

СИНТЕЗ ФАЗОМАНИПУЛИРОВАННЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ С ХОРОШИМИ АВТОКОРРЕЛЯЦИОННЫМИ СВОЙСТВАМИ

ГОРБЕНКО И.Д., ЗАМУЛА А.А.,
КОЛОВАНОВА Е.П., КИЯНЧУК Р.И.,
ЯРЫГИНА Т.Е.

Рассматривается задача синтеза дискретных последовательностей с заданными корреляционными свойствами. Приводятся результаты исследований автокорреляционных функций одного класса дискретных последовательностей.

Введение

Синтез семейств сигналов с необходимыми авто- и взаимно-корреляционными свойствами заключается в отыскании семейства дискретных последовательностей, обладающего соответствующими авто- и взаимно-корреляционными функциями. Искусство проектирования широкополосных систем во многих аспектах базируется на нахождении сигналов с соответствующими корреляционными свойствами.

Рассмотрим кодовую последовательность $(a_0, a_1, \dots, a_{N-1})$. Если она используется для формирования импульсного сигнала S , комплексная огиба-

ющая которого имеет вид: $S(t) = \sum_{i=-\infty}^{\infty} a_i * S_0(t - i\Delta)$, аperiодическая или импульсная автокорреляционная функция (АКФ) вычисляется как [1]

$$P_a(m) = \begin{cases} \frac{1}{\|a\|^2} \sum_{i=m}^{N-1} a_i * a_{i-m}^*, m \geq 0 \\ \frac{1}{\|a\|^2} \sum_{i=0}^{N-1+m} a_i * a_{i-m}^*, m \leq 0 \end{cases}, \quad (1)$$

где $\|a\|$ – длина (евклидова норма) кодового вектора

$a = \{a_0, a_1, \dots, a_{N-1}\}$, или $\|a\|^2 = \sum_{i=0}^{N-1} |a_i|^2$ – энергия N -элементарной последовательности $\{a_0, a_1, \dots, a_{N-1}\}$;

m – число тактов сдвига кодовой последовательности относительно копии; $*$ – знак комплексного сопряжения.

Основное содержание исследований

Минимизация уровня боковых лепестков АКФ имеет наибольшее значение при конструировании сигнала для таких приложений как измерение времени запаздывания, временное разрешение и др. Следует иметь

в виду, что равенство нулю всех боковых лепестков невозможно для финитных или аperiодических ФМ сигналов. Действительно, если сигнал имеет длину N , то это влечет выполнение равенства $a_0 \neq 0$ и $a_{N-1} \neq 0$, поскольку в противном случае длина сигнала была бы меньше N . Тогда крайний правый боковой лепесток нормированной аperiодической АКФ кода (1) подобного сигнала будет:

$$P_a(N-1) = \frac{a_0 a_{N-1}^*}{\|a\|^2} \neq 0. \quad (2)$$

Последнее соотношение приводит к применению минимаксного критерия при синтезе сигналов, который требует достижения минимально возможной величины максимального бокового лепестка АКФ аperiодического кода. Формальная запись данного критерия имеет вид:

$$P_{a,\max} = \max_{m \neq 0} \{|P_a(m)|\} = \min. \quad (3)$$

В соответствии с критерием (3) предпочтительными являются кодовые последовательности с наименьшим значением максимального бокового лепестка. Таким образом, требования, предъявляемые к наилучшему сигналу, могут быть сформулированы в виде следующей оптимизационной задачи: на множестве всех возможных последовательностей длины N с символами из заранее выбранного алфавита найти последовательность или последовательности с минимальной величиной максимального бокового лепестка аperiодической АКФ.

Сформулированная выше оптимизационная задача, как и многие другие задачи дискретной оптимизации, не имеет общего аналитического решения, и типичной процедурой ее выполнения является осуществление исчерпывающего поиска.

Для любого ФМ сигнала $|a_i| = 1, i = 0, 1, \dots, N-1$, так что $|a_0 a_{N-1}^*| = 1$, и крайний правый боковой лепесток аperiодической АКФ (2) $|P_a(N-1)| = 1/N$. Следовательно, максимальный боковой лепесток ФМ сигнала ограничен снизу величиной:

$$P_{a,\max} \geq 1/N. \quad (4)$$

Естественно, что ФМ сигналы, удовлетворяющие данной границе, будут оптимальными. К числу оптимальных сигналов, удовлетворяющих границе (4), относят коды Баркера. Однако бинарные коды Баркера существуют лишь для длин 2, 3, 4, 5, 7, 11, 13, что конечно же не удовлетворяет многочисленным практическим нуждам. Указанное стимулирует поиск бинарных последовательностей большей длины с уровнем боковых лепестков, превышающих нижнюю границу. Поскольку ненормированная АКФ:

$$P(m) = \sum_{i=0}^{N-1} a_i * a_{i-m}^*, \quad P_{kl}(m) = \sum_{i=0}^{N-1} a_{k,i} * a_{l,i-m}^*$$

