УДК 621.391

В. А. Едемский, А. В. Иванов
Новгородский государственный университет им. Ярослава Мудрого

Синтез последовательностей на основе классов степенных вычетов двенадцатого порядка по простому модулю

Получены регулярные правила кодирования последовательностей с хорошими периодическими автокорреляционными свойствами и пик-фактором, равным 3 или 4. Последовательности формируются на основе классов степенных вычетов двенадцатого порядка по простому модулю.

Последовательности, синтез, автокорреляция, пик-фактор

Изменение кодируемого параметра (амплитуды, фазы, частоты) в дискретных сигналах задается числовой последовательностью, которая в этом случае называется дискретно-кодированной (кодовой, кодом) и определяет свойства сигнала [1]. Важными характеристиками дискретно-кодированной последовательности комплексных чисел $X=\{x_0, \ldots, x_{N-1}\}$ с периодом N являются ее периодическая автокорреляционная функция (ПАКФ) $\lambda_X(\tau)=\sum_{j=0}^{N-1} x_j\overline{x}_{j+\tau}$ (черта сверху обозначает комплексное сопряжение) и пик-фактор pf – отношение периода последовательности к $\lambda_X(0)$ [1].

В настоящей статье рассматриваются последовательности с алфавитом $\{e^{2\pi ik/n},\ k=0,\ 1,\ \ldots,\ n-1\}$ (i – мнимая единица; $n\geq 3$ – натуральное число), формируемые на основе классов степенных вычетов двенадцатого порядка по простому модулю. Определены регулярные правила кодирования последовательностей с хорошими периодическими автокорреляционными свойствами и $pf\approx 3$ или $pf\approx 4$.

Метод анализа ПАКФ последовательностей. Пусть $p=dR+1$ – простое число (d, R – натуральные числа). Обозначим через θ первообразный корень по модулю p, а через $H_0=\{\theta^{dt},\ t=0,\ 1,\ \ldots,\ R-1\}$ – класс вычетов степени d [2]. Пусть $H_k=\theta^k H_0$, $k=1,\ \ldots,\ d-1$ (все действия выполняются по модулю p). H_k называются классами смежности подгруппы H_0 в мультипликативной группе конечного поля порядка p или циклотомическими классами порядка d.

В [1] разработан математический аппарат для анализа периодических корреляционных функций троичных последовательностей, сформированных на циклотомических классах порядка d. На его основе создана методика синтеза троичных последовательностей с заданными ограничениями на их основные характеристики, в частности на ПАКФ и пик-фактор [1], [3], [4]. Получены многочисленные результаты синтеза последовательностей [1], [4].

В [5], [6] показано, что эта же методика применима и для анализа ПАКФ комплексных последовательностей. В частности, если u, v – комплексные числа и последовательности Y_k, Y_l, $k,\ l=0,\ 1,\ \ldots,\ d-1$, формируются на основе одного циклотомического класса по правилам кодирования:

$$U_{Y_k}(j)=\begin{cases} u, & j\in H_k;\\ 0, & j\notin H_k;\end{cases}\quad U_{Y_l}(j)=\begin{cases} v, & j\in H_l;\\ 0, & j\notin H_l,\end{cases} \qquad (1)$$

то справедливы взаимно однозначные соответствия [5]:

$$\lambda_k(\tau)\Leftrightarrow u\overline{u}S(k,\ k);\ r_{k,\ l}(\tau)\Leftrightarrow u\overline{v}S(k,\ l), \qquad (2)$$

где $\lambda_k(\tau)$ – ПАКФ последовательности Y_k; $r_{k,l}(\tau)$ – периодическая взаимно корреляционная функция пары последовательностей Y_k и Y_l; $S(k, l)$ – спектр разностей классов вычетов (СРКВ) H_k и H_l [1]. Взаимно однозначные соответствия, отмеченные в (2) знаком $\Leftrightarrow$, указывают, что если $\tau \in H_f$, то корреляционная функция равняется f-й гармонике соответствующего СРКВ.

