УДК 621.391

СИНТЕЗ ЧЕРЕДУЮЩИХСЯ ТРОИЧНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ С ХОРОШИМИ АВТОКОРРЕЛЯЦИОННЫМИ СВОЙСТВАМИ И ВЫСОКОЙ ЭКВИВАЛЕНТНОЙ ЛИНЕЙНОЙ СЛОЖНОСТЬЮ

В. А. Едемский

Новгородский государственный университет им. Ярослава Мудрого

Статья получена 13 января 2014 г.

Аннотация. Предложен метод синтеза чередующихся троичных последовательностей, позволяющий получать последовательности с хорошими периодическими автокорреляционными свойствами и высокой эквивалентной линейной сложностью.

Ключевые слова: троичные последовательности, синтез, автокорреляция, линейная сложность.

Abstract: We propose the technique of synthesizing interleaved ternary sequences with low autocorrelation and high linear complexity.

Key words: ternary sequences, synthesis, autocorrelation, linear complexity.

Введение

Троичные периодические последовательности $X = \{x_0, \ldots, x_i, \ldots, x_{N-1}\}$, $x_i \in \{0, \pm 1\}$, где N – период последовательности, наряду с бинарными относятся к одному из наиболее востребованных видов последовательностей [1, 2]. Для многих приложений важными характеристиками троичной последовательности (ТП) являются её периодическая автокорреляционная функция (ПАКФ) $\lambda_X(m) = \sum_{i=0}^{N-1} x_i x_{i+m}$ и эквивалентная линейная сложность (ЭЛС). ЭЛС последовательности Y над конечным полем третьего порядка $GF(3)$ определяется как наименьшее натуральное число L, для которого существуют константы $c_1, \ldots, c_L$ из $GF(3)$ такие, что выполняется рекуррентное соотношение

$x_g = -c_1 x_{g-1} - c_2 x_{g-2} - \ldots - c_L x_{g-L}$ для всех $g \geq L$ [3].

Последовательности, обладающие высокой ЭЛС $\left(L > N/2\right)$, важны для криптографических приложений.

На настоящее время известны регулярные правила кодирования ТП с нечетным периодом N и идеальной ПАКФ $\left(\lambda_X(m) = 0,\ m = \overline{1,\ N-1}\right)$, максимально возможной ЭЛС, равной N [2,4,5]. В то же время ТП с периодом $4N$ и идеальной ПАКФ можно получить посредством произведения бинарной последовательности длинны 4 и ТП с периодом N [2].

В настоящей статье предлагается другой метод синтеза ТП с периодом $4N$, обладающих идеальной ПАКФ и высокой ЭЛС. Метод основан на подходе, предложенном в [6], для синтеза бинарных последовательностей с периодом $4N$ и оптимальной ПАКФ $\left(\lambda_X(m) \in \{0, -4\},\ m = \overline{1,\ 4N-1}\right)$.

2. Определение последовательностей

Пусть $X_k = \{x_{k,i}\}, k = \overline{0,3}; i = \overline{0,\ N-1}$ - последовательности с периодом N и матрица U порядка $N \times 4$ образована размещением последовательностей X_0, X_1, X_2, X_3 в её 1, 2, 3 и 4 столбцах соответственно. Тогда чередующая последовательность Y периода $4N$ получается путем последовательного объединения строк матрицы U и обозначается $Y = I(X_0, X_1, X_2, X_3)$, где I - оператор чередования. Таким образом, $Y = \{x_{0,0}, x_{1,0}, x_{2,0}, x_{3,0}, x_{0,1}, \ldots, x_{3,N-1}\}$.

