Инфокоммуникационные и радиоэлектронные технологии. 2018. Т. 1. № 3. С. 297—305.
Infocommunications and Radio Technologies, vol. 1, no. 3, pp. 297–305, 2018.
ISSN: 2587-9936 print / 0000-0000 online
DOI: 10.15826/icrt.2018.01.3.23

УДК 621.391

Координатный базис на основе псевдослучайных последовательностей

Дегтярев А. Н., Прудиус Е. С.
ФГАОУ ВО «Севастопольский государственный университет»
ул. Университетская, 33, г. Севастополь, 29905, Российская Федерация
degtyaryov1966@yandex.ru

Получено: 4 июня 2018 г.
Отрецензировано: 19 июня 2018 г.
Принято к публикации: 2 июля 2018 г.

Аннотация: *В широкополосных системах передачи информации используются шумоподобные сигналы, полученные на основе псевдослучайных последовательностей. Наибольшее распространение получили М-последовательности, которые имеют хорошие корреляционные свойства. Однако М-последовательности не являются ортогональными. В настоящей работе обосновывается методика создания ортогональных базисов на основе М-последовательностей. Доказываются две теоремы о линейной независимости функций, полученных путем циклического сдвига некоторой исходной дискретной функции. Для ортогонализации М-последовательностей используется метод ортогонализации, состоящий в определении веса ортогональности линейно независимых функций.*

Ключевые слова: *широкополосные системы связи, шумоподобные сигналы, М-последовательность, ортогональные функции, вес ортогональности.*

Для цитирования (ГОСТ 7.0.5—2008): Дегтярев А. Н., Прудиус Е. С. Координатный базис на основе псевдослучайных последовательностей // Инфокоммуникационные и радиоэлектронные технологии. 2018. Т. 1, № 3. С. 297—305.

Для цитирования (ГОСТ 7.0.11—2011): Дегтярев, А. Н. Координатный базис на основе псевдослучайных последовательностей / А. Н. Дегтярев, Е. С. Прудиус // Инфокоммуникационные и радиоэлектронные технологии. — 2018. — Т. 1, № 3. — С. 297—305.

Coordinate basis which foundation on pseudo-random sequences

A. N. Degtyaryov and E. S. Prudius
Sevastopol State University
33, Universitetskaya Str., Sevastopol, 299053, Russian Federation
degtyaryov1966@yandex.ru

Received: June 4, 2018
Peer-reviewed: June 19, 2018
Accepted: July 2, 2018

Abstract: *Broadband data transmission systems are used noise-like signals derived from pseudorandom sequences. The most widely used m-sequences have good correlation properties. However, M-sequences are not orthogonal sequences. In this work the methods of creation of orthogonal bases on the basis of M-sequences are proved. Two theorems on the linear independence of the functions obtained by cyclic shift of some of the original discrete functions are provide. For orthogonalization of M-sequences, the method of orthogonalization is used, which consists in determining the weight of orthogonality of linearly independent functions.*

Keywords: *broadband communication systems, noise-like signals,M-sequence, orthogonal functions, weight of orthogonality*.

For citation (IEEE): A. N. Degtyaryov and E. S. Prudius, “Coordinate basis which foundation on pseudo-random sequences” *Infocommunications and Radio Technologies*, vol. 1, no. 3, pp. 297–305, 2018. (In Russ.). doi: 10.15826/icrt.2018.01.3.23

1. Введение

В широкополосных системах передачи информации используются шумоподобные сигналы (ШПС). Наибольший интерес представляют ШПС, сформированные на основе псевдослучайных последовательностей (ПСП). В силу простоты реализации и хороших корреляционных свойств широкое применение нашли М-последовательности.

Напомним, что формируются М-последовательности с помощью линейных переключающих схем на основе сдвигающих регистров. При этом, если применяется регистр с k разрядами, а в М-последовательности используются p различных видов импульсов (отличающихся, например, фазами), то длина М-последовательности равна $p^k - 1$.

Все множество М-последовательностей, соответствующих одному образующему полиному, получается с помощью одного цифрового автомата. М-последовательности, принадлежащие одному множеству, являются циклически смещенными друг относительно друга.

Отметим, что сумма по модулю числа *p* двух М-последовательностей одного множества, является М-последовательностью, того же множества. Кроме того, произведение двух двоичных М-последовательностей является М-последовательностью того же множества, умноженной на минус единицу.

Существенным недостатком М-последовательностей является отсутствие ортогональности, наличие которой позволило бы упростить техническую реализацию приемных устройств систем передачи информации и устранить межсимвольную интерференцию, возникающую при демодуляции сигналов.

