40
Some Remarks on Bezout's Theorem and Complexity Theory

MICHAEL SHUB*

We begin by establishing the smoothness and irreducibility of certain algebraic varieties. Whereas these facts must be standard to algebraic geometers, they do not seem readily available.

For d and n positive integers, let $\mathscr{F}_{d,n}$ and $\mathscr{H}_{d,n}$ denote the spaces of polynomial mappings and homogeneous polynomial mappings $f\colon \mathbb{C}^n \to \mathbb{C}$ of degree less than or equal to d in the case of $F_{d,n}$ and equal to d in the case of $H_{d,n}$. For a multi-index $D = (d_1, \ldots, d_k)$, let $\mathscr{F}_{D,n}$ and $\mathscr{H}_{D,n}$ be the products

$$\prod_{i=1}^{k} \mathscr{F}_{d_i,n} \quad \text{and} \quad \prod_{i=1}^{k} \mathscr{H}_{d_i,n}.$$

So an element $F \in \mathscr{F}_{D,n}$ or $\mathscr{H}_{D,n}$ is a polynomial mapping $F\colon \mathbb{C}^n \to \mathbb{C}^k$. The evaluation map ev: $\mathscr{F}_{D,n} \times \mathbb{C}^n \to \mathbb{C}^k$ and ev: $\mathscr{H}_{D,n} \times \mathbb{C}^n \to \mathbb{C}^k$ is just the map $(F, x) \to F(x)$. For fixed F, $F^{-1}(0) \subset \mathbb{C}^n$ is the algebraic set determined by the simultaneous vanishing of the $f_{d_i,n}$.

Lemma 1. *Any $y \in \mathbb{C}^k$ is a regular value for*

$$\text{ev}\colon H_{D,n} \times (\mathbb{C}^n - \{0\}) \to \mathbb{C}^k$$

and

$$\text{ev}\colon F_{D,n} \times \mathbb{C}^n \to \mathbb{C}^k.$$

PROOF. $D\text{ev}_{(F,x)}(h, v) = h(x) + DF_x(v)$. The values of $h(x)$ alone are sufficient to make $D_{(F,x)}\text{ev}$ surjective.

Thus, by the implicit function theorem the union of the algebraic sets determined by the F's is smooth in the product. For $F \in \mathscr{F}_{D,n}$, let $Z_F = \{x | F(x) = 0\}$, $Z_{F_{D,n}} = Z_{\mathscr{F}} = \{(F, x) | F(x) = 0\}$. Similarly for $F \in H_{D,n}$, let $Z_F = \{x \in \mathbb{C}^n - \{0\} | F(x) = 0\}$, $Z_{\mathscr{H}_{D,n}} = Z_{\mathscr{H}} = \{(F, x) \in \mathscr{H}_{D,n} \times (\mathbb{C}^n - \{0\}) | F(x) = 0\}$, and $Z_{\hat{\mathscr{H}}_{D,n}} = Z_{\hat{\mathscr{H}}} = \{(F, x) \in Z_{\mathscr{H}} | F \not\equiv 0\}$; $Z_{\mathscr{F}}$ and $Z_{\mathscr{H}}$ are $\text{ev}^{-1}(0)$, so we have:

Proposition 1. (a) *$Z_{\mathscr{F}}$ is a connected smooth variety in $\mathscr{F}_{D,n} \times \mathbb{C}^n$ of codimension k;*

* Partially supported by an NSF grant.

(b) *$Z_{\mathscr{H}}$ and $Z_{\hat{\mathscr{H}}}$ are connected smooth varieties in $\mathscr{H}_{D,n} \times (\mathbb{C}^n - \{0\})$ of codimension k.*

Proof. (b) It remains to prove the connectedness. The group of linear isomorphisms acts transitively on $\mathbb{C}^n - \{0\}$, and on $\mathscr{H}_{D,n} \times (\mathbb{C}^n - \{0\})$ by $(F, x) \rightarrow (F \circ L^{-1}, Lx)$, this action preserves $Z_{\mathscr{H}}$ and $Z_{\hat{\mathscr{H}}}$. Thus, the maps $Z_{\mathscr{H}} \rightarrow \mathbb{C}^n - \{0\}$, $Z_{\hat{\mathscr{H}}} \rightarrow \mathbb{C}^n - \{0\}$ are surjective locally trivial fibrations with connected base and connected fiber so they are connected, as follow: Given (f_1, x_1) and (f_2, x_2) in $Z_{\hat{\mathscr{H}}}$, choose a path x_t from x_1 to x_2, for $1 \leq t \leq 2$. Now lift x_t to $(\hat{f}_t, x_t)$ such that $\hat{f}_1 = f_1$; the endpoint of this path is in the fiber over x_2. This is a complex linear space minus 0 and, hence, is connected, so we continue the path in the fiber to (f_2, x_2). The same argument holds for $Z_{\mathscr{H}}$; for $Z_{\mathscr{F}}$, simply replace the linear group by the affine group.

