ограничениями на их характеристики / НовГУ. Великий Новгород, 2009. 189 с.

5. Вагунин И. С., Едемский В. А. Определение параметров унимодулярных дельта-коррелированных последовательностей // Вестн. НовГУ. Сер. "Техн. науки". 2007. № 44. С. 20–23.

6. Едемский В. А., Вагунин И. С. О синтезе фазокодированных последовательностей с ограничениями на периодическую автокорреляционную функцию и пик-фактор // Изв. вузов России. Радиоэлектроника. 2010. Вып. 5. С. 3–9.

7. Гантмахер В. Е., Едемский В. А. Результаты синтеза пар двоичных последовательностей простого периода с одноуровневой и двухуровневой взаимной корреляцией // Изв. вузов. Радиоэлектроника. 2006. Вып. 4. С. 26–33.

8. Холл М. Комбинаторика. М.: Мир, 1970. 423 с.

9. Платонов С. М., Головняк Г. А., Гантмахер В. Е. База данных таблиц циклотомических чисел // Свидетельство о государственной регистрации базы данных № 2013620492 от 10.04.13.

10. Whiteman A. L. The cyclotomic numbers of order twelve // Acta arithmetica. 1960. № 6. P. 53–76.

V. A. Edemskiy, A. V. Ivanov
Novgorod state university n. a. Yaroslav-the-Wise

Synthesis of sequences formed on the basis of power residue classes of order twelve modulo a prime

Regular rules of sequences coding with good periodic auto correlated properties and the peak-factor equal three or four are received. Sequences are formed on the basis of power residue classes of order twelve on a prime modulo.

Sequences, synthesis, autocorrelation, peak factor

Статья поступила в редакцию 18 декабря 2013 г.

УДК 621.391

В. Е. Гантмахер, М. В. Залешин
Новгородский государственный университет им. Ярослава Мудрого

Обобщенная модель периодических последовательностей, формируемых над расширенными полями Галуа

Предложена обобщенная модель периодических последовательностей, формируемых над расширенными полями Галуа. Отличительная особенность модели заключается в возможности формирования двоичных, троичных, q-ичных, многофазных, многочастотных последовательностей, а также последовательностей, заданных над алфавитом комплексных чисел с целочисленными коэффициентами. Предложены обобщенное правило кодирования таких последовательностей и обобщенная формула расчета периодических корреляционных функций.

Обобщенная модель, периодическая последовательность, расширенное поле Галуа, периодическая корреляционная функция, анализ, синтез, М-последовательность

Развитие современных радиотехнических, радиолокационных, навигационных, вычислительных, космических и других информационных систем тесно связано с применением сложных широкополосных шумоподобных сигналов, свойства которых определяют дискретно-кодированные последовательности. В настоящее время синтезировано множество семейств последовательностей, формируемых над расширенными полями Галуа, которые отличаются алфавитом, периодом, корреляционными свойствами, методом модуляции, криптостойкостью, помехозащищенностью и целым рядом других параметров и характеристик.

Задачам формирования, анализа и синтеза последовательностей посвящено большое число фундаментальных исследований. Среди них следует отметить работы отечественных [1] и зарубежных [2] авторов. Актуальность темы исследований подтверждается регулярным проведением Всемирной конференции "Sequences and their applications"[1] и целым рядом публикаций [3], [4].

[1] Официальные сайты конференции: http://www.telecom-paristech.fr/SETA2010/sequences-applications.htm. http://seta2012.uwaterloo.ca/index.html.

Известные семейства последовательностей синтезированы, как правило, для конкретных систем. Требования, предъявляемые к таким последовательностям, во многом противоречивы. Например последовательности для систем связи, не применимы для радиолокационных систем с квазинепрерывным режимом работы. Задача поиска оптимальных последовательностей для произвольных приложений решения в общем виде не имеет.

Аналитический расчет оптимальной многокритериальной системы представляется чрезвычайно сложной задачей, особенно для многофункциональных адаптивных всепогодных комплексов. В этих условиях наиболее разумным и популярным является создание обобщенной модели, включающей в себя обширную библиотеку последовательностей с различными параметрами, характеристиками и свойствами. Выбор конкретной последовательности осуществляется в зависимости от назначения системы, приоритетов ее свойств, помеховой обстановки.

