Computing Characteristic Polynomials of Matrices of Structured Polynomials

Marshall Law & Michael Monagan, Department of Mathematics, Simon Fraser University, Burnaby, Canada
mylaw@sfu.ca & mmonagan@cecm.sfu.ca

SFU

Objective

Compute the characteristic polynomial

$$C(\lambda, x, y) = \det(A(x,y) - \lambda I_n) \in \mathbb{Z}[\lambda, x, y]$$

for specific structured matrices $A(x,y) \in \mathbb{Z}^{n\times n}$ from [5]. Size $n \in \{16, 32, 64, 128, 256\}$ and

$$A_{ij} = c_{ij}x^a y^b, \text{ for } a, b, \in \mathbb{N}\cup\{0\}, c_{ij} \in \mathbb{Z}.$$

Matrix: 16×16

$$\begin{bmatrix} x^8 & x^5y & x^5y & x^4y^2 & x^5y & \cdots & x^3y^3 & x^4y^4 \\ x^7 & x^6y & x^4y & x^5y^2 & x^4y & \cdots & x^2y^3 & x^5y^4 \\ x^7 & x^4y & x^6y & x^5y^2 & x^4y & \cdots & x^4y^3 & x^5y^4 \\ x^6 & x^5y & x^5y & x^6y^2 & x^3y & \cdots & x^3y^3 & x^6y^4 \\ x^7 & x^4y & x^4y & x^3y^2 & x^6y & \cdots & x^4y^3 & x^5y^4 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ x^5 & x^2y & x^4y & x^3y^2 & x^4y & \cdots & x^6y^3 & x^7y^4 \\ x^4 & x^3y & x^3y & x^4y^2 & x^3y & \cdots & x^5y^3 & x^8y^4 \end{bmatrix}$$

Magma

- Bareiss fraction-free algorithm [1].
- Modification of Gaussian elimination based on Sylvester's identity.
- $O(n^3)$ arithmetic operations in $\mathbb{Z}[\lambda, x, y]$ with exact divisions.

Maple

- Berkowitz algorithm [2].
- $O(n^4)$ arithmetic operations in ring $\mathbb{Z}[x,y]$ with no divisions.

Hessenberg Algorithm

- Hessenberg [3] form:

$$\begin{bmatrix} h_{1,1} & h_{1,2} & h_{1,3} & \cdots & h_{1,n} \\ k_2 & h_{2,2} & h_{2,3} & \cdots & h_{2,n} \\ 0 & k_3 & h_{3,3} & \cdots & h_{3,n} \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \ldots & 0 & k_n & h_{n,n} \end{bmatrix}$$

- Recurrence relation, $C_0(x) = 1$: $C_m(x) = (x - h_{m,m})C_{m-1}(x) - \sum_{i=1}^{m-1}(h_{i,m}C_{i-1}(x)\prod_{j=i+1}^{m} k_i)$
- $O(n^3)$ field operations.

Parallel Modular Alg.

Figure 1: Modular algorithm [4] homomorphism diagram. (CRA for Chinese Remainder Algorithm)

$$\begin{tikzcd} \mathbb{Z}^{n\times n}[x,y] \arrow[rr, "\text{Characteristic Polynomial}"] \arrow[d, "\text{Mod } p \in \{p_1, p_2, \ldots, p_m\}"'] & & \mathbb{Z}[\lambda, x, y] \\ \mathbb{Z}_p^{n\times n}[x,y] \arrow[d, "\text{Evaluate } x = \alpha_i,\ y = \beta_j"'] & & \mathbb{Z}_p[\lambda, x, y] \arrow[u, "\text{CRA}"'] \\ \mathbb{Z}_p^{n\times n} \arrow[rr, "\text{Hessenberg Algorithm mod } p", "O(n^3) \text{ arithmetic operations in } \mathbb{Z}_p"'] & & \mathbb{Z}_p[\lambda] \arrow[u, "\text{Interpolate } y, x"'] \end{tikzcd}$$

Structures

$$C(\lambda, x, y) = \sum_{i=0}^{n} c_i(x,y)\lambda^i$$

$$c_i(x,y) = x^{f_i}y^{g_i}(x^2-1)^{h_i}s_i(x,y)$$

$n = 16$:

$$c_0(x,y) = x^{32}y^{32}(x^2-1)^{32}$$

$$c_1(x,y) = x^{32}y^{28}(x^2-1)^{28}s_1(x,y)$$

$$s_1(x,y) = -(2x^4y^2 + 4x^2y^3 + 4x^2y^2 + y^4 + 4x^2y + 1)$$

Table 1: $n = 16$ Parameters

i	f_i	g_i	h_i	$\deg_{x}$ s_i	$\deg_{y}$ s_i	$\lVert s_i\rVert_\infty$	$\lVert c_i\rVert_\infty$
0	32	32	32	0	0	1	601080390
1	32	28	28	4	4	4	160466400
2	24	25	25	14	6	31	28428920
3	26	22	22	12	8	128	16535016
4	20	19	19	18	10	382	3868248
5	22	16	16	16	12	684	946816
6	16	14	14	20	12	1948	183648
7	18	12	12	16	12	3738	82492
8	12	10	10	20	12	4730	35264
9	14	8	8	16	12	3740	10876
10	8	6	6	20	12	2116	3242
11	10	4	4	16	12	806	1556
12	4	3	3	18	10	454	322
13	6	2	2	12	8	142	108
14	0	1	1	14	6	31	22
15	4	0	0	4	4	4	4