We use $P(V)$ to denote the projective space of the vector space V, i.e., $V - 0$ mod the action of the nonzero scalars $\mathbb{C}^* = \mathbb{C} - 0$ and $P\mathbb{C}(n-1)$ for the projective space of $\mathbb{C}^n$.

$$\mathbb{C}^* \times \mathbb{C}^* \text{ acts freely on } (\mathscr{H}_{D,n} - \{0\}) \times (\mathbb{C}^n - \{0\})$$

by coordinatewise multiplication. Let N denote the dimension of $\mathscr{H}_{D,n}$:

$$N = \sum_{i=1}^{k} \binom{n + d_i - 1}{d_i}.$$

The $\mathbb{C}^* \times \mathbb{C}^*$ action leaves $Z_{\hat{\mathscr{H}}} \subset \mathscr{H}_{D,n} \times \mathbb{C}^n - \{0\}$ invariant. As the action is transversal to $S^{2N-1} \times S^{2n-1}$, $Z_{\hat{\mathscr{H}}} \cap S^{2N-1} \times S^{2n-1}$ is a smooth manifold, and, therefore, the quotient of $Z_{\hat{\mathscr{H}}}$ by the $\mathbb{C}^* \times \mathbb{C}^*$ action is the same as $Z_{\hat{\mathscr{H}}} \cap S^{2N-1} \times S^{2n-1}$ by the unit complexes $S^1 \times S^1$. This later group is compact. So the quotient by the free action is a smooth subvariety $\mathscr{Z}_{D,n} = \mathscr{Z}$ of $P(\mathscr{H}_{D,n}) \times P\mathbb{C}(n-1)$. As $Z_{\hat{\mathscr{H}}}$ is connected, so is the quotient manifold $\mathscr{Z}$. A connected, smooth projective variety is irreducible.

Theorem 1. *$\mathscr{Z}_{D,n}$ is a connected, smooth irreducible projective subvariety of $P(\mathscr{H}_{D,n}) \times P\mathbb{C}(n-1)$ of codimension k.*

Let $C_{D,n} = \{F \in \mathscr{H}_{D,n} - \{0\} | \exists x \in \mathbb{C}^n - \{0\} \text{ with } F(x) = 0\}$, i.e., $C_{D,n}$ is the set of those systems with a common root. Let $\mathscr{C}_{D,n}$ be the image of $C_{D,n}$ in $P(\mathscr{H}_{D,n})$.

Corollary 1. *$\mathscr{C}_{D,n}$ is an irreducible subvariety of $P(\mathscr{H}_{D,n})$.*

Proof. It is the projection of $\mathscr{Z}_{D,n}$ on $P(\mathscr{H}_{D,n})$; as $\mathscr{Z}_{D,n}$ is irreducible, its image must be.

The case of $(n-1)$ homogeneous polynomials in n variables is the case of Bezout's theorem; there are generically

$$\prod_{i=1}^{n-1} d_i$$

roots and $\mathscr{C}_{D,n} = P(\mathscr{H}_{D,n})$ has the same dimension as $\mathscr{Z}_{D,n}$, i.e., the map $\mathscr{Z}_{D,n} \subset P(\mathscr{H}_D) \times \mathbb{C}P(n-1)$ induced by projection on the first factor is a surjection, almost every point is a regular point of the projection, and the fiber has πd_i points. We give a proof here.

Bezout's Theorem

Let $F = (f_1, \ldots, f_{n-1}) \in P(\mathscr{H}_{D,n})$, where f_i is homogeneous of degree $d_i > 0$, not all identically zero. Let $Z_j = Z_j(F)$, $j = 1, \ldots, k$, be the connected components of $\mathscr{Z}_F \subset \mathbb{C}P(n-1)$, where $\mathscr{Z}_F$ is the projection into $\mathbb{C}P(n-1)$ of $Z_F - \{0\} = \{x \in \mathbb{C}^{n-1} - \{0\} \mid F(x) = 0\}$. Then we may assign an index $i(Z_j)$ to each Z_j which is

(a) positive,
(b) $\sum i(Z_j) = \prod_{i=1}^{n} d_i$,
(c) $i(Z_j) = 1$ for a nondegenerate isolated zero, and
(d) there are neighborhoods U_j of Z_j in $\mathbb{C}P(n-1)$ and $\mathscr{N}$ of F in $\mathscr{H}_{D,n}$ such that if $G = (g_1, \ldots, g_{n-1}) \in \mathscr{N}$, then $Z(G) \subset \bigcup_j U_j$ and $\sum i(Z_\ell(G)) = i(Z_j)$, where the sum is taken over all components of $Z(G)$ contained in U_j.

Proof. First consider closed disjoint neighborhoods U_j of Z_j in $\mathbb{C}P(n-1)$ and a ball $\mathscr{N}$ around $F = (f_1, \ldots, f_{n-1}) \in P(\mathscr{H}_{D,n})$ such that $Z(G) \subset \bigcup \mathring{U}_j$ for all $G \in \mathscr{N}$. The critical values of the projection $\pi\colon \mathscr{Z}_{D,n} \to P(\mathscr{H}_{D,n})$ lie in a subvariety $\mathscr{D}$ of $P(\mathscr{H}_{D,n})$ (the "discriminant variety"). A fairly standard calculation shows that the regular points of the projection π are precisely those F with nondegenerate zeros. If we consider the polynomial system

$$F = (f_1, \ldots, f_{n-1}), \qquad f_i(x_1, \ldots, x_n) = x_i^{d_i} - x_n^{d_i},$$

