УДК 519.7

ЛИНЕЙНАЯ СЛОЖНОСТЬ ОБОБЩЁННЫХ ЦИКЛОТОМИЧЕСКИХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ С ПЕРИОДОМ $2^m p^n$

В. А. Едемский, О. В. Антонова

Пусть $X = \{x_i\}, x_i \in \{0,1\}$ — последовательность с периодом $N = 2^m p^n$, где p — нечётное простое число, а m, n — натуральные числа. Её минимальный многочлен $m(t)$ и линейную сложность L над полем GF(2) можно определить по следующим формулам:

$$m(t) = (t^N - 1)/\left((t^{p^n} - 1)^{2^m}, S(t)\right), \qquad L = N - \deg\left((t^{p^n} - 1)^{2^m}, S(t)\right),$$

где $S(t)$ — производящая функция цикла последовательности. Следовательно, если α — примитивный корень степени p^n из единицы в расширении поля GF(2), то для вычисления минимального многочлена и линейной сложности последовательности X достаточно найти корни многочлена $S(t)$ в множестве $\{\alpha^v : v = 0, 1, \ldots, p^n - 1\}$ и определить их кратность. Метод вычисления значений $S(\alpha^v)$ для обобщённых циклотомических последовательностей с периодом p^n предложен в [1, 2], здесь обобщим его на последовательности с периодом $2^m p^n$.

Пусть $H_k = \{\theta^{k+td} \pmod{p^n} : t = 1, \ldots, p^{n-1}(p-1)/d\}$, $k = 0, 1, \ldots, d-1$ — циклотомические классы порядка d по модулю p^n, где θ — первообразный корень по модулю p^n, а d — делитель $p-1$, $d \geqslant 2$. Справедливо разбиение

$$\mathbb{Z}_{p^n} = \bigcup_{j=0}^{n-1} \bigcup_{k=0}^{d-1} p^j H_k \cup \{0\}.$$

Кольцо классов вычетов $\mathbb{Z}_N$ изоморфно прямому произведению $\mathbb{Z}_{2^m} \otimes \mathbb{Z}_{p^n}$ относительно изоморфизма $\varphi(a) = (a \bmod 2^m, a \bmod\ p^n)$. Пусть $H_{l,k} = \varphi^{-1}\left(\{l\} \otimes \bigcup\limits_{j=0}^{n-1} p^j H_k\right)$ для $l = 0, 1, \ldots, 2^m - 1; k = 0, 1, \ldots, d-1$, тогда $H_{l,k}$ и множество $\{0, p^n, \ldots, (2^m - 1)p^n\}$ образуют разбиение $\mathbb{Z}_N$.

Рассмотрим последовательность X, определяемую следующим образом:

$$x_i = \begin{cases} 1, & \text{если } i \bmod N \in C, \\ 0 & \text{иначе.} \end{cases} \tag{1}$$

Здесь $C = \bigcup\limits_{l=0}^{2^m-1} \bigcup\limits_{k \in I_l} H_{l,k} \cup \{0, 2p^n, \ldots, 2^{m-1}p^n\}$; I_l, $l = 0, 1, \ldots, 2^m - 1$ — подмножества индексов, элементы которых могут принимать значения от 0 до $d-1$.

Пусть $\mathbf{S}_d(x) = \left(S_d(x), S_d(x^\theta), \ldots, S_d(x^{\theta^{d-1}})\right)$, $\mathbf{R}(x) = \sum\limits_{k \in I} \mathbf{S}_d(x^{\theta^k})$ и $\mathbf{Q}(x) = \sum\limits_{k \in J} \mathbf{S}_d(x^{\theta^k})$, где $S_d(t) = \sum\limits_{u \in H_0} t^{u \bmod p}$, а I, J — множества, состоящие из номеров k, входящих нечётное число раз в подмножества I_l, $l = 0, 1, \ldots, 2^m - 1$, с чётными и нечётными номерами соответственно. Обозначим координаты вектор-функций $\mathbf{R}(x)$ и $\mathbf{Q}(x)$ при $x = \alpha^{p^{n-1}}$ через r_i, q_i для $i = 0, 1, \ldots, d-1$. Пусть $\delta = 1$ для $m = 1$ и $\delta = 0$ при $m > 1$.

