pxl & 0x80000000L) *pxh^=0x00000001L;
       *pxl<<=1;
       *pxl^=0x00000003L;
    }
   else
    { *pxh<<=1;  *pxh &=0x7fffffffL ;
       if(*pxl & 0x80000000L) *pxh^=0x00000001L;
       *pxl<<=1;
      }
 }

 void multi_uv( REG u, REG v, REG *z)
  { int i;
    z->xh=0; z->xl=0;
    for(i=0;i<32;i++)
    { if(v.xl & 0x00000001L) { z->xh^=u.xh;  z->xl^=u.xl; }
       multi_xa(&u.xl,&u.xh) ;
       v.xl>>=1;
      }
    for(i=0;i<31;i++)
    { if(v.xh & 0x00000001L) { z->xh^=u.xh;  z->xl^=u.xl; }
       multi_xa(&u.xl,&u.xh) ;
       v.xh>>=1;
      }
   }
```

Программа моделирования скремблирования потока данных последовательностью GMW. длины $2^{63}-1$

```
#include <stdio.h>
#include <memory.h>
#include <PROCESS.H>
#include <conio.h>
#include <graphics.h>

  main( )
 {  short p=0;

   int j,n,g,k=0,s=0;

   char b[81];
```

```
    char buf[3840];
    char x,y,z,gmw,cod,q,mp;
/*  char str[]="01001110";*/
    char str[]="00110110";
    char tst[]="11110000";
    char avt[]="This algorithm was designed by Evgeny Krengel ";
    unsigned long  mskl[3]={0x473782e7,0xf701b3d4,0x89cfc6bd},i;
    unsigned int   mskh[3]={0x0205,0x00f3,0x0280};
    unsigned long  s1,y1,z1;
    unsigned int   s2,y2,z2;
    unsigned  long xl=1,yl,zl,sl;
    unsigned int xh=0,yh,zh,sh ;
         b[80]='\0';
        /*  setcolor(6);*/

     textmode(C80);
     textbackground(1);
     textcolor(14);
     window(1,1,80,25);
     clrscr();
     _setcursortype(_NOCURSOR);

    for(i=0;;i++ )
    {  p++;
        sl=xl & mskl[0];
        yl=xl & mskl[1];
        zl=xl & mskl[2];
        sh=xh & mskh[0];
        yh=xh & mskh[1];
        zh=xh & mskh[2];
        s1=0; y1=0; z1=0;
        s2=0; y2=0; z2=0;
        for(j=0;j<32;j++)
         {  s1^=sl;
            y1^=yl;
            z1^=zl;
            sl>>=1;
            yl>>=1;
            zl>>=1;

         }

            for(j=0;j<10; j++)
         {  s2^=sh;
            y2^=yh;
            z2^=zh;
            sh>>=1;
            yh>>=1;
```

```
            zh>>=1;
           }

          if(s1 & 0x00000001) s2^=0x0001; s2 &=0x0001;
          if(y1 & 0x00000001) y2^=0x0001; y2 &=0x0001;
          if(z1 & 0x00000001) z2^=0x0001; z2 &=0x0001;

           if(xl & 0x00000001) x='1'; else x='0';

           xh<<=1;
           if(xl & 0x80000000L) {xh|=0x0001;mp='1';} else mp='0';
           xl<<=1;
           xl+=s2; /* printf("%lx  ",xl);*/
           if(y2==1) y='1'; else y='0';
           if(z2==1) z='1'; else z='0';

         g=0;
       if(x=='1') g+=4;
     if(y=='1') g+=2;
       if(z=='1') g+=1;
     gmw=str[g];

       if(k==8) k=0;
       if(tst[k]==gmw) cod='0'; else cod='1';

            if(i>24)
           { p=25;
              gettext(1,2,80,25,buf);
              puttext(1,1,80,24,buf);
             }
           gotoxy(1,p);
    cprintf("shift=%-12ld scrambler GMW PNS %c + %c input data = coded %c  output data %c  ",
i,gmw,tst[k],cod,tst[k]);
       k++;

