Вычисление характеристических полиномов плотных матриц: последовательные и параллельные алгоритмы

Переславцева О.Н.

Семинар «Компьютерная алгебра»
факультета ВМК МГУ и ВЦ РАН

29 августа 2012

Цель и задачи исследования

Цель работы:
Разработка эффективных алгоритмов для вычисления характеристических полиномов матриц в многопроцессорных вычислительных системах.

Задачи работы:

- получение выражений, характеризующих сложность известных алгоритмов вычисления характеристических полиномов матриц;
- разработка эффективного алгоритма для вычисления характеристических полиномов матриц в коммутативных кольцах;
- разработка алгоритмов и программ для вычисления характеристических полиномов целочисленных матриц и полиномиальных матриц;
- разработка алгоритмов и программ для параллельного вычисления характеристических полиномов целочисленных и полиномиальных матриц;
- экспериментальное исследование эффективности полученных алгоритмов и программ.

Содержание

1.1 Методы вычисления характеристических полиномов в коммутативных кольцах. Выражения для количества кольцевых операций

Метод	**Количество операций**		
	сложения	**умножения**	**сокращения**
Метод Леверье	$\sim n^4$	$\sim n^4$	$n-1$
Метод Леверье-Фаддеева	$\sim n^4$	$\sim n^4$	$n-1$
Алгоритм Чистова	$\sim 1/3n^4$	$\sim 1/3n^4$	
Алгоритм Берковича	$\sim 1/4n^4$	$\sim 1/4n^4$	
Алгоритм Сейфуллина	$\sim 1/4n^4$	$\sim 1/4n^4$	
Метод Леверье-Винограда	$\sim n^{3.5}$	$\sim n^{3.5}$	$n-1$
Алгоритм Малашонка	$\sim 4/3n^3$	$\sim n^3$	$\sim 1/3n^3$
Новый алгоритм	$\sim 4/3n^3$	$\sim n^3$	$\sim 1/2n^2$

Таблица 1. Выражения для количества кольцевых операций при вычислении характеристического полинома матрицы порядка n.

1.2 Новый алгоритм

$A = \left(a_j^i\right)$ — квадратная матрица порядка n.
$A = BD$, B — квазитреугольная матрица, D — диагональная матрица.

1. Вычисление матриц B и D

2.Вычисление характеристического полинома матрицы A
- $d^n = \det(xD - B)$ по формуле Хессенберга:
$d^n = b_{nn}d^{n-1} + \sum_{i=1}^{n-1} b_{in}\left(\prod_{j=i+1}^{n}(-b_{jj-1})\right)d^{i-1}$, где $d^0 = 1$,
$xD - B = (b_{ij}),\ i,j = 1,\ldots,n$.
- $F(x) = (-1)^n \det(xD - B)/\det(D)$.

$\sim 7/3n^3$ кольцевых операций.

2.1 Сложность алгоритмов, выраженная в числе машинных операций умножения

Обозначим через φ_b количество машинных слов, необходимых для записи числа b. $\varphi_{bc} = \varphi_b + \varphi_c$.
Пусть A — квадратная матрица порядка n.
Будем считать, что элементы матрицы A – содержат k слов.

Метод	**Число машинных операций умножения для** $\mathbb{Z}^{n\times n}$
Метод Леверье	$\sim \frac{k}{2}(k+\varphi_n)n^{4.81}$
Метод Леверье-Винограда	$\sim \frac{k}{2}(k+\varphi_n)n^{4.81}$
Метод Леверье-Фаддеева	$\sim \frac{k}{2}(k+\varphi_n)n^{4.81}$
Алгоритм Сейфуллина	$\sim \frac{k}{10}(k+\varphi_n)n^{5}$
Алгоритм Берковича	$\sim \frac{1}{120}(13k^2+14k\varphi_n+\varphi_n^2)n^{5}$
Алгоритм Чистова	$\sim \frac{k}{96}(19k+3\varphi_n)n^{5}$
Алгоритм Малашонка	$\sim$ экспонента
Новый алгоритм	$\sim$ экспонента

Таблица 2. Выражения для количества мультипликативных операций в словах.

