KYBERNETIKA — VOLUME 23 (1987), NUMBER 5

MINIMAL DEGREE SOLUTIONS FOR THE BEZOUT EQUATION

EDOARDO BALLICO, DANIELE C. STRUPPA

We prove two results on the existence of bounds on the (global) degrees of polynomials X_i, solutions to the Bezout equation $A_1X_1 + \ldots + A_rX_r = C$, with A_i, C, X_i in $\mathbb{C}[x_1, \ldots, x_n]$. In the first theorem we require an algebraic hypothesis on the maximum degree homogeneous component of $A_1, \ldots, A_r$; while the second result holds for all Bezout equations, but $r = 2$ is needed. Several variations and examples are discussed.

0. Many concrete problems in the theory of multidimensional systems and control theory lead naturally to the study of various aspects of the so called Bezout equation

$$(1) \qquad A_1X_1 + \ldots + A_rX_r = C$$

with A_i, C given polynomials in $\mathbb{C}[x_1, \ldots, x_n]$, and X_i unknown ones, [2], [7]. Solvability conditions and explicit constructions for the solutions of (1), even in the case of matrices, are well known, see e.g. [1], but some recent papers, [3], [6], have now focalized on the problem of finding minimal degree solutions for (1). However, both in [3] and in [6], the results which one obtains are for minimal degree solutions with respect to a chosen variable, and no global bounds are given.

In the first part of this paper we slightly modify the techniques used in [3] to obtain global bounds for the degree of solutions of (1); we actually give several versions of such a result; the drawback of our approach is that a very strong algebraic hypothesis is needed on $A_1, \ldots, A_r$ to make the machinery work; on the other hand we can use our result as a theorem on the non-solvability of (1).

We feel that many optimal results in this area are probably hidden in the vast literature on algebraic geometry, whose methods we employ in the last section of the paper, to give a more applicable theorem for Bezout equations in which, however, $r = 2$. We finally give some examples for which our bounds cannot be improved.

1. In this section we improve some results contained in [3]; the techniques we employ do not differ very much from those of [3] itself.

We start with an algebraic definition which we take from [6]:

Definition 1. Let $p_1, \ldots, p_k$ be polynomials in $\mathbb{C}[x_1, \ldots, x_n]$. We say that $(p_1, \ldots, p_k)$ form a ***regular sequence*** if p_j is not a zero divisor in $\mathbb{C}[x_1, \ldots, x_n]/(p_1, \ldots, p_{j-1})$, for all $j = 2, \ldots, k$.

If A is a polynomial in $\mathbb{C}[x_1, \ldots, x_n]$, we denote by $A^{\max}$ its maximum degree homogeneous component; with these notation we can state the following:

Theorem 2. Let $A_1, \ldots, A_r \in \mathbb{C}[x_1, \ldots, x_n]$ be such that, for each subset $(i_1, \ldots, i_k)$ of $(1, \ldots, r)$, the family $(A_{i_1}^{\max}, \ldots, A_{i_k}^{\max})$ is a regular sequence. Let $C \in \mathbb{C}[x_1, \ldots, x_n]$ be such that (1) has a solution. Then there exists a solution $X_1, \ldots, X_r$ of (1) with $\deg(X_i) + \deg(A_i) \leqq \deg(C)$, for all $i = 1, \ldots, r$.

Proof. Let $X_1, \ldots, X_r$ be a solution of (1) and let $(i_1, \ldots, i_k) \subseteq (1, \ldots, r)$ be the set of indices j for which $\deg(A_j) + \deg(X_j)$ is maximal. If $\deg(A_{i_1}) + \deg(X_{i_1}) \leqq \leqq \deg(C)$ the theorem is proved; otherwise we can suppose $\deg(A_{i_1}) + \deg(X_{i_1}) > > \deg(C)$; this implies that

$$A_{i_1}^{\max} . X_{i_1}^{\max} + \ldots + A_{i_k}^{\max} . X_{i_k}^{\max} = 0\,,$$

and by the hypothesis of regularity we deduce

$$X_{i_1}^{\max} = \alpha_2 A_{i_2}^{\max} + \ldots + \alpha_k A_{i_k}^{\max}\,,$$

for $\alpha_2, \ldots, \alpha_k$ homogeneous polynomials (not all identically zero) of degrees $\deg(\alpha_j) = = \deg(X_{i_1}^{\max}) - \deg(A_{i_j}^{\max})$. We now construct a new solution of (1) by

$$\begin{aligned} X'_{i_1} &= X_{i_1} - \alpha_2 A_{i_2} - \ldots - \alpha_k A_{i_k} \\ &\vdots \\ X'_{i_j} &= X_{i_j} + \alpha_j A_{i_1} \quad j = 2, \ldots, k \\ &\vdots \\ X'_t &= X_t \qquad\qquad t \notin (i_1, \ldots, i_k)\,; \end{aligned}$$

the new solution obtained in this way is now such that $\deg(X'_{i_1}) < \deg(X_{i_1})$, while $\deg(X'_t) \leqq \deg(X_t)$, for all $t \neq i_1$. The thesis now follows by iterating the argument. □

Remark 3. (a) Notice that the definition of regular sequence implies, in the case of $p_1, \ldots, p_k$ homogeneous polynomials, that the dimension of the variety $\{z \in \mathbb{C}^n : p_1(z) = \ldots = p_k(z) = 0\}$ is exactly $n - k$.