Под обобщенной моделью понимается система методик формирования, анализа и синтеза последовательностей для решения широкого спектра прикладных задач. Над простыми полями Галуа существуют обобщенные модели семейств последовательностей с заданным набором свойств и характеристик [5], [6]. Однако применение этих моделей в расширенных полях Галуа невозможно из-за разной циклической структуры полей, сложности расчета классов степенных вычетов и соответствующих циклотомических чисел в расширенных полях. Поэтому задача построения обобщенной модели над расширенными полями Галуа остается актуальной.

Цель настоящей статьи заключается в создании обобщенной модели периодических последовательностей, формируемых над расширенными полями Галуа.

Обобщенное правило кодирования периодических последовательностей над расширенными полями Галуа. Для достижения поставленной цели в составе разрабатываемой модели должен быть блок формирования большой библиотеки периодических последовательностей. В математической модели таким блоком является обобщенное правило кодирования (ОПК) периодических последовательностей, отличающихся периодом, методом модуляции и алфавитом символов.

Массив допустимых периодов определяется циклической структурой мультипликативных групп поля Галуа. Циклические группы предлагается формировать на основе генераторов М-последовательностей, обладающих оптимально малой эквивалентной линейной сложностью.

Пусть $GF(q^m)$ – расширенное поле Галуа, где $q = p^s$ – характеристика расширенного поля $GF(q)$; p – простое число; s и m – натуральные числа. Число различных символов алфавита можно изменять выбором характеристики q расширенного поля.

Обозначим $\{d_n\}$ – М-последовательность периода $L = q^m - 1$. На основе $\{d_n\}$ сформируем q двоичных последовательностей (ДП), которые назовем "структурными последовательностями" (СП), так как они определяют циклическую структуру формируемых последовательностей. СП, соответствующие ненулевым элементам расширяемого поля, определяются следующим образом:

$$x_n^{(r)} = \begin{cases} 1, & d_n \equiv \theta^r; \\ 0, & d_n \neq \theta^r, \end{cases}$$

где x – собственно структурная последовательность; r – степень первообразного элемента поля $GF(q)$, которому соответствует СП; n – порядковый номер символов последовательности; θ – первообразный элемент $GF(q)$. Сформированные СП имеют одинаковый период $L = q^m - 1$ и различаются только циклическим сдвигом. Всего таких последовательностей $q-1$.

СП, соответствующая нулевому символу расширяемого поля, имеет период $\left(q^m - 1\right)/(q-1)$ и определяется как

$$\xi_n = \begin{cases} 1, & d_n \equiv 0; \\ 0, & d_n \neq 0. \end{cases}$$

СП широко используются в известных правилах кодирования для формирования двоичных, троичных и многофазных последовательностей с различными периодами и корреляционными свойствами [3], [8]. Обобщенное правило кодирования периодических последовательностей является отображением, которое ставит в соответствие каждой СП (группе СП) значение амплитуды, фазы, частоты из определенного алфавита.

Таким образом, ОПК примет вид

$$y_n = \sum_{r=0}^{T-1} z_r x_n^{(r)} + \beta\xi_n = \begin{cases} z_r, & x_n^{(r)} = 1; \\ \beta, & \xi_n = 1. \end{cases} \quad (1)$$

где z_r и β – элементы выбранных алфавитов.

Последовательности $\{y_n\}$, формируемые с помощью ОПК (1), будем называть обобщенными последовательностями (ОП).

Многообразие формируемых последовательностей определяется циклической структурой поля Галуа, выбранным алфавитом (комбинацией алфавитов) и их объемами. Таким образом, ОПК обеспечивает многообразие не только последовательностей, но и методов модуляции.

Расчет периодических корреляционных функций последовательностей, формируемых на основе обобщенного правила кодирования. Как показано в предыдущем разделе, с помощью одного правила кодирования можно формировать огромную библиотеку последовательностей с большим набором различных параметров. Это создает предпосылку для вывода единой формулы расчета периодических корреляционных функций последовательностей, формируемых на основе ОПК.

Найдем ненормированную периодическую взаимную корреляционную функцию (ПВКФ) двух ОП.

Под моделирующей последовательностью (МП) далее будем понимать последовательность, используемую для формирования ОП. Ее элементами являются символы z_r из ОПК (1).

