Quantitative Estimates for Polynomials in One or Several Variables :

From Analysis and Number Theory to Symbolic and Massively Parallel Computation.

by

Bernard Beauzamy
Institut de Calcul Mathématique
Paris, France

Per Enflo
Department of Mathematical Sciences
Kent State University, Kent, Ohio

and

Paul Wang
Department of Mathematical Sciences
Kent State University, Kent, Ohio

This research theme is supported by the *National Science Foundation* (U.S.A.), the *C.N.R.S.* (France), the *Ministry of Defense* (France) and *DIGITAL Eq. Corp.*

June 1992.

0. Introduction.

Polynomials are basic objects in mathematics. The behavior of any system usually depends on several constraints (the variables) and so is given by one or several functions of one or several variables. These functions, in turn, provided they are sufficiently continuous (which is usually the case), can be approximated by polynomials, in some range and within some accuracy. So the study of any system, no matter how complicated it is, starts with the study of polynomials.

As an example, the position of a robot in a plane will be given by two polynomials (one for each coordinate), each of them depending on several variables : directions of wheels, current in each motor, and so on.

Polynomials appear also as technical tools. For instance, for a system depending linearly on the data (thus given by a matrix), the stability depends on the zeros of the characteristic polynomial of the matrix (cf. Marden [B11]), and so locating zeros is a major problem in the theory of automata.

Polynomials also play a central rôle in many areas of mathematics, for instance Analysis (complex or real), Number Theory, Approximation Theory, Numerical Analysis.

Classical results about polynomials fall into two types. The first one is purely qualitative : it says that something exists. An easy example is Bezout Identity : if P and Q are two polynomials, with no root in common, there exist two other polynomials, A, B such that $A\,P + B\,Q = 1$ (no information is provided on A and B ; nobody even knows on what this information should depend). The second type depends on the degree. This is the case for Bernstein's Inequality, a basic result in Complex Analysis :

If P is a polynomial of degree n and P' its derivative,

$$\|P'\|_\infty \;\leq\; n\,\|P\|_\infty \ ,$$

where $\|P\|_\infty = \max_{|z|=1} |P(z)|$ (the value of $|P'|$ indicates the size of a slope, so, for instance, it shows how large the polynomial remains near one of its maxima). This is also the case for Gelfond's theorem in Number Theory (a result which is useful for the study of transcendental numbers) : if P and Q are two polynomials with degree m and n respectively,

$$|P \cdot Q|_\infty \;\geq\; 2^{-m+n}\,|P|_\infty \cdot |Q|_\infty \ ,$$

where, this time, $|P|_\infty = \max |a_j|$, if $P = \sum_j a_j z^j$.

Both types of results are quite unsatisfactory for two reasons. The first one is that sharp estimates are often needed, especially for computational purposes (and precisely when the degree is high) ; the second one is that, in fact, some problems are not connected with the degree. For instance, how many zeros does a polynomial have in the disk, centered at 0, with radius 1/2 ? One may say : at most its degree, but this answer is trivial and useless. The correct –and useful– one depends on the relative importance of the low degree terms inside the polynomial, as we shall see later.

We present here new directions for research and recent results, with a general purpose : to get new instruments of measure for polynomials, allowing us to obtain quantitative estimates, where only qualitative ones were known, or more precise ones, when some were already known. This article should be considered as an introduction to a research topic : no proofs are given (only references), but we try instead to present the motivations and the ways for further development. The field is entirely new (it was created in 1985), so the reader should not expect either an historical presentation. On the contrary, we emphasize the links with other branches of mathematics ; some of these branches (such as Number Theory) are extremely old, but our new concept gives a fresh approach, a fresh point of view, which brings new questions very quickly ; on such a new topic, time for research comes almost immediately.

Interactions with Computer Science are also emphasized ; as will be seen in § 3, the need for fast factorization algorithms brings very interesting questions about polynomials, on which our work casts a new light. Conversely, the strict requirements of massively parallel programming obliged us to invent a new spatial representation for polynomials in many variables, and this new representation finally turned out to be very fruitful, at the theoretical level.

Perhaps shall we convince the reader that research in mathematics is not what people usually think, and does not necessarily require many years of study before the first question can be met. But let us now be more specific.

Technically, two tools will be essential. The first one is a measure of the importance of the terms of low degree inside the whole polynomial ; the second is a new norm, with weighted coefficients. Both of them are very simple.

In order to measure the importance of the low degree terms, we have to use a norm on the space of polynomials, and which norm we use will depend on the specific problem we investigate. For $P = \sum a_j z^j$, we already met

$$\|P\|_\infty \;=\; \max_{|z|=1} |P(z)| \;,\quad |P|_\infty \;=\; \max_j |a_j|.$$

We can also use

$$\|P\|_2 \;=\; \Big(\int_0^{2\pi} |P(e^{i\theta})|^2 \frac{d\theta}{2\pi}\Big)^{1/2} \;,\quad |P|_2 \;=\; \Big(\sum_j |a_j|^2\Big)^{1/2} \;,$$

and

$$\|P\|_1 \;=\; \int_0^{2\pi} |P(e^{i\theta})| \frac{d\theta}{2\pi} \;,\quad |P|_1 \;=\; \sum_j |a_j|.$$

These notations refer to the following convention : for the double-bar norms, $\|\cdot\|$, P is considered as a function on the unit circle ; for the single-bar norms, $|\cdot|$, P is identified to the sequence of its coefficients, $(a_0, a_1, \dots, a_n)$.

These norms are comparable :

$$|P|_\infty \;\le\; \|P\|_1 \;\le\; |P|_2 \;=\; \|P\|_2 \;\le\; \|P\|_\infty \;\le\; |P|_1 \;\le\; \sqrt{deg(P)}\, |P|_\infty \;.$$

Since the $|\cdot|_1$-norm is simplest, we use it first, in order to define our concept.