Целью настоящей работы является разработка методики создания ортогональных базисов на основе ПСП.

2. Обоснование разрабатываемой методики

Теорема 1. М-последовательности, полученные путем циклического сдвига одной М-последовательности на $i=1,2,3,\ldots,\ p^k-2$ позиций (p и k некоторые целые числа), являются линейно независимыми [1].

Доказательство: Зададим некоторую М-последовательность. Путем циклического сдвига этой М-последовательности на $i=1,2,3,\ldots,\ p^k-2$ позиций получим остальные p^k-2 М-последовательности. Составим из значений всех полученных функций квадратную матрицу размерностью $(p^k-1)\times(p^k-1)$. Строки и столбцы этой матрицы являются линейно независимыми, так как все они получаются друг из друга с помощью нелинейной операции суммирования по модулю числа p. Таким образом, определитель этой матрицы не равен нулю. Следовательно, М-последовательности, полученные путем циклического сдвига одной М-последовательности на $i=1,2,3,\ldots,\ p^k-2$ позиций (p и k некоторые целые числа), являются линейно независимыми.

Теорема доказана.

Если $p=2$, то приходим к двоичным М-последовательностям, которые принимают только два значения «+1» и «–1». Этот класс ПСП и согласованные фильтры для них наиболее просто реализуются технически.

Недостатком разложения функции по М-последовательностям является ограничение длины разлагаемой функции. Она должна строго равняться $p^k - 1$. Частично обойти этот недостаток можно на основе следующей теоремы.

Теорема 2. Дискретные функции нечетной длины *2n+1* (n = 1, 2, 3…), принимающие значения «–1» и «1» (положительных значений на одно больше, чем отрицательных), полученные путем циклического сдвига образующей функции на *i=1,2,3,…,2n* позиций являются линейно независимыми. Полученные аналогичным образом дискретные функции четной длины *2n*, (число положительных значений равно числу отрицательных значений) являются линейно зависимыми [1].

Доказательство: Зададим некоторую дискретную функцию длиной *2n*. Получим 2*n*-1 функцию, путем циклического сдвига заданной функции на 1, 2,…, 2*n*-1 позицию. Из значений полученных функций составим определитель порядка *2n.* Первая строка содержит *n* единиц со знаком «+» и *n* единиц со знаком «-». Переставим столбцы так, чтобы в первой строке определителя стояло подряд *n* единиц со знаком «+». При этом каждая последующая строка определителя может быть получена путем циклического сдвига предыдущей строки. Имеем

$$\begin{matrix} \\ n \\ \\ \\ (n+1) \end{matrix} \begin{vmatrix} 1 & 1 & 1 & \dots & 1 & -1 & -1 & -1 & \dots & -1 \\ -1 & 1 & 1 & \dots & 1 & 1 & -1 & -1 & \dots & -1 \\ . & . & . & . & . & . & . & . & . & . \\ -1 & -1 & -1 & \dots & -1 & 1 & 1 & 1 & \dots & 1 \\ . & . & . & . & . & . & . & . & . & . \end{vmatrix}. \qquad (1)$$

Определитель (1) содержит две строки (1-ю и n+1 – ю), которые отличаются только знаком, следовательно, определитель равен 0. Все определители такого вида отличаются только знаком, т.е. они также равны нулю. Таким образом, дискретные функции четной длины являются линейно зависимыми.

Рассмотрим теперь определитель нечетного порядка (2n+1). Путем перестановок столбцов получим в первой строке подряд n единиц со знаком «+» и n+1 единиц со знаком «-».При этом каждая последующая строка определителя может быть получена путем циклического сдвига предыдущей строки. Имеем

$$\begin{vmatrix} 1 & 1 & 1 & \dots & 1 & -1 & -1 & -1 & -1 & \dots & -1 \\ -1 & 1 & 1 & \dots & 1 & 1 & -1 & -1 & -1 & \dots & -1 \\ -1 & -1 & 1 & \dots & 1 & 1 & 1 & -1 & -1 & \dots & -1 \\ . & . & . & \dots & . & . & . & . & . & \dots & . \\ -1 & -1 & -1 & \dots & -1 & -1 & 1 & 1 & 1 & \dots & 1 \\ 1 & -1 & -1 & \dots & -1 & -1 & -1 & 1 & 1 & \dots & 1 \\ 1 & 1 & -1 & \dots & -1 & -1 & -1 & -1 & 1 & \dots & 1 \\ . & . & . & \dots & . & . & . & . & . & \dots & . \\ 1 & 1 & 1 & \dots & -1 & -1 & -1 & -1 & \dots & -1 & 1 \end{vmatrix}. \quad (2)$$

Если все строки определителя (2) прибавить к первой строке, то в ней все элементы будут равны –1. Вычтем первую строку из всех остальных строк.