любой бинарной последовательности всегда определяется суммой ± 1 , то возможные значения $R_{a,max}$ для не баркеровских кодов принадлежит множеству $2/N, 3/N \dots$. Гарантированное нахождение глобально-оптимального (т.е. имеющего минимально возможное $R_{a,max} > 2/N$ при заданном N) бинарного кода может быть осуществлено только путем полного перебора возможных комбинаций. При этом вычислительный объем, необходимый для такой оптимизации, экспоненциально возрастает с увеличением длины N и становится нереализуемым при величинах N , превышающих 50.

Очевидно, что нахождение оптимальных бинарных последовательностей большой длины практически не реализуемо, задача (3) может быть сформулирована в виде: найти бинарный код с удовлетворительно малым уровнем периодического бокового лепестка $R_{a,max}$. Общая идея алгоритмов, направленных на решение этой задачи, состоит в предварительном отборе некоторого ограниченного множества последовательностей, которое кажется многообещающим в плане корреляционных свойств, и последующем поиске кода с минимальным значением $R_{a,max}$ только среди последовательностей, вошедших в указанное множество. Одним из примеров подобной стратегии является использование соотношения (4), связывающего аperiodическую АКФ со своим периодическим аналогом. Обозначая через $R_{p,max}$ максимальный боковой лепесток периодической АКФ: $R_{p,max} = \max_{m=1,2,\dots,n-1} \{ |R_p(m)| \}$ и используя неравенство:

$\max \{ |x + y| \} \leq \max \{ |x| + |y| \} \leq \max \{ |x| \} + \max \{ |y| \}$,
приходим к оценке $R_{p,max} \leq R_{a,max}$ или:

$$R_{a,max} \geq \frac{1}{2} R_{p,max}. \quad (5)$$

Из (5) следует, что последовательности с хорошей аperiodической АКФ могут быть найдены среди последовательностей с хорошей периодической АКФ.

Принято считать «идеальной» такую периодическую АКФ, которая обладает нулевыми боковыми лепестками, т.е. нулевыми значениями между периодическими основными лепестками, повторяющимися с периодом N . Указанное условие (с использованием нормированной версии АКФ) можно записать в виде:

$$R_p(m) = \frac{1}{E} \sum_{i=0}^{N-1} a_i * a_{i-m}^* = \begin{cases} 1 & m = 0 \bmod N \\ 0 & m \neq 0 \bmod N \end{cases}, \quad (6)$$

где запись $m = 0 \bmod N$ означает m кратно N (делится на N). Очевидно, что для идеальной АКФ $R_{p,max} = 0$.

В [1] показано, что необходимое условие получения идеальной АКФ для бинарной последовательности может быть записано как $N = 4h^2$, где h – целое. В

[2] было показано, что для длин $N \leq 12100$ единственным бинарным кодом с идеальной ПАКФ является код длины 4 вида: $+1+1+1-1$.

С учетом указанного вызывает интерес определение потенциала минимизации максимального бокового лепестка ПАКФ бинарных кодов.

Очевидно, что в отсутствие бинарных кодов с идеальной ПАКФ следующими по привлекательности являются бинарные последовательности, для которых $R_p(m)$ принимает значения ± 1 , при $m = 1, 2, \dots, N-1$, т.е. обладают $R_{p,max} = 1/N$, могут иметь только два возможных значения ненормированных ПАКФ либо:

$$R_p(m) = \begin{cases} N, & m = 0 \bmod N \\ +1, & m \neq 0 \bmod N \end{cases} \quad (7)$$

при длине $N = 4h + 1$, либо

$$R_p(m) = \begin{cases} N, & m = 0, \bmod N \\ -1, & m \neq 0, \bmod N \end{cases} \quad (8)$$

при длине $N = 4h - 1$.

Последовательности, удовлетворяющие соотношениям (7)–(8) и, следовательно, обладающие теоретически минимальным уровнем боковых лепестков ПАКФ ($R_{p,max} = 1/N$) для бинарных кодов нечетной длины, называются минимаксными. Известны только два примера ($N = 5$ и $N = 13$) последовательностей, подчиняющихся соотношению (7), тогда как существуют регулярные правила формирования минимаксных последовательностей, удовлетворяющих (8). К указанным типам последовательностей относят m -последовательности или последовательности максимальной длины, последовательности Лежандра.