(b) Theorem 2 extends immediately to the case of weighted homogeneous polynomials. In this case the regularity assumption is required on the components $A_i^{\max}$ of A_i of maximum weight, and then the theorem runs as above, with "degree" everywhere substituted by 'weight".

(c) Theorem 2 can be interpreted as giving strong restrictions on the polynomials C for which (1) can be solved; in particular one can never hope to find a solution with $C = 1$, whenever the A_i's satisfy the regularity hypothesis mentioned in the theorem (which, on the other hand, implies $r \leqq n$).

Following through the proof of Theorem 2, one can immediately obtain two small modifications, which appear as corollaries to its proof:

Corollary 4. Suppose that the equation

$$A_1X_1 + \ldots + A_rX_r + B_1Z_1 + \ldots + B_kZ_k = C \tag{2}$$

has a solution $(X_1^0, \ldots, X_r^0, Z_1^0, \ldots, Z_k^0)$, and suppose that every subset of $A_1^{\max}, \ldots$ $\ldots, A_r^{\max}$ is a regular sequence. Then (2) has a solution $(X_1, \ldots, X_r, Z_1, \ldots, Z_k)$ with $Z_i = Z_i^0$ for all i, and $\deg(X_i) + \deg(A_i) \leqq \max(\deg(C), \deg(B_j) + \deg(Z_j^0))$.

Proof. Simply move $B_1Z_1^0 + \ldots + B_kZ_k^0$ on the right hand side, and then apply Theorem 2. □

Corollary 5. Suppose that (2) has a solution, that every subset of $A_1^{\max}, \ldots, A_r^{\max}$ is a regular sequence and that the ideal generated by $A_1^{\max}, \ldots, A_r^{\max}$ contains $(x_1, \ldots, x_n)^t$ for some positive t (this, in particular, implies that $r = n$). Then (2) admits a solution $(X_1, \ldots, X_r, Z_1, \ldots, Z_k)$ with $\deg(Z_j) \leqq t - 1$ for all j, and $\deg(X_i) + \deg(A_i) \leqq \max(\deg(C), t - 1 + \deg(B_i))$.

Proof. First one reduces a solution of (2) to the case in which $\deg(Z_j) \leqq t - 1$ for all j (this can be easily achieved by using the trivial syzygies of (2), and using the fact that $(A_1^{\max}, \ldots, A_r^{\max})$ contains $(x_1, \ldots, x_n)^t$); one then uses Corollary 4. □

Remark 6. Notice that the use of the Koszul complex, see e.g. [4], shows that, for $r \geqq 2$, it is $t \leqq \sum_{i=1}^{r} \deg(A_i) - r + 1$, with equality if $\deg(A_i) > 0$ for all i (indeed $H^i(\mathbb{P}^r, \mathcal{O}(t)) = 0$ if $1 \leqq i \leqq r - 1$ or $i = r$, $t \geqq 1 - r$, while it is different from zero if $i = r$, $t = -r$).

2. In this section we use a completely different technique to prove a theorem similar to Theorem 2, which, however is true for $r = 2$ and needs no other hypotheses.

Theorem 7. Let $A, B \in \mathbb{C}[x_1, \ldots, x_n]$ have no common zeroes. Then if $\deg(A) > 0$, $\deg(B) > 0$, equation

$$AX + BY = 1 \tag{3}$$

has solutions X, Y with $\deg(X) \leqq (\deg(B) - 1) \cdot \deg(A)$, and $\deg(Y) \leqq (\deg(A) - 1) \cdot \deg(B)$.

Proof. Add a new variable x_0 and let A', B' be the polynomials obtained from A, B by homogenizing them with x_0. For (X, Y) a solution of (3), which certainly exists as A, B have no common zeroes, denote by (X', Y') the corresponding homogenized polynomials, and let $k = \deg(A) + \deg(X) = \deg(B) + \deg(Y)$; then

