Some Useful Bounds

M. Mignotte, Strasbourg

Abstract

Some fundamental inequalities for the following values are listed: the determinant of a matrix, the absolute value of the roots of a polynomial, the coefficients of divisors of polynomials, and the minimal distance between the roots of a polynomial. These inequalities are useful for the analysis of algorithms in various areas of computer algebra.

I. Hadamard's Inequality

Hadamard's theorem on determinants can be stated as follows:

Theorem 1. *If the elements of the determinant*

$$D = \begin{vmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{vmatrix}$$

are arbitrary complex numbers, then

$$|D|^2 \leqslant \prod_{h=1}^{n} \left(\sum_{j=1}^{n} |a_{hj}|^2 \right)$$

and equality holds if and only if

$$\sum_{h=1}^{n} a_{hj}\bar{a}_{hk} = 0 \qquad \textit{for} \qquad 1 \leqslant j < k \leqslant n,$$

where $\bar{a}_{hk}$ is the conjugate of a_{hk}.

We do not give a proof of this classical result, it can be found in many textbooks on linear algebra (for example: H. Minc and M. Marcus, Introduction to Linear Algebra, Macmillan, New York, 1965).

II. Cauchy's Inequality

The following result gives an upper bound for the modulus of the roots of a polynomial in terms of the coefficients of this polynomial.

Theorem 2. *Let*

$$P(X) = a_0X^d + a_1X^{d-1} + \cdots + a_d, \qquad a_0 \neq 0, \qquad d \geqslant 1, \tag{$*$}$$

B. Buchberger et al. (eds.), *Computer Algebra*

be a polynomial with complex coefficients. Then any root z of P satisfies

$$|z| < 1 + \frac{\operatorname{Max}\{|a_1|, \ldots, |a_d|\}}{|a_0|}.$$

Proof. Let z be a root of P. If $|z| \leqslant 1$ the theorem is trivially true so we suppose $|z| > 1$. Put

$$H = \max\{|a_1|, \ldots, |a_d|\}. \quad \text{height of } P$$

By hypothesis z satisfies

$$a_0 z^d = -a_1 z^{d-1} - \cdots - a_d,$$

so that by the triangle inequality

$$|a_0|\,|z|^d \leqslant H(|z|^{d-1} + \cdots + 1) < \frac{H|z|^d}{|z|-1},$$

and

$$|a_0|(|z| - 1) < H.$$

This proves the result. ■

Corollary. *Let P be given by* $(*)$ *and $a_d \neq 0$. Then any root z of P satisfies*

$$|z| > \frac{|a_d|}{|a_d| + \operatorname{Max}\{|a_0|, |a_1|, \ldots, |a_{d-1}|\}}.$$

Proof. If z is a root of P then z^{-1} is a root of the polynomial

$$a_d X^d + a_{d-1} X^{d-1} + \cdots + a_0.$$

Applying the theorem to this polynomial gives the result. ■

There are many other known bounds for the modulus of the roots of a polynomial, most of which can be found in the book of Marden [3].

III. Landau's Inequality

Cauchy's inequality gives an upper bound for the modulus of *each* root of a polynomial. Landau's inequality gives an upper bound for the product of the modulus of *all* the roots of this polynomial lying outside of the unit circle. Moreover this second bound is not much greater than Cauchy's.

Theorem 3. *Let P be given by* $(*)$. *Let $z_1, \ldots, z_d$ be the roots of P. Put*

$$M(P) = |a_0| \prod_{j=1}^{d} \operatorname{Max}\{1, |z_j|\}.$$

Then

$$M(P) \leqslant (|a_0|^2 + |a_1|^2 + \cdots + |a_d|^2)^{1/2}.$$

To prove this theorem a lemma will be useful. If $R = \sum_{k=0}^{m} c_k X^k$ is a polynomial we put

$$||R|| = \left(\sum_{k=0}^{m} |c_k|^2 \right)^{1/2}.$$

Lemma. *If Q is a polynomial and z is any complex number then*

$$||(X + z)Q(X)|| = ||(\bar{z}X + 1)Q(X)||.$$

Proof. Suppose

$$Q(X) = \sum_{k=0}^{m} c_k X^k.$$

The square of the left hand side member is equal to

$$\sum_{k=0}^{m} (c_{k-1} + z\bar{c}_k)(\bar{c}_{k-1} + \bar{z}\bar{c}_k) = (1 + |z|^2)||Q||^2 + \sum_{k=0}^{m} (zc_k\bar{c}_{k-1} + \bar{z}\bar{c}_k c_{k-1})$$

where $c_{-1} = 0$.

