JOURNAL OF COMPLEXITY 3, 81–89 (1987)

On the Topology of Algorithms, I

STEVE SMALE

University of California, Berkeley, California 94720

1

This paper deals with the structure of algorithms for finding approximations of the zeros of a complex polynomial, especially lower bound estimates.

Consider the problem:

> Poly(d): Data, a complex polynomial of degree d, leading coefficient 1 and $\varepsilon > 0$. Find all the roots of f within ε.

So if $\zeta_1, \ldots, \zeta_d$ are the roots of f, perhaps multiple, the problem is to find $z_1, \ldots, z_d$ such that $|z_i - \zeta_i| < \varepsilon$, each i.

Eventually we will specify $\varepsilon(d)$ and require $\varepsilon < \varepsilon(d)$.

For the purposes of this paper, an algorithm will be a rooted tree: root at the top (!) for the input, leaves at the bottom for the output. Internal nodes will be of two types:

Computation nodes,  , which transmit a program of real numbers, modified by a rational operation $+, -, \times, \div$;

Branching nodes,  , which go right or left according to whether an inequality is true or false (precision will be given in Section 2).

We call such an algorithm a computation tree.

A computation tree for the problem Poly(d) has input the coefficients of a polynomial f (in terms of real and imaginary parts). The output must consist of $(z_1, \ldots, z_d)$ (again given in terms of real and imaginary parts), each z_i being within ε of ζ_i, the ζ_i being the roots of f.

The computation nodes do not contribute to the topology of the computation tree, so we define the *topological complexity* of the tree, as the number of branching nodes. The topological complexity of problem Poly(d) is the minimum of the topological complexity of all computation trees for that problem.

0885-064X/87 $3.00

Our main result is:

MAIN THEOREM. *For all* $\varepsilon < \varepsilon(d)$, *the topological complexity of the problem Poly*(d) *is greater than* $(\log_2 d)^{2/3}$.

The proof goes by topology, especially algebraic topology. Eventually Fuchs' results on the cohomology ring of the braid group play a decisive role.

Some of the ideas of the proof seem quite universal, but unsolved problems in algebraic topology prevent extension of the result to several variables.

Steele and Yao (1982) used algebraic topology to study decision trees for very different problems. Subsequently, Ben-Or (1983) extended this work. The braid group enters into McMullen's work (1985; 1986a, b) on algorithms for zero finding. His negative results and those of the present paper are different in character.

Two conversations with Emery Thomas were very helpful to me in understanding the work of Fuchs.

2

We now formally state what we mean by an algorithm. The notion of a computation tree of Section 1 is made precise (some of the computation nodes of Section 1 are collapsed, but the number of branching nodes is the same).

The following foundational account is a little more systematic than necessary here, but it will be useful later.

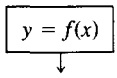
The definition of a Flowchart Program in Manna (1974, p. 163) is modified in this way. No loops are allowed (for the present paper), the variables are real numbers, and "predicates" of Manna are defined in terms of rational functions.

Thus the input domain, denoted here by $\mathcal{I}$, the program domain $\mathcal{P}$, and the output domain $\mathcal{O}$, are each real cartesian spaces of some dimension. The set of usable inputs (satisfying an input predicate in the terminology of Manna, 1974) is supposed to be a real *semialgebraic* set Y in $\mathcal{I}$. Therefore Y has the form $Y = \{y \in \mathcal{I} | s_i(y) = 0, t_j(y) < 0, u_k(y) \leq 0\}$ for some finite set of rational functions, $\{s_i, t_j, u_k\}$. Moreover we always suppose that rational functions have integer coefficients in this paper.

The set of acceptable outputs is defined by another semialgebraic set $X \subset Y \times \mathcal{O}$. Define $f: X \to Y$ as the restriction of the projection $Y \times \mathcal{O} \to Y$; we require that f be surjective.

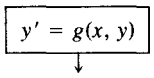
Nodes of the computation tree are of four types: root (or start), computation (or assignment), branching (or test), and leaf (or halt). Each has an associated rational map.

The *root* is defined by a rational map $f\colon \mathcal{I} \to \mathcal{P}$ (each coordinate of f is a rational function).



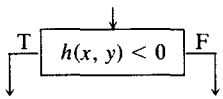
or $y \leftarrow f(x)$

A *computation node* is described by a rational map $g\colon \mathcal{I} \times \mathcal{P} \to \mathcal{P}$.



or $y \leftarrow g(x, y)$

To a *branch node* is associated a rational function $h\colon \mathcal{I} \times \mathcal{P} \to \mathbb{R}$.



(could be $h(x, y) \leq 0$)

Finally a *leaf* is defined by a rational map $l\colon \mathcal{I} \times \mathcal{P} \to \mathbb{C}$.

or $z \leftarrow l(x, y)$

Each $x \in \mathcal{I}$ defines a path starting down the tree. We require that if $x \in Y$, then division by zero is not encountered along the path. This condition on the computation tree ensures that each such path leads to a leaf. A final requirement is that for $x \in Y$, the endpoint z of this path satisfy $(x, z) \in X \subset \mathcal{I} \times \mathbb{C}$.