         if(kbhit()!=0) {  textbackground(0);  textcolor(15);  clrscr(); exit(2);}

    }

 /*   _setvideomode( _DEFAULTMODE );*/

 }
```

Приложение 2

Псевдослучайные последовательности типа Адамара длины 127

m-последовательности

m1

00001000011010000011111011000000101011011111111001101101010100010010011001111000111011101011110100101100101001110010001100010111

m2

11011001011000110011011010001111100001110001010011000000110101110100101010110111001000010001001001111010100000101111001110111111

m3

00101100011100100001011100000110100000001001111111000101010111100110010100010001100001111011111010110101001101100111011011101001

m4

11011011111001111111010010010101110101010011100011001011001100010111101110010001000011010110100011110000010011011000010100000001

m5

11111101010100110011101110100101100011011110110101101100100100011100001011111001010111001101000100111100010100001100000100000001

m6

11110101101110111100011101000101011100000011110110011000100100111001111100100000100011010101001101101001010000101100001100101111

m7

11111101111110001110101010010101111010011001110011010110001000101110110010000111100101101110000010100011011010000000110000100100

m8

11111101110110111101000101100101111100010000001100110110001110011101011100001001100000101010110100100101001111001000110101000011

m9

00100110100111101110000111111100011101100010100101111101010100001011011110011100101011001100000110110101110100011001000100000001

m10

11010001100010011100101001101001011110101110111000111100110010010001010101101100111111101101010000001101111110000010110000100001

m11

11110111001111010000010101111001001000100001001110110101010010111010110000001100101000111000011111000101101100110001101001101111

m12

00101110110111001101100101011010111110111100001100010001010011001111010101000111111100100000001011000001110100001001110001101001

m13

00000010100001101100100000111100010110101100001000100111011110100011001101001100011100101010111010100100101111111001111101101111

m14

00000010000011000010100011110010001011001110101001111101000011100010010011011010110111110110001101001011101110011001010101111111

m15

11010011000011010000101001011011001010101100010000010011111001110010010001100110111100000001110101000101110001111011101101011111

m16

00100100001100000001011011000101000001110110100111100001001101110100010001101011001110011001011110101001010101110001111101111111

m17

00001010110001001111001010010010110101010000011001000011101011100111000110110011000000100011111010011010001011110110111011111111

m18

0000001000100110001011101011011000001100110101001110011110110100001010101111101001010001101110001111111000011101111001011001001

Последовательности класса A

A1

0000100001100010000111100000110010001011111111001000101011110010010010100110010101111101011110100110100011001110110101110010111

A2

1101100101100011001101001000011110000101001110101100100000011111010010101001001100000111101000110011100100110001010101011111111

A3

111111101010111000100110001011110000001001011010000101110110101111000100010001100001100011110011010101001001101111001011001001

A4

1111010110110011111011011000010101011100111110011100101000110001100110111101000001011101011010010111000001001100100001010000001

A5

1111110111010001111100111010000111010101001011010110110010000011110100011011100100001100110100110001110001010010010000100010111

A6

1111010110111011110001110110011101110000000101011011010010010101100111110010101010000001100100010110111100010000111000011001001

A7

0010110011111000110101010110100011110011001110011011111001100000110111010000110110101101111010010100010111011100000101000000001

A8

110110011100101111110000111011011111011100000010011101000101100101010111001110110100010100001000011010110110000100110010100001

A9

0010011000011110000000110111110000100010001011110011110111011000101001100010110010101110110101011010110111110001110110010100001

A10

1101001110101101110011000101100101111010111110101001100101001001001111010100010011111111010001001100000111100001000110000100001

A11

11111111010101010001100100111001100010111100001100100101010010111110000001001101
01110010100001111000010010110011000110100110111

A12

00100110100111101100100101010110011110001100001100010001000111101011011101000010
11010010000001111010001100100011101010111111111

A13

00000010100001001100100000111010010110101110100000101111011001100011000101001110
01111100111010101000011011011111001101101011111

A14

11010001000010010010100011100011001011001100001001110110001011110000010011011010
11010010101011100001011100111110001011101111111

A15

00100110000111000010001111011010001001100000010101010011111001101010010010110110
10100000001110111001101110001111011101101011111

A16

00000000101000001110111010001010010111101101011011000010111011000001100111110110
01110011001111000101101010101100011111001101001

A17

00001010011001000011011010110000100001010001011011100111101010100110100010111001
00000011101111101101110000111111010011100110111

A18

00001010011011100011111011010110101011011101010011010001100101000110111011110011
11010001000100001111101100000001111000011001001

Последовательности класса B

B1

00000010001011000000111001010010001010001111111010011001100011100010110001100010
11011111010101101100101101100011011010101111111

B2

11011011011001010001110000011011100010111101000010000011011001110110100001000111
01110001001010101100001010001111001101101011111

B3

00101100010100100011100110000110100011011100001101000010001111101100001011010011
01010010001011110011001000101110101011111111111

B4

