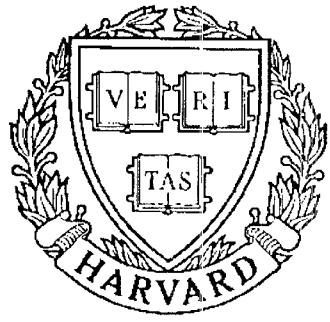
TECHNICAL RESEARCH REPORT

SYSTEMS RESEARCH CENTER



Supported by the National Science Foundation Engineering Research Center Program (NSFD CD 8803012), Industry and the University

Bounds for the Degrees in Polynomial Equations

by C.A. Berenstein and A. Yger

TR 90-5

Bounds for the degrees in polynomial equations

Carlos A. Berenstein and Alain Yger*

Let $p_1,\dots,p_m$ be polynomials in n variables, with coefficients in $\mathbb{C},\mathbb{Z}$ or other rings as indicated below. The purpose of this lecture is to indicate some estimates of the degrees and, occasionally, of the size of the coefficients of the polynomial solutions $q_1,\dots,q_m$ of the equations

$$p_1q_1+\dots+p_mq_m=1 \qquad \text{(Bezout equation)}, \tag{1}$$

and

$$p_1q_1+\dots+p_mq_m=f. \tag{2}$$

More importantly, we would like to clarify the role of complex analysis in a problem which is totally algebraic in nature.

I will not discuss the background and applications of the Bezout equation since the reader can consult [B-S1] for that purpose. Let us only recall the most recent results.

Assume that $V=\{z\in\mathbb{C}^n : p_1(z)=\dots=p_m(z)=1\}=\emptyset$, $\deg p_j=d_j$, $d_1\geq d_2\geq\dots\geq d_m$. In 1987, Brownawell [B1] showed the existence of solutions q_j of (1) with the bound

$$\deg q_j\leq n\min\{n,m\}d_1\dots d_n\leq n^2d_1^n. \tag{3}$$

His proof uses analytic methods and therefore requires that the coefficients of p_j (and q_j) lie in a subfield of $\mathbb{C}$. Recently Kollár [K] and Fitchäs-Galligo [F-G] obtained the bounds:

$$\deg q_j\leq\left(\frac{3}{2}\right)^n d_1\dots d_n \qquad \text{(Kollár)}, \tag{4}$$

*The detailed version of this paper has been submitted for publication elsewhere.

where x = number of indices i for which $d_i = 2$. Clearly this leads to the bound

$$\deg q_j \leq \{\max(3, d_1)\}^n. \tag{4'}$$

The bound of [F-G] is

$$\deg q_j \leq 3d_1 \ldots d_n. \tag{5}$$

In either case (4) or (5) the proof is completely algebraic and works over any field of characteristic zero. This is the pattern, analytic methods may be useful to guess or obtain a result about polynomial equations, but when a purely algebraic proof is found, then the estimates are sharper and the field of coefficients is not usually restricted to a subfield of $\mathbb{C}$.

Let us recall that d_1^n is the best possible estimate for the degrees of the q_j, as order of magnitude goes, given that there is an example showing that $\max_j \deg q_j \geq d_1^n - d_1^{n-1}$ [M-M] and [Ba-S].

The three above proofs are only existence proofs. Then the polynomials q_j could be effectively found considering the Bezout equation as a system of linear equations in the coefficients of q_j. Namely, each polynomial can be considered as a vector Q_j of length (approximately) $d_1^{n^2}$ and (1) becomes the system

$$(P_1 \mid P_2 \mid \ldots \mid P_m) \begin{pmatrix} Q_1 \\ \vdots \\ Q_m \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \tag{6}$$

where P_j is the (Toeplitz) matrix of multiplication by p_j. Therefore a solution to the system of equations (6) exists if and only if $V \neq \emptyset$. This provides a method to decide whether $V = \emptyset$, the number of operations is approximately $d_1^{n^2}$ (where factors depending only on n are disregarded). In fact, one can do better. By a convenient modification of the work of

Christov, Grigori'ev and Vorobjov [GV], Regenar and Canny have recently shown [R], [C] that there is an algorithm to decide whether a system of polynomial equations

$$p_1(x) = \ldots = p_m(x) = 0, \quad x \in \mathbb{R}^n, \tag{7}$$

$p_j \in \mathbb{Z}[z]$, $\deg p_j \leq D$, has a solution or not, with complexity $M(mD)^n$, where M depends on the size of the coefficients of the p_j. Independently, this result was obtained in [C-G-H] together with bounds on the complexity for parallelizable algorithms.

