journal of inequalities in pure and applied mathematics
http://jipam.vu.edu.au
issn: 1443-5756
Volume 8 (2007), Issue 2, Article 31, 6 pp.

BOUNDS ON THE COEFFICIENTS OF THE CHARACTERISTIC AND MINIMAL POLYNOMIALS

JEAN-GUILLAUME DUMAS
LABORATOIRE JEAN KUNTZMANN
UNIVERSITÉ JOSEPH FOURIER
GRENOBLE I, UMR CNRS 5224,
51 AVENUE DES MATHÉMATIQUES
38041 GRENOBLE, FRANCE.
Jean-Guillaume.Dumas@imag.fr
URL: http://ljk.imag.fr/membres/Jean-Guillaume.Dumas

Received 25 October, 2006; accepted 23 April, 2007
Communicated by D. Ştefănescu

ABSTRACT. This note presents absolute bounds on the size of the coefficients of the characteristic and minimal polynomials depending on the size of the coefficients of the associated matrix. Moreover, we present algorithms to compute more precise input-dependant bounds on these coefficients. Such bounds are e.g. useful to perform deterministic Chinese remaindering of the characteristic or minimal polynomial of an integer matrix.

Key words and phrases: Characteristic polynomial, Minimal polynomial, Coefficient bound.

2000 *Mathematics Subject Classification.* 15A45, 15A36.

1. INTRODUCTION

The Frobenius normal form of a matrix is used to test two matrices for similarity. Although the Frobenius normal form contains more information on the matrix than the characteristic polynomial, the most efficient algorithms to compute it are based on computations of characteristic polynomials (see for example [8, §9.7]). Now the Smith normal form of an integer matrix is useful e.g. in the computation of homology groups and its computation can be done via the integer minimal polynomial [2].

In both cases, the polynomials are computed first modulo several prime numbers and then only reconstructed via Chinese remaindering [4, Theorem 10.25]. Thus, precise bounds on the integer coefficients of the integer characteristic or minimal polynomials of an integer matrix are used to find how many primes are sufficient to perform a Chinese remaindering of the modularly computed polynomials. Some bounds on the minimal polynomial coefficients, respectively the characteristic polynomial, have been presented in [2], respectively in [1]. The aim of this note is to present sharper estimates in both cases.

For both polynomials we present two kinds of results: *absolute estimates*, useful for comparing complexity constants, and *algorithms* which compute more precise estimates based on

the properties of the input matrix discovered at runtime. Of course, the goal is to provide such estimates at a cost negligible when compared to that of actually computing the polynomials.

2. BOUND ON THE MINORS FOR THE CHARACTERISTIC POLYNOMIAL

2.1. **Hadamard's Bound on the Minors.** The first bound of the characteristic polynomial coefficient uses Hadamard's bound, $|\det(A)| \leq \sqrt{nB^2}^n$, see e.g. [4, Theorem 16.6], to show that the coefficients of the characteristic polynomial could be larger, but only slightly:

Lemma 2.1. *Let $A \in \mathbb{C}^{n\times n}$, with $n \geq 4$, whose coefficients are bounded in absolute value by $B > 1$. The coefficients of the characteristic polynomial C_A of A are denoted by c_j, $j = 0, \ldots, n$ and $||C_A||_\infty = \max\{|c_j|\}$. Then*

$$\log_2(||C_A||_\infty) \leq \frac{n}{2}\left(\log_2(n) + \log_2(B^2) + 0.21163175\right).$$

Proof. Observe that c_j, the j-th coefficient of the characteristic polynomial, is an alternate sum of all the $(n-j)\times(n-j)$ diagonal minors of A, see e.g. [3, §III.7]. It is therefore bounded by

$$F(n,j) = \binom{n}{j}\sqrt{(n-j)B^2}^{(n-j)}.$$

First note, that from the symmetry of the binomial coefficients we only need to explore the $\lfloor n/2 \rfloor$ first ones, since

$$\sqrt{(n-j)B^2}^{(n-j)} > \sqrt{jB^2}^{j} \quad \text{for} \quad j < \lfloor n/2 \rfloor.$$

The lemma is true for $j = 0$ by Hadamard's bound.