Тогда определитель будет иметь следующий вид

$$\begin{vmatrix} -1 & -1 & -1 & \dots & \dots & \dots & \dots & \dots & \dots & -1 & -1 & -1 \\ 0 & 2 & 2 & \dots & 2 & 0 & 0 & 0 & \dots & \dots & 0 & 0 \\ 0 & 0 & 2 & 2 & \dots & 2 & 0 & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & 0 & 2 & 2 & \dots & 2 & 0 & 0 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 2 & 0 & 0 & 0 & \dots & \dots & \dots & \dots & 2 & 2 & \dots & 2 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 2 & 2 & \dots & 2 & 0 & 0 & \dots & 0 & 0 & \dots & 0 & 2 \end{vmatrix}.$$

Разложим полученный определитель по элементам первого столбца

$$\Delta_{2n+1} = -1 \cdot \begin{vmatrix} 2 & 2 & 2 & \dots & 2 & 0 & 0 & 0 & \dots & 0 \\ 0 & 2 & 2 & \dots & 2 & 2 & 0 & 0 & \dots & 0 \\ . & . & . & . & . & . & . & . & . & \\ 0 & 0 & 0 & \dots & 0 & 2 & 2 & 2 & \dots & 2 \\ 2 & 0 & 0 & \dots & 0 & 0 & 2 & 2 & \dots & 2 \\ . & . & . & . & . & . & . & . & . & \\ 2 & 2 & \dots & 2 & 0 & 0 & 0 & \dots & 0 & 2 \end{vmatrix} + \sum_{k=2} 2(-1)^{n+k} J_k .$$

Любой из определителей J_k равен нулю, так как путем перемещений столбцов можно из J_k получить определитель вида

$$J_k = \begin{vmatrix} -1 & -1 & -1 & \dots & -1 & -1 & -1 & -1 & \dots & -1 \\ 2 & 2 & 2 & \dots & 2 & 0 & 0 & 0 & \dots & 0 \\ . & . & . & . & . & . & . & . & . & . \\ 0 & 0 & 0 & \dots & 0 & 2 & 2 & 2 & \dots & 2 \\ . & . & . & . & . & . & . & . & . & . \end{vmatrix}.$$

Умножая первую строку на 2 и вычитая результат из второй строки, получим одну из строк этого же определителя. Таким образом, в силу линейной зависимости строк определители типа J_k равны нулю, и определитель $\Delta_{2n+1} = \pm 2^{2n}$. Знак определяется количеством перестановок столбцов, необходимых для того, чтобы привести определитель к виду, в котором в первой строке стоят подряд все единицы, а затем все «–1», а также количеством «–1» в образующей последовательности. Таким образом, дискретные функции нечетной длины являются линейно независимыми.

Линейная независимость рассмотренных последовательностей позволяет получить из них ортогональный базис с помощью процедуры ортогонализации Грама — Шмидта. Однако эта процедура изменяет форму последовательностей, а, следовательно, и их корреляционные свойства и свойства произведения.

Для создания ортогонального базиса будем использовать метод ортогонализации, состоящий в определении веса ортогональности линейно независимых функций [2]. Рассмотрим применение указанного метода для построения указанного базиса из двоичных М-последовательностей, принадлежащих одному множеству.

Пусть двоичная М-последовательность представляет собой последовательность символов

$$M_0 = \{x_1, x_2, \dots, x_N\},$$

вес ортогональности записывается как

$$H = \{h_1, h_2, \dots, h_N\},$$

где h_i — неизвестные значения веса.

С учетом свойства произведения двоичных М-последовательностей система уравнений, позволяющая определить неизвестные h_i, запишется в виде

$$\begin{cases} x_1^2 h_1 + x_2^2 h_2 + \ldots + x_{N-1}^2 h_{N-1} + x_N^2 h_N = E, \\ x_1 h_1 + x_2 h_2 + \ldots + x_{N-1}^2 h_{N-1} + x_N h_N = 0, \\ x_N h_1 + x_1 h_2 + \ldots + x_{N-2} h_{N-1} + x_{N-1} h_N = 0, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ x_2 h_1 + x_3 h_2 + \ldots + x_N h_{N-1} + x_1 h_N = 0. \end{cases} \quad (3)$$

Первое уравнение системы (3) задает энергию М-последовательностей E.

