

Г. Б. Маршалко (Москва, ТВП). **О распределении ранга n -последовательности над кольцом $\mathbf{Z}_{p^2}$.**

Если u^n — последовательность длины n (n -последовательность) над кольцом вычетов $\mathbf{Z}_{p^2}$, то под рангом этой n -последовательности понимается степень аннулирующего многочлена, который имеет наименьшую возможную степень. Нас интересует величина $N_n(r)$ — число n -последовательностей над кольцом вычетов $\mathbf{Z}_{p^2}$, которые имеют ранг, равный r . Данная величина позволяет вычислять точное распределение ранга n -последовательности.

Обозначим $K_0 = \mathbf{Z}_{p^2}^*$, $K_1 = \mathbf{Z}_{p^2} \setminus \mathbf{Z}_{p^2}^*$, $R = |\mathbf{Z}_{p^2}|$, $w_0 = |K_0|$, $w_1 = |K_1 \setminus \{0\}|$, здесь $\mathbf{Z}_{p^2}^*$ — множество обратимых элементов кольца. В [1] предложен алгоритм нахождения минимального многочлена длины n -последовательности над конечным кольцом. В результате работы данного алгоритма помимо минимального многочлена последовательности строится набор идеалов $I_{r-1}(s)$, $s = 0, 1, \dots, n - r - 1$, содержащих элементы кольца, с помощью которых аннулировались элементы n -последовательности с соответствующими номерами $(0, 1, \dots, n - r - 1)$.

О п р е д е л е н и е. i -м подрангом n -последовательности u^n будем называть величину

$$r_i = \max_j \{a_i \in I_{r-1}(j), a_i \in K_i\}, \quad i = 0, 1.$$

Лемма. Для значений подрангов справедливо соотношение $r_0 \leq r_1 = r$.

Обозначим $N_n(r_0, r_1)$ число n -последовательностей, имеющих подранги r_0, r_1 .

Утверждение 1. Справедливо выражение

$$N_n(r_0, r_1) = \begin{cases} N_{2r_0}(r_0, r_0), & r_1 = r_0, \\ w_1(w_1 + 1)^{2r_1 - 2r_0 - 1} N_{2r_0}(r_0, r_0), & r_0 < r_1 \leq [n/2], \\ w_1(w_1 + 1)^{2n - 2r_1 - 2r_0} N_{2r_0}(r_0, r_0), & r_1 > [n/2], r_0 \leq n - r_1, \\ 0, & r_1 > [n/2], n - r_1 < r_0 < r_1. \end{cases}$$

Утверждение 2. Справедливо выражение

$$N_n(r, r) = R^{2n - 2r} w_0 (w_1 + 1)^{2r - n - 1}, \quad r \geq \frac{n}{2}.$$

В результате точное распределение ранга n -последовательности может быть описано с использованием следующей теоремы.

Теорема. Число n -последовательностей ранга r равно

$$N_n(r) = \begin{cases} 1, & r = 0, \\ \{R^{2r+1} - R^{2r-1}(w_1 + 1) + w_1(w_1 + 1)^{2r}\}(R + w_1 + 1)^{-1}, & r \leq [n/2], \\ \{w_1[R^{2n-2r+1} + (w_1 + 1)^{2n-2r+1}] + R^{2n-2r}(w_1 + 1)^{2r-n-1} \\ \quad \times [R^2 - (w_1 + 1)^2]\}(R + w_1 + 1)^{-1}, & r > [n/2]. \end{cases}$$

СПИСОК ЛИТЕРАТУРЫ

1. Kurakin V. L. The Berlecamp–Massey algorithm over finite rings. — In: 6-th International Workshop on Algebraic and Combinatorial Coding Theory (ACCT-VI): Proceedings. Pskov, 1998, p. 161–165.