# НАХОЖДЕНИЕ БАЗИСА ОДНОРОДНОЙ СИСТЕМЫ ЛИНЕЙНЫХ УРАВНЕНИЙ НАД КОЛЬЦОМ ПОЛИНОМОВ

© О.А. Сажнева

Sazhneva O.A. Finding of the basis of a homogeneous system of linear equations over a circle of polynomials.

В этой работе рассматривается метод нахождения базиса целых решений однородной системы линейных уравнений над кольцом полиномов.

Пусть $R$ – поле, $R[x]$ – кольцо полиномов. $R^m[x]$ – $m$-мерный модуль над $R[x]$. $v^i \in R^m[x]$ – векторы в этом модуле. Пусть $V = (v^1, v^2, \dots, v^n)$ – $n$ векторов в $R^m[x]$, порождающих подмодуль $M \subset R^m[x]$ ранга $n$. Будем говорить, что векторы $V$ образуют *канонический базис* в $M$, если они обладают следующими свойствами:

1) первые $(i-1)$ компоненты вектора $v^i$ нулевые;

2) $i$-я компонента вектора $v^j$ имеет степень меньшую, чем $i$-я компонента вектора $v^i$: $\deg v_i^j < \deg v_i^i$, для всех $i$ и $j$, таких, что $j < i \le n$;

3) коэффициент при старшей переменной $i$-ой компоненты $i$-ого вектора ($i = 1, 2, \dots, n$) равен единице;

4) все компоненты каждого вектора не имеют общего полиномиального множителя.

Т е о р е м а. Канонический базис единственный.

Д о к а з а т е л ь с т в о. Пусть имеются два различных канонических базиса: $V = (v^1, v^2, \dots, v^n)$ и $\overline{V} = (\overline{v}^1, \overline{v}^2, \dots, \overline{v}^n)$. Так как только первый вектор в каждом базисе имеет отличную от нуля первую компоненту, то, очевидно, что эти первые компоненты должны совпадать: $v_1^1 = \overline{v}_1^1$.

Вектор $v^2$ может быть получен как линейная комбинация всех векторов второго базиса за исключением $\overline{v}^1$, иначе у него была бы отлична от нуля первая компонента. Поскольку все вторые компоненты у векторов $\overline{v}^3, \overline{v}^4, \dots, \overline{v}^n$ равны нулю, то $v_2^2 = \lambda \overline{v}_2^2$ и наоборот $\overline{v}_2^2 = \overline{\lambda} v_2^2$. Так как старшие переменные у $v_2^2$ и $\overline{v}_2^2$ имеют коэффициенты, равные единице, то $v_2^2 = \overline{v}_2^2$. Аналогично доказывается, что $v_i^i = \overline{v}_i^i$ для $i = 3, 4, \dots, n$.

Пусть $v^1 = \sum_{j=1}^{n} \lambda_j \overline{v}^j$. (1)

По условию $i$-я компонента вектора $\overline{v}^j$ имеет степень меньшую, чем $i$-я компонента вектора $\overline{v}^i$: $\deg \overline{v}_i^j < \deg \overline{v}_i^i$, $j < i \le n$, поэтому, если в сумме (1) $\lambda_j \neq 0$, то степень $j$-й компоненты вектора $v^1$ совпадает со степенью $j$-й компоненты вектора $\overline{v}^j$: $\deg v_j^1 = \deg \overline{v}_j^j = \deg v_j^j$. Но по условию, степень $j$-й компоненты вектора $v^1$ меньше, чем степень $j$-й компоненты вектора $v^j$: $\deg v_j^1 < \deg v_j^j$. Следовательно, в сумме (1) все $\lambda_j = 0$ для $j > 1$. Таким образом, $v^1 = \lambda_1 \overline{v}^1$, и наоборот $\overline{v}^1 = \overline{\lambda}_1 v^1$. Так как $v_1^1 = \overline{v}_1^1$, то $\lambda_1 = \overline{\lambda}_1 = 1$ и $v^1 = \overline{v}^1$. Аналогично доказывается, что $v^j = \overline{v}^j$, $j = 2, 3, \dots, n$. Теорема доказана.

