УДК 621.391

ОБОБЩЕННОЕ ПРАВИЛО КОДИРОВАНИЯ ПЕРИОДИЧЕСКИХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ НАД РАСШИРЕННЫМИ ПОЛЯМИ ГАЛУА

М.В.Залешин, В.Е.Гантмахер

GENERALIZED CODING RULE OF PERIODIC SEQUENCES OVER EXTENDED GALOIS FIELDS

M.V.Zaleshin, V.E.Gantmakher

Институт электронных и информационных систем НовГУ, mikhailzaleshin@gmail.com

Построено обобщенное правило кодирования периодических последовательностей над полями Галуа произвольного расширения. В качестве базовой циклической структуры применяются М-последовательности. Полученное правило кодирования обладает высокой универсальностью, которая достигается широким выбором параметров, включая алфавит и период формируемых последовательностей.

Ключевые слова: обобщенное правило кодирования, расширенное поле Галуа, М-последовательность, периодическая последовательность

The generalized coding rule of periodic sequences over Galois fields of arbitrary extension is constructed. M-sequences are used as a basic cyclic structure. The obtained coding rule is highly multipurpose which is achieved by a wide variety of parameters including alphabet and period of generated sequences.

Keywords: generalized coding rule, extended Galois field, M-sequence, periodic sequence

1. Введение

Одно из главных направлений развития современных информационных технологий лежит в сфере широкополосных систем связи, локации, навигации, сотовых, волоконно-оптических, спутниковых и других информационных комплексов. Базовым элементом таких систем являются бинарные, двоичные, троичные, *P*-ичные, многофазные и псевдослучайные периодические последовательности.

Вопросам формирования последовательностей и изучению их свойств посвящено большое количество фундаментальных исследований отечественных [1-4] и зарубежных [5-8] авторов. Регулярно проводится всемирный форум «Sequences and Their Applications».

Отметим некоторые известные семейства последовательностей:

— последовательности Ипатова [9]. Формируются над троичным алфавитом на основе М-последовательностей и обладают идеальной периодической автокорреляционной функцией (ПАКФ) с пик-фактором, близким к единице;

— семейства многофазных последовательностей. Например, последовательности Чу [10], Милевского [11], Ли [12] и Люка [13], которые имеют низкий уровень боковых лепестков ПАКФ. Также несколько новых правил кодирования многофазных последовательностей предложено в работах Кренгеля [14];

— последовательности Лежандра [15]. Определяются классами квадратичных вычетов над простыми полями Галуа и имеют одноуровневую ПАКФ со значением бокового лепестка, равным –1;

— в [16] разработаны алгоритмы формирования ансамблей квазиортогональных последовательностей с идеальной ПАКФ.

Несмотря на значительное число научных работ, объектом исследования которых выступают периодические последовательности, актуальной остается задача разработки обобщенных правил кодирования (ОПК). Такие правила кодирования позволяют строить универсальные устройства формирования больших массивов периодических последовательностей, отличающихся алфавитом, периодом, структурой, корреляционными и другими свойствами. Подобные устройства необходимы для многофункциональных адаптивных комплексов различного назначения. В теоретическом плане ОПК позволяют систематизировать известные семейства последовательностей с различными свойствами, что особенно важно при синтезе последовательностей с заданным набором свойств.

По способу формирования большинство последовательностей можно разделить на две группы. Первая группа последовательностей определяется над простыми полями Галуа, вторая — над расширенными. Для простых полей Галуа крайне результативными являются ОПК, основанные на классах степенных вычетов и циклотомических числах [17,18]. Однако в общем случае распространить это ОПК на расширенные поля Галуа не представляется возможным из-за сложности расчета соответствующих циклотомических чисел. С другой стороны, определение ОПК на основе циклической структуры М-последовательностей над расширенными полями Галуа представляется исключительно актуальной задачей.

Таким образом, целью настоящей работы является построение ОПК периодических последовательностей над расширенными полями Галуа на основе М-последовательностей.

2. Общие положения

Пусть дано расширенное поле Галуа $GF(q^m)$, где $q = p^s$ — характеристика поля, p — простое число, а s и m – натуральные числа. Выбор кратности расширения поля не ограничен.

Соответствующую М-последовательность периода $L = q^m - 1$ над $GF(q^m)$ обозначим $\{d_n\}$. Выполним разложение $\{d_n\}$ на q двоичных последовательностей (ДП), поставив их в соответствие каждому элементу поля $GF(q)$. Так, для последовательности, отвечающей элементу $\mu \in GF(q)$, единица ставится на тех позициях n, для которых соответствующий элемент М-последовательности $\{d_n\}$ равен μ, и нуль в остальных случаях.