2.1 Сложность алгоритмов, выраженная в числе машинных операций умножения

n	Алгоритм Берковича	Алгоритм Чистова	Метод Леверье-Винограда	Метод Леверье-Фаддеева
30	90%	160%	510%	540%
40	95%	160%	510%	520%
50	99%	170%	510%	520%
60	98%	170%	500%	500%
70	99%	170%	510%	500%
80	104%	180%	550%	510%
90	101%	180%	530%	510%
100	103%	180%	550%	520%
Теоретические оценки	110%	200%	500%	500%

Таблица 3. Время вычисления характеристического полинома с использованием алгоритмов Берковича, Чистова, Леверье-Винограда, Леверье-Фаддеева по отношению к алгоритму Сейфуллина (%).

В экспериментах использовались плотные матрицы над целыми числами длиной 50 бит, которые выбирались случайным образом, n — порядок матрицы.

2.2 Применение метода гомоморфных образов для вычисления характеристических полиномов матриц в кольце целых чисел

Пусть A — данная матрица.

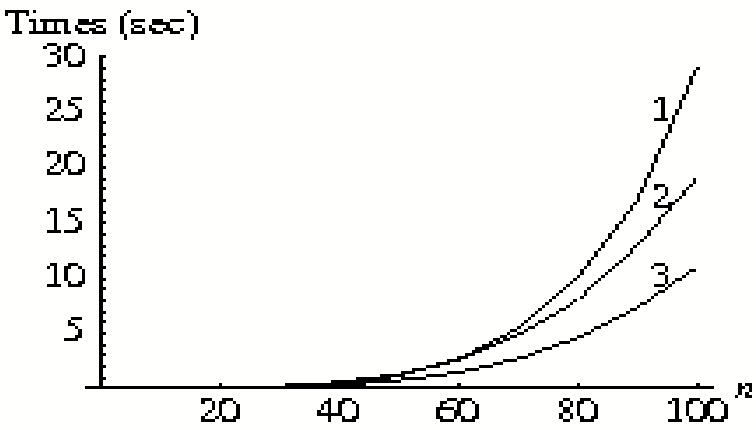
1. Выберем m простых чисел $p_1, \ldots, p_m$.

2. Перейдем к гомоморфным образам $\mathbb{Z} \to \mathbb{Z}/p_i = \mathbb{Z}_{p_i}$.

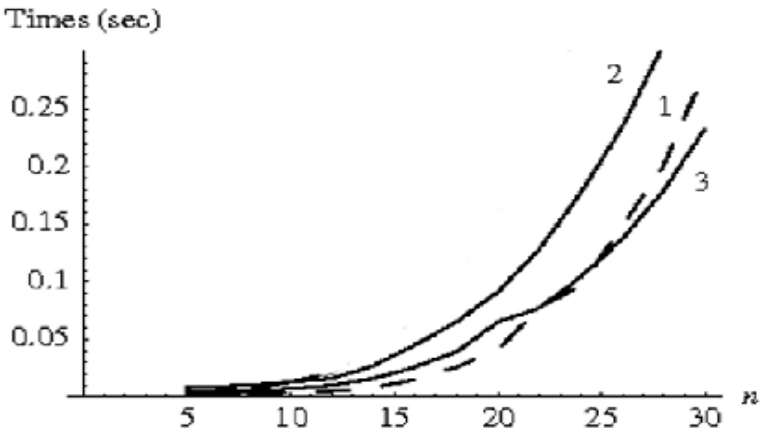
3. Будем вычислять m характеристических полиномов $f_1(x), \ldots, f_m(x)$ для матриц $M_i \in \mathbb{Z}_{p_i}^{n \times n}$, $1 \leq i \leq m$.

4. Восстановим коэффициенты полиномов $f_1(x), \ldots, f_m(x)$ по числовым модулям $p_1, \ldots, p_m$ в полином $F(x)$, который является характеристическим полиномом данной матрицы A.