К числу привлекательных с точки зрения ФАК относятся характеристические коды с числом позиций $N = 4x + 2$ и $N = 4x$, $x = 1, 2, \dots$ [3]. Построение данных кодов базируется на использовании характера мультипликативной группы $(\Psi(x))$ поля $GF(P^n)$, $n \geq 1$.

Несомненным достоинством данных кодов являются хорошие ансамблевые свойства. Характеристические коды, как было отмечено выше, существуют для всех $N = P^n - 1$ ($n \geq 1$). Более того, мощность метода кодирования для $N = P^n - 1$ равна числу классов неинверсно-изоморфных коэффициентов, которые могут быть получены разложением мультипликативной группы $T = \{t\} \{t, N\} = 1$ на смежные классы по классу автоморфных коэффициентов, и равна $\Psi(N)/2n$, где $\Psi(N)$ – функция Эйлера. Так, для характеристического кода с числом элементов $N = 2038$ существует 1018 изоморфизмов данного кода. Для размерности кода $N = 4x + 2$ максимальные боковые лепестки ПАКФ принимают значение $\{-2, 2\}$. В случае применения характеристических кодов с числом позиций $N = 4x$ боковые лепестки

ПАКФ $P_{a, \max}$ принимают значения $\{0, -4\}$. На рис. 1 представлен вид ПАКФ для характеристического кода с периодом $N = 256$ ($\Theta = 2$).

Естественно полагать, что данный класс кодов, обладающая хорошими корреляционными свойствами в части ПАКФ, будет иметь и малые значения боковых лепестков АФАК. Как было показано выше, любой циклический сдвиг последовательности $a_0, a_1, \dots, a_{N-1}$ длины N обладает такой же периодической АКФ, что и исходная последовательность, поскольку периодическая АКФ – инвариантна к циклическому сдвигу. Аperiodическая ФАК (АФАК) циклически сдвинутой копии может отличаться от АФАК первоначальной.

На рис. 2 представлен вид АФАК циклического сдвига ($m = 6$) одного из изоморфизмов характеристического кода с периодом $N = 256$. Для указанного циклического сдвига ($m = 6$) минимальное значение бокового лепестка АФАК равно -41 . На рис. 3 представлен вид АФАК для последовательности с таким же периодом, но при другом циклическом сдвиге ($m = 41$). В этом случае, минимальное значение максимального бокового лепестка АФАК равно 27 .

Факт отличия АФАК циклически сдвинутой копии от АФАК первоначальной последовательности вместе с границей (5) составляет основу метода поиска характеристических последовательностей с приемлемой АФАК. Суть метода состоит в следующем. Из множества значений длин, для которых существуют характеристические коды, выбираются последовательности с требуемыми периодом и значениями боковых лепестков функции корреляции (-4 , 0 , либо $+2$, -2). Затем осуществляется поиск по критерию наименьшего уровня максимума АФАК среди всех одно-периодных сегментов после-

довательностей кандидатов (изоморфизмов характеристического кода). В частности, берется одно-периодный сегмент первой последовательности кандидата, вычисляется его аperiodическая АКФ и запоминается в памяти уровень максимального бокового лепестка наряду с номерами последовательности кандидата (типа) и его сдвига.