Пусть θ — первообразный элемент поля $GF(q)$. Любой ненулевой элемент этого поля выражается через первообразный как θ^r. Всего таких элементов $T = q - 1$. Каждому элементу θ^r поставим в соответствие ДП, как было описано выше:

$$x_n^{(r)} = \begin{cases} 1, & \text{если } d_n \equiv \theta^r; \\ 0, & \text{в противном случае.} \end{cases}$$

Индекс r принимает значения от нуля до $T - 1$. А период всех $\{x_n^{(r)}\}$ совпадает с периодом М-последовательности $\{d_n\}$, т. е. равен L.

С другой стороны, для нулевого элемента поля $GF(q)$ получаем:

$$\xi_n = \begin{cases} 1, & \text{если } d_n = 0; \\ 0, & \text{в противном случае.} \end{cases}$$

По свойствам М-последовательностей [19] ДП $\{\xi_n\}$ имеет период $h = L/T$.

Определение 1. ДП $\{x_n^{(r)}\}$ и $\{\xi_n\}$ назовем структурными последовательностями (СП). Они отражают структуру М-последовательности.

В силу свойств расширенных полей Галуа [1,5,17] имеют место следующие свойства СП:

Свойство 1. Для произвольной СП $\{x_n^{(r)}\}$ справедливо равенство: $x_{n+kh}^{(r)} = x_n^{(r-k)}$.

Свойство 2. Для произвольной СП $\{x_n^{(r)}\}$ справедливо равенство: $x_n^{(r-T)} = x_n^{(r)}$.

3. Обобщенное правило кодирования

Построим ОПК, поставив в соответствие каждой СП некоторый символ. Для достижения большей универсальности используем комплексный алфавит.

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

СП $\{x_n^{(r)}\}$, отвечающей элементу θ^r из $GF(q)$, соответствует комплексный символ z_r. СП $\{\xi_n\}$, которая определяется нулевым элементом $GF(q)$, в соответствие ставится комплексное число β. То есть (1) эквивалентно следующей формуле:

$$\gamma_n = \begin{cases} z_r, & \text{если } d_n \equiv \theta^r; \\ \beta, & \text{в противном случае.} \end{cases}$$

На основе символов z_r сформируем последовательность $\{z_r\}$ периода ρ, который должен делить $T = q - 1$ без остатка.

Определение 2. Назовем $\{z_r\}$ моделирующей последовательностью (МП).

Чтобы расширить функциональные возможности формирования последовательностей, введем вспомогательный коэффициент α, являющийся в общем случае комплексным числом. Такой, что $|\alpha| = 1$, а последовательность $\{\alpha^n\} = (\alpha^0, \alpha^1, \ldots)$ имеет период, делящий $h = L/T$ без остатка. Окончательно ОПК принимает вид:

$$y_n = \alpha^n \gamma_n = \alpha^n \left(\sum_{r=0}^{T-1} z_r x_n^{(r)} + \beta\xi_n \right) = \\ = \alpha^n \begin{cases} z_r, & \text{если } d_n \equiv \theta^r; \\ \beta, & \text{в противном случае.} \end{cases} \qquad (2)$$

Определение 3. Последовательность $\{y_n\}$, формируемую с помощью ОПК (2), назовем обобщенной последовательностью (ОП).

Таким образом, ОПК (2) определяется следующими параметрами:

1) характеристикой и степенями расширения поля Галуа, над которым строится множество СП;

2) алфавитом. В общем случае ОПК определено над комплексным алфавитом, следовательно, допустимы любые его частные случаи. Это позволяет формировать большинство известных семейств последовательностей;

3) моделирующей последовательностью. Оказывает влияние на вид и свойства формируемой ОП;

4) коэффициентами α и β. Параметр β позволяет снизить уровень бокового лепестка периодической корреляционной функции, а α — изменить период формируемой ОП.

Оценим период ОП $\{y_n\}$, определяемой ОПК (2).

Теорема 1. Период ОП $\{y_n\}$, которая соответствует МП $\{z_r\}$ периода ρ, равен или делит ρh без остатка.

Доказательство. Достаточно показать, что $y_{n+\rho h} = y_n$. Поскольку $y_n = \alpha^n \gamma_n$, то необходимо установить истинность равенства $\alpha^{n+\rho h}\gamma_{n+\rho h} = \alpha^n \gamma_n$. По построению период последовательности $\{\alpha^n\}$ делит h без остатка. Следовательно, $\alpha^{n+\rho h} = \alpha^n$.