then we see that F has $\pi\, d_i$ nondegenerate zeros. Thus, the regular values of π are open and $\mathscr{D}$ has codimension at least one. Therefore, $P(\mathscr{H}_{D,n}) - \mathscr{D}$ is arc connected. Continuing the roots along paths in $P(\mathscr{H}_{D,n}) - \mathscr{D}$, we see the number of roots is constant, off $\mathscr{D}$. Moreover, $\mathscr{N} - \mathscr{D}$ is also arc connected, and we define $i(Z_j)$ to be the number of roots of any G in $\mathscr{N} - \mathscr{D}$ which lie in U_j. This establishes (b), (c), and (d). To prove (a), we return to the projection $\pi\colon \mathscr{Z}_{D,n} \to P(\mathscr{H}_{D,n})$. Given $F \in P(\mathscr{H}_{D,n})$, the connected components Z_j, $j = 1, \ldots, k$, of $\mathscr{Z}_F$, and disjoint neighborhoods V_i of $\{F\} \times Z_j$ in $\mathscr{Z}_{D,n}$, we find points in $\mathscr{N} - \mathscr{D}$ which are in $\pi(V_i)$ for each i, as follows: Since $\mathscr{Z}_{D,n}$ is irreducible, the noncritical values of π are open and dense, the image of every open set contains interior, and since $\mathscr{N} - \mathscr{D}$ is open and dense in $\mathscr{N}$, there must be points in V_i with image in $\mathscr{N} - \mathscr{D}$. Now given neighborhoods U_j of Z_j, choose $\mathscr{N}$ small enough so that the zeros of all G in $\mathscr{N}$ are in $\bigcup U_j$ and let $V_i = (\mathscr{N} \times U_i) \cap \mathscr{Z}_{D,n}$. This finishes the proof.

Remark 1. The indices $i(Z_j)$ may be given several topological definitions. Let $F = (f_1, \dots, f_{n-1})$, where the f_i are irreducible and let $\mathscr{Z}_{f_i}$ be the projection into $\mathbb{C}P(n-1)$ of the set Z_{f_i}. Thus, $\mathscr{Z}_F = \bigcap \mathscr{Z}_{f_i}$. Let

$$\mathscr{Z} = \mathscr{Z}_{f_1} \times \mathscr{Z}_{f_2} \times \cdots \times \mathscr{Z}_{f_{n-1}} \subset \underbrace{\mathbb{C}P(n-1) \times \cdots \times \mathbb{C}P(n-1)}_{n-1}$$
$$\equiv \mathbb{C}P^{n-1}(n-1).$$

Let $\Delta = \{(z_1, \dots, z_{n-1}) \in \mathbb{C}P^{n-1}(n-1) | z_i = z_j \ \forall_{i,j}\}$ be the small diagonal. $\mathscr{Z}_F$ is homeomorphic to $\mathscr{Z} \cap \Delta$. We can now compute the homological intersection of $\mathscr{Z}$ and Δ in two ways. First, since f_i is irreducible, $Z(f_i)$ represents d_i times the generator in $H_{2_{n-4}}(\mathbb{C}P(n-1))$. Now the algebraic structure on $\mathbb{C}P^{n-1}(n-1)$ and the Kunneth formula gives πd_i for the intersection of $\mathscr{Z}$ and Δ.

Next consider

$$\begin{tikzcd}
 & & H_0(\Delta) \\
H_{(2n-4)(n-1)}(\mathscr{Z}) \arrow[r] \arrow[dr] & H_{(2n-4)(n-1)}(\mathbb{C}P^{n-1}(n-1)) \arrow[r] & H_{(2n-4)(n-1)}(\mathbb{C}P^{n-1}(n-1), \mathbb{C}P^{n-1}(n-1) - \Delta) \arrow[u] \\
 & H_{(2n-4)(n-1)}(\mathscr{Z}, \mathscr{Z} - \mathscr{Z} \cap \Delta) \approx \sum_{i=1}^{k} H_{(2n-4)(n-1)}(V_i, V_i - Z_i) \arrow[ur] &
\end{tikzcd}$$

where V_i are disjoint closed neighborhoods of the connected components Z_i of $\mathscr{Z} \cap \Delta$ in $\mathscr{Z}$. The intersection number is the image of the generator of $H_{(2n-4)(n-1)}(\mathscr{Z})$ in $H_0(\Delta)$. All the maps are induced by inclusion, except for the isomorphism in the bottom row which is given by excision and the map

$$H_{(2n-4)(n-1)}(\mathbb{C}P^{n-1}(n-1), \mathbb{C}P^{n-1}(n-1) - \Delta) \to H_0(\Delta)$$

which is the Thom isomorphism (see [Dold]). This gives a topological method of computing $i(Z_j)$ when $F = (f_1, \dots, f_{n-1})$ has irreducible components. If Z_i is a nondegenerate zero, $H_{(2n-4)(n-1)}(V_i, V_i - Z_i)$ contributes a plus 1 to the sum.

Remark 2. We can also give a topological computation of the index as the degree of the map

$$\pi_Y \colon H_{\text{top}}(\mathscr{Z}_{D,n}, \mathscr{Z}_{D,n} - \{f\} \times Z_i) \to H_{\text{top}}(P(\mathscr{H}_{D,n}), P(\mathscr{H}_{D,n}) - \{f\})$$

(see [Dold]).

