



# ЛИНЕЙНАЯ РЕКУРРЕНТНАЯ ПОСЛЕДОВАТЕЛЬНОСТЬ

Авторы: А. А. Нечаев

**ЛИНЕЙНАЯ РЕКУРРЕНТНАЯ ПОСЛЕДОВАТЕЛЬНОСТЬ** порядка  $m \geq 1$  над коммутативным кольцом  $R$  с единицей  $e$ , последовательность  $u = (u(0), u(1), \dots)$  элементов кольца  $R$  такая, что  $u(i+m) = c_{m-1}u(i+m-1) + \dots + c_1u(i+1) + c_0u(i)$ ,  $i = 0, 1, 2, \dots$ ,  $\text{tag}1$

для некоторых фиксированных  $c_0, \dots, c_{m-1} \in R$ . Соотношение (1) называется законом рекурсии, многочлен  $F(x) = x^m - c_{m-1}x^{m-1} - \dots - c_0 \in R[x]$  – характеристич. многочленом, вектор  $(u(0), u(1), \dots, u(m-1))$  – начальным вектором Л. р. п. и. Одна и та же Л. р. п. и с данным начальным вектором может задаваться разл. соотношениями вида (1). Характеристич. многочлен Л. р. п. и наименьшей степени (определяемый, вообще говоря, неоднозначно) называется её минимальным многочленом, а его степень – рангом или линейной сложностью Л. р. п. и.

Широкое применение Л. р. п. в разл. разделах дискретной математики и её приложений обусловлено в значит. степени тем, что Л. р. п. (1) может быть получена как выходная последовательность простого автомата, называемого линейным регистром сдвига.

Примерами Л. р. п. являются следующие последовательности.

Геометрич. прогрессия  $u(i) = cq^i$ ,  $i = 0, 1, 2, \dots$ , где  $c, q \in R \setminus \{0\}$ , – Л. р. п. ранга 1 с минимальным многочленом  $f(x) = x - q$ .

Арифметич. прогрессия  $u(i) = ai + b$ ,  $i = 0, 1, 2, \dots$ , где  $a \in R \setminus \{0\}$ ,  $b \in R$ , – Л. р. п. ранга 2 с минимальным многочленом  $(x - e)^2$ .

Конгруэнтная последовательность  $u(i+1) = qu(i) + a$ ,  $i = 0, 1, 2, \dots$ , где  $q, a, u(0) \in R \setminus \{0\}$ , – Л. р. п. ранга 2 с минимальным многочленом  $(x - q)(x - e)$ . Такие последовательности используются для генерирования псевдослучайных чисел в ЭВМ.

Последовательность Фибоначчи  $f(i+2) = f(i+1) + f(i)$ ,  $i = 0, 1, 2, \dots$ ,  $f(0) = 0$ ,  $f(1) = 1$ , – Л. р. п. над кольцом целых чисел с минимальным многочленом  $x^2 - x - 1$ . Эта последовательность рассматривалась [Леонардо](#) Пизанским (Фибоначчи).

Периодические последовательности. Последовательность  $u$  над кольцом  $R$  называется периодической, если существуют параметры  $d \in \mathbb{N}_0 = \mathbb{N} \cup \{0\}$ ,  $t \in \mathbb{N}$  такие, что  $u(i+t) = u(i)$  для всех  $i \geq d$ . Такая последовательность есть Л. р. п. с характеристич. многочленом  $F(x) = x^d(x^t - e)$ . Если  $R$  – конечное кольцо, то любая Л. р. п. над  $R$  является периодич. последовательностью. На множестве  $R^{\langle \text{tag}1 \rangle}$  всех последовательностей над  $R$  естественным образом задаются операции сложения и

умножения на константы из  $R$ . Операция умножения последовательности  $u \in R^{\mathbb{N}}$  на многочлен  $H(x) = \sum_{s \geq 0} h_s x^s \in R[[x]]$  по правилу  $(xu) = \sum_{i \geq 0} u(i+1)x^i$ , где  $u(i) = \sum_{s \geq 0} h_s u(i+s)$ ,  $\sum_{s \geq 0} h_s = 0$ , позволяет сформулировать условие (1) в виде равенства  $F(x)u = 0$ . Условие периодичности последовательности  $u$  означает существование параметров  $d \in \mathbb{N}_{>0}$ ,  $t \in \mathbb{N}$  таких, что  $x^d(x^t - e)u = 0$ .  $\square$

Для периодич. последовательности  $u$  существуют параметры  $D(u) \in \mathbb{N}_{>0}$ ,  $T(u) \in \mathbb{N}$  (называемые соответственно дефектом и периодом  $u$ ) такие, что для любых  $d \in \mathbb{N}_{>0}$ ,  $t \in \mathbb{N}$  условие (2) равносильно паре условий:  $d \geq D(u)$ ,  $T(u)$  делит  $t$ .