Обозначим через $i \bmod 4$ наименьший положительный вычет i по модулю 4, а через $[i/4]$ - целую часть рационального числа $i/4$, тогда, согласно определению последовательности Y, получаем:

$$y_i = x_{i \bmod 4, [i/4]}, i = 0,1,\ldots,4N-1. \quad (1)$$

3. ПАКФ последовательностей

Пусть $Y = I(X_0, X_1, X_2, X_3)$ и $\lambda_k(m)$ - ПАКФ последовательности X_k,

$k = 0,1,2,3$, а $r_{k,j}(m) = \sum_{i=0}^{N-1} x_{k,i} x_{j,i+m}$ - периодическая взаимно корреляционная функция пары последовательностей X_k, X_j, здесь $k, j = 0,\ldots,3$. Тогда, из (1) следует, что для ПАКФ $\lambda_Y(m)$ последовательности Y справедливо соотношение [7]:

$$\lambda_Y(m) = \begin{cases} \sum_{i=0}^{3} \lambda_k([m/4]), & m \equiv 0 (\mathrm{mod}\, 4); \\ \sum_{i=0}^{3} r_{k,(k+m) \bmod 4}([m/4] + \delta), & m \not\equiv 0 (\mathrm{mod}\, 4), \end{cases} \quad (2)$$

где $\delta = 0$, если $(k+m) < 4$ и $\delta = 1$ при $(k+m) \geq 4$.

Обозначим через A оператор циклического сдвига последовательности на единицу влево.

Лемма 1. Если X, Z - ТП, то:

1. $\lambda_{A^k X}(m) = \lambda_X(m)$ для любых целых значений m и k;

2. $r_{X,A^k Z}(m) = r_{X,Z}(m+k)$.

Доказательство. Первое утверждение леммы 1 хорошо известно (впрочем, оно является частным случаем второго). Во втором же случае согласно определениям периодической взаимно корреляционной функции и оператора A получаем

$$r_{X,A^k Z}(m) = \sum_{i=0}^{N-1} x_i z_{i+k+m} = r_{X,Z}(m+k).$$

Лемма 1 доказана

Теорема 1. Пусть N - нечетное число и $a = (N+1)/2$. Если ТП $X_i, i = 0,\ldots,3$ имеют одинаковое число ненулевых элементов и

$$Y = I(X_0, X_1, A^a X_0, -A^a X_1), \quad (3)$$

то

$$\max_{m \neq 0} |\lambda_Y(m)| = 2 \max_{f \neq 0} |\lambda_0(f) \pm \lambda_1(f)|.$$

Доказательство. Рассмотрим несколько случаев.

1. Пусть $m \equiv 0(\mathrm{mod}\,4)$. Тогда, по лемме 1 и (2), получаем $\lambda_Y(m) = 2\left(\lambda_0(f) + \lambda_1(f)\right)$, где $f = [m/4]$.

2. Пусть $m \equiv 1(\mathrm{mod}\,4)$. В этом случае по лемме 1 имеем

$$\lambda_Y(m) = r_{0,1}(f) + r_{1,0}(f+a) - r_{0,1}(f) - r_{1,0}(f-a+1).$$

Так как $f + a \equiv f - a + 1(\mathrm{mod}\,N)$, то $r_{1,0}(f+a) = r_{1,0}(f-a+1)$ и $\lambda_Y(m) = 0$.

3. Пусть $m \equiv 2(\mathrm{mod}\,4)$. Здесь

$$\lambda_Y(m) = \lambda_0(f+a) - \lambda_1(f+a) + \lambda_0(f-a+1) - \lambda_1(f-a+1)$$

или

$$\lambda_Y(m) = 2\left(\lambda_0(f+a) - \lambda_1(f+a)\right).$$

При этом если $f \equiv -a(\mathrm{mod}\,N)$, то $\lambda_Y(m) = 0$, так как по условию $\lambda_0(0) = \lambda_1(0)$.

4. Если $m \equiv 3(\mathrm{mod}\,4)$, то, как и в первом подпункте, получаем, что $\lambda_Y(m) = 0$.

Теорема 1 доказана.

Следствие 1.1. Если ТП X_0 и X_1 имеют идеальную ПАКФ, то последовательность Y также имеет идеальную ПАКФ.

Следствие 1.2. Если ТП X имеет идеальную ПАКФ, то для любого целого k последовательность $Y = I(X_0, A^k X_0, A^a X_0, -A^{a+k} X_0)$ также имеет идеальную ПАКФ.