Zulehner has proposed using continuation techniques along a projective line to solve systems of equations [Zulehner]. Canny's generalized characteristic polynomial methods show some of the same geometric features, which we state in the next theorem. Let L be a projective line contained in $P(\mathscr{H}_{D,n})$ and suppose that L is not contained in $\mathscr{D}$. Then for an open dense set of points U in L, $G \in U$ has πd_i zeros and $W = \mathscr{Z}_{D,n} \cap \pi^{-1}(U)$ is a πd_i-to-one covering space of U. $\pi^{-1}(L)$ is a subvariety of $\mathscr{Z}_{D,n}$ and W is Zariski dense in $R(L) = V_1 \cup \cdots \cup V_k$, where V_i are irreducible curves. We claim $R(L) = \overline{W}$ in the usual topology and is, in fact, W union a finite number of points. Suppose U' is an open set in $R(L) - W$, then it intersects some V_i in an open set and, hence, by irreducibility of V_i, W in an open set which is a contradiction. Thus, $R(L) = \overline{W}$. Moreover, $R(L) - W$ only contains points in $\pi^{-1}(L \cap \mathscr{D})$ which are π^{-1} of a finite number of points. These fibers which intersect $R(L)$ cannot contain varieties of dimension one, for these curves would then have open sets disjoint from $U \cap V_i$ for each i. So we have proven:

Theorem 2. *Let $L \subset P(\mathscr{H}_{D,n})$ be a projective line not contained in $\mathscr{D}$ and $U = L - \mathscr{D}$. Let $\mathscr{Z}_{D,n} \subset P(\mathscr{H}_{D,n}) \times \mathbb{C}P(n-1)$ be the projection of $\{(F, x) \in \mathscr{H}_{D,n} - \{0\} \times \mathbb{C}^n - \{0\} | F(x) = 0\}$ and $\pi \colon \mathscr{Z}_{D,n} \to P(\mathscr{H}_{D,n})$ the projection. Let $W = \overline{\pi^{-1}(U)}$. Then W is $\pi^{-1}(U)$ union a finite number of points. π maps W onto L. If $G_i \in U$ and converge to F, then the roots of G_i converge to $\pi^{-1}(F) \cap W$. Moreover, they have a limit point in each connected component of $\mathscr{Z}_F$.*

Proof. The discussion immediately preceding the theorem proves all assertions but the last sentence, which follows from Bezout's Theorem.

Zulehner suggests using a variant of Newton's method to do continuation of roots on real lines contained in a projective line L. Since $L \cap \mathscr{D}$ has at most degree $\mathscr{D}$ points, most real lines in L do not meet $\mathscr{D}$. We are back to a familiar situation, the projective line L is the Riemann sphere with degree $\mathscr{D}$ points removed representing the discriminant variety in L. We may choose a polynomial, say $F = f_i = z_i^{d_i} - z_n^{d_i}$, and consider real lines connecting F to the system we wish to solve, G. For example, we may take the projective line

$$uG + vF$$

and let the ratios of u and v lie on the $2 \deg \mathscr{D}$ lines of ratio

$$\frac{u}{v} = \exp\left(i \frac{2\pi j}{2 \deg \mathscr{D}}\right) \qquad \text{for } j = 1, \ldots, 2 \deg \mathscr{D}.$$

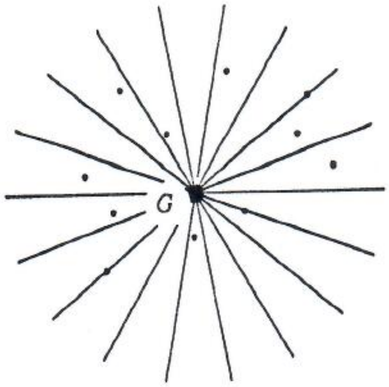

Figure 1

This is reminiscent of Smale's original approach to the fundamental theorem of algebra.

Recall that the polynomial f is thought of as taking the complex number $f\colon \mathbb{C} \to \mathbb{C}$. In the target space

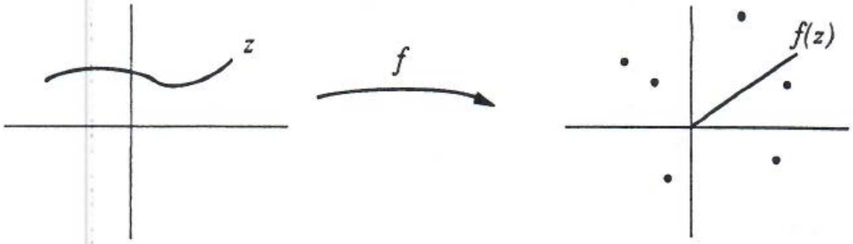

FIGURE 2

a point z is chosen in the domain and a straight line drawn from $f(z)$ to 0; as long as the critical values of f are avoided, the line can be lifted back and continued to a root ξ of f. If we think of the image plane as a plane of polynomials given by changing the constant terms, we have sloved $f - f(z)$ (with z) then drawn the straight line to f, i.e., $(1-t)(f - f(z)) + tf = G_t$, so $G_0 = f - f(z)$ and $G_1 = f$. Avoiding the critical points of f exactly says that the line of polynomials G_t never has a double root, i.e., that this line misses the discriminant variety in the space of polynomials. Now the analogy is complete. It is not so easy to find polynomials whose roots we know and which are not in $\mathscr{D}$, but $F = (f_1, \ldots, f_{n-1})$ and $f_i = z_i^{d_i} - z_n^{d_i}$, $i = 1, \ldots, n$, is a simple example.