For $j = 1$ and $n \geq 2$, we set

$$f(n) = \frac{2}{n}\left(\log_2\left(F(n,1)\right) - \frac{n}{2}\log_2(n) - (n-1)\log_2(B)\right).$$

Now

$$\frac{df}{dn} = \frac{2n - 2 + n\ln(n-1) - 2n\ln(n) + 2\ln(n) - ln(n-1)}{n^2(n-1)\ln(2)}.$$

Thus, the numerator of the derivative of $f(n)$ has two roots, one below 2 and one between 6 and 7. Also, $f(n)$ is increasing from 2 to the second root and decreasing afterwards. With $n \geq 4$ the maximal value of $f(n)$ is therefore at $n = 6$, for which it is

$$\frac{5}{6}\log_2(5) - \frac{2}{3}\log_2(6) < 0.21163175\,.$$

For other j's, Stirling's formula has been extended for the binomial coefficient by Stănică in [9], and gives $\forall i \geq 2$,

$$\binom{n}{j} < \frac{e^{\frac{1}{12n} - \frac{1}{12j+1} - \frac{1}{12(n-j)+1}}}{\sqrt{2\pi}}\sqrt{\frac{n}{j(n-j)}}\left(\frac{n}{j}\right)^j\left(\frac{n}{n-j}\right)^{n-j}.$$

Now first

$$\frac{1}{12n} - \frac{1}{12j+1} - \frac{1}{12(n-j)+1} < \frac{1}{12n} - \frac{2}{6n+1},$$

since the maximal value of the latter is at $j = \frac{n}{2}$. Therefore,

$$\log_2\left(\frac{e^{\frac{1}{12n} - \frac{1}{12j+1} - \frac{1}{12(n-j)+1}}}{\sqrt{2\pi}}\right) \leq \log_2\left(\frac{1}{\sqrt{2\pi}}\right) < -1.325.$$

Then $\frac{n}{j(n-j)}$ is decreasing in j for $2 \leq j < \lfloor n/2 \rfloor$ so that its maximum is $\frac{n}{2(n-2)}$.

Consider now the rest of the approximation

$$K(n,j) = \binom{n}{j}^{j} \left(\frac{n}{n-j}\right)^{n-j} \sqrt{(n-j)B^2}^{(n-j)}.$$

We have

$$\log_2(K(n,j)) = \frac{n-j}{2}\log_2(B^2) + \frac{n}{2}\log_2(n) + \frac{n}{2}T(n,j),$$

where

$$T(n,j) = \log_2\left(\frac{n}{n-j}\right) + \frac{j}{n}\log_2\left(\frac{n-j}{j^2}\right).$$

$T(n,j)$ is maximal for $j = \frac{-1+\sqrt{1+4en}}{2e}$. We end with the fact that for $n \geq 4$,

$$T\left(n, \frac{-1+\sqrt{1+4en}}{2e}\right) - \frac{2}{n}\log_2\left(\sqrt{2\pi}\right) + \frac{1}{n}\log_2\left(\frac{n}{2(n-2)}\right)$$

is maximal over $\mathbb{Z}$ for $n = 16$ where it is lower than 0.2052. The latter is lower than $0.\,21163175$. □

We show the effectiveness of our bound on an example matrix:

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & -1 \\ 1 & -1 & -1 & -1 & 1 \end{bmatrix}. \tag{2.1}$$

This matrix has $X^5 - 5X^4 + 40X^2 - 80X + 48$ for its characteristic polynomial and $80 = \binom{5}{1}\sqrt{4}^4$ is greater than Hadamard's bound 55.9, and less than our bound 80.66661.