Таким образом, правило кодирования (3) позволяет синтезировать семейства ТП с идеальными, а также квазиидельными периодическими автокорреляционными свойствами.

Пример 1. Пусть $X_0 = \{0,0,1,-1,1,0,-1,-1,1,1,1,0,1\}$ и $X_1 = \{0,1,0,1,1,0,\ 0,-1,-1,\ \ 1,1,\ \ -1,1\}$ - ТП с идеальной ПАКФ. Первая построенна на основе разностного множества Зингера [1, 2], а вторая с помощью множества биквадратичных вычетов и нуля [1].

Тогда

$$Y = I(X_0, X_1, A^7 X_0, -A^7 X_1) = \{0,0,-1,1,0,1,1,1,1,0,1,-1,-1,1,1,-1,1,1,0,1,0,0,$$

$1,-1,-1,0,0,\ 0,-1,-1,0,-1,1,-1,1,0,1,1,-1,-1,1,1,1,-1,0,-1,0,0,1,1,-1,0\}$

имеет идеальную ПАКФ, что несложно проверить непосредственным вычислением. Варьируя последовательности X_0 и X_1 получаем другие ТП с идеальной ПАКФ.

4. Эквивалентная линейная сложность последовательностей

Если $Y = \{y_i\}$ - последовательность с периодом $4N$, то её ЭЛС (L) можно вычислить по следующей формуле [3]:

$$L = 4N - \deg \text{НОД}(x^{4N} - 1, s(x)), \qquad (4)$$

где $s(x) = y_0 + y_1 x + ... + y_{4N-1} x^{4N-1}$- производящая функция цикла последовательности.

Пусть $s_i(x)$, в свою очередь, соответствует последовательности X_i, $i = 0,1,2,3$ с периодом N.

Следующие утверждения доказаны в [8] для бинарых последовательностей, для ТП доказательства аналогичны.

Лемма 2.

1. Если $Y = I(X_0, X_1, X_2, X_3)$, то $s(x) = s_0(x^4) + x s_1(x^4) + x^2 s_2(x^4) + x^3 s_3(x^4)$.

2. Если $X_2 = A^k X_0$, где k - целое число, то $s_2(x) = x^{N-k} s_0(x)$.

Лемма 3. Если $Y = I(X_0, X_1, A^a X_0, -A^a X_1)$, где, как и ранее, $a = (N+1)/2$ для нечетного значения N, то

$$s(x) = s_0(x^4)(1 + x^{2N}) + x s_1(x^4)(1 - x^{2N}).$$

Доказательство. По условию $X_2 = A^a X_0$ и $X_3 = -A^a X_1$, тогда, в силу второго утверждения леммы 2, $s_2(x^4) = x^{4(N-a)} s_0(x^4) = x^{2N-2} s_0(x^4)$ и $s_3(x^4) = x^{2N-2} s_1(x^4)$. Подставляя выражения для $s_2(x^4), s_3(x^4)$ в формулу для вычисления $s(x)$ из первого пункта леммы 2, завершаем доказательство леммы 3.

Теорема 2. Пусть, соответственно, L_0, L_1 - ЭЛС ТП X_0, X_1 над полем третьего порядка, а L - последовательности Y и $N \not\equiv 0 (\mathrm{mod}\, 3)$. Тогда, если $Y = I(X_0, X_1, A^a X_0, -A^a X_1)$, то $L = 2(L_0 + L_1)$.

Доказательство. Пусть K - расширение поля $GF(3)$, являющееся полем разложения многочлена $x^{4N} - 1$ (оно всегда существует [3]). Обозначим через $\alpha_1, ..., \alpha_{4N}$ различные корни многочлена $x^{4N} - 1$ в поле K. Тогда $x^{4N} - 1 = \prod_{j=1}^{4N}(x - \alpha_j)$ и $\text{НОД}(x^{4p} - 1, s(x)) = \prod_{j: s(\alpha_j)=0}(x - \alpha_j)$. Следовательно, по (4) имеем

$$L = 4N - \left|\{ j \,|\, s(\alpha_j) = 0, j = \overline{1, 4N}\}\right| \tag{5}$$