Теорема 1. Если $v \in p^f H_j$, $f = 0, 1, \ldots, n-1$, $j = 0, 1, \ldots, d-1$, то α^v — корень многочлена $S(t)$ тогда и только тогда, когда $r_j + q_j = (|I| + |J|)f(p-1)/d + \delta$, и корень α^v многочлена $S(t)$ кратный тогда и только тогда, когда $r_j = |I|f(p-1)/d + \delta$.

Теорема 1 показывает, что известные значения $\mathbf{R}(x), \mathbf{Q}(x)$, а фактически $\mathbf{S}_d(x)$, позволяют оценить линейную сложность последовательности X. Метод вычисления значений $\mathbf{S}_d(x)$ предложен в [1], следовательно, теорема 1 определяет метод анализа линейной сложности последовательностей с периодом $2^m p^n$, сформированных по правилу (1).

Воспользовавшись теоремой 1, несложно получить следующие утверждения.

Лемма 1. Если $d = 2$ и $I_0 = I_1 = \{0\}$, то для последовательности X, сформированной по правилу (1) при $N = 2p^n$, линейная сложность $L = 2p^n$, а её минимальный многочлен $m(t) = t^{2p^n} - 1$.

Лемма 2. Если $d = 4$ и $I_0 = \{0, 1\}$, то для линейной сложности последовательности X, сформированной по правилу (1) при $N = 2p^n$, справедливо:

1) $L = 2p^n$, если $I_1 = \{0, 1\}$, или $I_1 = \{0, 2\}$ и $\left(\dfrac{2}{p}\right)_4 \neq 1$, или $I_1 = \{0, 3\}$ и $\left(\dfrac{2}{p}\right) \neq 1$, где $\left(\dfrac{2}{p}\right)$ — символ Лежандра, а $\left(\dfrac{2}{p}\right)_4$ — символ 4-степенного вычета;

2) $L = (3p^n + 1)/2$, если $I_1 = \{0, 3\}$ и $\left(\dfrac{2}{p}\right) = 1$, $\left(\dfrac{2}{p}\right)_4 \neq 1$;

3) $L = (5p^n + 1)/4$, если $\left(\dfrac{2}{p}\right)_4 = 1$ и $I_1 = \{0, 2\}$ или $I_1 = \{0, 3\}$.

Аналогично можно получить следующие оценки линейной сложности последовательностей.

Лемма 3. Если $d = 2$ и последовательность X с периодом $4p^n$ определена правилом (1) при $I_0 = I_1 = I_2 = \{0\}, I_3 = \{1\}$, то $L \geqslant 4p^n - 4$.

Лемма 4. Если $d = 4$ и последовательность X с периодом $8p^n$ определена правилом (1) при $I_0 = I_1 = I_2 = I_5 = \{0\}$, $I_3 = \{1\}$, $I_4 = I_6 = \{2\}$ и $I_7 = \{3\}$, то $L \geqslant 8p^n - 8$, если $\left(\dfrac{2}{p}\right) \neq 1$, и $L \geqslant 4p^n - 8$, если $\left(\dfrac{2}{p}\right) = 1$.

Таким образом, предложен метод анализа линейной сложности последовательностей с периодом $2^m p^n$, построенных на основе обобщённых циклотомических классов. Метод позволяет как явно рассчитать линейную сложность и минимальный многочлен рассматриваемых последовательностей, так и оценить её, а также определить характеристики последовательностей, обладающих заведомо высокой линейной сложностью.

Подробное изложение представленных результатов можно найти в [3].

ЛИТЕРАТУРА

1. *Едемский В. А.* О линейной сложности двоичных последовательностей на основе классов биквадратичных и шестеричных вычетов // Дискретная математика. 2010. Т. 22. №1. С. 74–82.
2. *Edemskiy V. A.* About computation of the linear complexity of generalized cyclotomic sequences with period p^{n+1} // Designs, Codes and Cryptography. 2011. V. 61. No. 3. P. 251–260.
3. *Едемский В. А., Антонова О. В.* Линейная сложность обобщённых циклотомических последовательностей с периодом $2^m p^n$ // Прикладная дискретная математика. 2012. №3 (в печати).