Query

Random $1 < \gamma < p$, compute for $0 \le i < n$ ($\bullet \in \mathbb{Z}_p$):

$$C(\lambda, x, \gamma) \pmod p = \bullet x^{\bar{f}_i} + \cdots + \bullet x^{f_i}$$

$$C(\lambda, \gamma, y) \pmod p = \bullet y^{\bar{g}_i} + \cdots + \bullet y^{g_i}$$

$$\Pr(\bar{f}_i, f_i, \bar{g}_i, g_i \text{ is wrong}) = \frac{2(256)(4096)}{2^{31}-1} < 0.1\%$$

Naive number of points ($n = 16$):

$$e_x := \deg_x C(\lambda, x, y) + 1 = 96 + 1$$

$$e_y := \deg_y C(\lambda, x, y) + 1 = 32 + 1$$

By taking advantage of the largest and smallest degrees, factors and even degrees (in x), the number of required points is reduced only to recover $s_i(x,y)$.

Savings:

$$n = 16 : (97)(33) = 3201 \Rightarrow (11)(13) = 143$$
$$n = 32 : (209)(81) = 16929 \Rightarrow 868$$
$$n = 64 : (577)(193) = 111361 \Rightarrow 4087$$
$$n = 128 : (1217)(449) = 546433 \Rightarrow 18471$$
$$n = 256 : (3073)(1025) = 3149825 \Rightarrow 73341$$

Integer Bound

Hadamard-type bound [6] on the integers size of the determinant of matrix with polynomial entries:

$$\lVert C(\lambda, x, y)\rVert_\infty \le \prod_{i=1}^{n}\sqrt{\sum_{j=1}^{n} t_{ij}^2}$$

where $t_{ij} = \lVert A_{ij}\rVert_1$.
For our matrices $t_{ii} = 2$ and $t_{ij} = 1$ for $i \ne j$, so

$$\lVert C(\lambda, x, y)\rVert_\infty \le (n+3)^{n/2}.$$

It gives $\lVert C(\lambda, x, y)\rVert_\infty \le \{34, 83, 195, 451, 1027\}$ (in bits) for $n \in \{16, 32, 64, 128, 256\}$ respectively.

Mixed Radix CRA

$$u \equiv c_i \pmod{p_i} \quad \text{for } 1 \le i \le m$$

$$u = v_1 + v_2p_1 + v_3p_1p_2 + \cdots + v_mp_1p_2\ldots p_{m-1}$$

Solve in the symmetric range $\frac{-p_i}{2} < v_i < \frac{p_i}{2}$, and terminate early if $v_j = 0$ for some $1 < j < m$.

Table 2: Benchmarks

Timings on Intel Core i7-3930K six core at 3.2 GHz (3.8 GHz turbo) with 64 GB RAM.

Size	#points		#primes		Time	
n	x	y	actual	bound	1 core	6 cores
16	11	13	1	2	0.04s	0.01s
32	28	31	1	3	0.64s	0.14s
64	67	61	3	7	21.52s	4.16s
128	131	141	6	16	16.85m	2.87m
256	261	281	12	35	16.53h	2.74h

Size	degrees		Maple		Magma
n	x	y	real	cpu	cpu
16	96	32	0.32s	0.36s	0.32s
32	208	80	32.7s	46.3s	99.7s
64	576	192	2.86h	3.91h	15.1h
128	1216	448	Not attempted		
256	3072	1024	Not attempted		

References

[1] E.H. Bareiss. Sylvester's Identity and Multistep Integer-Preserving Gaussian Elimination. *Mathematics of Computation* **22**(103): 565–578, 1968.

[2] S.J. Berkowitz. On Computing The Determinant in Small Parallel time using a Small Number of Processors. *Inf. Processing Letters* **18**(3): 147–150, 1984.

[3] H. Cohen. *A Course in Computational Algebraic Number Theory*. Springer–Verlag, 1995.

[4] M. Law, M. Monagan. Computing Characteristic Polynomials of Matrices of Structured Polynomials. To appear in *Proceedings of CASC 2016*, Springer-Verlag LNCS, 2016.

[5] M. Kauers, Personal Communication.

[6] O.P. Lossers. A Hadamard-Type Bound on the Coefficients of a Determinant of Polynomials. *SIAM Rev.*, **16**(3): 394–395 solution to an exercise by A. Goldstein and R. Graham, 2006.

NSERC CRSNG

Maplesoft
Mathematics • Modeling • Simulation
A Cybernet Group Company

cecm