2.3 Экспериментальное сравнение алгоритмов в кольце целых чисел



$40 < n < 100$, $k = 20$ бит.



$5 < n < 30$, $k = 50$ бит.

Рис. 1. Время вычисления характеристического полинома с использованием алгоритма Сейфуллина (1), алгоритмов, основанных на методе гомоморфных образов, в которых в конечном поле используются новый алгоритм (2) и алгоритм Данилевского (3)

2.3 Экспериментальное сравнение алгоритмов в кольце целых чисел

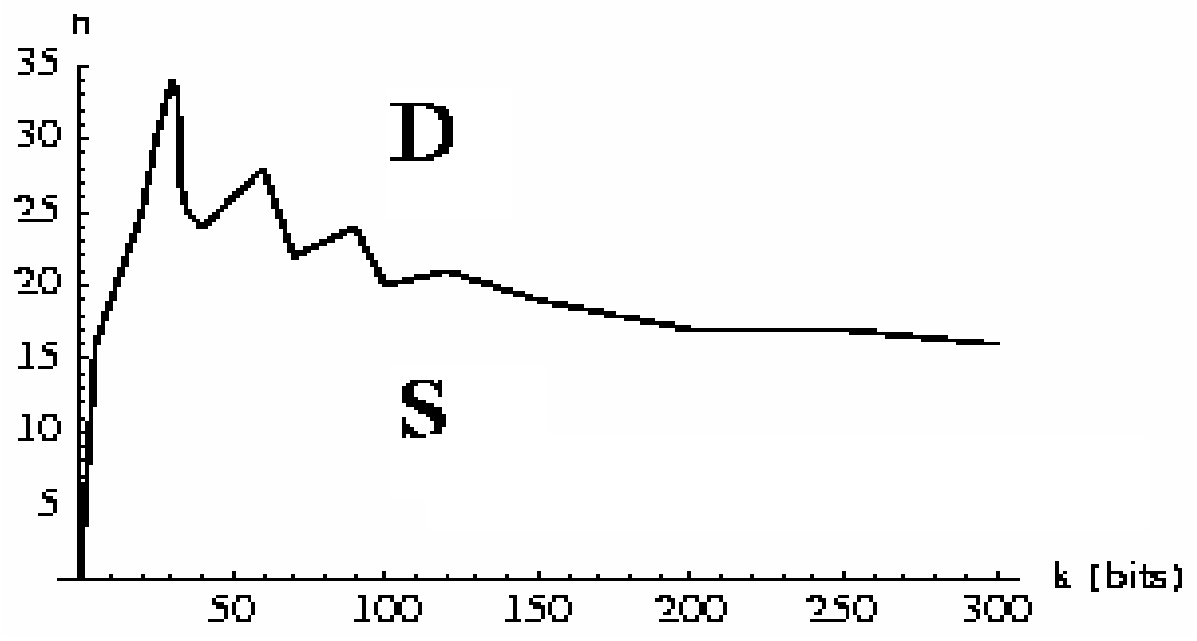


Рис. 3. Граничная линия, разделяющая плоскость на две области S и D. В области S под линией лежат матрицы, для которых время вычисления алгоритма Сейфуллина наименьшее, а в области D над линией лежат матрицы, для которых время вычисления алгоритма, основанного на методе гомоморфных образов, наименьшее. k – разрядность коэффициентов матрицы, n – порядок матрицы.

2.3 Экспериментальное сравнение алгоритмов в кольце целых чисел

n	(1)	(2)	(3)	(4)
20	0.14	0.05	0.03	0.01
40	2.5	1.2	0.3	0.2
60	12.8	8.6	1.4	0.8
80	41.7	33.6	4.5	2.5
100	105.2	99.6	10.6	6.0
200	2048	3192	172	102

Таблица 4. Время (с) вычисления характеристического полинома с использованием алгоритмов, реализованных в системах
(1) Maple 9.5,
(2) Mathematica 7.0,
(3) алгоритма, основанного на методе гомоморфных образов, в котором в конечном поле используется новый алгоритм,
(4) алгоритма, основанного на методе гомоморфных образов, в котором в конечном поле используется алгоритм Данилевского.

