УДК 519.688

ВЕРОЯТНОСТНЫЙ АЛГОРИТМ ВЫЧИСЛЕНИЯ ХАРАКТЕРИСТИЧЕСКОГО ПОЛИНОМА, ИМЕЮЩИЙ СЛОЖНОСТЬ МАТРИЧНОГО УМНОЖЕНИЯ

© **О.Н. Переславцева, О.О. Бобков**

Ключевые слова: характеристический полином, вероятностный алгоритм.

Рассматривается вероятностный алгоритм вычисления характеристического полинома в конечном поле, который предложили в 2007 г. К. Пернет и А. Сториоханн. Алгоритм имеет сложность матричного умножения. В работе проводится экспериментальное сравнение алгоритма Пернета-Сториоханна с алгоритмом Данилевского.

В работе [1] Клемент Пернет и Арне Сториоханн (2007) предложили вероятностный алгоритм вычисления характеристического полинома в конечном поле. Этот алгоритм является асимптотически лучшим в конечном поле, он требует выполнения $\Theta(n^\omega)$ операций в поле. Здесь $\Theta(n^\omega)$ обозначает сложность матричного умножения.

Пусть F — конечное поле, B_* обозначает любую квадратную матрицу, у которой только последний столбец может содержать ненулевые элементы, а остальные столбцы нулевые.

О п р е д е л е н и е 1. *Матрица* $\widetilde{A}^{[k]} \in F^{n\times n}$, *которая имеет вид*

$$\widetilde{A}^{[k]} = \begin{pmatrix} C_1 & B_* & \dots & B_* \\ B_* & C_2 & \dots & B_* \\ \vdots & \vdots & \ddots & \vdots \\ B_* & B_* & \dots & C_m \end{pmatrix},$$

где $C_i \in F^{k\times k}$, $i = 1,\dots,\lfloor n/k \rfloor$, *имеют форму Фробениуса, называется* k*-смещенной формой Хессенберга.*

Алгоритм вычисления характеристического полинома матрицы $A \in F^{n\times n}$ состоит из $n-1$ шага.

На k-м шаге матрица, имеющая $(k-1)$-смещенную форму Хессенберга, с помощью нормального преобразования Крылова приводится к k-смещенной форме Хессенберга, $k = 2,\dots,n$: $\widetilde{A}^{[k]} = K^{-1}\widetilde{A}^{[k-1]}K$, $\widetilde{A}^{[1]} = A$. Матрица K строится из единичной матрицы размера $n \times \lfloor n/k \rfloor$ сдвигом ki-того столбца единичной матрицы на 1 столбец, на освободившееся место записывается $(k-1)i$-ый столбец матрицы $\widetilde{A}^{[k-1]}$, $i = 1,\dots,\lfloor n/k \rfloor$.

Если матрица K на некотором шаге получилась вырожденной, то алгоритм заканчивается неудачей. Это существенный недостаток алгоритма по сравнению с детерминистскими алгоритмами (см.: [2]).

Если на шаге k полученную матрицу можно представить в виде $A^{[k]} = \left(\begin{array}{c|c} \overline{A} & B \\ \hline 0 & D \end{array}\right)$, то характеристический полином матрицы $A^{[k]}$ равен произведению характеристических

полиномов матриц $\overline{A}$ и D. При этом матрица $\overline{A}$ имеет вид k-смещенной формы Хессенберга, матрица D имеет вид формы Хессенберга. Характеристический полином матрицы $D \in F^{m\times m}, m < n$, вычисляется по формуле Хессенберга [3, с. 91]. Тогда на шаге $k+1$ принимаем $\widetilde{A}^{[k]} = \overline{A}$, размер которой будет меньше n.