1. Concentration at low degrees for polynomials in one variable, and applications.

The notion of *concentration at low degrees* for a polynomial was introduced by Bernard Beauzamy and Per Enflo in 1985. It gives, with just **one** new concept, quantitative results in several branches of mathematics, and governs seemingly unrelated phenomena, such as the location of the zeros, and the size of the polynomial in a given interval. Moreover, the estimates obtained are *independent of the degree.*

A. – Definition of the concentration.

Let $P(z) = a_0 + a_1 z + \cdots + a_k z^k + \cdots + a_n z^n$ be a polynomial with complex coefficients. Let d, $0 < d \le 1$, and let k, $0 \le k \le n$. We say that P has *concentration d at degree k* if :

$$\sum_{j=0}^{k} |a_j| \;\ge\; d \sum_{j=0}^{n} |a_j|. \tag{1}$$

Of course, if the degree of the polynomial is precisely k, this polynomial has concentration $d = 1$ at this degree. Of course also, if P has concentration d at degree k, it will also have concentration d', for any d', $0 < d' \le d$. So, in order to be more precise, we consider the quotient $\sum_{j\le k} |a_j| / \sum_{j=0}^{n} |a_j|$ and we call it the *concentration factor* of the polynomial $P(z)$ at degree k.

For instance, the polynomial $1+z^{100}$ has degree 100, but concentration 1/2 at degree 0. For some applications, it may be more interesting, more accurate, and quicker (in terms of computing speed) to consider it as a polynomial with concentration 1/2 at degree 0 than as a polynomial of degree 100. Also, all the polynomials

$$P_n(z) \ = \ 1+(1-\frac{1}{n})z+(1+\frac{1}{n})z^2+z^n \quad (n \geq 3)$$

have one thing in common : they all have concentration 3/4 at degree 2. They do not have the same number of zeros, and their zeros do not stay at the same place when n increases, but, as we will see, due to the concentration property, the number of their zeros in any given disk remains uniformly bounded, independently of n.

More generally, we wish to replace the actual degree of the polynomial by the concentration factor (at a given degree) in order to obtain estimates *independent* of the actual degree of the polynomial.

The first application of the concept is that of a *generalized Jensen's Inequality*, which governs the size of the subset of the unit circle on which a polynomial with concentration at low degree is large :

B. – Generalized Jensen's Inequality.

Classical Jensen's Inequality asserts that, for a polynomial $P=\sum a_j z^j$, with $a_0 \neq 0$,

$$\int_0^{2\pi} \log|P(e^{i\theta})|\frac{d\theta}{2\pi} \ \geq \ \log|a_0|. \tag{2}$$

If $a_0=0$ but $a_1 \neq 0$, applying the above inequality to $P(z)/z$ gives $\log|a_1|$ on the right-hand side ; if both a_0 and a_1 are 0 but a_2 is not, applying it to $P(z)/z^2$ gives $\log|a_2|$, and so on.

This inequality is quite important, for the following reason : if $|P(z)|$ is small at some z, then $\log|P|$ is extremely negative. Thus, to control from below the whole integral $I=\int_0^{2\pi}\log|P(e^{i\theta})|\frac{d\theta}{2\pi}$ (that is, to give a statement of the form $I \geq c$, for some c) allows one to control at once the size of any set of the type $\{\theta\ ,\ |P(e^{i\theta})|<\varepsilon\}$ and make sure that none of these sets is too big.

The proof of Jensen's inequality is not obvious, and the fact the integral converges is not immediate either. To see this, one writes P as a product $P=\lambda\prod_{j=1}^n(z-z_j)$, where the z_j's are the zeros of P. Then a term $\int_0^{2\pi}\log|e^{i\theta}-z_j|\frac{d\theta}{2\pi}$, with $|z_j|\neq 1$, causes no difficulty, since $|e^{i\theta}-z_j|$ is bounded away from zero, $\theta \in \Pi$. So the only difficulty comes from the terms $\int_0^{2\pi}\log|e^{i\theta}-z_j|\frac{d\theta}{2\pi}$, with $|z_j|=1$. By a change of variables, they reduce to $\int_0^{2\pi}\log|e^{i\theta}-1|\frac{d\theta}{2\pi}$. This integral is handled by a contour integration in the complex plane, and its value is 0 (see Rudin [B15]).

Connected with Jensen's Inequality is Mahler's Measure

$$M(P) \ = \ \exp\int_0^{2\pi}\log|P(e^{i\theta})|\frac{d\theta}{2\pi}\ ,$$

which plays an important role in Number Theory, since it is multiplicative : $M(PQ)=M(P)\cdot M(Q)$.

Now, inequality (2) has a serious drawback : it depends on the sole coefficient a_0 and therefore it is discontinuous. When a_0 is small, you apply it as it is, and when a_0 vanishes, you apply it to a_1. For instance, consider the family of polynomials

$$P_n(z) \ = \ \frac{1}{n}+z+z^2\ .$$

For each n, by (2),

$$\int_0^{2\pi}\log|P_n(e^{i\theta})|\frac{d\theta}{2\pi} \ \geq \ \log\frac{1}{n} \ \to \ -\infty \ \text{ when } n\to\infty,$$

whereas $P_n \to P$, with $P = z + z^2$, and

$$\int_0^{2\pi} \log |P(e^{i\theta})| \frac{d\theta}{2\pi} \;\geq\; 0.$$

Therefore, there is a need for a better inequality, not using just a_0. Such an inequality exists. If $P(z) \not\equiv 0$ is of exact degree k, a result due to Kurt Mahler [B9] (1960) asserts that :

$$\int_0^{2\pi} \log \left(\frac{|P(e^{i\theta})|}{\sum_0^k |a_j|} \right) \frac{d\theta}{2\pi} \;\geq\; -k \log 2.$$