Note that this numerical bound improves on the one used in [5, lemma 2.1] since $0.\,21163175 < 2 + \log_2(e) \approx 3.4427$. While yielding the same asymptotic result, their bound would state e.g. that the coefficients of the characteristic polynomial of the example are lower than 21793.

2.2. **Locating the Largest Coefficient.** The proof of Lemma 2.1 suggests that the largest coefficient is to be found between the $\mathcal{O}(\sqrt{n})$ last ones. In next lemma we take B into account in order to sharpen this localization. This gives a simple search procedure, computing a more accurate bound as soon as B is known.

Lemma 2.2. *Let $A \in \mathbb{C}^{n\times n}$, with $n \geq 4$, whose coefficients are bounded in absolute value by $B > 1$. The characteristic polynomial of A is C_A. Then*

$$||C_A||_\infty \leq \max_{i=0,\ldots,D} \binom{n}{i} \sqrt{(n-i)B^2}^{(n-i)}$$

where $D = \frac{-1+\sqrt{1+2\delta B^2 n}}{\delta B^2}$, $\delta \approx 5.418236$. Moreover, the cost of computing the associated bound on the size is

$$\mathcal{O}\left(\frac{\sqrt{n}}{B}\right).$$

This localization improves by a factor close to $\frac{1}{B}$, the localization of the largest coefficient proposed in [1, Lemma 4.1].

Proof. Consider

$$F(n,j) = \binom{n}{j}\sqrt{(n-j)B^2}^{(n-j)} \text{ for } j = 2,\ldots,\left\lfloor \frac{n}{2} \right\rfloor.$$

The numerator of the derivative of F with respect to j is

$$n!\sqrt{(n-j)B^2}^{n-j}\left(2H(n-j) - 2H(j) - \ln(n-j) - \ln(B^2) - 1\right),$$

where $H(k) = \sum_{l=1}^{k} \frac{1}{l}$ is the k-th Harmonic number. We have the bounds

$$\ln(k) + \gamma + \frac{1}{2k + \frac{1}{1-\gamma} - 2} < H(k) < \ln(k) + \gamma + \frac{1}{2k + \frac{1}{3}}$$

from [7, Theorem 2]. This bound proves that $F(n,j)$ has at most one extremal value for $2 \leq j \leq \lfloor \frac{n}{2} \rfloor$. Moreover,

$$\frac{\partial F}{\partial j}\left(n, \frac{n}{2}\right) < \frac{2}{\lceil \frac{n}{2} \rceil} - 1 + \ln\left(\frac{2}{nB^2}\right)$$

is thus strictly negative, as soon as $n \geq 4$. Now let us define

$$G(j) = 2H(n-j) - 2H(j) - \ln(n-j) - \ln(B^2) - 1.$$

Using the bounds on the Harmonic numbers, we have that

$$\begin{aligned}\frac{2}{2n - 2j + \frac{1}{1-\gamma} - 2} - \frac{2}{2j + \frac{1}{3}} &< G(j) - \ln\left(\frac{n-j}{j^2}\right) + 1 + \ln(B^2) \\ &< \frac{2}{2n - 2j + \frac{1}{3}} - \frac{2}{2j + \frac{1}{1-\gamma} - 2}\end{aligned}$$

Then, on one hand, we have that $\frac{2}{2n-2j+\frac{1}{1-\gamma}-2} - \frac{2}{2j+\frac{1}{3}}$ is increasing for $2 \leq j \leq \frac{n}{2}$ so that its minimal value is

$$M_i(n) = \frac{2}{2n - 6 + \frac{1}{1-\gamma}} - \frac{6}{13} \quad \text{at} \quad j = 2.$$

Finally, $M_i(n) > -\frac{6}{13}$ if we let n go to infinity.

On the other hand, $\frac{2}{2n-2j+\frac{1}{3}} - \frac{2}{2j+\frac{1}{1-\gamma}-2}$ is also increasing and therefore its maximal value is

$$M_s(n) = \frac{2(-4+7\gamma)}{(n - n\gamma - 1 + 2\gamma)(3n+1)} \quad \text{at} \quad j = n/2.$$

Finally, $M_s(n) \leq \frac{2(7\gamma-4)}{13(3-2\gamma)}$, its value at $n = 4$.