Пусть теперь $Ay = c$ – система линейных уравнений над $R[x]$. Алгоритмы решения таких систем рассматриваются в [1]. Пусть $z_1, z_2, \dots, z_n$ – базис пространства целых решений этой системы.

Приведем алгоритм построения канонического базиса для решений соответствующей однородной системы. Рассматриваемый метод состоит из трех этапов.

На ***первом этапе*** получаем

$$v^1 = z_2 - z_1,\ v^2 = z_3 - z_1, \dots, v^{n-1} = z_n - z_1 \tag{2}$$

базис пространства решений однородной системы $Ay = 0$.

На ***втором этапе*** приведем этот базис к треугольному виду. Сначала сократим все компоненты первого вектора на наибольший общий делитель его компонент, если он отличен от единицы и обнулим все первые компоненты у векторов, кроме первого вектора. Затем сократим все компоненты второго вектора на их наибольший общий делитель, если он отличен от нуля, и обнулим первые и вторые компоненты у всех векторов, кроме первого и второго и т. д.

Пусть после $(k-1)$-го шага мы получили $v^{k-1}$, $v^k, \dots, v^{n-1}$ в качестве базиса пространства решений однородной системы. Вычисления на $k$-ом шаге сводятся к следующему.

Пусть $GCD(v_1^s, v_2^s, \dots, v_m^s) = q_s$. Если $q_s \neq 1$, то

$$v^s := v^s / q_s,\ s = k-1, k, \dots, n-1. \tag{3}$$

Пусть $GCD(v_k^k, v_k^{k+1}, \ldots, v_k^{n-1}) = g_k$ (4)

$$\sum_{i=k}^{n-1} \alpha_i^k v_k^i = g_k \qquad (5)$$

представление наибольшего общего делителя в виде линейной комбинации полиномов $v_k^k$, $v_k^{k+1}$, …, $v_k^{n-1}$. Тогда $k$-ый базисный вектор будет

$$v^k := \sum_{i=k}^{n-1} \alpha_i^k v^i \qquad (6).$$

Остальные векторы с номерами $i$ большими, чем $k$, будут $v^i := v^i - \left\lfloor v_k^i / g_k \right\rfloor \cdot v^k$, (7)

$i = k+1, k+2, \ldots, n-1$.

Отметим, что в частном случае, когда в сумме, стоящей справа в равенстве (6), коэффициент при $v^k$ равен нулю, то в (7) индекс $i$ пробегает все значения от $k$ до $n-1$, за исключением одного из номеров $s$, при котором $\alpha_s^k \neq 0$, например наименьшего из таких номеров.

Запишем векторы $v^1$, $v^2$, …, $v^{n-1}$ в виде матрицы:

$$\begin{pmatrix} v^1 \\ v^2 \\ v^3 \\ \vdots \\ v^k \\ \vdots \\ v^{n-1} \end{pmatrix} = \begin{pmatrix} g_1, v_2^1, v_3^1, v_4^1, \ldots, v_{n-1}^1, \ldots, v_m^1 \\ 0, g_2, v_3^2, v_4^2, \ldots, v_{n-1}^2, \ldots, v_m^2 \\ 0, \quad 0, g_3, v_4^3, \ldots, v_{n-1}^3, \ldots, v_m^3 \\ \vdots \\ 0, \ldots, 0, g_k, v_{k+1}^k, \ldots, v_{n-1}^k, \ldots, v_m^k \\ \vdots \\ 0, 0, \ldots, 0, g_{n-1}, v_n^{n-1}, \ldots, v_m^{n-1} \end{pmatrix}.$$

На ***третьем этапе*** будем строить такой базис, у которого в каждом столбце матрицы, состоящей из векторов базиса, наддиагональный элемент имел бы степень меньшую, чем элемент, стоящий на диагонали.

Перед этим сократим каждый вектор $v^i$ ($i$ = 1, 2, …, $n$ – 1) на наибольший общий делитель его компонент, если он отличен от единицы.