Now we need a Newton's method. There does not seem to be a natural Newton's method on projective space. In fact, what we propose is not analytic and fails to be the classical method even for a polynomial of one complex variable which is then homogenized as a two-variable polynomial which gives us a method back on $\mathbb{C}P(1) = S^2$. But this method is well-suited for Smale's α-theory.

Newton's Method in Projective Space

Let $F \in \mathscr{H}_{D,n}$, where $D = (d_1, \ldots, d_n)$, $F\colon \mathbb{C}^{n+1} \to \mathbb{C}^n$, $F = (f_1, \ldots, f_n)$, and f_i is homogeneous of degree $d_i \geq 1$. For $x \in \mathbb{C}^{n+1}$, let $PT(x) = \text{Null}(\bar{x})$, i.e., if $x = (x_1, \ldots, x_{n+1})$, $\text{Null}(\bar{x}) = \{w \in \mathbb{C}^{n+1} | w = (w_1, \ldots, w_{n+1})$ and $\sum \bar{x}_i w_i = 0\}$. Let $Df(x)|PT(x) = P(x)$.

The projective Newton vector field is

$$PNV(x) = PNV_F(x) = -P(x)^{-1}F(x)$$

and is defined where $P(x)^{-1}$ exists.

The projective Newton method is

$$PN(x) = PN_F(x) = x - P(x)^{-1}F(x) = x + PNV(x).$$

Proposition 2. *$PNV(x)$ and $PN(x)$ transform appropriately and, hence, are defined on $\mathbb{C}P(n)$.*

PROOF. For $\lambda \in \mathbb{C}$, let $\Delta(\lambda^{d_i})$ be the linear map which takes $(x_1, \ldots, x_n) \to (\lambda^{d_1}x_1, \ldots, \lambda^{d_n}x_n)$.

By the chain rule for nonzero $\lambda \in \mathbb{C}$, $DF(\lambda x) = \Delta(\lambda^{d_i})DF(x)\lambda^{-1}$ and $PT(\lambda x) = PT(x)$. Thus,

$$\begin{aligned} PNV(\lambda x) &= -P(\lambda x)^{-1}F(\lambda x) \\ &= -(\Delta(\lambda^{d_i})P(x)\lambda^{-1})^{-1}\Delta(\lambda^{d_i})F(x) \\ &= -\lambda P(x)^{-1}F(x) = \lambda PNV(x). \end{aligned}$$

Thus,

$$PN(\lambda x) = \lambda x + PNV(\lambda x) = \lambda(x + PNV(x)) = \lambda PN(x)$$

and PNV and PN are defined on $\mathbb{C}P(n)$. See [Zulehner] for the same differential equations.

There is also a spherical version of PN, SN

$$SN(x) = \frac{x - PNV(x)}{\|x - PNV(x)\|} \quad \text{for } x \text{ of norm one.}$$

The figure following Theorem 2 shows rays which do not intersect the discriminant variety in a projective line L. Renegar gives bounds on Newton's method in terms of the distance to the discriminant variety in $P(\mathscr{H}_{D,n})$ [Renegar]. In [Shub], I give a lower bound to the distance in $P(\mathscr{H}_{D,n})$ compared to the distance in L.

Theorem 3. *Let $H \subset \mathbb{C}P(n)$ be a hypersurface of degree m and L a projective line. Let R be the furthest distance of a point in L from H. Then, for $x \in L$,*

$$m^{1/m}\pi(\csc R)d_{\mathbb{C}P(n)}(x, H)^{1/m} \geq d_L(x, H \cap L) \geq d_{\mathbb{C}P(n)}(x, H).$$

But I do not think that this estimate is good enough to get good complexity bounds. Canny and Renegar use the u resultant and generalizations; we will return to these later. The most problematical polynomial systems are those with excess components, i.e., the algebraic set of zeros has dimension larger than zero. The simplest example is two linear equations in three variables which are dependent:

$$\begin{aligned} ax + by + cz &= 0, \\ ax + by + cz &= 0. \end{aligned}$$

The homotopy then can add t times

$$x - z = 0,$$
$$y - z = 0$$

to the system, obtaining

$$(a + t)x + by + (c - t)z = 0,$$
$$ax + (b + t)y + (c - t)z = 0.$$

This is solved by the 2×2 determinants giving

$$(-tc + t^2, -tc + t^2, t(a + b) + t^2),$$

dividing by t gives

$$(-c + t, -c + t, (a + b) + t).$$

Letting t tend to zero selects the zero $(-c, -c, a + b)$ in the line of zeros of the original system.