Then, the monotonicity of G and its bound prove that the maximal value of $F(n,j)$ is found for j^* between the solutions j_i and j_s of the two equations below:

$$\ln\left(\frac{n-j_i}{j_i^2}\right) = 1 + \ln(B^2) + \frac{6}{13}. \tag{2.2}$$

$$\ln\left(\frac{n-j_s}{j_s^2}\right) = 1 + \ln(B^2) - \frac{2(7\gamma-4)}{13(3-2\gamma)}. \tag{2.3}$$

This proves in turn that

$$j* \leq \max\left\{0; \frac{-1 + \sqrt{1 + 2\delta B^2 n}}{\delta B^2}\right\}$$

where

$$\delta = 2e^{1 - \frac{2(7\gamma-4)}{13(3-2\gamma)}} \approx 5.418236.$$

Now for the complexity, we use the following recursive scheme to compute the bound:

$$\begin{cases} \log(F(n,0)) = \frac{n}{2}\log(nB^2) \\ \log(F(n,j+1)) = \log\left(\frac{F(n,j)}{B}\right) + \log\left(\frac{n-j}{j+1}\right) + \frac{n-j-1}{2}\log(n-j-1) - \frac{n-j}{2}\log(n-j) \end{cases}$$

□

For instance, if we apply this lemma to matrix 2.1 we see that we just have to look at $F(n,j)$ for

$$j < \frac{-1+\sqrt{1+2\delta B^2 n}}{\delta B^2} \approx 1.183.$$

3. EIGENVALUE BOUND ON THE MINIMAL POLYNOMIAL

For the minimal polynomial the Hadamard bound may also be used, but is too pessimistic an estimate, in particular when the degree is small. Indeed, one can use Mignotte's bound on the minimal polynomial, as a factor of the characteristic polynomial. There, $||\operatorname{minpoly}_A||_\infty \leq 2^d||C_A||_\infty$, see [6, Theorem 4]. This yields that the bit size of the largest coefficient of the minimal polynomial is only d bits less than that of the characteristic polynomial.

Therefore, one can instead use a bound on the eigenvalues determined by consideration e.g. of the Gershgörin disks and ovals of Cassini (see [10] for more details on the regions containing eigenvalues, and [2, Algorithm OCB] for a blackbox algorithm efficiently computing such a bound). This gives a bound on the coefficients of the minimal polynomial of the form β^d, where β is a bound on the eigenvalues and d is the degree of the minimal polynomial.

We can then use the following lemma to bound the coefficients of the minimal polynomial:

Lemma 3.1. *Let $A \in \mathbb{C}^{n\times n}$ with its spectral radius bounded by $\beta \geq 1$. Let* $\operatorname{minpoly}_A(X) = \sum_{k=0}^{d} m_i X^i$. *Then*

$$\forall i,\ |m_i| \leq \begin{cases} \beta^d & \text{if } d \leq \beta \\ \min\left\{\sqrt{\beta d}^d\ ;\ \sqrt{\frac{2}{d\pi}}2^d\beta^d\right\} & \text{otherwise} \end{cases}$$

This improves the bound given in [2, Proposition 3.1] by a factor of $\log(d)$ when $d \gg \beta$.

Proof. Expanding the minimal polynomial yields $|m_i| \leq \binom{d}{i}\beta^{d-i}$ by e.g. [6, Theorem IV.§4.1]. Then, if $d \leq \beta$, we bound the latter by $d^i\beta^{d-i}$.