Как и в [1], соотношения (2) обобщаются на правила кодирования, использующие большее число циклотомических классов.

Согласно [7] $S(k,l)=\left[(-k, l-k), (1-k, l-k), \ldots, (d-1-k, l-k)\right]$, где (k, l) – циклотомические числа порядка d [8]. Расчет таблиц циклотомических чисел не вызывает затруднений [9]. Таким образом, соотношение (2) определяет метод численного анализа ПАКФ последовательностей, формируемых на циклотомических классах. Как отмечено в [1], [4], в этом случае разработка соответствующей программы не вызывает затруднений, а характер операций и то, что все они выполняются над целыми числами, гарантируют ее быстродействие.

С другой стороны, для $d = 2, 3, 4, 6, 8, 12$ существуют формулы для вычисления циклотомических чисел посредством разложений модуля p на суммы квадратов целых чисел. Последнее позволяет получать регулярные правила кодирования последовательностей с заданными ограничениями на их характеристики [4]. Примеры регулярных правил кодирования последовательностей с ограничениями на ПАКФ и пик-фактор для $d = 2, 3, 4, 6, 8$ представлены в [1], [4]–[7]. Рассмотрение в настоящей статье выполнено для $d = 12$.

Регулярные правила кодирования последовательностей для $d = 12$. Согласно [10] циклотомические числа двенадцатого порядка определяются разложениями

$$p = x^2 + 4y^2 = A^2 + 3B^2;\ \mathrm{ind}_\theta 2,\ \mathrm{ind}_\theta 3,$$

где $x \equiv 1 (\mathrm{mod}\, 4)$, y, $A \equiv 1 (\mathrm{mod}\, 3)$, B – целые числа; $\mathrm{ind}_\theta a$ – дискретный логарифм по основанию θ числа a по модулю p. Знаки y и B выбираются в зависимости от первообразного корня. Таблицы циклотомических чисел двенадцатого порядка и их свойства приведены в [10]. Расчет СРКВ в символьном виде существенно упрощается при применении пакета прикладных математических программ, например Mathcad.

Предварительный численный анализ ПАКФ последовательностей, сформированных на основе циклотомических классов двенадцатого порядка, позволил выделить ряд закономерностей, представленных далее.

Рассмотрим последовательность $X = \{x_j\}$ периода p, сформированную по одному из правил кодирования:

$$U_X(j) = \begin{cases} 1, & j \in H_0; \\ e^{2\pi i/3}, & j \in H_2; \\ -1, & j \in H_6; \\ e^{5\pi i/3}, & j \in H_8; \\ 0, & j \notin H_0 \cup H_2 \cup H_6 \cup H_8; \end{cases} \quad (3)$$

$$U_X(j) = \begin{cases} 1, & j \in H_0; \\ e^{\pi i/3}, & j \in H_4; \\ -1, & j \in H_6; \\ e^{4\pi i/3}, & j \in H_{10}; \\ 0, & j \notin H_0 \cup H_4 \cup H_6 \cup H_{10}. \end{cases} \quad (4)$$

Теорема 1. Если последовательность X сформирована по (3), (4) для $p = x^2 + 4y^2$ при $y \equiv \pm 1 (\mathrm{mod}\, 3)$, то она имеет двухуровневую ПАКФ

$$\lambda_X(\tau) \in \left\{(\pm y - 1)/3,\ (\mp 2y - 1)/3\right\},\ \tau = 1, \ldots, p-1 \quad (5)$$

и пик-фактор $pf \approx 3$. В (5) знак "+" используется, если $y \equiv 1 (\mathrm{mod}\, 3)$, знак "–" – если $y \equiv -1 (\mathrm{mod}\, 3)$.