По формуле (1) имеем:

$$\gamma_{n+\rho h} = \sum_{r=0}^{T-1} z_r x_{n+\rho h}^{(r)} + \beta\xi_{n+\rho h}.$$

СП $\{\xi_n\}$ имеет период $h = L/T$, следовательно, $\xi_{n+\rho h} = \xi_n$. Осталось показать, что

$$\sum_{r=0}^{T-1} z_r x_{n+\rho h}^{(r)} = \sum_{r=0}^{T-1} z_r x_n^{(r)}.$$

По свойству 1 имеем:

$$\sum_{r=0}^{T-1} z_r x_{n+\rho h}^{(r)} = \sum_{r=0}^{T-1} z_r x_n^{(r-\rho)} = \sum_{r=0}^{T-1} z_{r-\rho} x_n^{(r-\rho)} = \\ = \sum_{v=-\rho}^{T-1-\rho} z_v x_n^{(v)} = \sum_{v=-\rho}^{-1} z_v x_n^{(v)} + \sum_{v=0}^{T-1-\rho} z_v x_n^{(v)}.$$

В первой сумме произведем замену $w = T + v$ и воспользуемся свойством 2, а также условием периодичности МП:

$$\sum_{v=-\rho}^{-1} z_v x_n^{(v)} = \sum_{w=T-\rho}^{T-1} z_{w-T} x_n^{(w-T)} = \sum_{w=T-\rho}^{T-1} z_w x_n^{(w)}.$$

Тогда окончательно:

$$\sum_{r=0}^{T-1} z_r x_{n+\rho h}^{(r)} = \sum_{w=T-\rho}^{T-1} z_w x_n^{(w)} + \sum_{v=0}^{T-1-\rho} z_v x_n^{(v)} = \sum_{r=0}^{T-1} z_r x_n^{(r)}.$$

То есть равенство $\gamma_{n+\rho h} = \gamma_n$ выполняется. Отсюда вытекает истинность $y_{n+\rho h} = y_n$. Теорема доказана.

4. Апробация ОПК

Чтобы продемонстрировать универсальность ОПК (2), приведем несколько примеров. Покажем, что многие известные последовательности являются частным случаем ОП при конкретных значениях параметров ОПК.

Теорема 2. ОП, формируемая на основе расширенного поля Галуа $GF(3^2)$, вырожденной МП $\{z_r\} = (+)$ периода $\rho = 1$, коэффициентов $\alpha = 1$ и $\beta = -1$ над бинарным алфавитом, совпадает с бинарной последовательностью (БП) (+,–,+,+) (с точностью до эквивалентных преобразований, см. [20]), которая имеет идеальную ПАКФ.

Доказательство. М-последовательность $\{d_n\}$ над $GF(3^2)$ имеет период $L = 8$ и для примитивного многочлена $f(x) = 2 + x + x^2$ принимает вид: (1,0,1,1,2,0,2,2). Поскольку первообразный элемент θ поля $GF(3)$ равен двум, то получаем следующее множество СП:

— элементу $\theta^0 = 1$ отвечает $\{x_n^{(0)}\} = (1,0,1,1,0,0,0,0)$;

— элементу $\theta^1 = 2$ отвечает $\{x_n^{(1)}\} = (0,0,0,0,1,0,1,1)$;

— нулевому элементу поля $GF(3)$ отвечает $\{\xi_n\} = (0,1,0,0)$.

Подстановка параметров в ОПК дает:

$$\{y_n\} = 1^n\left(+\sum_{r=0}^{1}\{x_n^{(r)}\}-\{\xi_n\}\right) = +(1,0,1,1,0,0,0,0)+$$

$$+(0,0,0,0,1,0,1,1)-(0,1,0,0) = (+,-,+,+,+,-,+,+) = (+,-,+,+).$$

Что и требовалось показать.

Теорема 3. ОП, формируемые над расширенными полями Галуа $GF(3^3)$ и $GF\left(\left[2^2\right]^2\right)$ на основе МП $\{z_r\} = (+)$ периода $\rho = 1$ и коэффициентов $\alpha = 1$ и $\beta = -1$, соответствуют БП $(+,-,+,+,+)$ и $(+,-,-,+,+,+,-,+,+,+,+,-)$ (или их равносильным преобразованиям, см. [21]), которые обладают одноуровневыми ПАКФ со значением бокового лепестка, равным единице.

Те же параметры ОПК используются выше при формировании БП $(+,-,+,+)$. Доказательство заключается в простой подстановке значений параметров в ОПК и полностью аналогично доказательству теоремы 2.