Пример. Вычислим характеристический полином матрицы A в поле $F = \mathbb{Z}/29$,

$$A = \begin{pmatrix} 1 & 8 & 2 & 8 & 7 & 1 \\ 12 & 1 & 5 & 2 & 4 & 5 \\ 2 & 1 & 8 & 7 & 9 & 9 \\ 2 & 1 & 3 & 4 & 6 & 7 \\ 5 & 2 & 1 & 4 & 6 & 1 \\ 0 & 2 & 0 & 7 & 27 & 1 \end{pmatrix}.$$

Шаг k=2; $K = \begin{pmatrix} 1 & 1 & 0 & 8 & 0 & 2 \\ 0 & 12 & 1 & 1 & 0 & 5 \\ 0 & 2 & 0 & 1 & 1 & 8 \\ 0 & 2 & 0 & 1 & 0 & 3 \\ 0 & 5 & 0 & 2 & 0 & 1 \\ 0 & 0 & 0 & 2 & 0 & 0 \end{pmatrix}$, $A^{[2]} = \begin{pmatrix} 0 & -23 & 0 & -4 & 0 & -3 \\ 1 & -14 & 0 & 10 & 0 & 0 \\ 0 & 5 & 0 & 22 & 0 & 23 \\ 0 & 14 & 1 & 18 & 0 & 0 \\ 0 & -2 & 0 & -2 & 0 & -4 \\ 0 & -5 & 0 & -25 & 1 & 17 \end{pmatrix}$.

Шаг k=3; $K = \begin{pmatrix} 1 & 0 & -23 & 0 & 0 & -4 \\ 0 & 1 & -14 & 0 & 0 & 10 \\ 0 & 0 & 5 & 1 & 0 & 22 \\ 0 & 0 & 14 & 0 & 1 & 18 \\ 0 & 0 & -2 & 0 & 0 & -2 \\ 0 & 0 & -5 & 0 & 0 & -25 \end{pmatrix}$, $A^{[3]} = \begin{pmatrix} 0 & 0 & -16 & 0 & 0 & -26 \\ 1 & 0 & -20 & 0 & 0 & 9 \\ 0 & 1 & 17 & 0 & 0 & 3 \\ 0 & 0 & 23 & 0 & 0 & 0 \\ 0 & 0 & -10 & 1 & 0 & -5 \\ 0 & 0 & 2 & 0 & 1 & 4 \end{pmatrix}$.

Шаг k=4; $K = \begin{pmatrix} 1 & 0 & 0 & -16 & 0 & 0 \\ 0 & 1 & 0 & -20 & 0 & 0 \\ 0 & 0 & 1 & 17 & 0 & 0 \\ 0 & 0 & 0 & 23 & 1 & 0 \\ 0 & 0 & 0 & -10 & 0 & 1 \\ 0 & 0 & 0 & 2 & 0 & 0 \end{pmatrix}$, $A^{[4]} = \begin{pmatrix} 0 & 0 & 0 & -10 & 0 & -21 \\ 1 & 0 & 0 & 11 & 0 & -19 \\ 0 & 1 & 0 & 3 & 0 & 6 \\ 0 & 0 & -28 & -13 & 0 & -14 \\ 0 & 0 & 0 & 23 & 0 & -26 \\ 0 & 0 & 0 & 3 & -28 & -24 \end{pmatrix}$.

Шаг k=5; $K = \begin{pmatrix} 1 & 0 & 0 & 0 & -10 & 0 \\ 0 & 1 & 0 & 0 & 11 & 0 \\ 0 & 0 & 1 & 0 & 3 & 0 \\ 0 & 0 & 0 & 1 & -13 & 0 \\ 0 & 0 & 0 & 0 & 23 & 1 \\ 0 & 0 & 0 & 0 & 3 & 0 \end{pmatrix}$, $A^{[5]} = \begin{pmatrix} 0 & 0 & 0 & 0 & -4 & -16 \\ 1 & 0 & 0 & 0 & 16 & 6 \\ 0 & 1 & 0 & 0 & 20 & 28 \\ 0 & 0 & -28 & 0 & 0 & -15 \\ 0 & 0 & 0 & 1 & -10 & -19 \\ 0 & 0 & 0 & 0 & -2 & -27 \end{pmatrix}$.