But this result is not completely satisfactory either, because it involves the degree, and you get no uniform bound on the family of polynomials

$$P_n(z) \;=\; \frac{1}{n} + z + z^2 + \frac{1}{n} z^n.$$

A more satisfactory answer is a lower bound for $\int_0^{2\pi} \log |P(e^{i\theta})| \frac{d\theta}{2\pi}$ depending only on the importance of the low degree terms in the polynomial. This is given by a result of the first two authors [3] (1985), which asserts that, if $P(z)$ satisfies (1) (and thus does not need to be of degree k anymore), then :

$$\int_0^{2\pi} \log \left(\frac{|P(e^{i\theta})|}{\sum_0^k |a_j|} \right) \frac{d\theta}{2\pi} \;\geq\; B(d,k), \tag{3}$$

where the constant $B(d,k)$ is defined as the maximum value of the function :

$$f_{d,k}(t) \;=\; t \log \frac{2d}{(t-1)((\frac{t+1}{t-1})^{k+1} - 1)} \qquad (t > 1), \tag{4}$$

thus giving the rough estimate

$$B(d,k) \;\geq\; 2 \log(2d/3^k).$$

Let $C(d,k)$ be the *best* (that is the largest) constant satisfying (3). The precise value of $C(d,k)$ is unknown. However, we showed in [4] (1986) that, for $d = 1/2$,

$$C(1/2,k) \;\leq\; -2k \log 2, \tag{5}$$

and that, asymptotically, when $k \to +\infty$,

$$C(1/2,k) \;\geq\; -2k. \tag{6}$$

The precise value of $C(d,k)$ has been computed by A.K. Rigler, S.Y. Trimble and R.S. Varga [21] (1989), for the class of *Hurwitz polynomials*, i.e. polynomials having real positive coefficients, and their roots being either real and negative, or pairwise conjugate with negative real parts. For this class, the best constant, denoted by $C^H(d,k)$, is, for $d = 1/2$, given by :

$$C^H(1/2,k) \;=\; -(2k+1) \log 2 \;, \qquad k = 0, 1, \ldots, \tag{7}$$

which agrees with the result of (5) and (6). The *extremal polynomial*, in the class of Hurwitz polynomials (that is, the one which gives equality in (3) with the constant $C^H(1/2,k)$), is explicitly given by $(z+1)^{2k+1}$, $k = 0, 1, \ldots$ (it should be observed that, since the binomial coefficients satisfy $\binom{2k+1}{j} = \binom{2k+1}{2k+1-j}$, these polynomials are symmetric, and so have concentration $1/2$ at degree k). A complete representation for all the constants $C^H(d,k)$ is given in [21], for every $0 < d \leq 1$ and $k = 0, 1, \ldots$.

Instead of (1), the concentration can be measured with other norms : l_p or L_p, $1 \le p \le \infty$. For instance, one may consider the problem : Find

$$\inf \left\{ \int_0^{2\pi} \log \left(\frac{|P(e^{i\theta})|}{\|P\|_\infty} \right) \frac{d\theta}{2\pi} \; ; \; \sum_{j=0}^{k} |a_j| \ge d \, \|P\|_\infty \right\} \tag{8}$$

In the case $k = 1$, this problem was solved in [5] (1989). The solution is the unique constant $c < 0$ which satisfies the equation :

$$e^c (1 - 2c) \; = \; d.$$

The problem is still open for other values of k. Problems related to (8), but involving other norms than $\|P\|_\infty$, were studied by L. Bonvalot [11] (1986).

Besides the above results which are deduced from a generalized Jensen's Inequality, another area where striking results have already been obtained is that of *products of polynomials* :

C. – Products of polynomials in one variable, with complex coefficients.

To perform the product of two polynomials is of course a basic operation, on which one naturally wants quantitative estimates. But moreover, as we will see in § 3, these results are the key to fast factorization algorithms, in Computer Science.

The first result, due to the first two authors ([3]), is that if P and Q both have concentration at fixed degrees, the norm of their product is bounded from below, with a constant depending only on the concentration data, and not on the true degrees of the polynomials. If P, Q, $P \cdot Q$ are written :

$$P(z) \; = \; \sum_{j=0}^{J} a_j z^j \; , \quad Q(z) \; = \; \sum_{m=0}^{M} b_m z^m \; , \quad (P \cdot Q)(z) \; = \; \sum_{n=0}^{J+M} c_n z^n \; ,$$

and satisfy :

$$\sum_{j \le k} |a_j| \; \ge \; d \sum_{j \ge 0} |a_j| \quad , \qquad \sum_{j \le k'} |b_j| \; \ge \; d' \sum_{j \ge 0} |b_j|,$$

then :

$$\sum |c_n| \; \ge \; \lambda(d, d'; k, k') \sum_{j \ge 0} |a_j| \sum_{m \ge 0} |b_m|, \tag{9}$$

where (as stated) $\lambda(d, d'; k, k')$ depends only on d, d', k, k' and *not* on the precise degrees of $P(z)$ and $Q(z)$.

In Number Theory, a result of special importance is Gelfond's Theorem (see for instance M. Waldschmidt [B16]), which we already mentioned in the introduction. Here the constant $\lambda(d, d'; k, k')$, for fixed d, d', is also exponential in k, k', so the order of magnitude is the same as in Gelfond's theorem, but the scope of application is larger, since the degrees do not appear.

There is a much deeper result (also due to the same authors [3]), concerning products of polynomials : if one of them has a large coefficient and the other some concentration at a fixed degree, the product has a large coefficient. Precisely :

If P and Q satisfy :

$$\max_j |a_j| \; \ge \; d \sum_{j \ge 0} |a_j| \tag{10}$$

and

$$(\sum_{m=0}^{k} |b_m|^2)^{1/2} \ \geq\ d' \, (\sum_{m\geq 0} |b_m|^2)^{1/2} \ , \tag{11}$$

then :

$$\max |c_n| \ \geq\ \lambda(d, d'; k) \, (\sum_{j\geq 0} |a_j|^2)^{1/2} \, (\sum_{m\geq 0} |b_m|^2)^{1/2}, \tag{12}$$

where (as stated) $\lambda(d, d'; k)$ depends only on d, d', k, and *not* on the precise degrees of $P(z)$ and $Q(z)$.

The proof, using a complicated induction procedure, gives (for fixed d, d') a constant depending on k as a triple exponential (that is $e^{-(e^{e^k})}$). Further progress in this direction was later made by P. Enflo [15] (1987) : double exponential suffices (that is $e^{-(e^k)}$). It is quite likely (but has not been proven yet) that the correct order of magnitude is of exponential type.

D. – A Challenge.

Though products of polynomials look elementary, precise constants are not easy to obtain, even in very special situations. Let's take, as an example, a very special case of the Theorem above.

