

Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 621.391.8:519.72

Назаренко Евгений Сергеевич

Синтез и анализ систем ортогональных псевдослучайных
последовательностей

АВТОРЕФЕРАТ

на соискание степени магистра техники и технологии
по специальности 1-39 81 03 «Информационные радиотехнологии»

Научный руководитель

Карпушкин Эдуард Михайлович

Кандидат технических наук, доцент

Минск 2020

Нормоконтроль

Краткое введение

Сегодня широко распространяется в системах мобильной и фиксированной связи технология множественного доступа с кодовым разделением (CDMA), основными принципами которой являются расширение спектра в сочетании с кодовым разделением физических каналов за счет использования широкополосных шумоподобных сигналов на основе псевдослучайных последовательностей (ПСП). Основными достоинствами шумоподобных сигналов является то, что, обеспечивая одновременную работу в одном частотном спектре многих абонентов, с заданной помехоустойчивостью, они позволяют эффективно бороться с помехами, вызванными многолучевым распространением сигналов, повысить помехозащищенность и конфиденциальность связи, удовлетворить требованиям электромагнитной совместимости. Расширение спектра производится с помощью прямого метода модуляции (Direct Sequence или сокращенно DS) и модуляции скачкообразным переключением частоты (Frequency Hopping или сокращенно FH). Кодовое разделение осуществляется за счет присвоения каждому абонентскому каналу такой сигнатурной ПСП, которая максимально не коррелировала с сигнатурными последовательностями других абонентских каналов. Это означает, что в случае мобильных систем CDMA значение взаимокорреляционных функций (ВКФ) этих последовательностей при всех сдвигах должны быть малы, тогда как в случае фиксированных систем CDMA достаточно обеспечить малую взаимную корреляцию последовательностей только в одной точке. Для быстрого и надежного вхождения в синхронизм эти последовательности должны обладать малыми значениями боковых выбросов их автокорреляционных функций (АКФ).

Последовательности с малыми значениями ЛКФ и ВКФ требуются также и для борьбы с помехами, вызванными многолучевостью. Еще одним важным требованием, предъявляемым к современным коммерческим системам с CDMA,

является обеспечение конфиденциальности связи. С этой целью в таких системах применяются сверхдлинные ПСП с высокой степенью непредсказуемости символов, для оценки которой обычно используется параметр линейной сложности (ЛС).

Среди известных семейств ПСП с близкой к идеальной автокорреляцией длины $2N - 1$ (их еще называют последовательностями типа Адамара) большое распространение получили m -последовательности, поскольку генерация этих последовательностей крайне проста, а их свойства изучены значительно лучше. Однако сегодня на передний план выдвигается другое семейство последовательностей типа Адамара - семейство последовательностей Гордона, Милза, Велча (Gordon, Mills, Welch или сокращенно GMW). Они характеризуются большей численностью и ЛС, чем класс m -последовательностей. Построение таких ПСП существенно расширяет исходную базу формирования максимальных по объему подмножеств ПСП с приемлемым уровнем взаимной корреляции. Это позволяет увеличить число пользователей при заданной помехоустойчивости или снизить 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.

Краткое содержание работы

Во введении обосновывается актуальность темы исследования, излагаются его цель, задачи. В первой главе, посвященной современным принципам конструирования ПСП для систем CDMA, изложены особенности построения широкополосных систем связи на базе технологии DS-SS. Дан обзор некоторых известных и новых семейств двоичных ПСП с оптимальными ВКФ и приведены их основные сравнительные характеристики. Показано, что, несмотря

на удовлетворительные корреляционные параметры, большинство из них имеют малое значение ЛС.

В силу этого в центре внимания оказывается относящееся к последовательностям типа Адамара многочисленное семейство последовательностей GMW, уступающее по ВКФ, но обладающее большой ЛС. К последовательностям типа Адамара относятся: m - последовательности длины $2N-1$, последовательности Лежандра длины $k=4t-1$, последовательности Холла длины $k=4x^2+27$, где k – простое число, последовательности простых чисел-близнецов длины $k=p(p+2)$, где p и $p+2$ простые числа, последовательности Бомера-Фридриксена длины 127. Недавно были найдены еще два новых семейства последовательностей: конструкции Сегре и Глайиа и степенных функций Касами. Роль всех перечисленных последовательностей в построении неэквивалентных классов ПСП GMNV подробно обсуждается во 2-й главе. Помехоустойчивость системы связи CDMA в значительной степени зависит от корреляционных параметров используемых ПСП и может быть оптимизирована посредством выбора их соответствующего подмножества. В системах DS-CDMA при выборе последовательностей часто используют два критерия оптимизации: минимизации пиковых значений четной и нечетной ЛКФ и ВКФ (минимаксный) и минимизации сумм средних интерференционных параметров (Average Interference Parameter или сокращенно AIP), т.е. среднего отношения сигнал-шум на выходе каждого абонентского приемника. При этом оптимизация осуществляется как по самим ПСП, так и по их начальным фазам. В 1992г. К.Карккайнен, рассматривая применение t -последовательностей, последовательностей Голда и Касами в системах с CDMA, обнаружил, что для длин 255 и более асимптотически стремится к величине $2v^2$ и практически не зависит выбора последовательностей и их начальных фаз.