$k = 7$ бит.

2.4 Вычисление характеристических полиномов полиномиальных матриц

Пусть $A \in \mathbb{Z}^{n\times n}[(x_1, \ldots, x_t]$ — данная матрица, m_s — старшая степень переменной x_s у коэффициентов характеристического полинома, $1 \le s \le t$.

1. Выберем
   k простых чисел $p_1, \ldots, p_k$,
   полиномы $x_t, x_t - 1, \ldots, x_t - (m_t - 1)$,
   полиномы $x_{t-1}, x_{t-1} - 1, \ldots, x_{t-1} - (m_{t-1} - 1)$,
   $\ldots$,
   полиномы $x_1, x_1 - 1, \ldots, x_1 - (m_1 - 1)$.
2. Перейдем к гомоморфным образам $\mathbb{Z}[x_1, \ldots, x_t] \to \mathbb{Z}[x_1, \ldots, x_t]/p_i \to (\mathbb{Z}[x_1, \ldots, x_t]/p_i)/(x_t - j) \to ((\mathbb{Z}[x_1, \ldots, x_t]/p_i)/(x_t - j))/(x_{t-1} - q) \to \ldots \to (((\mathbb{Z}[x_1, \ldots, x_t]/p_i)/(x_t - j))/(x_{t-1} - q)/\ldots)/(x_1 - s) \cong \mathbb{Z}/p_i$.
3. Будем вычислять $km_t m_{t-1} \cdots m_1$ характеристических полиномов для матриц из $\mathbb{Z}_{p_i}^{n\times n}$, $1 \le i \le m$.
4. Восстановим коэффициенты полученных полиномов по полиномиальным и числовым модулям в полином, который является характеристическим полиномом данной матрицы A.

2.5.2 Оценка коэффициентов характеристического полинома полиномиальной матрицы

Обозначим через $||f||$ — наибольший по модулю числовой коэффициент этого полинома, $s(f)$ — количество мономов в полиноме f.
Пусть $A = (a_{ij}(x)),\ 1 \le i \le n,\ 1 \le j \le n$ – исходная матрица полиномов,
$d = max\{\deg a_{ij}(x)\}$,
$||A|| = max\{||a_{ij}||\} = a$ для $1 \le i \le n,\ 1 \le j \le n$;
$s(A) = max\{s(a_{ij}(x))\} = t$.

Theorem

Пусть

$$F(x, y) = y^n + f_1(x)y^{n-1} + \cdots + f_n(x) -$$

характеристический полином матрицы $A(x)$ *и*
$m = \max\{\deg f_1(x), \ldots, \deg f_n(x)\} + 1$.
Тогда $m \le n \cdot d + 1$ *и для наибольшего по модулю числового коэффициента полинома* $F(x, y)$ *выполняется неравенство*

$$\log_2 ||F(x, y)|| \le n(\log_2 n + \log_2 a + \log_2 t) - \log_2 t. \qquad (1)$$

2.5.3 Алгоритм, основанный на методе гомоморфных образов

INPUT: $A \in Z^{n\times n}[x_1, \ldots, x_t]$;

$intervals = \{(b_1, e_1), (b_2, e_2), .., (b_t, e_t), (m_b, m_e)\}$;