Another consequence of the method (6) to solve the equation (1) is the following. Let us recall that the (logarithmic) size of a rational number r/s, written in reduced form, is $\log \max(|r|,|s|)$. The size $h(q)$ of a polynomial $q \in \mathbb{Q}[z]$ is the maximum of the size of its coefficients. Suppose that the polynomials p_j in the Bezout equation (1) have size $h(p_j) \leq h$. Then, if $V = \emptyset$, there are solutions $q_j \in \mathbb{Q}[z]$ obtained via (6) for which

$$\deg q_j \leq d_1^n \quad \text{and} \quad h(q_j) \leq d_1^{n^2} h,$$

where we are only giving an order of magnitude estimate for $h(q_j)$. In order to improve on these estimates of size, one needs to explicitly exhibit polynomials $q_j \in \mathbb{Q}[z]$ solving (1), i.e., given by a formula. Following a suggestion from [B-S2], and formulas recently obtained in [B-Y1], [B-G-Y], one can show:

Theorem 1 [B-Y2]. Let $p_1,\ldots,p_m \in \mathbb{Z}[z]$, $\deg p_j \leq D$, $h(p_j) \leq h$, $V = \emptyset$. Then there exist $q_j \in \mathbb{Q}[z]$ solving the Bezout equation (1) such that

$$\deg q_j \leq nD^n$$

$$h(q_j) \leq c(n)\, D^{8n}\, (h + \log m).$$

This result is valid with D^n replaced by $d_1 \ldots d_n$ and $\mathbb{Z}$ replaced by $\mathcal{O}_k[t_1, \ldots t_\ell]$, $\mathcal{O}_k$ the integer ring of some extension k of the rationals.

It is clear that the constant $c(n)$ (explicitly computable) and the power $8n$ are not sharp. For that reason, it would be interesting to obtain this result by purely algebraic methods. The above proofs depend on Complex Analysis and, in particular, on the theory of Multidimensional Residues [B-G-Y]. On the other hand, even for generic situations one expects estimates of the order $D^n(h+\log m)$ for $h(q_j)$. We also note that this type of estimate seems to go hand in hand with the estimates for complexity of the decision problem "$V = \emptyset$ or not," reported above. It is plausible that there should be a theorem relating the sizes of solutions to polynomial equations to the complexity of finding them.

Let us turn now to the equation (2). This is only a new problem when $V \neq \emptyset$, which we will assume henceforth. Let us assume that $p_1, \ldots, p_m \in \mathbb{C}[z]$, I = ideal generated by them, $\deg p_j \leq D$ (bounds involving the degrees d_j can also be obtained). We will assume also that $\deg f = d$, and $f \in I$. Therefore, we know that a solution $q_1, \ldots, q_m$ of (2) exists. The question is how to estimate the degrees of the q_j, or more correctly, how to obtain q_j with good degree estimates.

The difficulty arises out of an example of Mayr-Meyer [M-M], as refined by Bayer-Stillman [Ba-S]. Given D, n (in fact $D \geq 5$) they show the existence of polynomials $p_1, \ldots, p_{n+1}$ of degree D, more precisely, they are sums and differences of monomials, and f, linear homogeneous, such that $f \in I(p_1, \ldots, p_{n+1})$ but whenever we write

$$f = \sum_{j=1}^{n+1} p_j q_j$$

it follows that

$$\max \deg q_j \geq D^{2^n}.$$

(In fact, the exponent they obtain is $2^{n/5}$.) The interest of these kinds of estimates is, among others, that it implies that in general the standard bases algorithm takes doubly exponential time to be completed.

On the other hand, Brownawell [B2] has introduced a very ingenious modification of Rabinowitsch's trick and shown that for any $p_1,\ldots,p_m$ if g vanishes on V, $\deg g \leq D$, then one can write

$$g^s = \sum_1^{n+1} a_j p_j,$$

with $s \leq D^n$ and $\deg q_j \leq D^n$. In particular, that means that in the example of Mayr-Meyer there are lots of compensations when we consider f^s, $s = D^n$. In fact, Philippon [P] has communicated to us that for that particular example of [Ba-S], there exist b_j of degree $\leq D^n$ such that

$$f^n = \sum_{j=1}^{n+1} b_j p_j.$$

It is plausible that this situation be time in general.

Using the same kind of analytic tools employed in Theorem 1, one can prove the following results.

Theorem 2 [B-Y3]. Let $p_1,\ldots,p_m \in \mathbb{Z}[z_1,\ldots,z_n]$, $f \in I(p_1,\ldots,p_m)$, $\deg f = d$, $\deg p_j \leq D$ and V be a discrete variety in $\mathbb{C}^n$. Then there are $q_j \in \mathbb{C}[z]$ such that $f \in \sum_1^m p_j q_j$ and

$$\deg q_j \leq c(n)(d+D^n).$$

Theorem 3 [B-Y3]. Under the same hypothesis of Theorem 2, except that V instead of being discrete is assumed to satisfy $\dim V = n-m$, we obtain the

same conclusion as in the previous theorem.

Amoroso [A] has recently found an algebraic proof of Theorems 2 and 3 using Kollár's method [K].