Система уравнений (3) содержит N неизвестных и N+1 уравнений и решений не имеет.

Таким образом, прямое использование метода работы [2] не позволяет получить искомый базис.

Совместная система уравнений может быть получена двумя путями:

— за счет исключения одного из уравнений системы (3), правая часть которого равна нулю;

— путем дописывания в начало или в конец каждой М-последовательности единицы.

Каждый из этих путей ведет к получению неполного ортогонального базиса, что вызывает определенные трудности при техническом использовании этого базиса.

Так, например, в первом случае, передача информации с помощью M-последовательностей будет осуществляться с пониженной скоростью. Если алфавит сигналов, построен с помощью полного набора М-последовательностей, то максимальная скорость передачи информации такими сигналами составит

$$R_0 = \frac{\log_2 N}{T},$$

где T — длительность сигналов алфавита.

Исключение одного из уравнений в системе (3) приводит к снижению максимальной скорости передачи информации до величины

$$R_0 = \frac{\log_2 N - 1}{T}.$$

Максимальная скорость передачи информации R_1 во втором случае уменьшается незначительно и составляет

$$R_1 = \frac{\log_2 N}{T\left(1 + \frac{1}{N}\right)} \exp \varphi_n .$$

3. Методика создания ортогонального базиса

Предлагается следующая методика создания ортогонального базиса. Каждую МП, полученную путем циклического сдвига исходной последовательности M_0, допишем в начало М-последовательности еще одним символ $x_0 = 1$. Система уравнений для определения координат веса примет вид

$$\begin{cases} x_0^2 h_0 + x_1^2 h_1 + \ldots + x_{N-1}^2 h_{N-1} + x_N^2 h_N = E, \\ x_0 h_0 + x_1 h_1 + \ldots + x_{N-1}^2 h_{N-1} + x_N h_N = 0, \\ x_0 h_0 + x_N h_1 + \ldots + x_{N-2} h_{N-1} + x_{N-1} h_N = 0, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ x_0 h_0 + x_2 h_1 + \ldots + x_N h_{N-1} + x_1 h_N = 0. \end{cases} \quad (4)$$

Система уравнений (4) разрешима относительно h_i. Например, если исходная последовательность и ее энергия равны соответственно

$$M_0 = \{-1,1,1,1,-1,-1,1\},\ \hat{A} = 6,$$

То

$$H = \{-1,1,1,1,1,1,1,1\}.$$

Кроме того, из (4) следует, что сохраняется свойство произведений М-последовательностей.

Предлагаемый ортогональный базис может быть сгенерирован с помощью автомата формирования М-последовательностей, который содержит дополнительные логические элементы, необходимые для дополнения М-последовательностей символом x_0.

4. Заключение

Разработанная методика получения ортогонального базиса может быть использована для создания алфавитов сигналов, применяемых в широкополосных системах передачи информации.

Список литературы

1. Дегтярьов А. М., Агаханянц Р. Е. Розкладання сигналу у ряд по неортогональним функціям // Вимірювальна та обчислювальна техніка в технологічних процесах. 1998. № 4. С. 177—182.
2. Дегтярев А. Н. Ортогонализация функций и повышение помехоустойчивости высокоскоростных систем передачи информации. М. : Инфра-М, 2015. 152 с.

References

[1] A. N. Degtyaryov and R. E. Agahanyantc, “Razlogenie signslov v ryad po neortogonalnim funktciyam [Decomposition of the signal into a series of non-orthogonal functions],” *Measuring and computing technique in technological processes*, no. 4. pp. 177–182, 1998. (In Ukr.).

[2] A. N. Degtyaryov, *Ortogonalizatciya funktciy i povishenie pomekhoustoychivosty visokoskorostnih sistem peredachi informatciy* [Orthogonalization of functions and increase of noise immunity of high-speed information transmission systems]. Moscow: Infra-M, 2015. (In Russ.).

Информация об авторах

Дегтярев Андрей Николаевич, кандидат технических наук, доцент кафедры «Информационная безопасность» Севастопольского государственного университета, г. Севастополь, Российская Федерация.

Прудиус Екатерина Сергеевна, магистрантка Института радиоэлектроники и информационной безопасности Севастопольского государственного университета, г. Севастополь, Российская Федерация.

Information about the authors

Andrey N. Degtyarev, Cand. Sci. (Eng.), associate professor of the Department of Information security of the Sevastopol State University, Sevastopol, Russian Federation.

Ekaterina S. Prudius, undergraduate of the Institute of radio electronics and information security of the Sevastopol State University, Sevastopol, Russian Federation.