Moreover, the zero of the system varies nicely with t. In general, one has for $\ell_1, \ell_2 \in L$ that the distance between the sets of zeros Z_{ℓ_1}, Z_{ℓ_2} given by Theorem 3 satisfy

$$d(Z_{\ell_1}, Z_{\ell_2}) \leq C_L d(\ell_1, \ell_2)^{1/\pi_{i=1}^{n-1} d_i},$$

but the Holder constant C_L which depends on L is not bounded, as computation even on linear examples shows.

Problem. Estimate C_L in terms of the distance from L to the subvariety of problems with excess components.

Given homogeneous polynomials $f_i: \mathbb{C}^n \to \mathbb{C}$, $i = 1, \ldots, n - 1$, add one more equation $u = \sum_{i=1}^n u_i x_i = 0$, where $(u_1, \ldots, u_n) \in \mathbb{C}^n$. The resultant of $R(f_1, \ldots, f_{n-1}, u)$, called the u resultant, is then a polynomial function $R(u)$ which vanishes precisely if there is a root $(\xi_1, \ldots, \xi_n)$ of the system $f_1, \ldots, f_{n-1}$ s.t. $\sum u_i \xi_i = 0$. If there are finitely many solution rays, then $R(u)$ vanishes on a finite union of hyperplanes see [Van der Waerden]. But if the system has excess components, $R(u)$ vanishes identically. Canny gets around this problem by considering the system $\hat{f}_i = f_i - s x_i^{d_i}$. The resultant now is a polynomial function in s and u, $R(s, u)$, $R(s, u) = \sum C_k(u) s^k$. Let k be the minimum integer such that $C_k(u) \not\equiv 0$. Call $C_k(u)$ the s, u resultant of f. Canny proves that $C_k(u)$ vanishes on a union of hyperplanes containing a subset corresponding to all the isolated roots of the system [Canny].

The situation is analogous to Theorem 2. Let $g_i(x) = x_i^{d_i}$ for $i = 1, \ldots, n - 1$. Then $f_i - s g_i$ represents a projective line L contained in $P(\mathscr{H}_{D,n})$, $D = (d_1, \ldots, d_{n-1})$. When $s = \infty$, the system of equations has a unique solution ray, $(0, \ldots, 0, 1)$. This implies that the set V of s for which there are finitely many solutions is open and dense in L. Now let $\pi: Z_{D,n} \to P(\mathscr{H}_{D,n})$, $Z_L = \pi^{-1}(L)$, and $W = \overline{\pi^{-1}(V)}$. π maps W onto L, the map is finite-to-one, and W contains all isolated solution points of the system $f_i - sg$, for any fixed s. Z_L is W union a finite number of excess components over finitely many values of s in L; this is because those s which correspond to excess components are determined by the u resultant being identically zero, which defines an algebraic subset of L. Now since the index of any connected component of zeros is positive, there are points of W arbitrarily close to any connected component of zeros. Therefore, W has nonempty intersection with every connected component of zeros of the system $f_i - sg_i$ for all s. We have thus proven an analogue of Theorem 2 for the line L and open dense subset V. I will not bother to restate this theorem except to draw a conclusion which partially answers a question in [Canny]. The s, u resultant of the system f_i, $C_k(u)$, vanishes on precisely the hyperplanes $\sum_{i=1}^{n} w_i U_i = 0$, where $(w_1, \dots, w_n) \in \pi^{-1}(0) \cap W$. This follows from [Canny, Theorem 3.2].

Theorem 4. *Let $f_i\colon \mathbb{C}^n \to \mathbb{C}$ be homogeneous polynomials of degree $d_i \geq 1$ for $i = 1, \dots, n-1$. Let $C_k(u)$ be the s, u resultant of the system. Then $C_k(u)$ vanishes on a finite union of hyperplanes $\sum_{i=1}^{n} w_{i,j} u_i = 0$, where $(w_{ij}, \dots, w_{nj})$ is a solution ray for every j. Moreover, for every connected component of solutions, there is a j s.t. $(w_{ij}, \dots, w_{nj})$ in this component.*

Problem. What continuation methods correspond to W? Are they practical?

We return to the irreducible varieties $\mathscr{C}_{D,n} \subset P(\mathscr{H}_{D,n})$, where $D = (d_1, \dots, d_k)$, $d_i \geq 1$. $\mathscr{C}_{D,n}$ is the projectivized set of homogeneous polynomials $(f_1, \dots, f_k)$ of degrees d_i which have a common solution ray in $\mathbb{C}^n$. We have shown that $\mathscr{C}_{D,n}$ is irreducible, and from Bezout's theorem it follows that $\mathscr{C}_{D,n} = P(\mathscr{H}_{D,n})$ for $k \leq n - 1$. Here we give the codimension of $\mathscr{C}_{D,n}$ in the other case.