Поэтому в качестве критерия при выборе последовательностей Адамара в диссертации в основном используется минимаксный критерий. 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 подсчета общего числа этих ПСП для любого допустимого 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 . Сделан полный расчет ЛС для всех 79 различных классов этих ПСП длины 16383.

В данной диссертации предложен следующий общий алгоритм построения ПСП GMW.

1. На основе примитивного многочлена $f(x)$ степени N над $GF(2)$ образуется m -последовательность $\{z_n\}$ с элементом $z_0=1$, соответствующая комплиментарному зингеровскому разностному множеству.

2. Строится таблица декомпозиции полученной m -последовательности, состоящая из k строк и l столбцов с элементами, определяемыми выражением: $a_{ij} = z_n$, где $n = i + kj$ с $0 \leq j \leq 2^m - 2$ и $0 \leq i \leq k - 1$.

3. Для всех строк, отличных от последовательности нулей, находится число m_i циклических сдвигов влево i -ой строки до ее совпадения с нулевой строкой таблицы.

4. На следующем шаге алгоритма осуществляется выбор базисной последовательности длины w , не являющейся ни каким сдвигом нулевой строки,

5. Затем производится замещение всех отличных от нулей строк исходной таблицы соответствующими сдвигами базисной последовательности так, что на место i -ой строки записывается сдвинутая на m_i разрядов вправо базисная последовательность. В результате образуется таблица декомпозиции последовательности GMW.

6. Из полученной таблицы восстанавливаем последовательность GMW.

Все изоморфные, т.е. связанные друг с другом изоморфными коэффициентами (децимациями) ПСП GMW образуют класс эквивалентности ПСП GMW, а множество всех различных неэквивалентных классов - семейство ПСП GMW. Как следует из теории разностных множеств Гордона-Миллза-Велча, различным базисным ПСП одной и той же длины соответствуют неэквивалентные ПСП GMW. На основе каждой такой ПСП с помощью децимаций были построены неэквивалентные классы GMW и доказано, что их мощности совпадают с мощностью класса t -последовательностей. При этом в качестве базисных последовательностей могут использоваться все перечисленные в Главе 1 последовательности типа Адамара, включая ПСП GMW. В результате общее число различных классов последовательностей GMW при фиксированном разложении числа N на целые множители k и t равно числу различных базисных последовательностей. Следует отметить, что похожие результаты применительно к двоичному случаю были получены Голомбом, Гонг и Дейем в 2000г. При этом авторы ограничились рассмотрением только ПСП GMW каскадного типа на основе коротких m -последовательностей.

В пятой главе, посвященной применению исследуемых ПСП в системах связи CDMA, рассматривается вопрос формирования максимальных по объему подмножеств квазиоптимальных последовательностей. Благодаря тому, что исходное число ПСП значительно превышает собственную мощность класса, эффективность выбора сигнатурных последовательностей с приемлемым уровнем взаимной корреляции существенно возрастает.

При длине последовательностей типа Адамара средняя вероятность ошибки в системе DS-CDMA с BPSK модуляцией не зависит от их выбора и определяется в основном количеством одновременно активных абонентов, число которых может превышать мощность одного класса. В этом случае в качестве сигнатурных рекомендуется использовать последовательности из разных классов или семейств. Найденные закономерности поведения пар m (GMW) последовательностей со сверхвысокими пиками взаимной корреляции создают

возможность для их совместного использования в квазисинхронных системах CDMA наряду с другими ПСП. Так, например, при $N=14$ максимальное число возможных для совместного использования ПСП одного класса увеличивается с 378 до 756, т.е. в 2 раза. При этом на этапе поиска сигнала периодичность сверхвысоких пиков может быть использована для уменьшения вероятности ложного захвата.

На основе исходной m -последовательности и производящей ПСП GMW построены ортогональные производные системы сигналов большой ЛС. Показано, в каких границах заключена ЛС.

Разработан метод повышения безопасности передачи данных в системах CDMA на основе стандартов IS-95 и cdma2000, в котором вместо m -последовательности в качестве скремблера выбрана последовательность GMW той же самой длины с параметрами $m=7$ и $k=6$. В результате ЛС полученной последовательности оказывается равной 326992, что в 7776 раз превышает ЛС исходной m -последовательности, порядка 128 на основе последовательностей типа Адамара длины 127. Приведены результаты математического моделирования разработанных систем сигналов и их сравнительные характеристики.