Согласно лемме 3 $s(\alpha_j) = s_0(\alpha_j^4)(1 + \alpha_j^{2N}) + \alpha_j s_1(\alpha_j^4)(1 - \alpha_j^{2N})$ или

$$s(\alpha_j) = \begin{cases} 2s_0(\alpha_j^4), & \alpha_j^{2N} = 1; \\ 2\alpha_j s_1(\alpha_j^4), & \alpha_j^{2N} = -1. \end{cases} \tag{6}$$

Формула (5) приведена для ТП Y, подобные же соотношения имеют место и для ТП X_0, X_1. Поэтому, в силу условия теоремы 2, имеем

$$L_0 = N - \left|\{\beta \,|\, s_0(\beta) = 0, \beta^N = 1, \beta \in K\}\right| \text{ и } L_1 = N - \left|\{\beta \,|\, s_1(\beta) = 0, \beta^N = 1, \beta \in K\}\right|.$$

А так как

$$\left|\{ j \,|\, s_0(\alpha_j^4) = 0, \alpha_j^{2N} = 1\}\right| = 2\left|\{\beta \,|\, s_0(\beta) = 0, \beta \in K\}\right|;$$

$$\left|\{ j \,|\, s_1(\alpha_j^4) = 0, \alpha_j^{2N} = -1\}\right| = 2\left|\{\beta \,|\, s_1(\beta) = 0, \beta \in K\}\right|,$$

то, из (6) получаем: $\left|\{ j \,|\, s(\alpha_j) = 0, j = \overline{1, 4N}\}\right| = 2(N - L_0) + 2(N - L_1)$. Применение (5) завершает доказательство теоремы 2.

Следствие 2.1. Если $Y = I(X_0, A^k X_0, A^a X_0, -A^{a+k} X_0)$, то $L = 4L_0$.

Таким образом, если ТП X_0, X_1 имеют высокую ЭЛС, то и ТП Y, определяемая (3), также имеет высокую ЭЛС. Формулу (6) можно применять для поиска минимального многочлена $m(x) = (x^{4N} - 1)/\text{НОД}(x^{4N} - 1, s(x))$ ТП Y

[6]. Заметим, что для последовательностей, расмотренных в примере 1, $L_0 = 3, L_1 = 6, L = 18$, здесь ТП Y не обладает высокой ЭЛС.

Вывод

Предложен новый метод синтеза чередующихся троичных последовательностей с идеальными (квазиидеальными) автокорреляционными свойствами, высокой эквивалентной линейной сложностью и периодом $4N$.

Литература

1. Винокуров В.И., Гантмахер В.Е. Дискретно-кодированные последовательности. Ростов-на-Дону: Ростовский ун-т, 1990. 283 с.

2. Ипатов, В.П. Периодические дискретные сигналы с оптимальными корреляционными свойствами. М.: Радио и связь, 1992. 152 с.

3. Лидл Р., Нидеррайтер Г. Конечные поля. М.: Мир, 1988. 820 с.

4. Ипатов В.П. Троичные последовательности с идеальными периодическими автокорреляционными свойствами // Радиотехника и электроника. 1979. № 10. С. 2053–2057.

5. Ипатов В. П., Камалетдинов Б.Ж. Эквивалентная линейная сложность троичных последовательностей с идеальными автокорреляционными свойствами // Радиотехника и электроника. 1989. Т. 34, № 11. С. 2451–2454.

6. Tang X. H., Ding C. New classes of balanced quaternary and almost balanced binary sequences with optimal autocorrelation value // IEEE Trans. Inf. Theory. 2010. V. 56, № 12, pp. 6398–6405.

7. Едемский В. А., Гантмахер В. Е. Синтез двоичных и троичных последовательностей с заданными ограничениями на их характеристики. Великий Новгород.: НовГУ, 2009. 189 с.

8. Wang Q., Du X. N. The linear complexity of binary sequences with optimal autocorrelation // IEEE Trans. Inf. Theory. 2010. V. 56, № 12, pp. 6388–6397.