Theorem 5. *$\mathscr{C}_{D,n}$ is an irreducible subvariety of $P(\mathscr{H}_{D,n})$ of codimension* $\max(0, n - k + 1)$. *For $k \geq n$, the map from $\mathscr{Z}_{D,n} \subset P(\mathscr{H}_{D,n}) \times \mathbb{C}P(n-1)$ to $\mathscr{C}_{D,n}$ induced by projection on the first factor is generically finite-to-one. When $k = n - 1$, the generic number of points is $\prod_{i=1}^{n-1} d_i$. When $k > n - 1$, the map is generally one-to-one.*

Proof. Add to the equations $f(x) = 0$, the equations $\det(M_i Df(x)) = 0$, where $M_i Df$ runs through the $(n-1) \times (n-1)$ minors of the derivative of f at x. Let $W_{D,n} \subset \mathscr{Z}_{D,n}$ be the subvariety defined by the vanishing of all the $\det(M_i Df(x))$. Let $V_{D,n} \subset \mathscr{C}_{D,n}$ be the image of $W_{D,n}$. First, we claim that if $F \in \mathscr{C}_{D,n} - V_{D,n}$, then every common zero ray of F is isolated and so they are finite in number. Next, to see that $\mathscr{C}_{D,n} - V_{D,n}$ is open and dense in $\mathscr{C}_{D,n}$, it suffices to produce an open set in $\mathscr{C}_{D,n} - V_{D,n}$. For this, find $(n-1)$ homogeneous polynomials with finitely many solution rays and with the derivative at each solution ray of rank $(n-1)$. Complete this system to one which still has common solution rays. Now, any perturbation of the initial $(n-1)$ polynomials still has only finitely many solutions and each has derivative of rank $(n-1)$. $f_i = x_i^{d_i} - x_n^{d_i}$, $i = 1, \ldots, n-1$, are such a system of $(n-1)$ polynomials. We can add an nth polynomial which is a power of a linear map (L^{d_n}), where L vanishes at only one of common roots of the f_i; this will establish the last statement.

Remark 3. The fact that, for overdetermined systems $k > n - 1$, the map from solutions to systems is generically one-to-one implies that the solution may be given as a rational function of the coefficients on a Zariski dense set of problems.

Remark 4. For $k = n$, that is, the case of n homogeneous equations in n variables of degree $D = (d_1, \ldots, d_n)$, $\mathscr{C}_{D,n} \subset P(\mathscr{H}_{D,n})$ is an irreducible hypersurface defined by an irreducible polynomial in the coefficients of the f_i. This is the resultant polynomial [Macauley, Van der Waerden, etc.]; it has degree

$$\left(\prod_{j=1}^{n} d_j\right) \sum_{i=1}^{n} 1/d_i.$$

If we specialize to homogeneous quadratic equations in n variables, the vector space $\mathscr{H}_{D,n}$ has dimension $n^2(n+1)/2$ and the resultant polynomial, the vanishing of which is necessary and sufficient for the system to have a nonzero root, has degree $n2^{n-1}$. Even in this case one may hope to prove that the resultant cannot be computed in polynomial cost in n and, thereby, establish that $P \neq NP$ as below.

Proposition 3. *Let $H \subset \mathbb{C}^N$ be an irreducible hypersurface given by the irreducible polynomial $P: \mathbb{C}^N \to \mathbb{C}$. Then any machine M over $\mathbb{C}$ which solves the decision problem $(\mathbb{C}^N, H)$ must compute a rational multiple of P on a Zariski dense open subset of H.*

Proof. For each path of nodes $n_1, \ldots, n_k$ which leads an input $h \in H$ to a yes output node, we have the corresponding subset $V_{n_1,\ldots,n_k} \subset H$ which outputs on this path. There are countably many $V_{n_1,\ldots,n_k}$, each of which is either contained in a hypersurface of H and, consequently, nowhere dense in H or contains an open set of H. As H is not the union of countably many nowhere dense sets, at least one $V_{n_1,\ldots,n_k}$ must be open.

Say the path of nodes encounter ℓ branch nodes and at each branch node the composite polynomial rational function computed is f_i/g_i, $i = 1, \ldots, \ell$. If f_i is not a multiple of P, then $V_{n_1,\ldots,n_k}$ must take the $\neq 0$ branch. If f_i is never a multiple of P, then $V_{n_1,\ldots,n_k}$ has always taken the $\neq 0$ branch, but then the same is true for a neighborhood of $V_{n_1,\ldots,n_k}$ in $\mathbb{C}^n$ and M has made an error, which finishes the proof. The argument actually also shows that $V_{n_1,\ldots,n_k}$ must be open and dense in H.

Corollary 2. *Any machine over $\mathbb{C}$ which solves the decision problem $(\mathscr{H}_{D,n}, \mathscr{C}_{D,n})$ must compute a multiple of the resultant on Zariski dense open subsets of $\mathscr{C}_{D,n}$ where $D = (d_1, \ldots, d_n)$, and in particular for n-quadratic homogeneous polynomials in n unknowns.*

This corollary was independently proven by Steve Smale. He was considering the question of $P \neq NP$ in various contexts. One context was machines over the integers with input size the bit input size, cost the bit cost, and branching over $=0$ or $\neq 0$.

Let Z_+ denote the non-negative integers. I suggested that (Z, Z_+) is not in P. Here is a proof worked out with Michael Ben-Or.