Преобразуем векторы $v^1$, $v^2$, …, $v^{n-2}$, используя следующие формулы. На $k$-ом ($k = n-2, n-3, \ldots, 1$) шаге будем вычислять

$q_{k+1} = GCD(v_1^{k+1}, v_2^{k+1}, \ldots, v_m^{k+1})$. Если $q_{k+1} \neq 1$, то

$$v^{k+1} := v^{k+1} / q_{k+1} \qquad (8)$$

$$v^i := v^i - \left\lfloor v_{k+1}^i / g_{k+1} \right\rfloor \cdot v^{k+1}, \; i = k, k-1, \ldots, 1. \qquad (9)$$

Последним действием будет нахождение общего делителя для компонент первого вектора и сокращение их на этот общий делитель.

Таким образом, мы получили *базис целых решений однородной системы уравнений*: $v^1, v^2, \ldots, v^{n-1}$.

**Пример**

Пусть задана система: Ay = c, где

$$A = \begin{pmatrix} x+3 & 2x+1 & -x-1 & 1 \\ x-2 & x+5 & x & x-1 \end{pmatrix}, \quad c = \begin{pmatrix} x \\ 1 \end{pmatrix}.$$

Получим базис целых решений однородной системы уравнений на основе *целых базисных решений неоднородной системы уравнений* $z_1, z_2, z_3$, построенных с помощью алгоритма из [1].

$z_1 = \lambda\,(4x-4, -3x^2-5x+5, -6x^2+6x+22, 9x^2+19x+29)$,

$\lambda = 1/4$.

На **первом этапе** производим вычисления с помощью формул (2).

$v^1 = \beta_1 (4x^3-8x^2-8x+12, -3x^4-8x^3+3x^2+10x-5, -6x^4+30x^2+12x-18, 9x^4+28x^3+51x^2+6x-49)$,

$\beta_1 = 1/4$.

$v^2 = \beta_2 (4x^3-12x^2-4x+24, -3x^4-2x^3+19x^2+14x-15, -6x^4+12x^3+34x^2-40x-66, 9x^4+10x^3-13x^2-102x-123)$,

$\beta_2 = 1/4$.

**Второй этап.** Используем формулы (3), (4), (5), (6), (7).

***1 шаг.***

$q_1 = \gcd(v_1^1, v_2^1, v_3^1, v_4^1) = 1/4$,

$q_2 = \gcd(v_1^2, v_2^2, v_3^2, v_4^2) = 1/4$.

$v^1 = (4x^3-8x^2-8x+12, -3x^4-8x^3+3x^2+10x-5, -6x^4+30x^2+12x-18, 9x^4+28x^3+51x^2+6x-49)$,

$v^2 = (4x^3-12x^2-4x+24, -3x^4-2x^3+19x^2+14x-15, -6x^4+12x^3+34x^2-40x-66, 9x^4+10x^3-13x^2-102x-123)$.

$\alpha_1^1 = 1$, $\alpha_2^1 = -1$.

$v^1 = (4x^2-4x-12, -6x^3-16x^2-4x+10, -12x^3-4x^2+52x+48, 18x^3+64x^2+108x+74)$.

$\left\lfloor v_1^2 / g_1 \right\rfloor = -x-2$.

$v^2 = (0, 3x^4+2x^3-9x^2-4x+5, 6x^4-8x^3-26x^2+16x+30, -9x^4-18x^3+7x^2+40x+25)$.

**Третий этап.**

Используем формулы (8) и (9).

$q_2 = \gcd(v_1^2, v_2^2, v_3^2, v_4^2) = (3x^2-x-5)$,

$v^2 = (0, x^2+x-1, 2x^2-2x-6, -3x^2-7x-5)$.

$\left\lfloor v_2^1 / g_2 \right\rfloor = -6x-10$.

$v^1 = (4x^2-4x-12, 0, 4x^2-4x-12, -8x^2+8x+24)$.

$q_1 = \gcd(v_1^1, v_2^1, v_3^1, v_4^1) = 4x^2-4x-12$.

Таким образом, получен канонический *базис целых решений однородной системы уравнений*:

$v^1 = (1, 0, 1, -2)$,

$v^2 = (0, x^2+x-1, 2x^2-2x-6, -3x^2-7x-5)$.

ЛИТЕРАТУРА

1. *Сажнева О.А.* Решение систем линейных уравнений над кольцом полиномов p-адическим методом // XI Державинские чтения ИМФИ ТГУ им. Г.Р. Державина, 3 февраля 2006 г. Тамбов, 2006. С. 83-85.

Поступила в редакцию 19 октября 2006 г.