

О. А. К о з л и т и н (Москва, ТВП). **О связи максимальных длин циклов многомерных полиномиальных подстановок над различными кольцами Галуа.**

Пусть $S = \text{GR}(q^n, p^n)$, $q = p^d$, $n \geq 2$, $d \geq 2$. Тогда $S \cong R[x]/F(x)$, где $R = \mathbf{Z}_{p^n}$, $F(x) \in R[x]$ — многочлен Галуа степени d . Согласно [1], верно равенство $S = R[\alpha]$, где α — корень многочлена $F(x)$. Система $\tilde{\alpha} = (e, \alpha, \alpha^2, \dots, \alpha^{d-1})$, где e — единица кольца S , есть базис модуля ${}_R S$. Пусть $m \in \mathbf{N}$, $\mathbf{x} = (x_1, x_2, \dots, x_m)$ есть строка переменных над кольцом S , $e_i = (0, \dots, 0, e, 0, \dots, 0) \in S^m$, где e стоит на i -м месте, $i = 1, \dots, m$. Тогда

$$\mathbf{x} = \sum_{i=1}^m x_i e_i = \sum_{i=1}^m \sum_{j=0}^{d-1} x_{i,j} \alpha^j e_i,$$

где $x_{i,j}$ — переменная над кольцом R . Аналогично, m -мерная полиномиальная подстановка $\Phi(\mathbf{x})$ кольца S представляется в виде

$$\Phi(\mathbf{x}) = \sum_{i=1}^m \Phi_i(\mathbf{x}) e_i = \sum_{i=1}^m \sum_{j=0}^{d-1} \Phi_{i,j}(\mathbf{x}) \alpha^j e_i,$$

где $\Phi_i: S^m \rightarrow S$ — некоторые полиномы над кольцом S , а $\Phi_{i,j}: S^m \rightarrow R$ — некоторые функции. Если

$$\mathbf{x} = (x_{1,0}, \dots, x_{1,d-1}, x_{2,0}, \dots, x_{2,d-1}, \dots, x_{m,0}, \dots, x_{m,d-1}),$$

то функции Φ_i , $\Phi_{i,j}$ можно считать функциями от $\mathbf{x}$. Дальнейшие усилия направлены на доказательство включения

$$\Phi_{i,j}(\mathbf{x}) \in R[\mathbf{x}]. \quad (1)$$

Если (1) доказано, то всякую m -мерную полиномиальную подстановку над кольцом S можно считать md -мерной полиномиальной подстановкой над кольцом R . Докажем включение (1). Обозначим для любых $x, y \in S$: $\varphi(x, y) = \text{Tr}_R^S(xy)$, где Tr_R^S — функция «след» из S в R . Пусть $\beta_0, \beta_1, \dots, \beta_{d-1}$ — базис модуля ${}_R S$, двойственный к $\tilde{\alpha}$. Согласно определению двойственного базиса, имеем:

$$\text{для любых } i, j \in \{0, \dots, d-1\}: \quad \varphi(\beta_i, \alpha^j) = \delta_{i,j} e, \quad (2)$$

где $\delta_{i,j}$ — символ Кронекера. Рассмотрим разложение $\Phi_i(\mathbf{x})$ по степеням α : $\Phi_i(\mathbf{x}) = \sum_{j=0}^{d-1} \Phi_{i,j}(\mathbf{x}) \alpha^j$. Тогда, в силу (2), имеем:

$$\Phi_{i,j}(\mathbf{x}) = \varphi(\beta_j, \Phi_i(\mathbf{x})). \quad (3)$$

С другой стороны, поскольку $\Phi_i(\mathbf{x}) \in S[\mathbf{x}]$, имеем:

$$\Phi_i(\mathbf{x}) = \sum_{(k_1, k_2, \dots, k_m) \in \mathbf{N}_0^m} \varphi_{k_1, k_2, \dots, k_m}^{(i)} x_1^{k_1} x_2^{k_2} \dots x_m^{k_m}, \quad (4)$$

где $\varphi_{k_1, k_2, \dots, k_m}^{(i)} \in S$. Введем обозначение

$$\mathbf{k} = (k_{1,0}, \dots, k_{1,d-1}, k_{2,0}, \dots, k_{2,d-1}, \dots, k_{m,0}, \dots, k_{m,d-1}) \in \mathbf{N}_0^{md}.$$

Из равенства (4) и соотношения $x_i = \sum_{j=0}^{d-1} x_{i,j} \alpha^j$, выполняющегося для всякого $i = 1, \dots, m$, вытекает возможность следующего представления:

$$\Phi_i(\mathbf{x}) = \sum_{\mathbf{k} \in \mathbf{N}_0^{md}} c_{\mathbf{k}}^{(i)} \mathbf{x}^{\mathbf{k}}, \quad (5)$$

где $c_{\mathbf{k}}^{(i)} \in S$. Комбинируя (3) и (5), а также учитывая, что $\varphi(x, y)$ принимает значения в R , получаем цепочку равенств:

$$\Phi_{i,j}(\mathbf{x}) = \varphi(\beta_j, \Phi_i(\mathbf{x})) = \varphi\left(\beta_j, \sum_{\mathbf{k} \in \mathbf{N}_0^{md}} c_{\mathbf{k}}^{(i)} \mathbf{x}^{\mathbf{k}}\right) = \sum_{\mathbf{k} \in \mathbf{N}_0^{md}} \varphi(\beta_j, c_{\mathbf{k}}^{(i)}) \mathbf{x}^{\mathbf{k}} \in R[\mathbf{x}].$$

Таким образом, включение (1) обосновано. Обозначим $L_k(Q)$ максимум длин циклов k -мерных полиномиальных подстановок над кольцом Галуа Q . Из доказанного включения (1) вытекает следующая теорема.

Теорема. Пусть $S = \text{GR}(q^n, p^n)$, $q = p^d$, $n \geq 2$, $d \geq 2$, $R = \mathbf{Z}_{p^n}$. Тогда $L_m(S) \leq L_{md}(R)$.

Таким образом, зная максимум длин циклов полиномиальных подстановок над кольцом вычетов, можно указать верхнюю оценку максимальной длины цикла полиномиальной подстановки над произвольным кольцом Галуа.

Автор выражает глубокую признательность профессору А. А. Нечаеву за постановку задачи и существенную помощь при подготовке этой работы.

Работа выполнена при поддержке гранта Президента РФ НШ-8564.2006.10.

СПИСОК ЛИТЕРАТУРЫ

1. Нечаев А. А. Код Кердока в циклической форме. — Дискретн. матем., 1989, т. 1, в. 4, с. 123–139.