Доказательство. Рассмотрим случай, когда последовательность X определена по (3). Обозначим $z = e^{2\pi i/3}$. Тогда из (3) имеем $X = Y_0 + zY_2 - Y_6 - zY_8$, где последовательности Y_k определены по (1). По (2) получим взаимно однозначное соответствие для ПАКФ последовательности X:

$$\begin{aligned} \lambda_X(\tau) \Leftrightarrow\ & S(0,\ 0) + S(2,\ 2) + S(6,\ 6) + S(8,\ 8) + \\ & + \bar{z}S(0,\ 2) + zS(2,\ 0) - S(0,\ 6) - S(6,\ 0) - \\ & - \bar{z}S(0,\ 8) - zS(8,\ 0) - zS(2,\ 6) - \bar{z}S(6,\ 2) - \\ & - S(2,\ 8) - S(8,\ 2) + \bar{z}S(6,8) + zS(8,\ 6). \end{aligned}$$

Применив свойства СРКВ, последнее соответствие можно преобразовать к следующему виду (здесь мнимая часть ПАКФ равна нулю):

$$\lambda_X(\tau) \Leftrightarrow S(0,\ 0)+S(2,\ 2)+S(6,\ 6)+ \\ +S(8,\ 8)+S(0,\ 8)+S(6,\ 2)- \\ -S(0,\ 6)-S(6,\ 0)-S(2,\ 8)- \\ -S(8,\ 2)-S(0,\ 2)-S(6,\ 8). \qquad (6)$$

Воспользовавшись явными формулами для циклотомических чисел 12-го порядка из [10], после суммирования получим, что СРКВ, соответствующий правой части соотношения (6), имеет только две различные гармоники: $(y-1)/3$, $(-2y-1)/3$ при $y \equiv 1 (\mathrm{mod}\, 3)$ и $(-y-1)/3$, $(2y-1)/3$ при $y \equiv -1 (\mathrm{mod}\, 3)$.

Если же последовательность X определена по (4), то СРКВ получается циклическим сдвигом СРКВ, стоящего в правой части формулы (6). Теорема 1 доказана.

Следствие 1.1. Если в условиях теоремы 1 $p = x^2 + 4$, то $\lambda_X(\tau) \in \{0,\ -1\}$, а если же $p = x^2 + 16$, то $\lambda_X(\tau) \in \{-1,\ 1\}$, $\tau = 1,\ \ldots,\ p-1$.

Приведем несколько значений p, удовлетворяющих условиям следствия 1.1: 13, 97, 229, 241, 457, 733, 1093, 2029, 2617, 3253, 5641, 6577, 7573, 9817, … .

Если в условиях теоремы 1 $p = x^2 + 64$, то $\lambda_X(\tau) \in \{1,\ -3\}$; при $p = x^2 + 100$ $\lambda_X(\tau) \in \{-2,\ 3\}$, $\tau = 1,\ \ldots,\ p-1$. Примеры значений p: 73, 109, 181, 829, 1153, 1621, … .

Таким образом, получены два регулярных правила построения последовательностей с хорошими периодическими автокорреляционными свойствами и $pf \approx 3$.

Замечание. В [1], [4]–[7] найдены регулярные правила кодирования последовательностей, формируемых на основе циклотомических классов четвертого – восьмого порядков, с хорошими автокорреляционными свойствами и $pf \approx 2$. Аналогичные правила существуют и для формирования последовательностей на циклотомических классах двенадцатого порядка. Например, если последовательность X при $p = x^2 + 4$ и $p \equiv 13 (\mathrm{mod}\, 24)$ сформирована по одному из следующих правил кодирования:

$$U_X(j) = \begin{cases} 1, & j \in H_0 \cup H_3; \\ e^{2\pi i/3}, & j \in H_4 \cup H_7; \\ e^{4\pi i/3}, & j \in H_8 \cup H_{11}; \\ 0, & j \notin H_0 \cup H_3 \cup H_4 \cup H_7 \cup H_8 \cup H_{11}; \end{cases}$$

$$U_X(j) = \begin{cases} 1, & j \in H_0 \cup H_9; \\ e^{2\pi i/3}, & j \in H_1 \cup H_4; \\ e^{4\pi i/3}, & j \in H_5 \cup H_8; \\ 0, & j \notin H_0 \cup H_1 \cup H_4 \cup H_5 \cup H_8 \cup H_9, \end{cases}$$

то $\max\limits_{\tau \neq 0} |\lambda_X(\tau)| = 1$, но в этом случае сетка периодов менее плотная, чем в [6]: $p = 13,\ 229,\ 733,\ 1093,\ 2029,\ 3253,\ 7573,\ \ldots$.