Assume, in this Theorem, that Q has concentration 1/2 at degree 0, that is

$$Q(z) \ = \ 1 + b_1 z + \cdots + b_m z^m \ , \tag{13}$$

with $\sum_1^m |b_j| \leq 1$ (which is stronger than (11)).

Assume that in P the largest coefficient is the last one :

$$P(z) \ = \ a_0 + a_1 z + \cdots + a_{n-1} z^{n-1} + z^n \ ,$$

with $\sum_0^{n-1} |a_j| \leq 1$ (thus P satisfies (10) with $d = 1/2$), then a precise result on these lines is due to C. Fabre [16](1988) : the product $P \cdot Q$ satisfies $|P \cdot Q|_\infty \geq 1/2$. Under these precise assumptions, the constant 1/2 is best possible.

But now, take the same Q as before, but P under the more general form

$$P \ = \ a_0 + a_1 z + \cdots + a_{n-1} z^{n-1} + z^n + a_{n+1} z^{n+1} + \cdots + a_N z^N,$$

with

$$\sum_{0}^{n-1} |a_j| + \sum_{n+1}^{N} |a_j| \ \leq\ 1$$

(so P satisfies also (10) with $d = 1/2$, but the largest coefficient is not necessarily the latest). Then, what is the greatest lower bound on $|P \cdot Q|_\infty$? We know it is $< 1/2$, but we do not know its value. This problem is not simple, and we would like to offer a prize for its solution : a week in Paris or in Kent (at the winner's choice !), trip included.

More generally, as we pointed out, in *most* cases previously mentioned, the precise values of the best constants mentioned are *unknown.* For polynomials of a fixed degree, the corresponding estimates have led to considerable study and deep theorems. Let us mention for instance Kurt Mahler [B9] (1960), [B10] (1962), Arestov [B1] (1979), Bell [B2] (1933), Newman [B14] (1964), Beller–Newman [B3] (1973), Kahane [B4] (1970), [B5] (1979). Study of problems such as (8), for large values of k, is clearly related to their work, and, as the solution of the case $k = 1$ already shows, involves deep considerations in Harmonic Analysis. The determination of the precise values in the estimates does not only involve computational accuracy but a better understanding of the problems themselves. They have been satisfactorily solved, so far, in only a very *limited* number of cases.

The techniques used in the existing proofs use either complex analysis or combinatorics. Probabilistic techniques might be used : for instance considering the coefficients of the polynomials as independent random variables, and trying to prove that, with some probability, the product is bounded from below. Such a probabilistic approach has been used by J.- P. Kahane in [B5], in a closely related context.

E. – Where the roots are.

Finding the location of the zeros is one of the major problems about polynomials. As it is well-known, if the degree is at least 5, no exact algebraic solution can be given, so the procedure has to be numerical. Many algorithms exist, either to find the complex zeros, or the real ones. Also, many results are known about the size of the smallest disk containing all zeros, or containing a given number of zeros (see Marden [11]). For instance, a result due to Cauchy says that all the zeros of the polynomial

$$P(z) \;=\; a_0 + a_1 z + \cdots + a_n z^n$$

are contained in the disk $|z| < r$, where r is the positive root of the equation

$$|a_0| + |a_1| x + \cdots + |a_{n-1}| x^{n-1} \;=\; |a_n| x^n \;.$$

If we come back to polynomials with concentration d at degree k, we observe that not all $a_0, a_1, \ldots, a_k$ can be zero, so 0 cannot be a root of order $k+1$. But in fact, a much more precise statement can be given, and not too many roots can be too close to 0. The following result was obtained by Sylvia Chou [12] (1990) :

There is a radius $r(d,k) > 0$ such that any polynomial P satisfying (1) has at most k roots in the open disk centered at 0, with radius $r(d,k)$. For $d \leq 1/2$, the value of this radius is

$$r(d,k) \;=\; \left(\frac{1}{1-d}\right)^{1/(k+1)} - 1$$

Precise numerical estimates for this radius, when $d > 1/2$, were obtained by the same author in [13] ; it was computed exactly for the class of Hurwitz polynomials.

If the zeros are written in increasing order of moduli :

$$0 \;\leq\; |z_1| \;\leq\; |z_2| \;\leq\; \cdots, \tag{14}$$

and if the polynomial has concentration d at degree k, B. Beauzamy and Sylvia Chou proved [9] (1991) that the quantity $|\sum_{j>k} 1/z_j|$ is bounded from above by a number depending only on d and k, for which they gave numerical estimates.

There is an extension of the classical Bernstein's inequality (cited in the introduction). This extension is valid for Hurwitz polynomials, and is independent of the degree. Indeed, if P is Hurwitz and has concentration d at degree k,

$$\|P'\|_\infty \;\leq\; C(d,k)\, \|P\|_\infty \;.$$

Conversely, if P is a Hurwitz polynomial satisfying

$$\|P'\|_\infty \;\leq\; C\, \|P\|_\infty \;,$$

it has concentration $d(C)$ at a degree $k(C)$ (S. Chou [12], [13], B. Beauzamy and Sylvia Chou [9]).

F. – From polynomials to analytic functions.

Instead of considering polynomials and defining the concentration with the sum of moduli of coefficients, one can use the l_2- norm, and extend the definition to the H^2 functions. This is the class of functions of the form

$$f(z) \;=\; \sum_0^\infty a_j z^j \ ,$$

which satisfy $(\sum_0^\infty |a_j|^2)^{1/2} < \infty$ (and so are analytic inside the unit disk). For such a function, we say it has concentration d at degree k (measured in the l_2-norm) if :

$$(\sum_0^k |a_j|^2)^{1/2} \;\geq\; d\,(\sum_0^\infty |a_j|^2)^{1/2} \ . \tag{15}$$

This definition looks slightly more complicated than the one we gave in (1), but it has a major advantage : we are now in a Hilbert space.

