В. Л. Куракин, Представление функцией след линейных рекуррент над кольцами и модулями,
УМН, 2001, том 56, выпуск 6, 157–158

ПРЕДСТАВЛЕНИЕ ФУНКЦИЕЙ СЛЕД ЛИНЕЙНЫХ РЕКУРРЕНТ НАД КОЛЬЦАМИ И МОДУЛЯМИ

В. Л. Куракин

Пусть M – модуль над коммутативным кольцом R с единицей. Последовательность u над M называется *линейной рекуррентной последовательностью* (ЛРП) с характеристическим многочленом $F(x) = x^m - c_{m-1}x^{m-1} - \cdots - c_1x - c_0 \in R[x]$, если

$$u(i+m) = c_{m-1}u(i+m-1) + \cdots + c_1u(i+1) + c_0u(i), \qquad i \geqslant 0.$$

Множество всех ЛРП над M с характеристическим многочленом $F(x)$ обозначим $L_M(F)$.

Пусть A – алгебра над R, являющаяся конечно порожденным проективным R-модулем. Согласно [1], [2], для любой системы образующих $a_1, \ldots, a_m$ модуля ${}_RA$ существуют гомоморфизмы $\varphi_i \in \operatorname{Hom}_R(A, R)$, $1 \leqslant i \leqslant m$, такие, что $a = \sum_{i=1}^m \varphi_i(a)a_i$ для всех $a \in A$. Набор (a_i, φ_i) называется координатной системой проективного модуля A. *Следом* из A в R называется гомоморфизм R-модулей

$$\operatorname{tr}_{A/R}\colon A \to R, \qquad \operatorname{tr}_{A/R}(a) = \sum_{i=1}^m \varphi_i(aa_i), \quad a \in A.$$

Это определение не зависит от выбора координатной системы [1], [3]. Если R – поле и A – его конечное алгебраическое расширение, то $\operatorname{tr}_{A/R}$ совпадает с обычной функцией след из поля A в подполе R.

Всюду далее R – коммутативное локальное кольцо с максимальным идеалом $J = J(R)$ и полем вычетов $R/J = \overline{R}$, $F(x) \in R[x]$ – унитарный многочлен степени m и $S = R[x]/F(x) = R[\theta]$ – расширение кольца R корнем $\theta = [x]_F$ многочлена $F(x)$. Модуль ${}_RS$ является свободным модулем ранга m с базисом $1, \theta, \ldots, \theta^{m-1}$, и произвольный элемент $a \in S$ однозначно записывается в виде $a = a_0 + a_1\theta + \cdots + a_{m-1}\theta^{m-1}$, где $a_i \in R$. Положим $\varphi_i(a) = a_i$, $0 \leqslant i \leqslant m-1$. Тогда (θ^i, φ_i) – координатная система модуля ${}_RS$. Многочлен $F(x)$ будем называть *сепарабельным*, если многочлен $\overline{F}(x)$ не имеет кратных корней в поле разложения, где $\overline{F}(x)$ – канонический образ многочлена $F(x)$ над полем вычетов $\overline{R}$.

Теорема 1. *Пусть R – локальное кольцо, $F(x) \in R[x]$ – унитарный сепарабельный многочлен такой, что его образ $\overline{F}(x)$ неприводим над полем $\overline{R}$. Тогда для любой ЛРП $u \in L_R(F)$ существует единственная константа $c \in S$ такая, что*

$$u(i) = \operatorname{tr}_{S/R}(c\theta^i), \qquad i \geqslant 0. \tag{1}$$

В случае, когда R – поле Галуа или кольцо Галуа, представление (1) совпадает с известными ранее представлениями [4]–[6]. Действие функции след, как и в [6], выразим в терминах автоморфизмов и p-адических разложений. Кольцо R называется *гензелевым* [7], если для всякого унитарного многочлена $F(x) \in R[x]$ и для любого разложения $\overline{F}(x)$ в произведение $\overline{F}(x) = g(x)h(x)$ унитарных взаимно простых многочленов существуют унитарные многочлены $G(x), H(x) \in R[x]$ такие, что $\overline{G}(x) = g(x)$, $\overline{H}(x) = h(x)$ и $F(x) = G(x)H(x)$. Для сепарабельного многочлена $F(x)$ над гензелевым кольцом R можно построить его кольцо разложения [3], [8], последовательно расширяя R корнями делителей многочлена $F(x)$, неприводимых по модулю радикала.

Теорема 2. *Пусть R – гензелево кольцо, $F(x)$ – сепарабельный многочлен степени m и T – его кольцо разложения над R. Тогда $\operatorname{tr}_{T/R}(a) = \sum_{\sigma \in G} \sigma(a)$, $a \in T$, где $G = \operatorname{Aut}(T/R)$, $|G| = [\overline{T} : \overline{R}]$. Если к тому же $\overline{F}(x)$ неприводим над полем $\overline{R}$, то $\operatorname{tr}_{S/R}(a) = \sum_{\tau \in H} \tau(a)$, $a \in S$, где H – множество всех гомоморфных вложений кольца S в T над R, $|H| = m$.*

Предположим теперь, что $\overline{R} = GF(q)$ – конечное поле характеристики p, $J(R)$ – нильпотентный идеал индекса нильпотентности n и $\overline{F}(x)$ – неприводимый над полем $\overline{R}$ многочлен. Тогда