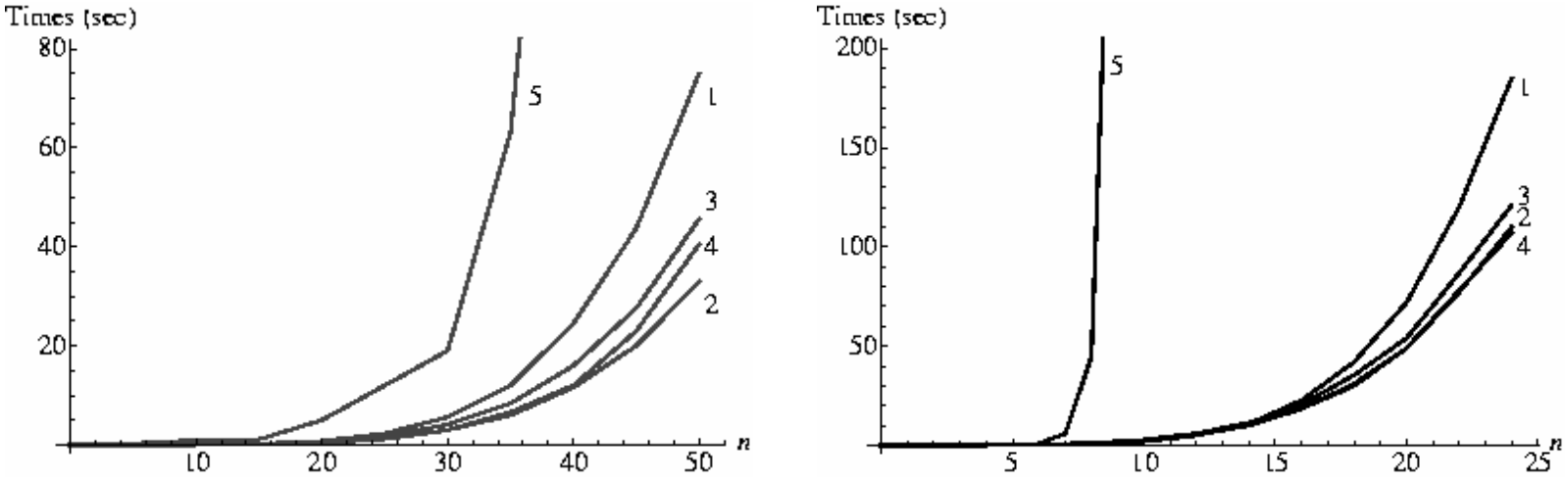
$number\ r,\ r < 2(1 + t)$;

OUTPUT: $f \in Z[x_1, \ldots, x_j, y],\ j = r/2 + 1$.

```
charPol(A, intervals, r){
    if(r < 0){
        M = matrixMod(A, intervals);
        f = charPolDanilevsky(M); }
    else{
        s = ⌊(intervals[r] + intervals[r + 1])/2⌋;
        intervals1 = intervals;  r1 = r;
        intervals2 = intervals;  r2 = r;
        intervals1[r + 1] = s;
        intervals2[r] = s;
        if (s == intervals1[r] + 1) r1− = 2;
        if (s == intervals2[r + 1] − 1) r2− = 2;
        f1 = charPol(A, intervals1, r1);
        f2 = charPol(A, intervals2, r2);
        f = recoveryNewton(f1, f2, r1, r2);
```

2.5.4 Вычислительные эксперименты

В экспериментах использовались плотные полиномиальные матрицы от одной переменной. Рассматривались плотные полиномы степени $d = 1$ и $d = 15$, коэффициенты полиномов длиной 20 бит выбирались случайным образом.



$d = 1$ $d = 15$

Рис. 3. Время вычисления характеристического полинома с использованием алгоритма Сейфуллина (1), алгоритмов, основанных на методе гомоморфных образов, в которых в конечном поле используются алгоритм Данилевского (2), новый алгоритм (3) и алгоритм Леверье (4), и алгоритма, реализованного в системе Mathematica 7.0 (5)

3. Параллельный алгоритм вычисления характеристических полиномов

Пусть k — количество процессоров кластера с номерами $0,\ 1,\ 2, \ldots,\ (k-1)$ и на нулевом процессоре имеется исходная матрица $A \in \mathbb{Z}^{n \times n}[x_1, \ldots, x_t]$.
Пусть множество M, которое содержит необходимый список простых чисел, имеется на каждом процессоре.
Параллельный алгоритм вычисления характеристического полинома матрицы состоит из четырех этапов.

Этап 1. Вычисление количества модулей.

Этап 2. Решение задачи в гомоморфных образах в конечном поле.

