Работа выполнена при частичной поддержке грантов РФФИ (проект 08-07-97507) и программы "Развитие потенциала высшей школы"(проект 2.1.1/1853).

Список литературы

1. *Икрамов Х.Д.* О конечных спектральных процедурах в линейной алгебре // Программирование. 1994. N 1. С. 56-69.

2. *Переславцева О.Н.* О вычислении коэффициентов характеристического полинома // Вычислительные методы и программирование. Издательство Московского университета, 2008. Т.9. N.2. С. 180-185.

3. *Сейфуллин Т.Р.* Вычисление определителя, присоединённой матрицы и характеристического полинома без деления // Кибернетика и системный анализ. 2002. N.5. С. 18-42.

4. *Данилевский А.М.* О численном решении векового уравнения // Матем. сб. 1937. Т.2(44). N1. С. 169-172.

5. *Фаддеев Д.К., Фаддеева В.Н.* Вычислительные методы линейной алгебры. М., Л.: Гос. изд. физ. мат. литературы, 1963.

Поступила в редакцию 17 ноября 2008 г.

РЕШЕНИЕ СИСТЕМ НЕОДНОРОДНЫХ И ОДНОРОДНЫХ ЛИНЕЙНЫХ УРАВНЕНИЙ НАД КОЛЬЦОМ ПОЛИНОМОВ

© **О.А. Сажнева**

Ключевые слова: система линейных неоднородных уравнений, p-адический метод, канонический базис целых решений однородной системы линейных уравнений над кольцом полиномов.

Аннотация

Рассматривается p-адический метод решения системы линейных неоднородных уравнений над кольцом полиномов. Приводится пример решения системы линейных неоднородных уравнений над кольцом полиномов. Описывается метод нахождения канонического базиса целых решений однородной системы линейных уравнений над кольцом полиномов. Приводится пример нахождения канонического базиса.

1 p-адический метод решения системы линейных неоднородных уравнений над кольцом полиномов

Существуют разные методы решения систем линейных неоднородных уравнений в области главных идеалов R. Сравнение по оценкам сложности этих методов показывает преимущество метода, предложенного в работе [1]. В этом методе выделяются два этапа. На первом этапе вычисляется базисное множество решений системы в поле частных области. На втором строится базис целых решений.

Для построения решения системы в поле частных области сначала находится решение в факторкольце R/p^k, где p - подходящий простой элемент кольца R, а степень k выбирается так, чтобы степень полинома p^k превосходила степень произведения числителя и знаменателя в каждой рациональной компоненте вектора решения.

Решение системы в кольце R/p^k осуществляется с помощью p-адического подъема [2]. Сначала найдем решение в R/p. Пусть $x_p = A_p^{-1} \cdot c_p$, где индекс p означает отображение $R \to R/p$. Чтобы найти решение в R/p^2, рассмотрим систему $A(xp + x_p) = c$. Так как $c' = c - Ax_p$ делится нацело на p, то достаточно решить систему $Ax = c'/p$ в R/p. Этот процесс продолжать до p^k.

Для того чтобы уменьшить вычислительные затраты при построении решения в поле частных также введем простой числовой элемент q кольца $\mathbb{Z}$. И все вычисления будем вести в поле $\mathbb{Z}/q\mathbb{Z}$.

Рассмотрим этот метод в кольце полиномов. Пусть задана система:

$$\begin{cases} (x+3)u + (2x+1)v + (-x-1)t = x, \\ (x-2)u + (x+5)v + xt = 1. \end{cases} \tag{1}$$

Выберем x в качестве простого элемента в $\mathbb{Q}[x]$. В качестве простого числового модуля возьмем 41.

