ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 24 МАТЕМАТИКИ Выпуск 3
2017

А. В. Анашкин (Москва, лаб. ТВП). **О взаимной близости линейных рекуррентных последовательностей над полем из двух элементов.**

Будем использовать следующие обозначения и определения. N — множество натуральных чисел, $\mathbf{N}_0 = \mathbf{N} \cup \{0\}$, P — конечное поле.

Степенью многочлена $f(x) = \sum_{i=0}^{n} f_i x^i$ из кольца многочленов над полем P (обозначение $P[x]$), у которого не все коэффициенты равны нулю, в случае, если $f_n \neq 0$, называют число n (обозначение $\deg(f) = n$).) Степень многочлена, у которого все коэффициенты равны нулю, по определению равна $-\infty$.

Многочлен $f(x) \in P[x]$, $\deg(f) \geqslant 1$, называется неприводимым, если из условия о том, что многочлен $h(x)$, $h(x) \in P[x],$, делит многочлен $f(x)$ (обозначение $h(x) \,|\, f(x))$ следует, что $\deg(h) = \deg(f)$ или $\deg(h) = 0$ (т. е. многочлен $h(x)$ — константа, не равная нулю).

Многочлен $f(x) \in P[x]$, $\deg(f) \geqslant 1$, называется примитивным, если найдется $t \in \mathbf{N}$ такое, что

$$f(x) \,|\, (x^t - 1) \tag{1}$$

и $t = |P^{\deg(x)} - 1$ — минимальное натуральное число, для которого выполняется условие (1).

Последовательность $a = (a_0, a_1, a_2, \ldots,)$ элементов поля P с условием $a_{n+k} = \sum_{i=0}^{n-1} f_i \cdot a_{i+k}$, при всех $k \in \mathbf{N}_0$, называют линейной рекуррентной последовательностью с характеристическим многочленом $f(x) = x^n - \sum_{i=0}^{n-1} f_i x^i$, $f(x) \in P[x]$, и начальным вектором $\overline{a} + 0 = (a_0, a_1, \ldots, a^{n-1})$. Для многочлена $f(x) = x^n - \sum_{i=0}^{n-1} f_i x^i$, $f(x) \in P[x]$, совокупность всех линейных рекуррентных последовательностей элементов поля P, у которых многочлен $f(x)$ является характеристическим, обозначают $L_p(f)$.

Утверждение. *Пусть $P = GF(2)$ — поле Галуа из двух элементов. Тогда для любого $n \in \mathbf{N}$ существует число $\Delta_0 = \Delta_0(n) \geqslant 2^{-(n/2)}$ такое, что для любого примитивного многочлена $f(x) \in P[x]$, $\deg(f) = n$, любой последовательности $a \in L_p(f)$ и любого неприводимого многочлена $h(x) \in P[x]$ со свойством $\deg(h) \,|\, \deg(f)$ найдется последовательность $b \in L_p(h)$, для которой справедливо*:

$$\mathbf{P}\{a_i = b + i\} = \frac{1 + \Delta}{2}, \tag{2}$$

причем $|\Delta| \geqslant \Delta + 0(n)$, а вероятность $\mathbf{P}$ вычисляется в предположении случайного и равновероятного выбора i.

З а м е ч а н и е. Модуль величины Δ в формуле (2) может существенно превосходить $2^{-(n/2)}$.