Осн. проблемами теории Л. р. п. считаются: задача вычисления общего члена  $u(i)$  Л. р. п.  $u$  без рекуррентного вычисления предыдущих знаков; задача оценки ранга Л. р. п., заданной к.-л. способом; оценка периода Л. р. п. над конечным кольцом; оценка частот появления элементов кольца на заданном отрезке Л. р. п.; задача восстановления начального вектора Л. р. п. и закона рекурсии по частичной информации о Л. р. п.; изучение построенных из отрезков Л. р. п. кодов, исправляющих ошибки.

Множество всех Л. р. п. над  $R$  с характеристич. многочленом  $F(x)$  обозначается  $L_R(F)$ . Формула для вычисления знака  $u(i)$  Л. р. п.  $u \in L_R(F)$  без рекуррентного вычисления предыдущих знаков строится с помощью т. н. биномиального представления Л. р. п.  $u$ . Если многочлен  $F(x)$  раскладывается на линейные множители над кольцом  $R$ , т. е. , причём разности  $\alpha_i - \alpha_j$  – обратимые элементы в  $R$ , то  $L_R(F)$  есть множество всех последовательностей вида  $u(i) = \sum_{s=1}^t (c_{s0} \alpha_{s1}^i + c_{s1} \alpha_{s1}^{i-1} + \dots + c_{sk_s} \alpha_{s1}^{i-k_s}) \alpha_{s1}^{\alpha_i - \alpha_{s1}}$ , где  $c_{sj} \in R$ ,  $\alpha_{s1}$  – биномиальные коэффициенты. Напр., общий член последовательности Фибоначчи над полем рациональных чисел имеет вид  $f(i) = (\alpha_1^i - \alpha_2^i) / \sqrt{5}$ , где  $\alpha_1 = (\sqrt{5} + 1)/2$ ,  $\alpha_2 = (\sqrt{5} - 1)/2$ .

В связи с приложениями в теории кодов и криптографии наиболее полно разработана теория Л. р. п. над конечными полями. Для Л. р. п.  $u$  над полем  $P$  существует единственный минимальный многочлен  $M_u(x)$ . Пусть  $P = GF(q)$  – поле из  $q$  элементов. Период  $T(u)$  и дефект  $D(u)$  Л. р. п.  $u$  равны соответственно наименьшим  $t \in \mathbb{N}$  и  $d \in \mathbb{N}_{>0}$  таким, что  $M_u(x)$  делит  $x^d(x^t - e)$ .

Если  $u$  – Л. р. п. ранга  $m$  над  $P = GF(q)$ , то  $T(u) \leq q^m - 1$ . В случае если  $T(u) = q^m - 1$ , Л. р. п.  $u$  называют Л. р. п. максимального периода  $t = q^m - 1$  ранга  $m$  над полем  $P$ . На отрезке  $(u(0), u(1), \dots, u(t-1))$  каждый ненулевой элемент поля  $P$  встречается  $q^{m-1}$  раз, а нулевой элемент –  $q^{m-1} - 1$  раз, и множество отрезков  $(u(i), \dots, u(i+m-1))$ ,  $i = 1, \dots, t-1$ , совпадает с множеством всех ненулевых строк длины  $m$  над полем  $P$ . Таким образом, Л. р. п. максимального периода по ряду свойств хорошо имитирует случайную равновероятную последовательность. Это является основанием для широкого использования таких Л. р. п. в криптографии.

Множество  $K$  всех отрезков  $(u(0), \dots, u(t-1))$ , соответствующих разл. Л. р. п.  $u \in L_P(G)$  с максимальным периодом  $t$  и нулевым дефектом, есть линейный циклич. код длины  $n = t$  размерности  $m$  с кодовым расстоянием  $d = q^m - q^{m-1}$ . Этот код является наилучшим в том смысле, что для него достигается т. н. граница Плоткина, согласно которой  $d \leq (|P| - 1) \lfloor (n - 1) / (|K| - 1) \rfloor$ .

Основы теории Л. р. п. были заложены в 18–19 вв. в работах А. де Муавра, Д. Бернулли, Л. Эйлера и Ж. Лагранжа. В кон. 19 – нач. 20 вв. теория Л. р. п. развивалась в трудах франц. математика Э. Люка, П. Л.

[Чебышева](#), А. А. [Маркова](#). Исследования свойств Л. р. п. над кольцами вычетов и конечными полями были начаты в 1920–30-х гг., дальнейшее развитие эта теория получила в работах амер. учёных С. Голомба, Г. Нидеррайтера, Н. Цирлера и рос. учёных М. М. Глухова, А. С. Кузьмина, А. В. Михалёва, А. А. Нечаева, В. И. Нечаева, В. М. Сидельникова.

## Литература

Лит.: Чебышев П. Л. Теория сравнений. 3-е изд. СПб., 1901; Марков А. А. Исчисление конечных разностей. 2-е изд. Од., 1910; Dickson L. E. History of the theory of numbers. Wash., 1919. Vol. 1. N. Y., 1952; Golomb S. W. Sift register sequencez. Laguna Hills, 1982; Нечаев А. А. Линейные рекуррентные последовательности над коммутативными кольцами // Дискретная математика. 1991. Т. 3. № 4; Глухов М. М., Елизаров В. П., Нечаев А. А. Алгебра. М., 2003. Ч. 2.

Processing math: 0%