Найдем решение системы (1) при $t = 0$. Система примет вид: $Ay = c$, где $y = (u, v)$. (2)

Обратная матрица коэффициентов A_x^{-1} системы (2) и вектор свободных членов c_x по модулю x:

$$A_x^{-1} = \begin{pmatrix} 5\xi & -1\xi \\ 2\xi & 3\xi \end{pmatrix}, \quad c_x = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \text{ где } \xi = 1/17; \; A_{41}^{-1} = \begin{pmatrix} 22 & -29 \\ 17 & 5 \end{pmatrix}.$$

Решение ищем в виде $y = y \cdot x + y_0$, $k = 1, 2, 3, 4$.

Вычислим вектор $y_0 = A_{41}^{-1} c_{41} = (-29, 5)$.

По модулю x^2 решение имеет вид $y' = y_1 x + y_0$. Подставим его в (2). После сокращения на x получим $Ay' = c'$, где $c = (20, 24)$. Вычислим $y_1 = A_{41}^{-1} c_{41} = (31, 5)$.

Следующее решение по модулю x^3 будет иметь вид: $y'' = y_2 x^2 + y_1 x + y_0$. . Проводя аналогичные рассуждения, в итоге получим следующее решение системы (2):

$u = 14x^4 + 38x^3 + 0x^2 + 31x - 29$,

$v = 34x^4 + 25x^3 + 33x^2 + 9x + 5$.

Найденное решение отобразим в поле частных области с помощью алгоритма реконструкции дробей П. С. Ванга [3].

Найдем $u = \frac{c_1(x)}{d_1(x)}$ и $v = \frac{c_2(x)}{d_2(x)}$ такие, что степени полиномов, стоящих в числителях, не превосходили наибольшей из степеней миноров, полученных заменой любого столбца матрицы коэффициентов на столбец свободных членов, а степени полиномов, стоящих в знаменателях, не превосходили степени определителя матрицы.

В ходе вычислений с помощью алгоритма Ванга также будем проводить вычисления в $\mathbb{Z}/q\mathbb{Z}$.б

В результате отображения в поле частных получим:

$$u = \frac{-x^2 - 3x + 1}{x^2 - 11x - 17}, \quad v = \frac{x^2 - 3x - 3}{x^2 - 11x - 17}.$$

Таким образом, первое решение системы (1) имеет вид:

$$g_1 = \left(\frac{-x^2 - 3x + 1}{x^2 - 11x - 17}, \; \frac{x^2 - 3x - 3}{x^2 - 11x - 17}, \; 0 \right).$$

Аналогично получаем второе решение системы:

$$g_2 = \left(\frac{x^2 + x + 1}{2x^2 + 2x - 2}, \; 0, \; \frac{-x^2 + 3x + 3}{2x^2 + 2x - 2} \right).$$

Множество решений данной системы в поле частных:

$$M = \{ \sum_{i=1}^{2} g_i h_i | h_i \in \mathbb{Q}[x], \sum_{i=1}^{2} h_i = 1 \}.$$

Это множество может быть также записано в виде

$$M = \{ \sum_{i=1}^{2} \mu_i q_i / \sum_{i=1}^{2} \chi_i q_i | q_i \in \mathbb{Q}[x], \sum_{i=1}^{2} \chi_i q_i | q_i \neq 0 \},$$

где μ_i и χ_i – это числители и знаменатели рациональных компонент вектора решений системы (1).

Теперь построим базис целых решений системы (1) с помощью алгоритма [1]. Целое решение может быть получено, когда $\sum_{i=1}^{2} \chi_i q_i = 1$, где $q_i \in \mathbb{Q}[x]$.

Так как идеал, порожденный знаменателями χ_1, χ_2 рационального базиса g_1 и g_2, является единичным, то с помощью расширенного алгоритма Евклида вычислим множители q_1 и q_2 такие, что

$\sum_{i=1}^{2} \chi_i q_i = 1$. Одно целое решение мы получим, вычисляя сумму $z_1 = \sum_{i=1}^{2} \mu_i q_i$. Другое целое решение $z_2 = \mu_2 - z_1(\chi_2 - 1)$. Все целые решения исходной системы имеют вид $\alpha z_1 + (1-\alpha)z_2$, где $\alpha \in \mathbb{Q}[x]$.