Теорема. Пусть на основе ОПК сформированы две последовательности:

$$y'_n = \sum_{r=0}^{T-1} z'_r x_n^{(r)} + \beta'\xi_n; \quad y''_n = \sum_{r=0}^{T-1} z''_r x_n^{(r)} + \beta''\xi_n. \quad (2)$$

Периоды соответствующих МП совпадают и равны произвольному натуральному числу ρ, делящему разность $q-1$ без остатка. Период ОП в $h = \left(q^m - 1\right)/(q-1)$ раз больше периода моделирующей последовательности.

Введем обозначения: $[\cdot]^*$ – операция комплексного сопряжения числа; $l = T/\rho \ \ (T = q-1)$; $R_{z', z''}(\tau)$ – ПВКФ МП $\{z'_r\}$ и $\{z''_r\}$ для $\tau = 0, 1, \ldots, \rho-1$; $\chi' = \sum_{r=0}^{\rho-1} z'_r$, $\chi'' = \sum_{r=0}^{\rho-1} z''_r$ – суммы элементов МП $\{z'_r\}$ и $\{z''_r\}$, соответственно, на одном периоде.

Тогда ПВКФ ОП $\{y'_n\}$ и $\{y''_n\}$ имеет вид

$$R_{y', y''}(\tau) = \frac{1}{l}\begin{cases} q^{m-1}\left[lR_{z', z''}(\tau/h) + \beta'[\beta'']^*\right] - \beta'[\beta'']^*, \\ \qquad \tau \equiv 0 (\mathrm{mod}\, h); \\ q^{m-2}(l\chi' + \beta')(l\chi'' + \beta'')^* - \beta'[\beta'']^*, \\ \qquad \tau \not\equiv 0 (\mathrm{mod}\, h). \end{cases} \quad (3)$$

Для доказательства теоремы воспользуемся следующей леммой.

Лемма. Периодические корреляционные функции СП определяются как

– для $\left\{x_n^{(r)}\right\}$:

$$R_r(\tau) = q^{m-2}\begin{cases} q, & \tau \equiv 0 (\mathrm{mod}\, L); \\ 0, & \tau \equiv 0 (\mathrm{mod}\, h); \\ 1, & \tau \not\equiv 0 (\mathrm{mod}\, L) \vee 0 (\mathrm{mod}\, h); \end{cases}$$

– для $\{\xi_n\}$:

$$R_\xi(\tau) = \frac{1}{T}\begin{cases} q^{m-1} - 1, & \tau \equiv 0 (\mathrm{mod}\, h); \\ q^{m-2} - 1, & \tau \not\equiv 0 (\mathrm{mod}\, h). \end{cases}$$

ПВКФ имеют вид

– для $\left\{x_n^{(r)}\right\}$ и $\{\xi_n\}$:

$$R_{r,\xi}(\tau) = R_{\xi, r}(\tau) = q^{m-2}\begin{cases} 0, & \tau \equiv 0 (\mathrm{mod}\, h); \\ 1, & \tau \not\equiv 0 (\mathrm{mod}\, h); \end{cases}$$

– для $\left\{x_n^{(j)}\right\}$ и $\left\{x_n^{(k)}\right\}$:

$$R_{j,k}(\tau) = R_j\left[\tau - (k-j)h\right] = R_0\left[\tau - (k-j)h\right].$$

Доказательство вытекает из соответствующих свойств М-последовательностей [7].

Доказательство теоремы. Применив ОПК для последовательностей (2), получим

$$R_{y', y''}(\tau) = \frac{1}{l}\sum_{n=0}^{L-1} y_n\left[y_{n+\tau}\right]^* =$$

$$= \frac{1}{l}\sum_{n=0}^{L-1}\left[\left(\sum_{r=0}^{T-1} z'_r x_n^{(r)} + \beta'\xi_n\right)\left(\sum_{r=0}^{T-1} z''_r x_{n+\tau}^{(r)} + \beta''\xi_{n+\tau}\right)^*\right] =$$

$$= \frac{1}{l}\left[\sum_{j,k=0}^{T-1} z'_j\left[z''_k\right]^* R_{j,k}(\tau) + \right.$$

$$\left. + R_{0,\xi}(\tau)\left([\beta'']^*\chi' + \beta'[\chi'']^*\right) + \beta'[\beta'']^* TR_\xi(\tau)\right].$$

Из леммы следует, что ПВКФ

$$R_{y',y''}(\tau) = \begin{cases} q^{m-1} l R_{z',z''}(\tau/h) - \beta'[\beta'']^* \left(q^{m-1} - 1\right), \\ \qquad \tau \equiv 0 (\mathrm{mod}\, h); \\ q^{m-2} l^2 \chi'[\chi'']^* + q^{m-2} l \left(\chi'[\beta'']^* + [\chi'']^* \beta'\right) + \\ \qquad + \beta'[\beta'']^* \left(q^{m-2} - 1\right), \ \tau \neq 0 (\mathrm{mod}\, h). \end{cases}$$

Упростив выражение, получим искомую формулу (3) ПВКФ ОП. Теорема доказана.