Now, when $d > \beta$, we get the first bound in two steps: first, for $i \leq \frac{d}{2}$, we bound the binomial factor by d^i and thus get

$$\binom{d}{i}\beta^{d-i} \leq d^i\beta^{\frac{d}{2}-i}\beta^{\frac{d}{2}} < d^{\frac{d}{2}}\beta^{\frac{d}{2}}$$

since $d > \beta$; second, for $i > \frac{d}{2}$, we bound the binomial factor by d^{d-i} and thus get

$$\binom{d}{i}\beta^{d-i} \leq d^{d-i}\beta^{d-i} < d^{\frac{d}{2}}\beta^{\frac{d}{2}}.$$

The second bound, when $d \geq \beta$ is obtained by bounding the binomial coefficients by the middle one, $\binom{d}{\frac{d}{2}}$, and using Stănică's bound [9] on the latter. This gives that

$$\binom{d}{i}\beta^{d-i} \leq \frac{1}{\sqrt{2\pi}}\sqrt{\frac{4}{d}}2^{\frac{d}{2}}2^{\frac{d}{2}}\beta^d.$$

□

For matrices of constant size entries, both β and d are $\mathcal{O}(n)$. However, when d and/or β is small relative to n (especially d) this may be a striking improvement over the Hadamard bound since the length of latter would be of order $n\log(n)$ rather than $d\log(\beta)$.

This is the case e.g. for the Homology matrices in the experiments of [2]. Indeed, for those, AA^t, the Wishart matrix of A, has very small minimal polynomial degree and has some other useful properties which limit β (e.g. the matrix AA^t is diagonally dominant). For example, the most difficult computation of [2], is that of the 25605×69235 matrix `n4c6.b12` which has a degree 827 minimal polynomial with eigenvalues bounded by 117. The refinement of lemma 3.1 yields there a gain *in size* on the one of [2] of roughly 5%. In this case, this represents saving 23 modular projections and an hour of computation.

4. CONCLUSION

We have presented in this note bounds on the coefficient of the characteristic and minimal polynomials of a matrix. Moreover, we give algorithms with low complexity computing even sharper estimates on the fly.

The refinements given here are only constant with regards to previous results but yield significant practical speed-ups.

REFERENCES

[1] J.-G. DUMAS, C. PERNET, AND ZHENDONG WAN, Efficient computation of the characteristic polynomial, *Proceedings of the 2005 International Symposium on Symbolic and Algebraic Computation, Beijing, China*, M. Kauers (Ed.), pages 140–147. ACM Press, New York, 2005.

[2] J.-G. DUMAS, B.D. SAUNDERS AND G. VILLARD, On efficient sparse integer matrix Smith normal form computations, *J. Symbolic Computation*, **32**(1/2) (2001), 71–99.

[3] F.R. GANTMACHER, *The Theory of Matrices*. Chelsea, New York, 1959.

[4] J. von zur GATHEN AND J. GERHARD, *Modern Computer Algebra*, Cambridge University Press, New York, NY, USA, 1999.

[5] M. GIESBRECHT AND A. STORJOHANN, Computing rational forms of integer matrices, *J. Symbolic Computation*, **34**(3) (2002), 157–172.

[6] M. MIGNOTTE, *Mathématiques pour le Calcul Formel*, Presses Universitaires Françaises, 1989.

[7] FENG QI, RUN-QING CUI, CHAO-PING CHEN AND BAI-NI GUO, Some completely monotonic functions involving polygamma functions and an application, *J. Math. Anal. Applics.*, **310**(1) (2005), 303–308.

[8] A. STORJOHANN, *Algorithms for Matrix Canonical Forms*. PhD thesis, Institut für Wissenschaftliches Rechnen, ETH-Zentrum, Zürich, Switzerland, November 2000.

[9] P. STĂNICĂ, Good lower and upper bounds on binomial coefficients. *J. Inequal. in Pure & Appl. Math.*, **2**(3) (2001), Art. 30. [ONLINE: `http://jipam.vu.edu.au/article.php?sid=146`].

[10] R.S. VARGA, *Geršgorin and his Circles*, Volume 36 of *Springer Series in Computational Mathematics*. Springer-Verlag, Berlin, 2004.