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

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

Оценим общее количество элементарных операций в алгоритме прямого хода. Пусть машинное слово имеет размер 32 бита. Примем за элементарную операцию сложение двух машинных слов. Умножение двух машинных слов занимает примерно столько же процессорного времени, сколько и сложение. Вычислительные эксперименты показали, что операция вычисления остатка от деления занимает столько же времени, как 7 сложений.

Для того, чтобы произведение простых модулей превосходило максимальный по модулю коэффициент определителя матрицы A, достаточно взять

$$r = \lceil \log_{32}(\sqrt{2\pi n}\left(\frac{n}{e}\right)^n e^{\frac{1}{12n}} s^{n-1}\alpha^n)\rceil$$

простых 32-разрядных модулей.

Оценим сложность вычисления прямого преобразования Фурье для одного элемента матрицы A. Так как количество мономов в a_{ij} не превосходит s, то необходимо выполнить $7sr\lceil \log_{32}\alpha\rceil$ операций вычисления остатка от деления коэффициентов на простые модули. Преобразование Фурье вычисляется на $N = 2^{\lceil \log_2 sn\rceil}$ точках. Тогда сложность БПФ по одному модулю составляет $9N\log_2 N$ операций. Тогда общая сложность, учитывая r модулей и n^2 элементов матрицы, составляет

$$n^2 r(7s\lceil \log_{32}\alpha\rceil + 9N\log_2 N) \tag{2}$$

элементарных операций.

Сложность любой кольцевой операции в алгоритме прямого хода составляет $8rN$ элементарных операций. Так как сложность прямого хода есть $O(n^3)$, то общее количество элементарных операций над образами элементов матрицы A равно

$$8n^3 rN. \tag{3}$$

Для восстановления полинома-прообраза для конкретного определителя необходимо выполнить r обратных преобразований Фурье и восстановить по китайской теореме об остатках ns чисел. Сложность обратного преобразования Фурье по r модулям равна $9rN\log_2 N$. Сложность восстановления одного числа из r остатков равна $2r^2$. Общее количество операций на этом шаге составляет

$$9rN\log_2 N + 2r^2 sn. \tag{4}$$

Получим количество всех операций в алгоритме:

$$r(7s\lceil \log_{32}\alpha\rceil + 9N\log_2 N) + 8n^3 rN + 9rN\log_2 N + 2r^2 sn. \tag{5}$$

Если подставить сюда значения r и N, то увидим, что переменные $n, s, \log_{32}\alpha$ входят в слагаемые со старшими своими степенями в виде $n^5, s, (\log_{32}\alpha)^2$.

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. *Ноден П., Китте К.* Алгебраическая алгоритмика. М: Мир, 1999.

2. *Кнут Д.* Искусство программирования. т. 2. Получисленные алгоритмы. Издательский дом "Вильямс", 2004.

3. *Малашонок Г.И.* Матричные методы вычислений в коммутативных кольцах. Издательство ТГУ им. Г.Р. Державина, 2002.

Поступила в редакцию 20 ноября 2008 г.