Схожему набору параметров (МП $(+)$, $\alpha = 1$ и $\beta = -1$) над расширенным полем Галуа $GF(2^m)$ соответствует семейство БП с одноуровневой ПАКФ и боковым лепестком, равным –1.

Теорема 4. ОП, формируемые на основе расширенного поля Галуа $GF(q^m)$ с нечетной характеристикой и степенью расширения, МП $\{z_r\} = (+,-)$ периода $\rho = 2$, коэффициентов $\alpha = -1$ и $\beta = 0$, эквивалентны ТП Ипатова [9] с идеальной ПАКФ.

Доказательство. Последовательности Ипатова определяются следующим правилом кодирования:

$$c_n = (-1)^n\begin{cases} 1, \text{ если } d_n - \text{квадратичный вычет;} \\ -1, \text{ если } d_n - \text{квадратичный невычет;} \\ 0, \text{ в противном случае.} \end{cases}$$

Подстановка параметров, указанных в формулировке теоремы, в ОПК приводит к эквивалентной формуле. Теорема доказана.

Теорема 5. ОП, формируемые на основе расширенного поля Галуа $GF(p^m)$, где p — простое число; МП $\{z_r\} = \{\theta^r\}$ периода $\rho = T-1 = p-2$ и коэффициентов $\alpha = 1$ и $\beta = 0$, равносильны с точностью до циклического сдвига соответствующим М-последовательностям над $GF(p^m)$.

Доказательство этого утверждения вытекает из определения ОПК.

Теорема 6. ОП, формируемые над расширенным полем Галуа $GF(p^m)$, где p — простое число, на основе МП $\{z_r\} = \left\{\exp\left(2\pi i\frac{\theta^r}{p}\right)\right\}$ периода $\rho = T-1 = p-2$ и коэффициентов $\alpha = 1$ и $\beta = 1$, совпадают с некоторыми многофазными последовательностями Люка [13].

Доказательство. На основании формулы (2) правило кодирования принимает вид:

$$y_n = 1^n\begin{cases} 2\pi i\frac{\theta^r}{p}, \text{ если } d_n \equiv \theta^r; \\ 1, \text{ в противном случае.} \end{cases} = \exp\left(2\pi i\frac{d_n}{p}\right).$$

Сформированная последовательность $\{y_n\}$ относится к последовательностям Люка I-го типа. Что и требовалось показать.

5. Заключение

Предложено обобщенное правило кодирования периодических последовательностей, которое позволяет формировать практически все известные семейства последовательностей над расширенными полями Галуа. Универсальность ОПК достигается широким выбором параметров:

— характеристикой, степенями и кратностью расширения поля Галуа;

— алфавитом;

— моделирующей последовательностью;

— периодом формируемых последовательностей.

Достоверность работы и практическая реализуемость ОПК проверены на компьютерной модели. Универсальность ОПК проиллюстрирована на многочисленных примерах.

1. Свердлик М.Б. Оптимальные дискретные сигналы. М.: Сов. радио, 1975. 200 с.
2. Тихонов В.И. Статистическая радиотехника. М.: Радио и связь, 1982. 624 с.
3. Тузов Г.И. Статистическая теория приема сложных сигналов. М.: Сов. радио, 1977. 400 с.
4. Ипатов В.П. Периодические дискретные сигналы с оптимальными корреляционными свойствами. М.: Радио и связь, 1992. 152 с.
5. Холл М. Комбинаторика. М.: Мир, 1970. 375 с.
6. Голомб С.У., Тейлор Х. Конструкции и свойства массивов Костата // ТИИ-ЭР. 1984. Т.72. №9. С.44-64.
7. Хаффмен Д. Синтез линейных цепей последовательного декодирования // Теория передачи сообщений. Изд-во иностранной литературы, 1957. 128 с.
8. Касами Т. и др. Теория кодирования. М.: Мир, 1978. 576 с.
9. Ипатов В.П. Широкополосные сигналы. N.Y.: Wiley, 2004. 373 с.
10. Chu D. Polyphase codes with good periodic correlation properties // IEEE Information Theory. 1972. V.18. №4. P.531-532.
11. Milewsky A. Periodic sequences with optimal properties for channel estimation and fast start-up equalization // IBM J. Res.Develop. 1983. V.27. №5. P.426-431.
12. Lee C.E. Perfect q-ary sequences from multiplicative characters over GF(p) // Electron. Lett. 1992. V.28. P.833-835.
13. Luke H.D. BTP-transform and perfect sequences with small phase alphabet // IEEE Transactions Aerosp. Syst. 1996. V.32. P.497-499.
14. Krengel E.I. Some constructions of almost-perfect, odd-perfect and perfect polyphase and almost-polyphase sequences // SETA. 2010. V.6338. P.387-398.
15. Кренгель Е.И. Новые идеальные 4- и 8-фазные последовательности с нулями // Радиотехника. 2007. №5. С.3-8.
16. Леухин А.Н., Тюкаев А.Ю., Парсаев Н.В., Корнилова Л.Г. Ансамбли квазиортогональных многофазных последовательностей с идеальной периодической автокорреляционной функцией // Известия вузов России. Радиоэлектроника. 2009. №6. С.36-43.
17. Гантмахер В.Е, Быстров Н.Е., Чеботарев Д.В. Шумоподобные сигналы. СПб: НиТ, 2005. 396 с.
18. Едемский В.А, Гантмахер В.Е. Синтез двоичных и троичных последовательностей с заданными ограничениями на их характеристики. В.Новгород: НовГУ, 2009. 189 с.