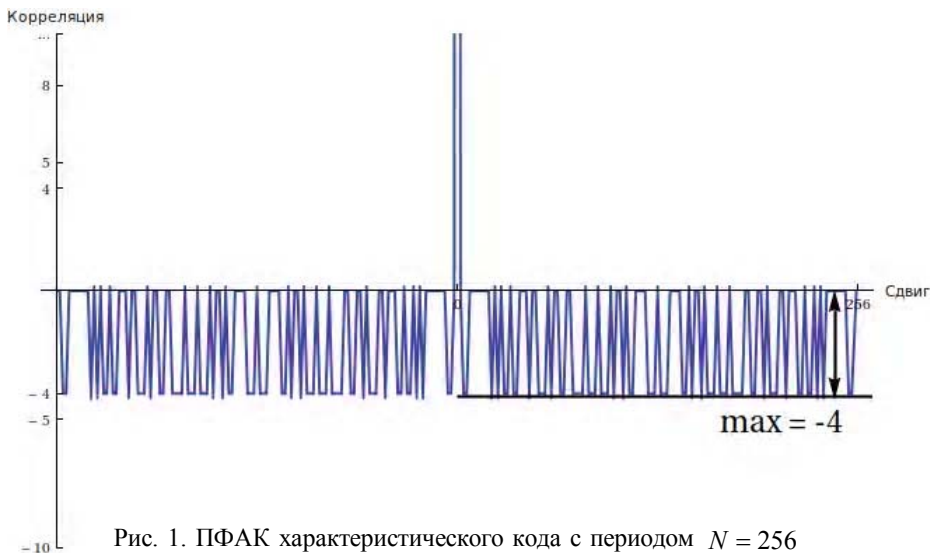


Рис. 1. ПАКФ характеристического кода с периодом $N = 256$

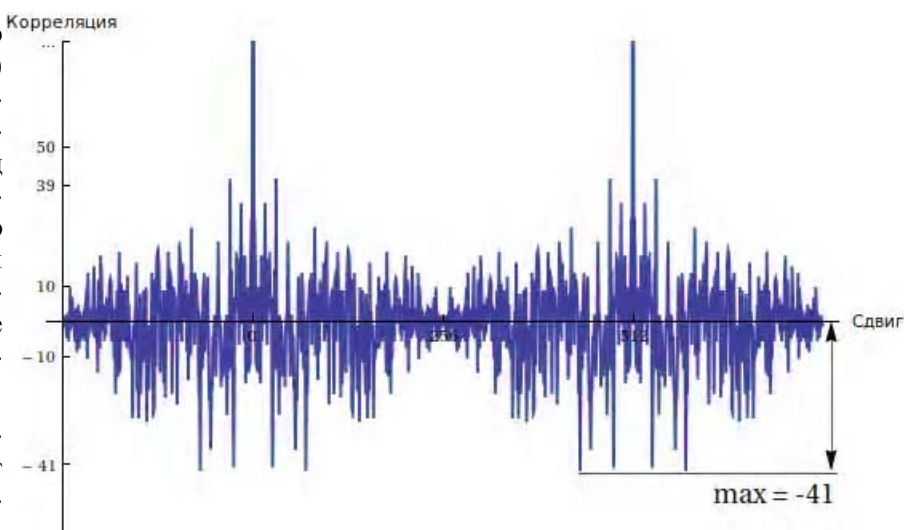


Рис. 2. АФАК циклического сдвига $m = 6$ для $N = 256$

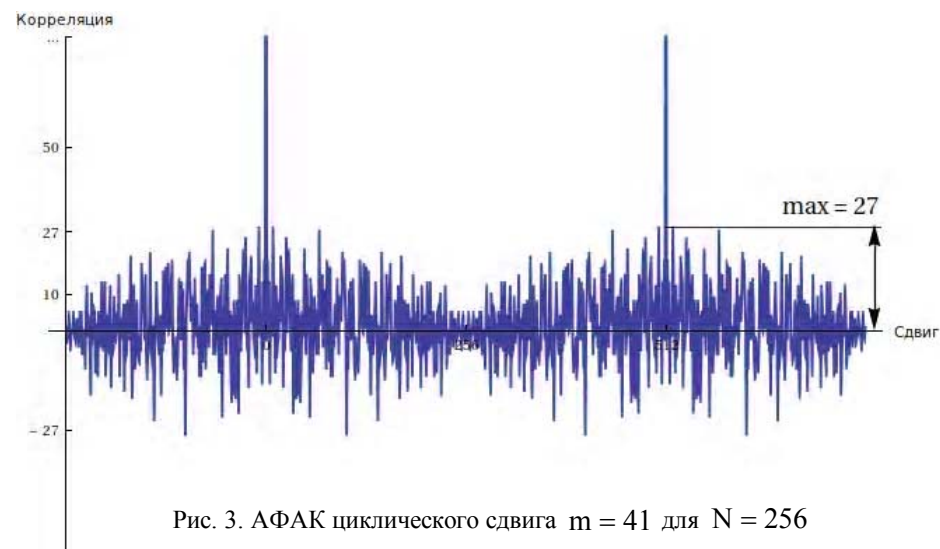


Рис. 3. АФАК циклического сдвига $m = 41$ для $N = 256$

Затем осуществляется циклический сдвиг сегмента на одну позицию и производятся необходимые вычисления. Если новое значение максимума апериодического токового лепестка окажется ниже предыдущего, то его значение и номер нового сдвига заменяют ранее записанные в памяти данные, в противном случае зарегистрированные значения сохраняются без изменения. Данная процедура повторяется N раз, т.е. для всех циклических сдвигов первой последовательности кандидата (для всех автоморфизмов исходного изоморфизма). Подобному исследованию подвергается следующая последовательность-кандидат (изоморфизм выбранного кода). Результатом поиска является последовательность с минимальным значением $R_{a,max}$ среди всего ансамбля последовательностей.