Пусть теперь последовательность X определена следующим образом:

$$U_X(j) = \begin{cases} 1, & j \in H_0; \\ e^{2\pi i/3}, & j \in H_4; \\ e^{4\pi i/3}, & j \in H_8; \\ 0, & j \notin H_0 \cup H_4 \cup H_8. \end{cases} \qquad (7)$$

Теорема 2. Если последовательность X сформирована по (7) для $p \equiv 13 (\mathrm{mod}\, 24)$, $\mathrm{ind}_\theta 2 \equiv 1 (\mathrm{mod}\, 6)$ и $\mathrm{ind}_\theta 3 \equiv 0 (\mathrm{mod}\, 4)$, то она имеет трехуровневую ПАКФ:

$$\lambda_X(\tau) \in \left\{ -(A+x+2)/8,\ (A+x-2)/8 \pm i\sqrt{3}B/4 \right\}, \\ \tau = 1,\ \ldots,\ p-1$$

и пик-фактор $pf \approx 4$.

Доказательство. Как и в теореме 1, получим, что в рассматриваемом случае для вещественной $(\mathrm{Re}\,\lambda_X(\tau))$ и мнимой $(\mathrm{Im}\,\lambda_X(\tau))$ частей ПАКФ справедливы следующие взаимно однозначные соответствия:

$$\mathrm{Re}\,\lambda_X(\tau) \Leftrightarrow \left(I + D^4 + D^8\right) S(0,\ 0) + \\ + 0.5\left(I + D^2 + D^4 + D^6 + D^8 + D^{10}\right) S(0,\ 4); \\ \mathrm{Im}\,\lambda_X(\tau) \Leftrightarrow \\ \Leftrightarrow -\left(\sqrt{3}/2\right)\left(I - D^2 + D^4 - D^6 + D^8 - D^{10}\right) S(0,\ 4),$$

где D – оператор циклического сдвига Хаффмана, причем $D^0 = I$ (I – тождественный оператор).

Воспользовавшись формулами для циклотомических чисел двенадцатого порядка, после вычислений получим, что

$$\mathrm{Re}\,\lambda_X(\tau) \Leftrightarrow (1/8)(-A-x-2,\ A+x-2,\ \ldots); \\ \mathrm{Im}\,\lambda_X(\tau) \Leftrightarrow -\left(\sqrt{3}/4\right)(0,\ B,\ 0,\ -B,\ \ldots).$$

Справедливость теоремы 2 вытекает из последних соответствий.

Из теоремы 2 вытекает, что последовательность X не может обладать идеальной ПАКФ.

Определим, при каких значениях периода последовательности модуль ПАКФ примет наименьшее возможное значение.

Лемма 1. Если последовательность X сформирована по (7) в условиях теоремы 2, то $\max\limits_{\tau\neq 0}|\lambda_X(\tau)|\le 1$ тогда и только тогда, когда ее период $p=(1+12u)^2+12$ при условии, что $1-12u$ – полный квадрат.

Доказательство. Согласно условию леммы 1 и теореме 2 имеем

$$\lambda_X(\tau)\in\left\{-(A+x+2)/8,\ (A+x-2)/8\pm i\sqrt{3}B/4\right\}.$$

Следовательно, если $|\lambda_X(\tau)|\le 1$, то $|B|=2$ (так как B – четное число) и

$$(A+x-2)/8=\pm 1/2. \qquad (8)$$

По условию $p\equiv 13(\mathrm{mod}\,24)$, значит, $A\equiv 1(\mathrm{mod}\,6)$. Пусть $A=1+6v$, $x=1+4t$, где v, t – целые числа. Тогда из (8) получим $3v+2t=\pm 2$. Значит, $v=2u$ (u – целое число) и $t=\pm 1-3u$.

