Coefficient bounds on the integer characteristic and minimal polynomials

Jean-Guillaume Dumas

Coefficient bounds on the integer characteristic and minimal polynomials

Jean-Guillaume Dumas

July 19, 2006

Abstract

In order to perform deterministic chinese remaindering of the characteristic or minimal polynomial, precise bounds on the size of their integer coefficients and ways to refine these bounds on the fly are presented.

1 Hadamard's bound on the minors

The first bound of the characteristic polynomial coefficient uses Hadamard's bound [2, Theorem 16.6] to show that any integer coefficient of the characteristic polynomial has the order of n bits:

Lemma 1.1. *Let $A \in \mathbb{Z}^{n\times n}$, with $n \geq 5$, whose coefficients are bounded in absolute value by $B > 1$. The coefficients of the characteristic polynomial of A are denoted by c_j. Then*

$$\log_2(|c_j|) \leq \frac{n}{2}\left(\log_2(n) + \log_2(B^2) + 0.21163175\right)$$

Proof. 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. It is therefore bounded by $H(n,j) = \binom{n}{j}\sqrt{(n-j)B^2}^{(n-j)}$. First note, that from the symmetry of the binomial coefficients we only need to explore the $\lfloor n/2\rfloor$ first ones, since $\sqrt{(n-j)B^2}^{(n-j)} > \sqrt{jB^2}^{j}$ for $i < \lfloor n/2\rfloor$. Now, the lemma claims that actually the maximal value must occur within the $\mathcal{O}(\sqrt{n})$ first ones. The lemma is true for $j = 0$ by Hadamard's bound. And for $j = 1$, we have $\log_2(H(n,j)) < \frac{n}{2}(\log_2(n) + \log_2(B^2) + 0.21163175)$ as soon as $n > 4$, since the difference is decreasing in n. Then from Stirling's formula ($n! = (1+\epsilon(n))\sqrt{2\pi n}\frac{n^n}{e^n}$), we have $\forall i \geq 2\ \binom{n}{i} < \frac{1+\epsilon(n)}{\sqrt{2\pi}}\sqrt{\frac{n}{i(n-i)}}\left(\frac{n}{i}\right)^i\left(\frac{n}{n-i}\right)^{n-i}$. Now first $\frac{1}{12n} < \epsilon(n) < \frac{1}{12n+1}$. Therefore for $n > 4$, $\log_2\left(\frac{1+\epsilon(n)}{\sqrt{2\pi}}\right) \leq -1.296$. Then $\frac{n}{i(n-i)}$ is decreasing in i for $i < \lfloor n/2\rfloor$ so that its maximum is $\frac{n}{2(n-2)}$.

Consider now $K(n,j) = \left(\frac{n}{j}\right)^j\left(\frac{n}{n-j}\right)^{n-j}\sqrt{(n-j)B^2}^{(n-j)}$. 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 $T(n,j)=\log_2(\frac{n}{n-j})+\frac{j}{n}\log_2(\frac{n-j}{j^2})$. Well $T(n,j)$ is maximal for $j=\frac{-1+\sqrt{1+4en}}{2e}$. We end with the fact that $T(n,j)-\frac{2}{n}1.296+\frac{1}{n}\log_2(\frac{n}{2(n-2)})$ is maximal over $\mathbb{Z}$ for $n=15$ where it is lower than 0.208935. The latter is lower than 0.21163175. □

Well,

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & -1 \\ 1 & -1 & -1 & -1 & 1 \end{bmatrix}$$

has $X^5-5X^4+40X^2-80X+48$ for 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 the one used in [3, lemma 2.1] since $0.21163175<2+\log_2(e)\approx 3.4427$.

2 Computing a bound

Lemma 2.1. *Let $A\in\mathbb{Z}^{n\times n}$, with $n\geq 4$, whose coefficients are bounded in absolute value by $B>1$. The coefficients of the characteristic polynomial of A are denoted by c_j. Then*

$$\forall j\ |c_j|\leq max_{i=0..\frac{-1+\sqrt{1+4eB^2n}}{2eB^2}}\binom{n}{i}\sqrt{(n-i)B^2}^{(n-i)}.$$

Moreover, the cost of computing the associated bound on the size is

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

The proof is similar to that of lemma 1.1, except that we cannot anymore bound expressions as we go. Indeed say that all values of a function $G(n,j)$ are below one of the values of a function $F(n,j)$ which happend to be e.g. $F(n,2)$, this does not prove that the maximum of G is at $j=2$. *Proof.* Consider $H(n,j)=\binom{n}{j}\sqrt{(n-j)B^2}^{(n-j)}=B^nG(n,j)B^{-j}$, for $j=2..\lfloor\frac{n}{2}\rfloor$. Then using Stirling's approximation, we have $G(n,j)=\frac{1+\epsilon(n)}{\sqrt{2_pi}}\frac{1}{(1+\epsilon(j))(1+\epsilon(n-j))}F(n,j)$. We now call $D(n,j)=\frac{2}{n}\log(F(n,j))=\left(\log(\frac{n}{n-j})+\frac{j}{n}\log(\frac{n-j}{j^2})+\frac{1}{n}\log(\frac{n}{j(n-j)})\right)$. Differentiating D with respect to j yields that the solution of $\ln(\frac{n-j}{j^2})=1+\frac{n-2j}{j(n-j)}$ gives an extremum of $D(n,j)$.

Now we multiply back $F(n,j)$ by both B^{-j} and $\frac{1}{(1+\epsilon(j))(1+\epsilon(n-j))}$ and consider then $Dt(n,j)=D(n,j)-\frac{j}{n}\log(B^2)-\frac{2}{n}\log((1+\epsilon(j))(1+\epsilon(n-j)))$. We approximate the latter with the taylor expansion of ϵ given e.g. in [1] ($\epsilon(i)\approx 1/12/i+1/288/i^2-139/51840/i^3\ldots$) and differentiate again with respect to j and multiply the obtained quotient by $i(n-i)n$. This yields that the solution $j*$ of $\ln(\frac{n-j}{j^2})=1+\ln(B^2)-\frac{n-2j}{6j^2(n-j)^2}(6j^2-6nj+n)+O(\frac{1}{i^3})$ gives an extremum of $D(n,j)$ Then, the roots of $(6j^2-6nj+n)$ are respectively

greater than $n/2$ and strictly lower than 1 (asymptotically close to $\frac{1}{6}$). Thus $\frac{n-2j}{6j^2(n-j)^2}(6j^2-6nj+n)$ is always negative and we have $\ln(\frac{n-j*}{j*^2}) \geq 1+\ln(B^2)$. This proves that

$$j* \leq \frac{-1+\sqrt{1+4eB^2n}}{2eB^2}.$$

Now for the complexity, we fist compute $\log(H(n,0)) = \frac{n}{2}\log(nB^2)$ and then $\log(H(n,i+1)) = \log(H(n,i)) + \log(\frac{n-i}{i+1}) + \frac{n-i-1}{2}\log(n-i-1) - \frac{n-i}{2}\log(n-i) - \log(B)$. □

References

[1] C. M. Bender and S. A. Orszag. *Advanced Mathematical Methods for Scientists and Engineers*. McGraw-Hill, New York, NY, USA, 1978.

[2] Joachim von zur Gathen and Jürgen Gerhard. *Modern Computer Algebra*. Cambridge University Press, New York, NY, USA, 1999.

[3] Mark Giesbrecht and Arne Storjohann. Computing rational forms of integer matrices. *Journal of Symbolic Computation*, 34(3):157–172, September 2002.