Previous results on polynomials about the number of zeros in a disk extend to H^2 functions with concentration d at degree k (but the proofs are very different, and use tools from Harmonic Analysis). The first author proved in [7] (1990) that in any disk $D(r)$ with $0<r<1$, the number of zeros of f is bounded by a number which depends only on d, k, r (for which precise numerical estimates are given). From this result it follows that if the zeros z_j of f are written in increasing order of modulus, as in (14), the speed of growth to 1 of the sequence $|z_j|$ is bounded from below by a function depending only on d and k. This was improved by Maria Girardi [18] (1991) who showed that for an H^2-function with concentration d at degree k, the quantity $\sum_{j\geq 1}(1-|z_j|)$ is bounded from above by a number depending only on d and k : this is one more example of a new quantitative theory, since the classical result asserts only that this sum is finite.

For such a function, for every $\varepsilon > 0$, the set of points where $|f| < \varepsilon$ can be covered by a union of disks, with sum of radii depending only on d, k, and ε, and tending to 0 when $\varepsilon \to 0$ ([7]). The importance of such results in Computer Science will be described in § 3.

2. – Polynomials in several variables.

The concept of concentration at low degrees also makes sense for a polynomial in several variables. Let :

$$P(z_1,\ldots,z_N) \;=\; \sum_\alpha a_\alpha z_1^{\alpha_1}\ldots z_N^{\alpha_N} \ , \tag{16}$$

(where $\alpha = (\alpha_1,\ldots,\alpha_N)$) be a polynomial, with complex coefficients and N variables. Let's define $|\alpha| = |\alpha_1| + \cdots + |\alpha_N|$. We say that P has concentration d at *total* degree k if :

$$\sum_{|\alpha|\leq k} |a_\alpha| \;\geq\; d \sum_\alpha |a_\alpha|. \tag{17}$$

As before, we define the l_1-norm of P by :

$$|P|_1 \;=\; \sum_\alpha |a_\alpha|.$$

A theorem due to P. Enflo [14] asserts that if P, Q are polynomials with concentration d, d' at degree k, k' respectively, that is satisfy :

$$\sum_{|\alpha|\leq k} |a_\alpha| \;\geq\; d \sum_\alpha |a_\alpha| \tag{18}$$

and

$$\sum_{|\beta|\le k'} |b_\beta| \ \ge\ d' \sum_\beta |b_\beta| \tag{19}$$

then if the product PQ is written as $\sum_\gamma c_\gamma z_1^{\gamma_1}\dots z_N^{\gamma_N}$, we have :

$$\sum_{|\gamma|\le k+k'} |c_\gamma| \ \ge\ \lambda(d,d';k,k') \sum_\alpha |a_\alpha| \sum_\beta |b_\beta|. \tag{20}$$

The interesting point is that λ depends neither on the specific degrees of P and Q, nor on the number of variables. This theorem was the key tool in the second author's construction of an operator without invariant subspaces [14]. But it is only an existence statement : nothing is known about the size of λ.

A paper by B. Beauzamy, E. Bombieri, P. Enflo, H. Montgomery [6] (1990) continues the research on these lines. If we define the l_p norm of P as $(\sum_\alpha |a_\alpha|^p)^{1/p}$, and the L_p norm of P as

$$\|P\|_p \ =\ \Big(\int\cdots\int |P(e^{i\theta_1},\dots,e^{i\theta_N})|^p \,\frac{d\theta_1}{2\pi}\cdots\frac{d\theta_N}{2\pi}\Big)^{1/p} \quad ,$$

similar results hold for all these norms, with constants independent both of the degrees, and of the number of variables, but of unknown size. However, there is a norm for which the product result has a sharp statement :

If P is a homogeneous polynomial of degree m, we define

$$[P]_2 \ =\ \big(\sum_{|\alpha|=m} \frac{\alpha!}{m!}|a_\alpha|^2\big)^2 \ , \tag{21}$$

(where $\alpha! = \alpha_1!\cdots\alpha_N!$). Then, if P and Q are homogeneous of degree m and n respectively,

$$[P\cdot Q]_2 \ \ge\ \sqrt{\frac{m!n!}{(m+n)!}}\,[P]_2[Q]_2 \ , \tag{22}$$

and this constant is best possible. The extremal pairs, that is the pairs of P's and Q's for which the smallest product is obtained, were characterized by J.-L. Frot, C. Millour [17] (1991) and by Bruce Reznick [20] (1991). We will come back on this result when we speak about parallel computation, in Section 4.

Comparison between real and complex sup-norms for polynomials in many variables was made by Richard Aron, Bernard Beauzamy, Per Enflo in [2] (1991), where sharp estimates were obtained. Previous results in related areas had been obtained by R. Aron and J. Globevnik [1], A. Tonge [25] , Y. Sarantopoulos [22], [23], [24]. Further estimates were recently given by Miguel Lacruz [19] (1991).

3. – Symbolic Computation.

This is one of the most striking applications of the concept "quantitative estimates". Two closely related problems are considered : upper bounds for coefficients in polynomial factorizations and fraction decompositions, and location of zeros. Both are highly related.

Let $P=\sum_0^n a_j z^j$ be a polynomial in one complex variable, with integer coefficients ($a_j\in\mathbb{Z}$). If P is factored as $P=Q.R$, where Q and R are themselves in $\mathbb{Z}[z]$, what is the maximum of the coefficients in Q and in R ? Can it be estimated before the decomposition is written ? This problem has received special attention, because the existence of such an a priori bound is an essential feature for the design of efficient factorization algorithms in Symbolic Computation (H. Zassenhaus [B17], Paul Wang and B. M. Trager [32], Paul Wang [29], [30], [31], Vilmar Trevisan and Paul Wang [28]).

Indeed, the classical computer algorithms for factorization work as follows : suppose we want to factor P in $\mathbb{Z}[z]$. We can assume that P is primitive (that is : no factor divides all coefficients in P) and that P and its derivative P' are relatively prime.

We choose a prime q, not dividing the leading coefficient of P. Let P_0 be the image of P in $\mathbb{Z}_q[z]$. The prime q has also to be chosen so that P_0 has no multiple zero in $\mathbb{Z}_q[z]$.