Если $t=1-3u$, то $A=1+12u$, $x=5-12u$. Из соотношения $p=x^2+4y^2=A^2+3B^2$ после подстановки x, A, B получим $25-120u+4y^2=13+24u$ или $y^2=36u-3$. Последнее уравнение не имеет решения в целых числах, поэтому равенство $t=1-3u$ невозможно.

Если же $t=-1-3u$, то $A=1+12u$, $x=-3-12u$. Тогда $9+72u+4y^2=13+24u$ или $y^2=1-12u$, т. е. $1-12u$ – полный квадрат и $p=(1+12u)^2+12$, что и требовалось доказать.

Наоборот, если $p=(1+12u)^2+12$, то $p\equiv 13(\mathrm{mod}\,24)$; $A=1+12u$ и $|B|=2$. Далее, если $1-12u$ – полный квадрат, то $p=(3+12u)^2+4(1-12u)$, следовательно, $x=-3-12u$. Подставив x, A, B в формулы для значений ПАКФ из теоремы 2, получим, что

$$\lambda_X(\tau)\in\left\{0,\ -1/2\pm i\sqrt{3}/2\right\},\ \tau=1,\ \ldots,\ p-1.$$

Лемма 1 доказана.

Условиям леммы 1 удовлетворяют последовательности с периодами $p=13$ $(u=0)$, 541 $(u=-2)$, 2221 $(u=-4)$, ….

Теорема 3. Если последовательность X сформирована по (7) для $p\equiv 13(\mathrm{mod}\,24)$, $\mathrm{ind}_\theta 2\equiv 1(\mathrm{mod}\,6)$ и $\mathrm{ind}_\theta 3\equiv 2(\mathrm{mod}\,4)$, то она имеет трехуровневую ПАКФ:

$$\lambda_X(\tau)\in\left\{(A-x-2)/8,\ (-A+x-2)/8\pm i\sqrt{3}B/4\right\},$$
$$\tau=1,\ \ldots,\ p-1$$

и пик-фактор $pf\approx 4$.

Эта теорема доказывается аналогично теореме 2, разница заключается лишь в применении другой таблицы для циклотомических чисел из [10].

Анализ утверждения теоремы 3 позволяет, как и при доказательстве леммы 1, определить параметры правила (7), при котором модуль значений ПАКФ при ненулевых сдвигах не превосходит 1.

Лемма 2. Если последовательность X сформирована по (7) в условиях теоремы 3, то $\max\limits_{\tau\neq 0}|\lambda_X(\tau)|=1$ тогда и только тогда, когда ее период составит $p=(5+12u)^2+12$ и $1-4u$ – полный квадрат или $p=(7+36h)^2+12$ и $1+4h$ – полный квадрат. Возможны следующие значения p: 37 $(u=0)$, 61 $(h=0)$, 853 $(u=-2)$, 49 471 $(h=6)$, … .

Таким образом, найдены регулярные правила кодирования последовательностей с хорошими автокорреляционными свойствами и $pf\approx 3$ или $pf\approx 4$.

СПИСОК ЛИТЕРАТУРЫ

1. Гантмахер В. Е., Быстров Н. Е., Чеботарев Д. В. Шумоподобные сигналы. Анализ, синтез, обработка. СПб.: Наука и техника, 2005. 400 с.

2. Айерлэнд К., Роузем М. Классическое введение в современную теорию чисел. М.: Мир, 1987. 415 с.

3. Gantmakher V. E., Edemskiy V. A. The synthesis methodology of periodic discretely coded sequences formed basing on cyclotomic classes with basic parameters constraints // Proc. of 2007 Int. workshop on signal design and its applications in communications (IWSDA'07). Chengdu, China. 23–27 Sept. 2007. Piscataway: IEEE, 2007. P. 4–8.

4. Едемский В. А., Гантмахер В. Е. Синтез двоичных и троичных последовательностей с заданными

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.