Следствие. ПАКФ ОП является частным случаем (3) при $\{y'_n\} = \{y''_n\} = \{y_n\}$ и имеет следующий вид:

$$R_y(\tau) = \begin{cases} q^{m-1} \left[l R_z(\tau/h) + |\beta|^2 \right] - |\beta|^2, \ \tau \equiv 0 (\mathrm{mod}\, h); \\ q^{m-2} |l\chi + \beta|^2 - |\beta|^2, \ \tau \neq 0 (\mathrm{mod}\, h). \end{cases} \quad (4)$$

Согласно (3) периодическую корреляционную функцию ОП в полной мере определяет МП, период которой в h раз меньше, что существенно сокращает необходимый объем вычислений.

Таким образом, доказанная теорема определяет единую формулу для расчета периодических авто- и взаимно корреляционных функций последовательностей, формируемых с помощью ОПК. Высокая эффективность вычислений по предлагаемой формуле обусловлена тем, что расчет корреляционных функций осуществляется в расширяемом поле Галуа, а не в расширенном.

Применение обобщенной модели для синтеза последовательностей с ограничением на значение бокового лепестка корреляционной функции. Обобщенное правило кодирования позволяет формировать обширную библиотеку последовательностей с различными наборами параметров, свойств и характеристик. Периодические корреляционные функции этих последовательностей рассчитываются по единой формуле, полученной в предыдущем разделе. Отсюда вытекает предпосылка к созданию единого алгоритма синтеза последовательностей с ограничением на уровень боковых лепестков их периодических корреляционных функций.

Основным принципом единого подхода к синтезу последовательностей является манипуляция параметрами ОПК. Алгоритм включает приведенную далее последовательность действий:

1. Выбор алфавита.

2. Выбор значения параметра β ОПК по заданным характеристикам последовательностей и по рельефу корреляционных функций.

3. Определение допустимых значений корреляционных функций ОП.

4. Расчет ограничений на характеристики МП.

5. Выбор моделирующих последовательностей.

6. Синтез правил кодирования.

7. Определение свойств корреляционных функций последовательностей, формируемых по каждому из синтезированных правил кодирования.

Проиллюстрируем предлагаемый алгоритм на примере синтеза фазоманипулированных последовательностей с одноуровневой ПАКФ $r(\tau) = -1$.

1. Пусть синтез проводится над Q-фазным алфавитом

$$A = \left\{ \exp\left[(2\pi i/Q) k \right] \right\}, \ k = 0, 1, \ldots, Q-1.$$

2. Выберем значение $\beta = 1$.

3. Для расчета допустимых значений корреляционных функций ОП подставим выбранные параметры ОПК в формулу (4):

$$R_y(\tau) = \begin{cases} q^{m-1} \left[l R_z(\tau/h) + 1 \right] - 1, \ \tau \equiv 0 (\mathrm{mod}\, h); \\ q^{m-2} |l\chi + 1|^2 - 1, \ \tau \neq 0 (\mathrm{mod}\, h). \end{cases}$$

Отсюда найдем, что заданный уровень бокового лепестка ПАКФ достигается при $l = 1$ и

$$\begin{cases} R_z(\tau) + 1 = 0; \\ |\chi + 1|^2 = 0. \end{cases}$$

4. Найдем ограничения на характеристики МП:

– уровень постоянного бокового лепестка ПАКФ равен $r(\tau) = -1$;

– сумма элементов $\chi = -1$;

– период равен $\rho = q - 1$.

5. Выбор моделирующей последовательности и ее периода определяется параметрами расширенного поля Галуа. Для разных значений характеристики q расширенного поля найдем МП:

– $q = 3$: $\{z_r\} = \left[\exp(2\pi i/3), \ \exp(4\pi i/3) \right]$;

– $q = 5$: $\{z_r\} = \left[\exp(2\pi i/5), \ \exp(4\pi i/5), \ \exp(8\pi i/5), \ \exp(6\pi i/5) \right]$;

– $q = 7$: $\{z_r\} = \left[\exp(2\pi i/7), \ \exp(6\pi i/7), \ \exp(4\pi i/7), \ \exp(12\pi i/7), \ \exp(8\pi i/7), \ \exp(10\pi i/7) \right]$;

– … .