$$A'X' + B'Y' = x_0^k. \tag{4}$$

If, viceversa, (X', Y') is a solution of (4) with X', Y' non both divisible by x_0, we can deduce, from (4), a solution (X, Y) for (3) with $\deg(A) + \deg(X) = \deg(B) + \deg(Y) = k$. Therefore, it is sufficient to find the smallest integer k for which (4) has a solution. Let E be the scheme in $\mathbb{P}^n$ defined by A', B'; since (A', B') are a regular sequence, it is well known (see e.g. [4]) that (4) has a solution if and only if x_0^k vanishes (counting multiplicities) on E. Therefore if we prove that x_0^{ab}, for $a = \deg(A)$, $b = \deg(B)$, vanishes on E, we get $k \leqq ab$, i.e. the thesis. Indeed, since E is a complete intersection and has no immersed components, we can reduce ourselves (by intersecting with a general $\mathbb{P}^2$) to the case $n = 2$, length $(E) = ab$. Let then L be the line $\{x_0 = 0\}$ and let L^k denote $\{x_0^k = 0\}$. By the Nullstellensatz we have $L^m \supset E$ if $m \gg 0$ and $L^{j+1} \cap E \supseteq L^j \cap E$. We can now show that if $L^{j+1} \cap E = L^j \cap E$, one has that $L^j \supseteq E$. Indeed if I denotes the ideal of E, from $L^{j+1} \cap E = L^j \cap E$ it follows that $x_0^j = \alpha x_0^{j+1} + \beta i$, with $i \in I$, α, β holomorphic in a neighborhood of E. Recursively we then obtain that, for all $m \gg 0$, $L^m \cap E = L^j \cap E$. This, in turn, implies that, for $m \gg 0$, $E = L^m \cap E = L^j \cap E$. Therefore, if x_0^d does not vanish on E, it is $\dim H^0(\mathcal{O}_{L^{j+1} \cap E}) > \dim H^0(\mathcal{O}_{L^j \cap E})$ for $d \geqq j + 1$, i.e., $\dim H^0(\mathcal{O}_E) \geqq d$; but by Bezout theorem $\dim H^0(\mathcal{O}_E) = ab$, and the thesis follows. □

Remark 8. From the proof one sees that, in the statement of Theorem 7, one has the equality if and only if (after cutting with a general $\mathbb{P}^2$) $\{A' = 0\}$ and $\{B' = 0\}$ intersect in a single point P, where they must be smooth and non-tangent to L. This observation enables us to provide a few examples in which our bounds cannot be improved: namely we can take: i) A to be a line in $\mathbb{C}^2$, B another line in $\mathbb{C}^2$, counted $b \geqq 1$ times, which intersect A at infinity; ii) A a conic in $\mathbb{C}^2$, B the line, counted $b \geqq 1$ times, tangent to A at infinity; iii) A a smooth cubic in $\mathbb{C}^2$, B the tangent to A, at the improper inflection point of A, counted $b \geqq 1$ times.

A simple extension of Theorem 7 is the following

Theorem 9. Let $A, B, C \in \mathbb{C}[x_1, \ldots, x_n]$, $\deg(A) > 0$, $\deg(B) > 0$, and suppose that

$$AX + BY = C \tag{5}$$

has a solution. Then (5) has a solution with

$$\deg(X) + \deg(A) \leqq \deg(C) + \deg(A) \cdot \deg(B) - s\,,$$

$$\deg(Y) + \deg(B) \leqq \deg(C) + \deg(A) \cdot \deg(B) - s\,,$$

where, if D is the greatest common divisor of A and B, and V is the variety defined in $\mathbb{C}^n$ by $\{A/D = B/D = 0\}$, $s = \sum \operatorname{mult}(V_j) \cdot \deg(V_j)$, the sum being extended to the irreducible components of V.

Proof. If $D = 1$, the proof runs as in Theorem 7; if $\deg(D) \geqq 1$, D also divides C, and one reduces to the case $D = 1$. □

Remark 10. a) It is obvious to notice that the bound in Theorem 9 is optimal in many concrete instances, e.g. when $\{A' = 0\} \cap \{B' = 0\} \cap \{x_0 = 0\} = \{0\}$. b) Theorem 7 and Theorem 9 might be extended to the case $r > 2$ by simply asking a regulatity condition on the homogenized of $A_1, \ldots, A_r$ $(r \leqq n + 1)$ (this condition is trivially satisfied when $r = 2$); in this case one would get the existence of a solution $(X_1, \ldots, X_r)$ with $\deg(X_i) \leqq \sum_{j=1}^{r} \deg(A_j) - \deg(A_i)$ (if $C = 1$), and a corresponding bound if $C \neq 1$.

(Received September 19, 1986.)

REFERENCES

[1] C. A. Berenstein and D. C. Struppa: On explicit solutions to the Bezout equation. Syst. Control Lett. *4* (1984), 33—39.

[2] N. K. Bose: Applied Multidimensional Systems Theory. Van Nostrand, New York 1982.

[3] G. Gentili and D. C. Struppa: Minimal degree solutions of polynomial equations. Kybernetika *23* (1987), 1, 44—53.

[4] P. Griffiths and J. Harris: Principles of Algebraic Geometry. Wiley-Interscience, New York 1978.

[5] H. Matsumura: Commutative Algebra. Benjamin, New York 1970.

[6] M. Šebek: 2-D polynomial equations. Kybernetika *19* (1983), 212—224.

[7] E. D. Sontag: Linear systems over commutative rings: a (partial) updated survey. In: Proceedings IFAC/81, Kyoto, Japan 1981.

Dr. Edoardo Ballico and Dr. Daniele Struppa, Scuola Normale Superiore, Piazza dei Cavalieri 7, 56100 Pisa. Italy.