Then P_0 is factored in $\mathbb{Z}_q[z]$. This is fast, since all coefficients of P_0 are smaller than q. Let $P_0 = Q_0 \cdot R_0$ be the factorization in $\mathbb{Z}_q[z]$ (we write only two factors for simplicity). Then

$$P \equiv P_0 = Q_0 \cdot R_0 \ , \qquad (\mathrm{mod}\ q).$$

A lemma due to Hensel (H. Zassenhaus [B17], 1969) says that we we can lift the factors modulo q into a decomposition modulo q^2. Precisely, we find Q_1, R_1 in $\mathbb{Z}_{q^2}[z]$ such that :

$$Q_1 \equiv Q_0 \quad (\mathrm{mod}\ q) \quad , \quad R_1 \equiv R_0 \quad (\mathrm{mod}\ q),$$

and if $P_1 = Q_1 \cdot R_1$, then $P \equiv P_1 \quad (\mathrm{mod}\ q^2)$.

Let B be the bound we are looking for, namely the maximum (in modulus) of all coefficients in any factor of P. We repeat the lifting procedure with q^2, q^4, ..., q^{2^k}, until $q^{2^k} \geq 2B$, so we find Q_2, Q_3, ..., Q_k, R_2, R_3, ... R_k, with

$$Q_j \equiv Q_{j-1} \quad (\mathrm{mod}\ q^{2^{j-1}}) \quad , \quad R_j \equiv R_{j-1} \quad (\mathrm{mod}\ q^{2^{j-1}}),$$

and

$$P \equiv Q_k \cdot R_k \quad (\mathrm{mod}\ q^{2^k}).$$

We stop the lifting process at this point, and the algorithm now becomes a trial process : in $\mathbb{Z}[z]$, we try to divide P by Q_k, R_k, ..., or by combinations of these factors. If P has true factors, they will appear this way. However, it may happen that P is irreducible, though each factor in $\mathbb{Z}_{q^j}[z]$ was non-trivial.

The existence of the a priori bound B is therefore essential to determine the stopping time for the lifting process. Since this process is costly, the bound should be as small as possible.

The connection with product results, given in § 1.C, is easy to describe. Assume $P = Q \cdot R$, both with integer coefficients, and assume we have proved a product result, such as

$$|Q \cdot R|_1 \geq \lambda \, |Q|_1 \cdot |R|_1 \ .$$

Since R has integer coefficients, $|R|_1 \geq 2$, and so

$$|Q|_1 \leq \frac{1}{2\lambda} \, |P|_1 \ , \tag{23}$$

the required bound.

The first estimates were given by Hans Zassenhaus [B17]. Later, M. Mignotte [B13] made use of Mahler's measure, and obtained the estimate

$$|Q|_1 \leq 2^n \, |P|_2 \ . \tag{24}$$

A result of the first author [8] (1991), using the tools of the previous section, strongly improves upon this estimate. Indeed, he showed that the coefficients b_j of any factor Q of P satisfy

$$\max_j |b_j| \ \leq \ \frac{3^{3/4}}{2\sqrt{\pi}} \frac{3^{n/2}}{\sqrt{n}} [P]_2 \ , \tag{25}$$

where $[P]_2$ is the norm defined in the previous paragraph, which, in the one-variable case, is just :

$$[P]_2 \ = \ \left(\sum_0^n \frac{1}{\binom{n}{j}} \ |a_j|^2 \right)^{1/2} \ . \tag{26}$$

The proof of (25) is very easy from the product result (22). Assume $P = Q \cdot R$, both factors having integer coefficients, so $[R]_2 \geq 1$. Then

$$[P]_2 \ \geq \ \sqrt{\frac{m_1!m_2!}{n!}} [Q]_2 \ ,$$

with $m_1 = deg(Q)$, $m_2 = deg(R)$. Taking the minimum of $m_1!m_2!$ when $m_1 + m_2 = n$ and using Stirling's formula yields (25).

The improvement over (24) is two-fold : first, 2^n is replaced by $3^{n/2}/\sqrt{n}$, which is smaller, and second the classical l_2-norm is replaced by the new norm $[P]_2$, which is usually much smaller, since it carries significant weights in the denominators.

Computer implementation was realized by Vilmar Trevisan [26], [27] (1991), and showed strong improvements due to the new method : the a priori bound may, for instance, become ten times smaller, already for low degree polynomials.

Future development of Symbolic Computation must include counting zeros of a given polynomial in a given region, for (as we have seen at the beginning), this is highly related to stability properties of dynamical systems. The work of the first author [7], described in section 1.F above, shows that inside a disk, the number of zeros depends only on the concentration of the polynomial at low degrees (and not on the degree itself) ; the subsequent works of Sylvia Chou [12], [13], and of Maria Girardi [18], provide precise estimates for this number. So, though the effective algorithms have not been written yet, the theoretical results already exist.

Another problem would also be worth considering : a priori bounds for coefficients in fraction decompositions.

4. – Massively parallel computation on polynomials.

The present development of parallel computing turns it into a very efficient tool, but quite rigid, especially when we deal with *Single Instructions Multiple Data* machines, meaning that all processors are executing the same instruction at the same time. So far, only a limited number of problems, of situations, have been handled by S.I.M.D. parallel computing : mostly matrix computations and partial differential equations, by discretization.

The results of Beauzamy-Bombieri-Enflo-Montgomery [6] (1990) provide a canonical way of writing a many-variable polynomial on a hypercube ; we now describe it.

We start with the polynomial written the usual way :

$$P(x_1, \ldots, x_N) \ = \ \sum_{|\alpha|=m} a_\alpha x_1^{\alpha_1} \cdots x_N^{\alpha_N} \ .$$

Then we use Taylor's formula in order to write it in *symmetric* form, that is

$$P(x_1, x_2, \ldots, x_N) \ = \ \sum_{i_1, \ldots, i_m = 1}^{N} c_{i_1, \ldots, i_m} x_{i_1} \cdots x_{i_m} \tag{27}$$

with

$$c_{i_1,\ldots,i_m} \ = \ \frac{\partial^m P}{\partial x_{i_1} \cdots \partial x_{i_m}} \ . \tag{28}$$

This just means that a term x_1x_2 is written as $\frac{1}{2}(x_1x_2 + x_2x_1)$, a term $x_1x_2^2$ becomes $\frac{1}{3}(x_1x_2x_2 + x_2x_1x_2 + x_2x_2x_1)$, and so on.