19. Цирлер Н. Линейные возвратные последовательности // Кибернетический сборник. 1963. С.55-79.
20. Schmidt B. Cyclotomic integers and finite geometry // J. Am. Math. Soc. 1999. V.12. P.929-952.
21. Eliahou S., Kervaire M. Barker sequences and difference sets // L'Enseignement Math. 1992. V.38. P.345-382.

Bibliography (Transliterated)

1. Sverdlik M.B. Optimal'nye diskretnye signaly. M.: Sov. radio, 1975. 200 s.
2. Tikhonov V.I. Statisticheskaia radiotekhnika. M.: Radio i sviaz', 1982. 624 s.
3. Tuzov G.I. Statisticheskaia teoriia priema slozhnykh signalov. M.: Sov. radio, 1977. 400 s.
4. Ipatov V.P. Periodicheskie diskretnye signaly s optimal'nymi korreliatsionnymi svoistvami. M.: Radio i sviaz', 1992. 152 s.
5. Kholl M. Kombinatorika. M.: Mir, 1970. 375 s.
6. Golomb S.U., Teilor Kh. Konstruktsii i svoistva massivov Kostata // TII-ER. 1984. T.72. №9. S.44-64.
7. Khaffmen D. Sintez lineinykh tsepei posledovatel'nogo dekodirovaniia // Teoriia peredachi soobshchenii. Izd-vo inostrannoi literatury, 1957. 128 s.
8. Kasami T. i dr. Teoriia kodirovaniia. M.: Mir, 1978. 576 s.
9. Ipatov V.P. Shirokopolosnye signaly. NY: Wiley, 2004. 373 s.
10. Chu D. Polyphase codes with good periodic correlation properties // IEEE Information Theory. 1972. V.18. №4. P.531-532.
11. Milewsky A. Periodic sequences with optimal properties for channel estimation and fast start-up equalization // IBM J. Res.Develop. 1983. V.27. №5. P.426-431.
12. Lee C.E. Perfect q-ary sequences from multiplicative characters over GF(p) // Electron. Lett. 1992. V.28. P.833-835.
13. Luke H.D. BTP-transform and perfect sequences with small phase alphabet // IEEE Transactions Aerosp. Syst. 1996. V.32. P.497-499.
14. Krengel E.I. Some constructions of almost-perfect, odd-perfect and perfect polyphase and almost-polyphase sequences // SETA. 2010. V.6338. P.387-398.
15. Krengel' E.I. Novye ideal'nye 4- i 8-faznye posledovatel'nosti s nuliami // Radiotekhnika. 2007. №5. S.3-8.
16. Leukhin A.N., Tiukaev A.Iu., Parsaev N.V., Kornilova L.G. Ansambli kvaziortogonal'nykh mnogofaznykh posledovatel'nostei s ideal'noi periodicheskoi avtokorreliatsionnoi funktsiei // Izvestiia vuzov Rossii. Radioelektronika. 2009. №6. S.36-43.
17. Gantmakher V.E, Bystrov N.E., Chebotarev D.V. Shumopodobnye signaly. SPb: NiT, 2005. 396 c.
18. Edemskii V.A, Gantmakher V.E. Sintez dvoichnykh i troichnykh posledovatel'nostei s zadannymi ogranicheniiami na ikh kharakteristiki. V.Novgorod: NovGU, 2009. 189 s.
19. Tsirler N. Lineinye vozvratnye posledovatel'nosti // Kiberneticheskii sbornik. 1963. S.55-79.
20. Schmidt B. Cyclotomic integers and finite geometry // J. Am. Math. Soc. 1999. V.12. P.929-952.
21. Eliahou S., Kervaire M. Barker sequences and difference sets // L'Enseignement Math. 1992. V.38. P.345-382.