О Б О З Р Е Н И Е
П Р И К Л А Д Н О Й И П Р О М Ы Ш Л Е Н Н О Й
Том 20 М А Т Е М А Т И К И Выпуск 4
2013

В. А. Е д е м с к и й (Великий Новгород, НовГУ). **Анализ линейной сложности чередующихся последовательностей Лежандра и Холла.**

Исследуется линейная сложность чередующихся бинарных последовательностей, обладающих оптимальной периодической автокорреляционной функцией (ПАКФ). Рассматриваемые последовательности формируются на основе последовательностей Холла или Лежандра и Холла.

Пусть $a=\{a_j\}$, $b=\{b_j\}$ $(j=0,1,\dots,N-1)$ — бинарные последовательности с периодом N, $N\equiv 3\,(\mathrm{mod}4)$ и

$$u=I(a,b,L^{1/2}a,L^{1/2}b+1), \tag{1}$$

где I — оператор чередования, L — оператор циклического сдвига последовательности на единицу влево. В [1] показано, что если последовательности a и b обладают оптимальной ПАКФ, то и чередующаяся последовательность u, сформированная по (1), также имеет оптимальную ПАКФ.

Другой важной характеристикой последовательности является ее линейная сложность. Последовательности, обладающие хорошими автокорреляционными свойствами и высокой линейной сложностью, важны для криптографических приложений. В частном случае, когда a — последовательность Лежандра, простых чисел-близнецов или m-последовательность и $b=L^{1/4+\eta}a+1$, η — натуральное число, минимальный многочлен последовательности u и ее линейная сложность были найдены в [2]. Случай последовательностей Холла, а также, когда a, b — последовательности различных типов, остался не исследованным.

Если $u=\{u_i\}$ — последовательность с периодом $4N$, то ее минимальный полином $m(t)$ и линейную сложность (LC) можно вычислить по следующим формулам:

$$m(x)=\big(x^{4N}-1\big)/\mathrm{НОД}\big(x^{4N}-1,s(x)\big),\quad LC=N-rmdeg\,\mathrm{НОД}\big(x^{4N}-1,s(x)\big), \tag{2}$$

где $s(x)=u_0+u_1x+\dots+u_{4N-1}x^{4N-1}$.

Для последовательности u, сформированной по (1), имеем

$$\mathrm{НОД}\big(x^{4N}-1,s(x)\big)=\frac{x^{2N}-1}{x^2-1}\mathrm{НОД}\left(\frac{x^{2N}-1}{x^2-1},s_a(x^4)+xs_b(x^4)\right). \tag{3}$$

Здесь $s_a(x)=a_0+a_1x+\dots+a_{N-1}x^{N-1}$.

Следовательно, согласно (2) и (3), если α — примитивный корень степени N из единицы в расширении поля GF(2), то для вычисления минимального многочлена и линейной сложности последовательности u, сформированной по (1), достаточно определить число корней многочлена $s_a(x^4)+xs_b(x^4)$ в множестве $\{\alpha^l,\ l=0,1,\dots,N-1\}$ и найти их кратность. В случае, когда a — последовательность Лежандра или Холла, значения $s_a(\alpha^l)$, $l=0,1,\dots,N-1$, вычислены в [3].

Таким образом определяем параметры чередующихся бинарных последовательностей, сформированных по (1) из последовательностей Холла или Холла и Лежандра, обладающих оптимальной ПАКФ и высокой линейной сложностью, рассчитываем их минимальный многочлен.

СПИСОК ЛИТЕРАТУРЫ

1. *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, p. 6398-6405.
2. *Li N.*, *Tang X. H.* On the linear complexity of binary sequences of period $4N$ with optimal autocorrelation value/magnitude. — IEEE Trans. Inf. Theory, 2011, v. 57, № 11, p. 7597-7604.
3. *Едемский В. А.*, *Гантмахер В. Е.* Синтез двоичных и троичных последовательностей с заданными ограничениями на их характеристики. Великий Новгород: НовГУ, 2009, 189 с.