Из приведенного примера видно, что количество МП является счетным множеством.

6. Синтезированные правила кодирования в общем виде запишутся как

$$y_n = \sum_{r=0}^{T-1} z_r x_n^{(r)} + \xi_n.$$

Многообразие правил кодирования последовательностей с заданными ограничениями на ПАКФ определяется выбором МП и СП.

7. Манипуляция моделирующими и структурными последовательностями в синтезированных правилах кодирования позволяет формировать счетное множество ОП с различными алфавитами, периодами и циклическими структурами при сохранении одноуровневой ПАКФ с $r(\tau) = -1$.

Синтезированные в примере правила кодирования относятся к последовательностям Люке I-го типа [8].

Рассмотренный пример демонстрирует возможности использования обобщенной модели для синтеза последовательностей с ограничением на уровень боковых лепестков их периодических корреляционных функций. Таким образом, предложен универсальный алгоритм синтеза, который позволяет удовлетворить широкий круг требований для правил кодирования последовательностей и их корреляционных функций.

Проверка адекватности модели проведена на многочисленных примерах формирования и синтеза семейств последовательностей с различными параметрами, а также анализа их корреляционных функций.

В настоящей статье разработана обобщенная модель периодических последовательностей, формируемых над расширенными полями Галуа. Элементами новизны представленной модели являются:

– единое правило кодирования, обеспечивающее формирование обширной библиотеки последовательностей с различными алфавитами; методами модуляции, периодами; циклическими структурами; корреляционными свойствами;

– простота формирования последовательностей, обусловленная построением расширенного поля Галуа на основе генератора М-последовательности, обладающего оптимально малой линейной сложностью;

– высокая эффективность вычислений, обусловленная расчетом корреляционных функций в расширяемом, а не в расширенном поле Галуа;

– применимость модели для расчета и анализа корреляционных функций семейств последовательностей, формируемых на основе обобщенного правила кодирования, поскольку для них получена единая расчетная формула;

– возможность применения модели для синтеза счетных множеств семейств последовательностей с заданным рельефом периодических корреляционных функций.

СПИСОК ЛИТЕРАТУРЫ

1. Свердлик М. Б. Оптимальные дискретные сигналы. М.: Сов. радио, 1975. 200 с.

2. Холл М. Комбинаторика. М.: Мир, 1970. 375 с.

3. Ипатов В. П. Широкополосные системы и кодовое разделение сигналов. Принципы и приложения. М.: Техносфера, 2007. 448 с.

4. Arasu K. T. Sequences and arrays with desirable correlation properties // NATO science for peace and security series. 2011. Vol. 29. P. 136–171.

5. Гантмахер В. Е, Быстров Н. Е., Чеботарев Д. В. Шумоподобные сигналы. СПб: Наука и техника, 2005. 396 с.

6. Едемский В. А, Гантмахер В. Е. Синтез двоичных и троичных последовательностей с заданными ограничениями на их характеристики / Новгородск. гос. ун-т им. Ярослава Мудрого. Великий Новгород, 2009. 189 с.

7. Цирлер Н. Линейные возвратные последовательности // Кибернетический сб. 1963. Вып. 6. С. 55–79.

8. Lüke H. D. Families of primitive-root sequences with good auto- and crosscorrelation functions // Archiv fur Elektronik und Ubertragungstechnik. 1993. Vol. 47, № 4. P. 269–270.

V. E. Gantmakher, M. V. Zaleshin
Yaroslav-the-Wise Novgorod state university

Generalized model of periodic sequences created over extended Galois fields

The generalized model of periodic sequences created over extended Galois fields is offered. Its distinctive characteristic consists of ability to construct binary, ternary, q-nary, polyphase, multifrequency sequences as well as sequences specified over alphabet of complex numbers with integral coefficients. The generalized coding rule for such sequences and the generalized formula for configuring periodic correlation functions are offered.

Generalized model, periodic sequence, extended Galois field, periodic correlation function, analysis, synthesis, M-sequence

Статья поступила в редакцию 6 февраля 2014 г.