Этап 3. Восстановление элементов характеристического полинома матрицы в исходное кольцо.

Этап 4. Сбор результата на нулевом процессоре.

3. Параллельный алгоритм вычисления характеристических полиномов

Этап 1. Вычисление количества модулей.

- Нулевой процессор находит верхнюю оценку наибольшего по абсолютной величине числового коэффициента элементов характеристического полинома матрицы и верхние оценки наибольших степеней элементов характеристического полинома матрицы по каждой переменной.
- По найденным оценкам и множеству числовых модулей M вычисляется необходимое для данной задачи число числовых и полиномиальных по каждой переменной модулей.
- Затем производится рассылка исходной матрицы и количества модулей на все процессоры.

3. Параллельный алгоритм вычисления характеристических полиномов

Этап 2. Решение задачи в гомоморфных образах в конечном поле.

- Каждый из процессоров по количеству модулей вычисляет число r — общее количество точек.
- Каждый из процессоров выполняет вычисление характеристического полинома матрицы в конечном поле в $\left\lfloor \frac{r}{k} \right\rfloor + 1$ или в $\left\lfloor \frac{r}{k} \right\rfloor$ точках.

  В результате вычислений на каждом процессоре имеется массив полиномов с элементами из конечного поля.

3. Параллельный алгоритм вычисления характеристических полиномов

Этап 3. Восстановление элементов характеристического полинома матрицы в исходное кольцо.

- На всех процессорах каждый из полученных полиномов разбивается на k частей, которые содержат приблизительно одинаковое количество мономов. Причём, j-я часть одного полинома содержит мономы тех же степеней, что и j-я часть другого полинома, $j = 0, \ldots, n-1$. Для $j \neq i$ мономы, содержащиеся в j-й части любого полинома, имеют степени переменных, отличные от какого-либо монома, содержащегося в i-й части.
- Процессоры обмениваются полученными частями полиномов так, что i-й процессор получает все i-е части полиномов, $i = 0, \ldots, n-1$.
- Каждый процессор восстанавливает полученные полиномы в один полином.

3. Параллельный алгоритм вычисления характеристических полиномов

Этап 4. Сбор результата на нулевом процессоре.

- После восстановления каждый процессор посылает свой результат нулевому процессору.
- Затем нулевой процессор объединяет полученные данные в искомый характеристический полином матрицы.

Основные результаты

- Получены теоретические выражения, характеризующие сложность алгоритмов вычислений характеристических полиномов матриц, которые дают возможность выбирать лучший алгоритм.
- Разработан эффективный алгоритм для вычисления характеристических полиномов матриц в коммутативных кольцах.
- Разработаны алгоритмы и программы для вычисления характеристических полиномов целочисленных и полиномиальных матриц. Выделены области параметров входных данных и указаны лучшие алгоритмы в этих областях.
- Разработан параллельный алгоритм вычисления характеристических полиномов матриц.

Публикации

Статьи в изданиях по перечню ВАК:

1. Переславцева О.Н. О вычислении коэффициентов характеристического полинома. Вычислительные методы и программирование: новые вычислительные технологии. 2008. Т.9. №1. С. 366-370. (http://num-meth.sr.cc.msu.ru)
2. Переславцева О.Н. О вычислении характеристического полинома матрицы // Дискретная математика. Т. 23, вып. 1, 2011, с. 28-45. (Pereslavtseva O.N. Calculation of the characteristic polynomial of a matrix // Discrete Mathematics and Applications. Volume 21, Issue 1, 2011. P. 109-129.)
3. Переславцева О.Н. Вычислительные эксперименты с алгоритмами вычисления характеристических полиномов матриц // Вестник Тамбовского Университета. Серия: Естественные и технические науки. 2007. Т. 12. Вып.1. С.126-128.
4. Переславцева О.Н. Об оценке коэффициентов характеристического полинома // Вестник Тамбовского Университета. Серия: Естественные и технические науки. 2008. Т. 13. Вып.1. С.124-125.
5. Переславцева О.Н. Метод вычисления характеристического полинома матрицы // Вестник Тамбовского Университета. Серия: Естественные и технические науки. 2008. Т. 13. Вып.1. С.131-133.