It is easily verified that the square of the right hand side admits the same expansion. ■

Proof of the Theorem. Let $z_1, \ldots, z_k$ be the roots of P lying outside of the unit circle. Then $M(P) = |a_0|\,|z_1 \cdots z_k|$. Put

$$R(X) = a_0 \prod_{j=1}^{k} (\bar{z}_j X - 1) \prod_{j=k+1}^{d} (X - z_j) = b_0 X^d + \cdots + b_d.$$

Applying k times the lemma shows that $||P|| = ||R||$. But

$$||R||^2 \geqslant |b_0|^2 = M(P)^2. \quad ■$$

IV. Bounds for the Coefficients of Divisors of Polynomials

1. An Inequality

Theorem 4. *Let*

$$Q = b_0 X^q + b_1 X^{q-1} + \cdots, \qquad b_0 \neq 0$$

be a divisor of the polynomial P given by (*). *Then*

$$|b_0| + |b_1| + \cdots + |b_q| \leqslant |b_0/a_0| 2^q ||P||.$$

Proof. It is easily verified that

$$|b_0| + \cdots + |b_q| \leqslant 2^q M(Q).$$

But

$$M(Q) \leqslant |b_0/a_0| M(P)$$

and, by Landau's inequality,

$$M(P) \leqslant ||P||. \quad ■$$

Another inequality is proved in [4], Theorem 2.

2. *An Example*

The following example shows that the inequality in Theorem 4 cannot be much improved.

Let q be any positive integer and

$$Q(X) = (X-1)^q = b_0X^q + b_1X^{q-1} + \cdots + b_q;$$

then it is proved in [4] that there exists a polynomial P with integer coefficients which is a multiple of Q and satisfies

$$\|P\| \leqslant Cq(\operatorname{Log} q)^{1/2},$$

where C is an absolute constant.

Notice that in this case

$$|b_0| + \cdots + |b_q| = 2^q.$$

This shows that the term 2^q in Theorem 3 cannot be replaced by $(2-\varepsilon)^q$, where ε is a fixed positive number.

V. Isolating Roots of Polynomials

If $z_1, \ldots, z_d$ are the roots of a polynomial P we define

$$\operatorname{sep}(P) = \min_{z_i \neq z_j} |z_i - z_j|.$$

For reasons of simplicity we consider only polynomials with simple zeros (i.e. square-free polynomials); for the general case see Güting's paper [1].

The best known lower bound for $\operatorname{sep}(P)$ seems to be the following.

Theorem 5. *Let P be a square-free polynomial of degree d and discriminant D. Then*

$$\operatorname{sep}(P) > \sqrt{3}\, d^{-(d+1)/2}|D|^{1/2}\|P\|^{1-d}.$$

Proof. Using essentially Hadamard's inequality, Mahler [2] proved the lower bound

$$\operatorname{sep}(P) > \sqrt{3}\, d^{-(d+2)/2}|D|^{1/2}M(P)^{1-d}.$$

The conclusion follows from Theorem 3. ■

Corollary. *When P is a square-free integral polynomial* $\operatorname{sep}(P)$ *satisfies*

$$\operatorname{sep}(P) > \sqrt{3}\, d^{-(d+2)/2}\|P\|^{1-d}.$$

Other results are contained in [4], Theorem 5. It is possible to construct monic irreducible polynomials with integer coefficients for which $\operatorname{sep}(P)$ is "rather" small. Let $d \geqslant 3$ and $a \geqslant 3$ be integers. Consider the following polynomial

$$P(X) = X^d - 2(aX-1)^2.$$

Eisenstein's criterion shows that P is irreducible over the integers (consider the prime number 2). The polynomial P has two real roots close to $1/a$: clearly

$$P(1/a) > 0$$

and if $h = a^{-(d+2)/2}$

$$P(1/a \pm h) < 2a^{-d} - 2a^2 a^{-d-2} = 0,$$

so that P has two real roots in the interval $(1/a - h, 1/a + h)$. Thus

$$\mathrm{sep}(P) < 2h = 2a^{-(d+2)/2}.$$

References

[1] Güting, R.: Polynomials with Multiple Zeros. Mathematika **14**, 181 – 196 (1967).
[2] Mahler, K.: An Inequality for the Discriminant of a Polynomial. Michigan Math. J. **11**, 257 – 262 (1964).
[3] Marden, M.: The Geometry of the Zeros of a Polynomial in a Complex Variable. Publ. AMS **1949**, Math. Surv. 3.
[4] Mignotte, M.: Some Inequalities about Univariate Polynomials. SYMSAC **1981**, 195 – 199.

Prof. Dr. M. Mignotte
Centre de Calcul
Université Louis Pasteur
7, rue René Descartes
F-67084 Strasbourg
France