Для нашего примера:
$q_1(x^2 - 11x - 17) + q_2(2x^2 + 2x - 2) = 1$, $q_1 = (2 - 6x)\lambda$, $q_2 = (3x - 37)\lambda$, где $\lambda = -1/40$.

$$z_1 = \begin{pmatrix} -9x^3 + 18x^2 + 46x + 35 \\ 6x^3 - 20x^2 - 12x + 6 \\ 3x^3 - 46x^2 + 102x + 111 \end{pmatrix} \lambda, \quad z_2 = \begin{pmatrix} 18x^5 - 18x^4 - 155x^3 - 148x^2 + 28x + 65 \\ -12x^5 + 28x^4 + 82x^3 - 48x^2 - 48x + 18 \\ -6x^5 + 86x^4 - 103x^3 - 524x^2 - 36x + 213 \end{pmatrix} \lambda.$$

2 Метод нахождения канонического базиса целых решений однородной системы линейных уравнений над кольцом полиномов

Пусть R – поле, $R[x]$ – кольцо полиномов, $R^m[x]$ – m-мерный модуль над $R[x]$, $\nu^i \in R^m[x]$ – векторы в этом модуле. Пусть $V = (\nu^1, \nu^2, \ldots, \nu^n)$ – n векторов в $R^m[x]$, порождающих подмодуль M ранга n.

Определение Будем говорить, что векторы V образуют канонический базис в M, если они обладают следующими свойствами:
1) первые $(i-1)$ компоненты вектора ν^i нулевые;
2) i-ая компонента вектора ν^j имеет степень меньшую, чем i-ая компонента вектора ν^i: $deg\nu_i^j < deg\nu_i^i$, для всех i и j, таких, что $j < i \leq n$;
3) коэффициент при старшей переменной i-ой компоненты i-ого вектора $(i = 1, 2, \ldots, n)$ равен единице;
4) все компоненты каждого вектора не имеют общего полиномиального множителя.

Пусть теперь $Ay = c$ – система линейных уравнений над $R[x]$. Пусть $z_1, z_2, \ldots, z_n$ – базис пространства целых решений этой системы.

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

Алгоритм.

1. На этом этапе получаем

$$\nu^1 = z_2 - z_1, \ \nu^2 = z_3 - z_1, \ldots, \ \nu^{n-1} = z_n - z_{n-1} \tag{3}$$

базис пространства решений однородной системы $Ay = 0$.

2. Приводим полученный на этапе 1 базис к треугольному виду.

Для этого 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 $(k-1)$-ого шага мы получили $\nu^{k-1}, \nu^k, \ldots, \nu^{n-1}$ в качестве базиса пространства решений однородной системы. Вычисления на k-ом шаге сводятся к следующему.

Пусть $GCD(\nu_1^s, \nu_2^s, \ldots, \nu_m^s) = q_s$. Если $q_s \neq 1$, то

$$\nu^s := \nu^s / q_s, \ s = k-1, k, \ldots, n-1. \tag{4}$$

Пусть

$$GCD(\nu_k^k, \nu_k^{k+1}, \ldots, \nu_k^{n-1}) = g_k \tag{5}$$

и наибольший общий делитель представлен в виде линейной комбинации полиномов $\nu_k^k, \nu_k^{k+1}, \ldots, \nu_k^{n-1}$:

$$\sum_{i=k}^{n-1} a_i^k \nu_k^i = g_k. \tag{6}$$

Тогда k-ый базисный вектор будет

$$\nu^k := \sum_{i=k}^{n-1} a_i^k \nu^i. \tag{7}$$

Остальные векторы

$$\nu^i := \nu^i - (\nu^i_k/g_k)\nu^k,\ i = k+1, \ldots, n-1. \tag{8}$$

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

Запишем векторы $\nu^1, \nu^2, \ldots, \nu^{n-1}$ в виде матрицы:

$$\begin{pmatrix} \nu^1 \\ \nu^2 \\ \nu^3 \\ \ldots \\ \nu^k \\ \ldots \\ \nu^{n-1} \end{pmatrix} = \begin{pmatrix} g_1, & \nu^1_2, & \nu^1_3, & \nu^1_4, & \ldots, & \nu^1_{n-1}, & \ldots, & \nu^1_m \\ 0, & g_2, & \nu^2_3, & \nu^2_4, & \ldots, & \nu^2_{n-1}, & \ldots, & \nu^2_m \\ 0, & 0, & g_3, & \nu^3_4, & \ldots, & \nu^3_{n-1}, & \ldots, & \nu^3_m \\ . & . & . & . & . & . & . & . \\ 0, & \ldots, & g_k, & \nu^k_{k+1}, & \ldots, & \nu^k_{n-1}, & \ldots, & \nu^k_m \\ . & . & . & . & . & . & . & . \\ 0, & 0, & \ldots, & 0, & g_{n-1}, & \nu^{n-1}_n, & \ldots, & \nu^{n-1}_m \end{pmatrix}.$$

3. Строим 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 ν^i $(i = 1, 2, \ldots, n-1)$ на наибольший общий делитель его компонент, если он отличен от единицы. Преобразуем векторы $\nu^1, \nu^2, \ldots, \nu^{n-2}$, используя следующие формулы. На k-ом $(k = n-2, n-3, \ldots, 1)$ шаге будем вычислять
$q_{k+1} = GCD(\nu^{k+1}_1, \nu^{k+1}_2, \ldots, \nu^{k+1}_m)$.
Если $q_{k+1} > 1$, то

$$\nu^{k+1} := \nu^{k+1}/q_{k+1},\ \nu^i := \nu^i - (\nu^i_{k+1}/g_{k+1})\nu^{k+1},\ i = k, k-1, \ldots, 1. \tag{9}$$

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

В результате мы получили *базис целых решений однородной системы уравнений*: $\nu^1, \nu^2, \ldots, \nu^{n-1}$.

Рассмотрим пример.

Рассмотрим однородную систему, соответствующую ранее приведенной неоднородной системе уравнений:

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

Выше мы получили базис целых решений однородной системы уравнений на основе *целых базисных решений неоднородной системы уравнений* z_1, z_2.

1. Вычислим ν^1 с помощью формул (3).

$$\nu^1 = \begin{pmatrix} -9x^5 + 117x^4 + x^3 - 817x^2 - 1287x - 555 \\ 6x^5 - 86x^4 + 106x^3 + 518x^2 + 18x - 222 \\ 3x^5 - 79x^4 + 557x^3 - 229x^2 - 2955x - 1887 \end{pmatrix}.$$

2. Используем формулы (4), (5), (6), (7),(8).

3. Используем формулы (9).

В результате получен канонический базис целых решений однородной системы уравнения:

$$\nu^1 = (3x^2 + 7x + 5, -2x^2 - 2x + 2, -x^2 + 11x + 17).$$

Работа выполнена при частичной поддержке грантов РФФИ (проект 08-07-97507) и программы "Развитие потенциала высшей школы"(проект 2.1.1/1853).

Список литературы

1. *Малашонок Г.И.* О решении систем линейных уравнений p-адическим методом// Программирование, 2003. N2. С. 8-22.

2. *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. С. 83-85.

3. *Wang P. S.* A p-adic algorithm for univariate partial fractions. Proc. 1981 ACM Symp. Symbolic Algebraic Comp., 1981. P. 212-217.

4. *Сажнева О.А.* Нахождение канонического базиса целых решений однородной системы линейных уравнений над кольцом полиномов// Вестник ТГУ, 2007. Т. 12. Вып.1. С. 133-134.