Proposition 4. *(Z, Z_+) is in NP but not in P for machines over Z branching on $\neq 0$ or $=0$ and with bit input size and bit cost.*

Proof. First, to see that (Z, Z_+) is in NP, note that any non-negative integer is the sum of four squares. Now to see that the problem is not in P, we use the following lemma:

Lemma 2. *Let $f \in \mathscr{Z}[t]$ be an integral polynomial with at least k distinct integer roots. Suppose for some $w \in \mathscr{Z}$ that $f(w) \neq 0$, then $|f(w)| \geq ((k/2)!)^2$.*

Proof. Let $r_1, \ldots, r_k$ be distinct integral roots of f, and let $Q = \prod_{i=1}^{k} (t - r_i)$. Then $f(t) = Q(t)P(t)$, where $P(t)$ is an integral polynomial. Since $P(w) \neq 0$, $|P(w)| \geq 1$, and, hence, $|f(w)| \geq |Q(w)| \geq ((k/2)!)^2$ since it is the product of k distinct nonzero integers.

Since $(k/2)!$ has more than $k/2$ bits, we see that at a branch node if k elements of $\mathscr{Z}$ take the $=0$ branch, then the cost of the computation is at least k. Now if there is a polynomial cost machine, at each branch only polynomial many inputs of size n may take the $=0$ branch which gives a contradiction because 2^n inputs must be eliminated by polynomially many nodes.

Problem. Is this proposition still true if the cost is reduced to the number of algebraic operations?

This problem is related to Problem 5.1 of [Blum–Shub–Smale]. Given the integers Z, branching on ≥ 0 or < 0, and bit input size, does the class of polynomial cost decision problems P increase if the bit cost is reduced to the number of algebraic operations? In this context, the class NP certainly gets larger because it contains undecidable problems (Hilbert's tenth). Because the outputs are just 0 and 1, we might compute mod 2 which would make the algebraic and bit cost comparable. The problem is at branching nodes where inequalities are verified. A model problem is:

For fixed k and ℓ, give $2(k + \ell)$ positive integers.
$a_i, n_i, i = 1, \ldots, k, \quad b_j, m_j, j = 1, \ldots, \ell$.
Is $\prod_{i=1}^k a_i^{n_i} > \prod_{j=1}^{\ell} b_j^{m_j}$?

This problem is easily seen to be in P with cost the number of algebraic operations since the powers can be taken by repeated squaring. The bit size of the numbers, however, gets exponentially large in this procedure. Yet we have the following surprising theorem.

Theorem 6. *The decision problem, a_i, n_i, b_j, m_j positive integers, $i = 1, \ldots, k$, $j = 1, \ldots, \ell$, and $\prod_{i=1}^k a_i^{n_i} > \prod_{j=1}^{\ell} b_j^{m_j}$ is in P over Z with branching on ≥ 0 or < 0, bit input size, and bit cost.*

Proof. We use Baker's theorem [Baker, Theorem 3.1], and refer to [Lang, Chapter XI, Theorem 1.1]. There is a constant $B > 0$ with the following property. Let $M = \max_{i,j}(a_i, b_j)$. Then either

$$\sum_{i=1}^{k} n_i \log a_i - \sum_{j=1}^{\ell} m_j \log b_j = 0$$

or

$$\left| \sum_{i=1}^{k} n_i \log a_i - \sum_{j=1}^{\ell} m_j \log b_j \right| > B^{(k+\ell)(\log M)^{k+\ell} \log\log M}.$$

Thus, we need only compute

$$\sum_{i=1}^{k} n_i \log a_i - \sum_{j=1}^{\ell} m_j \log b$$

to accuracy 0 (input size) $^{k+\ell+1}$ to determine if it is positive, zero, or negative. This entails computing a polynomial number of bits of the logs of the a_i and b_j. This can be done rather naively by dividing by a power of two and using the Taylor series for the log near one, or by Newton's method or more sophisticatedly as in [Borwein and Borwein].

This theorem suggests the following naive problem.

Problem. Given an integral polynomial P in variables x_i and variable exponents n_{i_ℓ}, is it always possible to determine if $P = 0$, $P > 0$, or $P < 0$ in polynomial bit cost in the bit input size of the x_i and n_{i_ℓ}?

References

Baker, A., *Transcendental Number Theory*, Cambridge University Press, Cambridge, 1975.

Blum, L., Shub, M., and Smale, S., On a theory of computation and complexity over the real numbers: NP-completeness, recursive functions and universal machines, *Bull. Amer. Math. Soc.* **21** (1989), 1–46.

Borwein, J. and Borwein, P., *Pi and the AGM*, Wiley, New York, 1987.

Canny, J.F., Generalized characteristic polynomials, *J. Symbol. Comput.* **9** (1990), 241–250.

Dold, A., *Lectures on Algebraic Topology*, 2nd ed., Springer-Verlag, Berlin, 1980.

Lang, S., *Elliptic Curves Diophantine Analysis*, Springer-Verlag, Berlin, 1978.

Macauley, F.S., *The Algebraic Theory of Modular Systems*, Cambridge Tracts in Mathematics and Mathematical Physics, No. 10, Steckart-Hafner Service Agency, New York, 1964.

Renegar, J., On the worst case arithmetic complexity of approximating zeros of systems of polynomials, *SIAM J. Comput.* **18** (1989), 350–370.

Shub, M., On the distance to the zero set of a homogeneous polynomial, *J. Complexity* **5** (1989), 303–305.

Van der Waerden, B.L., *Modern Algebra*, Vol. II, Frederick Unger, New York, 1950.

Zulehner, W., A simple homotopy method for determining all isolated solutions to polynomial systems, *Math. Comp.* **50** (1988), 167–177.