6. Переславцева О.Н. Вычисление характеристического полинома для полиномиальных матриц // Вестник Тамбовского университета. Сер. Естественные и технические науки. Том 14, вып. 1, 2009. С.274-277.
7. Переславцева О.Н. Распараллеливание алгоритмов с применением китайской теоремы об остатках // Вестник Тамбовского университета. Сер. Естественные и технические науки. Том 14, вып. 4, 2009. С.779-781.
8. Переславцева О.Н. Параллельный алгоритм вычисления характеристических полиномов матриц, основанный на методе гомоморфных образов // Вестник Тамбовского университета. Сер. Естественные и технические науки. Том 15, вып. 4, 2010. С. 1413-1425.
9. Переславцева О.Н. Эксперименты с параллельным алгоритмом вычисления характеристических полиномов матриц в кольце полиномов // Вестник Тамбовского университета. Сер. Естественные и технические науки. Том 15, вып. 1, 2010. С. 346-349.
10. Переславцева О.Н. Параллельный модулярный алгоритм вычисления характеристического полинома матрицы в кольце полиномов многих переменных // Вестник Тамбовского университета. Сер. Естественные и технические науки. Том 17, вып. 2, 2012.

Прочие публикации:

11. Переславцева О.Н. Оценка числа бит-умножений в алгоритмах вычисления определителя, характеристического полинома и присоединённой матрицы //XI Державинские чтения. Тамбов.– 2006.– С. 79-83.

12. Переславцева О.Н. История и современное состояние теории алгоритмов вычисления характеристического полинома матрицы // Международная научная конференция «Современное математическое образование и проблемы истории и методологии математики». Тамбов: Изд-во Першина Р.В. – 2006.– С.130-134.

13. Переславцева О.Н. Вычисление характеристического полинома в кольце целых чисел // International Conference Polynomial Computer Algebra. С.-Петербург. 2008. 57-61.

14. Переславцева О.Н. Об алгоритмах вычисления характеристического полинома матрицы в кольце целых чисел// Международная научная конференция «Современное математическое образование и проблемы истории и методологии математики». Тамбов.– 2008.– С.196-198.

15. Малашонок Г.И., Переславцева О.Н., Сажнева О.А., Старов М.В. Алгоритмы компьютерной алгебры. Часть 1. Учебное пособие. Тамбов: Издательский дом ТГУ им. Г.Р. Державина, 2008.

16. Переславцева О.Н. Параллельное вычисление характеристического полинома матрицы // Параллельные вычислительные технологии (ПаВТ'2009): Труды международной научной конференции (Нижний Новгород, 30 марта – 3 апреля 2009 г.). – Челябинск: Изд. ЮУрГУ, 2009. – С. 817-821.

17. Переславцева О.Н. Вычисление характеристических полиномов матриц в кольце полиномов // International Conference Polynomial Computer Algebra. С.-Петербург. 2009. 35-39.

18. Переславцева О.Н. Вычисление характеристических полиномов матриц: последовательные и параллельные алгоритмы. Mathematical Modeling and Computational Physics (MMCP'2009): Book of Abstracts of the International Conference (Dubna, July 7-11, 2009). - Dubna: JINR, 2009. P. 130-131.

19. Малашонок Г.И., Старов М.В., Бетин А.А., Переславцева О.Н., Поздникин А.Г. Параллельная компьютерная алгебра. Часть 1. Учебное пособие. Тамбов: Издательский дом ТГУ им. Г.Р. Державина, 2010.

20. Pereslavtseva O. Parallel algorithm for computing characteristic polynomials of polynomial matrices and experiments // International Conference Polynomial Computer Algebra. С.-Петербург. 2011. 105-108.
21. Pereslavtseva O. Parallel algorithm for computing characteristic polynomials of polynomial matrices // International Conference Polynomial Computer Algebra. С.-Петербург. 2012. P. 67-69.