Поступила в редакцию 20 ноября 2008 г.

О ПРИМЕНЕНИИ ДПФ В АЛГЕБРАИЧЕСКИХ ВЫЧИСЛЕНИЯХ

© **А.О. Лапаев**

Ключевые слова: матричные алгоритмы, быстрое преобразование Фурье, полиномиальные алгоритмы.

Аннотация

В статье описывается один из способов вычисления определителя матрицы над кольцом $\mathbb{Z}[x]$ с использованием быстрого преобразования Фурье. Приводятся теоретические оценки сложности.

Известен алгоритм умножения многочленов одной переменной [1] при помощи быстрого преобразования Фурье. Такой алгоритм имеет сложность $O(n \log_2 n)$ и является одним из самых быстрых алгоритмов умножения полиномов.

В данной статье рассматривается способ вычисления определителя матрицы над кольцом $\mathbb{Z}[x]$ с использованием ДПФ. В алгоритме вычисления определителя мы заменяем арифметические операции над полиномами соответствующими операциями над их образами, полученными при преобразовании Фурье. А в конце делаем обратное ДПФ.

Для применения ДПФ необходимо знать верхние оценки максимальной степени и максимального коэффициента результата вычислений. Важно требовать, чтобы в вычислительном алгоритме не было операций деления с остатком. Допустимы только операции сокращения. Пусть степень искомого определителя $\det A$ не превосходит s, а максимальный модуль коэффициента в полиноме $\det A$ не превосходит числа α. Вычисления будут выполняться в несколько этапов:

1. Для всех элементов матрицы A вычисляется ДПФ на $2^{\lceil \log_2 s \rceil}$ точках. При этом берется такое количество простых модулей p_i, чтобы выполнялось неравенство $p_1 p_2 \dots p_k > 2\alpha$.

2. Вычисляется определитель по некоторому алгоритму, в котором нет операций деления.

3. Результат восстанавливается с помощью обратного ДПФ и КТО [2]. Для этого вычисляется обратное преобразование Фурье по каждому простому модулю и затем с помощью КТО восстанавливаются коэффициенты результата в кольце $\mathbb{Z}[x]$.

Оценим эффективность такого подхода на примере вычисления определителя матрицы с использованием алгоритма прямого хода [3].

Получим оценку для максимального коэффициента определителя матрицы.

Пусть $A = (a_{ij}(x))$ – матрица с элементами из $\mathbb{Z}[x]$, $a_{ij} = \sum_{k=0}^{s_{ij}-1} a_{ij}^k x^k$. Пусть $\max_{i,j,k} |a_{ij}^k| = \alpha$, а $\max_{ij} \deg a_{ij} = s-1$. Оценим максимальный коэффициент $\det A$. Для этого воспользуемся тем фактом, что определитель матрицы можно вычислить по следующей формуле:

$$\det A = \sum_{(j_1,\dots,j_n)} (-1)^t a_{1j_1} a_{2j_2} \dots a_{nj_n},$$

где $(j_1, \dots, j_n)$ – перестановка чисел от 1 до n. t – четность этой перестановки. Максимальный коэффициент $a_{1j_1} a_{2j_2} \dots a_{nj_n}$ по модулю не будет превосходить $s^{n-1}\alpha^n$. Так как количество возможных перестановок из n элементов равно $n!$, то максимальный коэффициент $\det A$ не превысит $n! s^{n-1} \alpha^n$. По формуле Стирлинга $n! < \sqrt{2\pi n} \left(\frac{n}{e}\right)^n e^{\frac{1}{12n}}$. Тогда максимальный модуль коэффициента $\det A$ не превышает

$$\sqrt{2\pi n} \left(\frac{n}{e}\right)^n e^{\frac{1}{12n}} s^{n-1} \alpha^n. \qquad (1)$$