00000010100001101110001010010110010101000010110001001011101101100011001110110010
00001100011110101011101001001111111001111011111

B5

11010001001000010010111010100011000011001111110011101110101001010000100011111010
01011101111110000101111001011100011001001001001

B6

11111101011110010011011111000001101001010001010111010010101000111100110010110001
10000001001110110101100100001110010001100010111

B7

00101100111100101111011110001110110101110001010111000000110101001101101110110111
00100001000100010111101010000000111100011001001

B8

00001000111000101101011000100100110100010011111010101110101110000101101100101001
00001111111111000110110001111100110011010100001

B9

11011011011011110011010011110101101001010011100011111101000100010110111010011001
10001101110000001111010101010001100000010000001

B10

11111010101101100011011010011011010101111101101000110001101000111000110011001010 1
111111000101000100101001110000001101000100000001

B11

11110101101100111100010100001101010100100011101110001000010110111001101100000100
001011110100011101100000111000101001101101101 11

B12

1111111111010101110100010011001111010001001010110010110100001101111100010000101 1
00001110110001011000011001110001001010001101001

B13

11110111100111111100100101110101011110001100000100110111001100011011011101001000
11010000101010011010010100011101100001010000001

B14

00100100100110001110100111101000011111101110100101111100010000101001010111011100
11111100110000110001010111010010000100100010111

B15

11010001100010011100001001101011011100100000011000110100110011110001010100101110
10100010100101100000111110110010011110101111111

B16

00100110001111000000010101111010001000100001001110110111011011001010110000001110
10100011101011011100011110111101001111001101001

B17

00001010110011001111100011011000111111111100001001010011011010000111010111010101
11110010001011001001000110101101000111000100001

B18

00000010000001100010101010111100000001110110001100110010111011010001000101111110 0
01110010100101101011110010110011110110110110111

Последовательности класса C

C1

00000010100011101100001001010110011100000010111000011011101111000011011100100010
1000111001111100101010110110110111101101110100 1

C2

11010011001001010010110010111001000011101111100011101111011000010010100011011100
01111101111010001101010011011101000101000000001

C3

11111010101100100111011110000011010110111000111010100001000101111000100111100 01
110100100000101110001100100100010010010100110111

C4

0010011010110110110001110001111001010010000101011000000111010110101110110010011000100000100010011111010101000001111110011101111 1

C5

0000100011100000110111000010001011011001111110101010111000101100010110010100101101011111111011000100011001111100001011001101001

C6

1101101101001111001100001111010110100101000000000111011100110011011001101001100110000000101010101011010100011111100001110010111

C7

0010010000011010001010111100111000101110111011010101100011010100100001101111011011111110001010001001110111100000011110001100100 1

C8

1101000110100001110001100000100101010010001111101000101011101011000110010010010000101111011111100100100011101110010111100110111

C9

1111111011101010011010110110011100001010001001111100101000011011110100010011011000000111000010111010110001100010010100011010 01

C10

0010111011011110110110110101010011111001110001010001001110110000111101110110000111010000000111001101010010000110111000101000000 1

C11

0000000010100010111011001010110001011110111111000111011000101001000011011110111000111110111000010011101001101001010010011001011 1

C12

1101100101001001000100100110001110100001001011100011110010001111010001000010101110001110110101100000111101110010011010101111111

C13

1111011100111111000001010101111110010001000010001100100110111010110101110000001101010000100101001111000111000110110110101100100 1

C14

0010110011010000111110011000100011011111111010110100101001101000110100011101010101111111001101101000100001110110000011100010000 1

C15

1101001110000111111000101011010101010100000000110011001011001101100110011101110000000001010010110101111000011001111001011011011 1

C16

0010011000111100000001111011100100010100011111101101111011000010010101100011010101101110111010001110011110101000101100000100100 1

C17

1101100111101001110111000100100111111011110100001001001001100011010111010100010111110001001010100100000110001110000101100010111

C18

0010110001010010001100011010111010000111000000110110010001011110110000101001111100100010100001110011011010110010101110111111111

Последовательности Холла

h1

0000000010101010110011000100111001111010111110001001101001110100000111110100011011111101011010000110001111001100101101011001001

h2

1101100101000001001100001010100110000111001010100110111001101011010000001001110100111011101110000101001111111000011110011011

h3

1111011100011111001000111101011100100100000001110101000110011101101001101011001010000010000101011011101100100001111010011101001

h4

0010011010110100110011110001100001011010111111011000101111100000101110010110010001111101011110011100100011001101010101000000001

h5

1101100111100001111111001010000111011101110100101110010000001011010110011101100101010011100001100101010000110010000010100110111

h6

0010111001011110000100110111011010100001000001010011010110010110111001100010101110010111011100100000010010011101011110001001111100011101111

Последовательности Лежандра

*l*1

0010111001010100000100110011100010000011001011010010111111100010111000000010110100101110111000110011011110100011000101111

*l*2

1110100011010101111101100110001110111110011010010110100000001110100011111110100101101001100000100011100110010000010101001110100