Now we construct the hypercube. For this, we divide the segment $[0,1]$ into N equal pieces, by introducing the points

$$0, \frac{1}{N}, \frac{2}{N}, \ldots, \frac{N}{N} \ .$$

In the hypercube $[0,1]^m$, we consider the points

$$M_{i_1,\ldots,i_m} \ = \ (\frac{i_1}{N}, \ldots, \frac{i_m}{N}),$$

where $i_1, \ldots, i_m$ take any value in $\{1, \ldots, N\}$. So there are N^m such points.

We now fill the hypercube the following way : at each point $M_{i_1,\ldots,i_m}$ we put the coefficient $c_{i_1,\ldots,i_m}$ defined in (28) : we have obtained a representation of the polynomial on the hypercube.

For example, the polynomial $P = 4x_1x_2 - x_3^2$ has degree 2 and 3 variables. So it will be represented as a cube of dimension 2, that is in a plane, by the matrix

$$H(P) \ = \ \begin{pmatrix} 0 & 2 & 0 \\ 2 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix} .$$

The weighted norm $[P]_2$ described and used previously appears simply as the l_2-norm on the hypercube, that is $(\sum_{i_1,\ldots,i_m} |c_{i_1,\ldots,i_m}|^2)^{1/2}$.

B. Beauzamy, J.-L. Frot, C. Millour [10] (1991) showed that this representation of a many-variable polynomial on a hypercube allows full use of the massively parallel structure of a S.I.M.D. machine, in order to perform basic operations on polynomials, such as sums, products, pointwise evaluations, partial derivatives, and so on. Computer implementation was realized on a *Connection Machine* (in $*$- LISP), and showed considerable improvements in computing time, compared with sequential processing, when the number of variables becomes high (see [10]).

Moreover, as an unexpected theoretical benefit, this new representation allowed an easy description of the extremal pairs in the product results, that is of the pairs (P, Q) such that $[P \cdot Q]_2$ is as small as possible. These extremal pairs are those for which every column of the cube associated to P is orthogonal (in the usual euclidean sense) to every column of the cube associated to Q.

One sees here a true interaction between Mathematics and Computer Science : the problem of representing a polynomial so it could be understood by special computers originated from Computer Science and required effective mathematical tools, but in turn these tools benefitted from the question.

5. – Conclusion.

We have seen throughout this presentation how quantitative estimates could be used in various and important areas of Mathematics and Computer Science. There is one feature, however, worth emphasizing : the estimates we obtain are independent of the number of variables.

This is of course essential for parallel computing, but this feature has a special meaning in modelling control theory.

Indeed, usually, one wants to act on a control variable u in order to maximize some data on some system. The control variable is taken in a Hilbert space, or at least in some reflexive space (Besov, Sobolev, ...), in order to make use of the classical tools of weak compactness.

But this is unrealistic in the case where the global constraint u is made up of a lot of small ones, $u = (u_1, u_2, \ldots, u_N)$, where each of them has a *right of veto*, that is should not fall below a certain level, $u_j < \varepsilon$ (we take $0 \le u_j \le 1$ for instance). Indeed, if u is in a Hilbert space, $u = \sum u_j e_j$, where e_j is some Hilbertian basis, and then $u_j \to 0$ when $j \to \infty$, which means that all constraints except a finite number are assumed to be negligible. That's exactly contrary to our "right of veto" situation.

So, in order to model such phenomena, one must allow each elementary variable to vary freely between 0 and 1. This means that $u = (u_1, u_2, \ldots)$ is to be taken in a space of *bounded* sequences, namely l_∞. However, this space is not reflexive, and the necessary tools for optimization will disappear. So, in order to solve the problem, one will first fix N, look at $(u_1, \ldots, u_N)$ and solve the problem in $l_\infty^{(N)}$, and then let $N \to \infty$. But, for given N, one needs the solution to be independent of N, that is precisely to be independent of the number of variables.

REFERENCES.

A. – Papers dealing with concentration at low degrees.

[1] ARON, Richard – GLOBEVNIK, Jossip : Interpolation by analytic functions on c_0. Math. Proc. Cambridge Ph. Soc., 1988, 104, pp. 295–302.

[2] ARON, Richard – BEAUZAMY, Bernard – ENFLO, Per : Polynomials with many variables : Real vs Complex Norms. To appear in the *Journ. of Approx. Theory.*

[3] BEAUZAMY, Bernard – ENFLO, Per : Estimations de produits de polynômes. *Journal of Number Theory*, 21–3 (1985), pp. 390–412.

[4] BEAUZAMY, Bernard : Jensen's Inequality for polynomials with concentration at low degrees. *Numerische Math.* 49 (1986), pp. 221–225.

[5] BEAUZAMY, Bernard : A minimization problem connected with generalized Jensen's Inequality. *Journal of Math. Anal. and Applications*, vol. 145, 1, jan. 1990, pp. 137–144.

[6] BEAUZAMY, Bernard – BOMBIERI, Enrico – ENFLO, Per – MONTGOMERY, Hugh : Products of polynomials in many variables. *Journal of Number Theory*, vol. 36, 2, oct. 1990, pp. 219–245.

[7] BEAUZAMY, Bernard : Estimates for H^2 functions with concentration at low degrees and applications to complex symbolic computation. To appear in *J. für die Reine und Angewandte Math.*

[8] BEAUZAMY, Bernard : Products of Polynomials and a priori estimates for coefficients in polynomial decompositions : a sharp result. To appear in the Journ. of Symbolic Computation, 1992.

[9] BEAUZAMY, Bernard - CHOU, Sylvia : On the zeros of polynomials with concentration at low degrees, II. To appear in *J. of Mathematical Analysis and Applications.*

[10] BEAUZAMY, B. - FROT, J.-L., MILLOUR, C. : Massively parallel computations on many-variable polynomials : when seconds count. *To appear.*

[11] BONVALOT, L. : Moyenne Géométrique des fonctions des espaces de Hardy et polynômes concentrés aux bas degrés. *Thèse de Troisième Cycle*, Université de Paris 7, 1986.