В табл. 1 представлены значения боковых лепестков АФАК для всех циклических сдвигов первого изоморфизма характеристического кода с периодом $N = 130$.

Таблица 1. Значения боковых лепестков АФАК для характеристического кода с периодом $N = 130$

Максимальный боковой лепесток	Соответствующие сдвиги
17	{76, 82}
18	{38, 56, 89, 102}
19	{3, 13, 50, 129}
20	{8, 19, 22, 40, 42, 43, 90, 108}
21	{2, 10, 30, 31, 36, 57, 68, 87, 96, 116, 119, 125}

В табл. 2 приведены результаты поиска циклических сдвигов характеристических последовательностей с периодом $N = 130$ и $N = 256$, при которых боковые лепестки АФАК имеют наименьшие значения.

Таблица 2. Циклические сдвиги характеристических последовательностей с наименьшими боковыми лепестками АФАК

N	Максимальные боковые лепестки	Соответствующие сдвиги
130	17	{76, 82}
256	27	{41, 114}

Как следует из данных табл. 1 и 2, минимальное значение боковых лепестков АФАК для периода $N = 130$ (при $m = 76, 82$) составляет 17, а при $N = 256$ и $m = 41, 114$ — равно 27.

Данный метод может быть использован при формировании ансамбля сигналов для различных приложений широкополосных систем. На первом этапе для заданной длины N некоторым образом формируется множество последовательностей с хорошей ПФАК. Оно может включать все известные последовательности заданной длины N , уровень боковых лепестков ПФАК которых согласно (5) позволяет надеяться на

получение низкого значения $R_{a,max}$. В такое множество, в качестве кандидатов, могут войти, как свидетельствуют представленные результаты, и характеристические последовательности. На втором этапе для каждой последовательности - кандидата, путем циклической перестановки его символов, находят оптимальные по минимаксному критерию апериодические коды и отбирают из них наилучшие.

Заключение

Автокорреляционная функция фазоманипулированного сигнала полностью определяется АКФ кодовой последовательности, и синтез фазоманипулированных сигналов с хорошими корреляционными свойствами состоит в отыскании последовательностей с хорошими АКФ. Результаты исследований, представленные в статье, показывают, что характеристические последовательности, вследствие хороших АКФ и ансамблевых свойств, могут найти применение в широкополосных системах для бинарной фазовой манипуляции несущей.

Литература: 1. Valery P. Ipatov Spread Spectrum and CDMA principles and Applications // Univesity of Turku. 2. Baumert L. D. Ciclic Difference Sets // Springer Verlage, 1971. 3. Свердлик М.Б. Оптимальные дискретные сигналы. М., 1975. 200 с.

Поступила в редколлегию 13.06.2011

Рецензент: д-р техн. наук, проф. Краснобаев В.А.

Горбенко Иван Дмитриевич, д-р техн. наук, профессор, зав. кафедрой безопасности информационных технологий ХНУРЭ. Научные интересы: проектирование и разработка систем защиты информации, исследование широкополосных систем связи. Адрес: Украина, 61202, Харьков, ул. Л.Свободы, 50А, кв. 49, тел. (057)702-14-25, e-mail: bit@kture.kharkov.ua.

Замула Александр Андреевич, канд. техн. наук, доцент, профессор кафедры безопасности информационных технологий ХНУРЭ. Научные интересы: проектирование и разработка систем защиты информации, исследование широкополосных систем связи. Адрес: Украина, 61085, Харьков, ул. Астрономическая, 35 А, кв. 61, тел. (057)702-14-25.

Колованова Евгения Павловна, ведущий инженер кафедры безопасности информационных технологий ХНУРЭ. Научные интересы: проектирование и разработка систем защиты информации, исследования широкополосных систем связи. Адрес: Украина, 61072, Харьков, ул. С.Есенина, 12, кв. 19, тел. (057)702-14-25.

Киянчук Руслан Игоревич, студент 4 курса ХНУРЭ. Научные интересы: блочные симметричные шифры, облегченная криптография (Lightweight Cryptography), стеганография, широкополосные системы связи. Адрес: Украина, 61166, Харьков, пр. Ленина, 14.

Ярыгина Татьяна Евгеньевна, студентка 4 курса ХНУРЭ. Научные интересы: криптография, блочные симметричные шифры, широкополосные системы связи. Адрес: Украина, 61166, Харьков, пр. Ленина, 14.