Note that under the above conditions of Theorems 2 and 3, the decision of whether $f \in I(p_1,\dots,p_m)$ is of complexity $O(D^{n^2})$ if $d \le D$.

Finally, we have a preliminary result that indicates that Philippon's remark about Mayr-Meyer's example might not be altogether unusual.

Theorem 4 [B-Y4]. Let $p_1,\dots,p_m \in \mathbb{C}[z]$ be such that the singular set of V is discrete, let $f \in I(p_1,\dots,p_m)$, $\deg f \le D$, $\deg p_j \le D$. Then there exist $q_j \in \mathbb{C}[z]$ such that

$$f^n = \sum_{j=1}^{m} p_j q_j$$

and

$$\deg q_j \le c(n)D^n.$$

It would be very interesting to know whether such a result holds in general.

I would like to conclude with some questions implicit in [B-S3]. They require a kind of algebraic (non-linear) Hahn-Banach separation theorem.

Question 1. Let K be a convex closed cone in $\mathbb{C}^n$, V an algebraic variety, $0 < \dim V < n-1$, $V \cap K = \emptyset$. Assume moreover that there exists $\varepsilon > 0$, $N \ge 0$ such that

$$\operatorname{dist}(z,K)(1+|z|)^N \ge \varepsilon \quad \text{for any } z \in V. \tag{8}$$

(a) Is there a polynomial P such that $V \subseteq \{P = 0\}$, $\{P = 0\} \cap K = \emptyset$, and ε', N' such that

$$\operatorname{dist}(z,K)(1+|z|)^{N'} \ge \varepsilon' > 0 \quad \text{for any } z,\ P(z) = 0? \tag{9}$$

(b) Does there exist the polynomial P if we do not assume (8)?

(c) Can one take $N' = N$?

The cases when $\dim V = 0$ or $n-1$ are trivial. If $K = \mathbb{R}^n$ the statement without conditions (8) and (9) is trivial, but otherwise it is a deep result of Lech (cf. [B-S3], for references and partial results).

Question 2. Let U be the open polydisk in $\mathbb{C}^n$, V an algebraic variety, $0 < \dim V < n-1$, $V \cap U = \emptyset$. Does there exist a polynomial P such that

$$\{P = 0\} \supseteq V \quad \text{and} \quad \{P = 0\} \cap U = \emptyset?$$

Can we do this construction purely algebraically?

Finally, let us mention that since this conference was given a report by Teissier has touched in more detail upon some of the above algebraic problems as well as our work, see [T].

Acknowledgements. This paper was written while on a visit to the Soviet Union in an exchange program between the National Academy of Sciences and the Soviet Academy of Sciences. I would like to thank both organizations for this opportunity, as well as the National Science Foundation and the AFOSR for the continuing support of my work.

References

[A] F. Amoroso, Tests d'appartenance d'après un Théorème de Kollár, preprint, 1989.

[Ba-S] D. Bayer and M. Stillman, Invent. Math. 87 (1987), 1-11.

[B-G-Y] C. Berenstein, R. Gay and A. Yger, Forum Math. 1 (1989).

[B-S1] C. Berenstein and D. Struppa, Linear Algebra Appl. 98 (1988), 41-52.

[B-S2] _____, Syst. Control Letters 4 (1984), 33-39.

[B-S3] _____, Syst. Control Letters 6 (1986), 309-314.

[B-Y1] C. Berenstein and A. Yger, Advances Applied Math. 10 (1989), 33-166.

[B-Y1] _____, Effective Bezout identities in $\mathbb{Q}[z_1,\ldots,z_n]$, preprint, 1988.

[B-Y2] _____, Bounds for the degrees in the division problem, to appear in Mich. Math. J.

[B-Y3] _____, work in progress.

[B1] D. Brownawell, Annals of Math. 126 (1987), 577-591.

[B2] _____, J. Amer. Math. Soc. 1 (1988), 311-322.

[C-G-H] L. Caniglia, A. Galligo and H. Heintz, Some new effectivity bounds in computational geometry, preprint, 1987.

[C] J. Canny, 20th Annual ACM Symp. Th. Comp. (1988), 460-467.

[F-G] N. Fitchäs and A. Galligo, Sém. Structures alg. ordonées 1987-88, Univ. Paris VII.

[GV] D. Yu. Grigor'ev and N.N. Vorobjov, Jr., J. Symbolic Computation 5 (1988), 37-64.

[K] J. Kollár, J. Amer. Math. Soc. 1 (1988), 963-975.

[M-M] E. Mayr and A. Meyer, Advances Math. 46 (1982), 305-329.

[P] Philippon, personal communication.

[R] J. Regenar, Proc. 29th Annual Symp. Found. Comp. Science 1988, 291-295.

[T] B. Teissier, Sém. Bourbaki 42 (1989-90), no. 718 (Nov. 1989), to appear.