[12] CHOU, Sylvia : On the roots of polynomials with concentration at low degrees. *Journal of Math. Analysis and Applications*, vol. 149, 2, July 1, 1990, pp. 424–436.

[13] CHOU, Sylvia : Séries de Taylor et concentration aux bas degrés. *Thèse*, Université de Paris VI, 1990.

[14] ENFLO, Per : On the invariant subspace problem in Banach spaces. *Acta Math.*, vol. 158 (1987), pp. 213–313.

[15] ENFLO, Per : The largest coefficient in products of polynomials. *To appear.*

[16] FABRE, C. : La meilleure constante dans un produit de polynômes. *Note Comptes Rendus*, Acad. Sci. Paris, t. 307, S I, pp. 767–770, 1988.

[17] FROT, J.-L. – MILLOUR, C. : Rank of a polynomial and extremality. *To appear.*

[18] GIRARDI, Maria : Bounding zeros of H^2 functions by concentrations. *To appear.*

[19] LACRUZ, Miguel : Ph.D. Thesis, Kent State University, 1991.

[20] REZNICK, Bruce : An Inequality for products of polynomials. *To appear.*

[21] RIGLER, A. – TRIMBLE, R.S. – VARGA, R. : Sharp lower bounds for a generalized Jensen's Inequality. *Rocky Mountain Journal of Maths*, 19, 1989, pp. 353–373.

[22] SARANTOPOULOS, Yannis : Estimates for polynomial norms on $L_p(\mu)$ spaces. *Math. Proc. Cambridge Phil. Soc.*, 1986, 99, pp. 263–271.

[23] SARANTOPOULOS, Yannis : Extremal multilinear forms on Banach Spaces. *Proc. A.M.S.*, vol. 99, 2, 1987, pp. 340– 346.

[24] SARANTOPOULOS, Yannis : Polynomials on certain Banach Spaces. *Bull. Greek Math. Soc.*, 28, 1987, pp. 89–102.

[25] TONGE, Andrew : The Von Neumann inequality for polynomials in several Hilbert-Schmidt operators. *Journal of the London Math. Soc.*, 18, 1978, pp. 519–526.

[26] TREVISAN, V. : Recognition of Hurwitz polynomials. *SIGSAM Bulletin*, vol. 24, 4, oct. 1990.

[27] TREVISAN, V. : Computing a sharp bound for the coefficients in polynomial factorizations. *To appear.*

[28] TREVISAN, V. – WANG, P. : Practical Factorization of Univariate Polynomials over Finite Fields. *Proceedings of the ISAAC'91*, Bonn, July 1991.

[29] WANG, P. : An improved Multivariate Polynomial Factoring Algorithm. *Math. Comp.*, vol.32, 144, oct. 1978, pp. 1215–1231.

[30] WANG, P. : Parallel p-adic Construction in the Univariate Polynomial Factoring Algorithm. *Proceedings*, Second Macsyma users conference, Washington D.C., June 1979, pp. 310–317.

[31] WANG, P. : A p-adic Algorithm for Univariate Partial Fractions. *Proceedings* of the 1981 ACM Symposium on Symbolic and Algebraic Computation, pp. 212–217.

[32] WANG, P. - TRAGER, B. M. : New algorithms for polynomial square-free decompositions over the integers. *SIAM Journal of Computing*, vol. 8, 3, Aug. 1979, pp. 300–305.

[33] WANG, P. : Early detection of true factors in univariate polynomial factorizations. *Proceedings A.C.M. Eurocal*, London, March 28-30, 1983.

B. Other papers :

[1] ARESTOV, V.V. : Inequalities for different metrics for trigonometric polynomials. *Mat. Zametki*, vol. 27 (1980), 4.

[2] BELL, E.T. : Exponential polynomials. *Annals of Maths*, vol. 35, 2 (1934), pp. 258–277.

[3] BELLER, E. – NEWMAN, D.J. : An extremal problem for the geometric mean of a polynomial. *Proc. A.M.S.*, 19 (1973), pp. 313–317.

[4] KAHANE, J.-P. : Séries de Fourier absolument convergentes. *Springer Verlag*, 1970.

[5] KAHANE, J.P. : Polynômes à coefficients unimodulaires sur le cercle unité. *Séminaire d'Analyse Fonctionnelle*, 1979-80, Exposé 9, Ecole polytechnique.

[6] LANGEVIN, M. : Estimations du module d'un polynôme dans le plan complexe. *Preprint.*

[7] LENSTRA, A.K. – LENSTRA, H. W. – LOVASZ, L. : Factoring polynomials with integer coefficients. *Math Annalen* 261 (1982), pp. 515–531.

[8] LEVIN, B. : On the distribution of zeros of entire functions. *A.M.S. publications*, vol. 5.

[9] MAHLER, K. : An application of Jensen's formula to polynomials. *Mathematika* 7, (1960), pp. 98–100.

[10] MAHLER, K. : On two extremum properties of polynomials. *Ill. J. of Maths*, 7 (1963), pp. 681–701.

[11] MARDEN, Morris : Geometry of Polynomials. *A.M.S. Math. Surveys*, 3rd edition, 1985.

[12] Mc GEHEE, O. – PIGNO, L. – SMITH, B. : Hardy's inequality and the L_1 norm of exponential sums. *Ann. of Maths*, 113 (1981), pp. 613–618.

[13] MIGNOTTE, M. : An Inequality About Factors of Polynomials. *Mathematics of Computation*, vol. 28, 128, (1974), pp. 1153–1157.

[14] NEWMAN, D.J. : An L_1-extremal problem for polynomials. *Proceedings A.M.S.*, 16-2, (1965), pp. 1287–1290.

[15] RUDIN, W. : Real and Complex analysis. 3rd Edition.

[16] WALDSCHMIDT, M. : Nombres Transcendants. *Springer Verlag*, Lecture Notes, 1978.

[17] ZASSENHAUS, Hans : On Hensel Factorization. *Journal of Number Theory*, 1, 1969, pp. 291–301.