множество $\Gamma(R) = \{b \in R : b^q = b\}$ состоит из q элементов, попарно несравнимых по модулю $J(R)$. Назовем его *p-адическим координатным множеством* кольца R. Зафиксируем базисы $\{e_{i\alpha} + J(R)^{i+1} : \alpha \in A_i\}$ пространств $J(R)^i/J(R)^{i+1}$ над полем $\overline{R}$, $0 \leqslant i \leqslant n-1$. Тогда $\{e_{i\alpha} + J(S)^{i+1} : \alpha \in A_i\}$ есть базис пространства $J(S)^i/J(S)^{i+1}$ над полем $\overline{S}$, и каждый элемент $a \in S$ однозначно представляется в виде

$$a = \sum_{i=0}^{n-1} \sum_{\alpha \in A_i} a_{i\alpha} e_{i\alpha}, \qquad a_{i\alpha} \in \Gamma(S) = \{b \in S : b^{q^m} = b\},$$

где лишь конечное число элементов $a_{i\alpha}$ отлично от нуля.

ТЕОРЕМА 3. $\operatorname{tr}_{S/R}(a) = \sum\limits_{s=0}^{m-1} \sum\limits_{i=0}^{n-1} \sum\limits_{\alpha \in A_i} a_{i\alpha}^{q^s} e_{i\alpha}, \quad a \in S.$

Для модуля M над локальным кольцом R рассмотрим S-модуль $N = S \otimes_R M$ и определим функцию *след* $\operatorname{tr}_{N/M} \colon N \to M$ соотношением

$$\operatorname{tr}_{N/M}(s \otimes m) = \operatorname{tr}_{S/R}(s)m, \qquad s \in S, \quad m \in M.$$

Предположим, что многочлен $F(x)$ представляется в виде $F(x) = F_1(x)^{k_1} \cdots F_t(x)^{k_t}$, где $\overline{F}_j(x)$, $1 \leqslant j \leqslant t$, – различные унитарные неприводимые над полем $\overline{R}$ сепарабельные многочлены. Обозначим $S_j = R[x]/F_j(x) = R[\theta_j]$, где $\theta_j = [x]_{F_j}$.

ТЕОРЕМА 4. *Для любой ЛРП $u \in L_M(F)$ существует единственный набор констант $c_{jr} \in N_j = S_j \otimes_R M$, $1 \leqslant j \leqslant t$, $0 \leqslant r < k_j$, такой, что*

$$u(i) = \sum_{j=1}^{t} \sum_{r=0}^{k_j-1} \binom{i}{r} \operatorname{tr}_{N_j/M}(\theta_j^{i-r} c_{jr}), \qquad i \geqslant 0.$$

Полученное представление функцией след позволяет находить произвольный знак $u(i)$ ЛРП u без рекуррентного вычисления предыдущих знаков. Для ЛРП над полями, кольцами Галуа и квазифробениусовыми модулями специального вида это представление использовалось для нахождения распределения элементов в линейных рекуррентных последовательностях [9], [10], оценок линейной сложности линейных рекуррент и их координатных последовательностей [11], [12], построения помехоустойчивых кодов [5], [6], [10], [13], [14].

СПИСОК ЛИТЕРАТУРЫ

[**1**] А. З. Боревич, Б. А. Толасов. Введение в теорию Галуа колец. Орджоникидзе: Изд-во Сев.-Осетин. гос. ун-та, 1984. [**2**] Ф. Каш. Модули и кольца. М.: Мир, 1981. [**3**] F. DeMeyer, E. Ingraham. Separable Algebras over Commutative Rings. Berlin: Springer-Verlag, 1971. (Lecture Notes in Math. V. 181.) [**4**] Р. Лидл, Г. Нидеррайтер. Конечные поля. Т. 2. М.: Мир, 1988. [**5**] А. А. Нечаев // V Всесоюзн. симп. по теории колец, алгебр и модулей. Новосибирск, 1982. С. 97. [**6**] А. А. Нечаев // Дискретн. матем. 1989. Т. 1. №4. С. 123–139. [**7**] Н. Бурбаки. Коммутативная алгебра. М.: Мир, 1971. [**8**] G. J. Janusz // Trans. Amer. Math. Soc. 1966. V. 122. P. 461–479. [**9**] О. В. Камловский // УМН. 1998. Т. 53. №2. С. 149–150. [**10**] V. Kurakin, A. Kuzmin, A. Nechaev // Proceedings of the Sixth International Workshop on Algebraic and Combinatorial Coding Theory. September 6–12, 1998, Pskov, Russia. P. 166–171. [**11**] А. А. Нечаев, А. С. Кузьмин, В. Л. Куракин // Труды по дискретной математике. Т. 3. М.: ТВП, 2000. С. 155–194. [**12**] V. L. Kurakin, A. S. Kuzmin, A. V. Mikhalev, A. A. Nechaev // J. Math. Sci. 1995. V. 76. №6. P. 2793–2915. [**13**] A. R. Hammons, P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, P. Sole // Bull. Amer. Math. Soc. 1993. V. 29. №2. P. 218–222. [**14**] A. A. Nechaev, A. S. Kuzmin // Lecture Notes in Comput. Sci. 1997. V. 1255. P. 277–290.

Принято редколлегией
24.09.2001