Шаг k=6; $K = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & -4 \\ 0 & 1 & 0 & 0 & 0 & 16 \\ 0 & 0 & 1 & 0 & 0 & 20 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -10 \\ 0 & 0 & 0 & 0 & 0 & -2 \end{pmatrix}$, $A^{[6]} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 11 \\ 1 & 0 & 0 & 0 & 0 & -19 \\ 0 & 1 & 0 & 0 & 0 & 7 \\ 0 & 0 & -28 & 0 & 0 & -8 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -28 & 21 \end{pmatrix}$.

Характеристический полином матрицы A равен $x^6 + 8x^5 + 0x^4 + 8x^3 - 7x^2 - 10x - 11$.

В работе [4] как наиболее эффективный способ точного вычисления характеристического многочлена матриц над конечными полями рекомендуется метод Данилевского [5].

Были проведены эксперименты, в которых использовались разреженные матрицы для алгоритма Пернета-Сториоханна и плотные матрицы для алгоритма Данилевского.

Эксперименты проводились на суперкомпьютере МВС-100К Межведомственного суперкомпьютерного центра РАН. Объем оперативной памяти составлял 8 Гб.

Результаты экспериментов приведены в табл. 1.

Таблица 1

Зависимость времени вычисления характеристических полиномов алгоритма Данилевского (t_D ,с) и алгоритма Пернета-Сториоханна (t_{PS} ,с) от размера матрицы n

n	500	750	1000	1250	1500	1750	2000	2250	2500	3000
t_{PS}	68	214	483	951	1576	2439	3606	5339	8235	18272
t_D	13	45	111	226	414	633	1030	1529	2383	4559
$\frac{t_{PS}}{t_D}$	5	5	4,3	4	3,9	3,8	3,6	3,5	3.5	4

Сравнение алгоритмов показывает, что алгоритм Пернета-Сториоханна требует в 3-5 раз больше операций, чем алгоритм Данилевского.

Так как в вычислениях в алгоритме Пернета-Сториоханна участвуют не все элементы матриц, а определенные столбцы, то мы предполагаем в дальнейшем разработать алгоритм, в котором вычисления будут проводиться только с плотными блоками, размер которых в несколько раз меньше размера исходной матрицы. Для этого случая можно применить алгоритмы быстрого умножения матриц.

ЛИТЕРАТУРА

1. *Pernet C., Storjohann A.* Faster Algorithms for the Characteristic Poynomial // ISSAC'07, July 29-August 1, 2007.

2. *Переславцева О.Н.* О вычислении характеристического полинома матрицы // Дискретная математика. Тамбов, 2011. Т. 23. Вып. 1. С. 28-45.

3. *Малашонок Г.И.* Матричные методы вычислений в коммутативных кольцах. Тамбов: Изд-во Тамбовского университета, 2002.

4. *Икрамов Х.Д.* О конечных спектральных процедурах в линейной алгебре // Программирование. 1994. № 1. С. 56-69.

5. *Данилевский А.М.* О численном решении векового уравнения // Матем. сб. 1937. Т. 2(44). № 1. С. 169-172.

БЛАГОДАРНОСТИ: Работа выполнена при поддержке гранта РФФИ № 12-07-00755-а.

Поступила в редакцию 20 декабря 2012 г.

Pereslavtseva O.N., Bobkov O.O. RANDOMIZED ALGORITHM FOR THE CHARACTERISTIC POYNOMIAL.

Randomized Pernet-Storjohann's algorithm for characteristic polynomials of matrix in a finite field is considered. The algorithm has the best asymptotic complexity in the finite field. We are discussed results of experiments with this algorithm.

Key words: characteristic polynomial, randomized algorithm.