A further reference on algorithms with an extensive up-to-date bibliography is Purdom and Brown (1985).

The number of paths equals the number of leaves equals the number of branches plus one.

3

Let $f\colon X \to Y$ be a continuous map. Define the *covering number* of f as the least k with this property; there is an open covering $\mathcal{U}_1, \ldots, \mathcal{U}_k$ of Y and continuous maps $g_i\colon \mathcal{U}_i \to X$ with $f(g_i(y)) = y$, each i and $y \in \mathcal{U}_i$. Note that if f is not surjective, the covering number is infinite.

Next let $\mathcal{P}_d$ be the space of complex polynomials of degree d with leading coefficient l. Thus a point of $\mathcal{P}_d$ may be thought of as either a vector $(a_0, \ldots, a_{d-1})$ with $a_i \in \mathbb{C}$ or as the polynomial $f(z) = \sum_0^d a_i z^i$, $a_d = 1$.

Let $\mathbb{C}^d$ be complex d-dimensional space and $\pi\colon \mathbb{C}^d \to \mathcal{P}_d$ the map which assigns to $(\zeta_1, \ldots, \zeta_d)$ the polynomial with roots $\zeta_1, \ldots, \zeta_d$. Thus π has as coordinates the symmetric functions a_i (cf. Lang, 1984) in the ζ_j.

Let

$$\Delta = \{\zeta = (\zeta_1, \ldots, \zeta_d) \in \mathbb{C}^d | \zeta_i = \zeta_j, \text{ some } i \neq j\}$$

and $\pi(\Delta) = \Sigma \subset \mathcal{P}_d$. One may describe Σ as the algebraic variety of polynomials f whose discriminant (Lang, 1984) is zero. Note that $\pi^{-1}(\Sigma) = \Delta$.

$\mathcal{P}_d$ is the input space of problem Poly(d) and $\mathbb{C}^d$ the output space. Moreover, the set of usable inputs (Y of Section 2) is B_K and the set of acceptable outputs is

$$X = \{(f,(z_1, \ldots, z_d)) \in B_K \times \mathbb{C}^d | \, |z_i - \zeta_i| < \varepsilon, f(z) = \prod_{i=1}^{d} (z - \zeta_i)\},$$

where $B_K = \{f \in \mathcal{P}_d | \, |a_i| \leq K, i = 0, \ldots, d-1\}$ and $K = K(d)$ is chosen large enough that if f has all roots in the unit disk, then $f \in B_K$.

THEOREM A. *The covering number of the restriction* π: $\mathbb{C}^d - \Delta \to \mathcal{P}_d - \Sigma$ *is less than or equal to the topological complexity of problem* Poly(d), *for all* $\varepsilon < \varepsilon(d)$, $\varepsilon(d)$ *described in the proof.*

Proof. Let a computation tree for Poly(d) be given with leaves numbered $i = 1, \ldots, k$. Denote by V_i the subset of B_K (inputs) which arrives at leaf i. Then $B_K = \cup_{i=1}^{k} V_i$ and $V_i \cap V_j = \emptyset$ if $i \neq j$. (The V_i are real semialgebraic subsets of $\mathcal{P}_d$.)

These input–output maps, denoted by ϕ_i: $V_i \to \mathbb{C}^d$, are continuous real rational maps with integer coefficients in the variables (Re a_i, Im a_i). The values satisfy $\phi_i(f) = (z_1, \ldots, z_d)$, $|z_i - \zeta_i| < \varepsilon$, where the ζ_i are the roots of f. For our purposes, we only need the ϕ_i to be continuous.

The V_i may be described by

$$V_i = \{a = (a_0, \ldots, a_{d-1}) \in B_K | \, g_j(a) < 0, j = 1, \ldots, l; h_k(a) \geq 0, \; k = 1, \ldots, m\},$$

where the g_j and h_k are continuous (even rational) functions. Thus V_i is a closed subset of an open set V_i' in B_K. By the Tietze Extension Theorem (see Munkres, 1975), ϕ_i can be extended to an open set $\mathcal{U}_i$ of V_i' and this map still denoted by ϕ_i; ϕ_i: $\mathcal{U}_i \to \mathbb{C}^d$ will satisfy: $\phi_i(f) = (z_1, \ldots, z_d)$, $|z_i - \zeta_i| < \varepsilon$, ζ_i the roots of f. These sets $\mathcal{U}_i$ are open in B_K and cover B_K since the V_i do.

If Y is a subspace of a space X, it is called a *deformation retract* of X provided there is a homotopy h_t: $X \to X$, $0 \leq t \leq 1$, satisfying: h_0 is the identity, $h_1(X) \subset Y$, and $h_1(y) = y$ for $y \in Y$.

The following well-known lemma is implicit in Spanier (1966, pp. 290–291).

LEMMA 1. *Let Y be a closed subspace of a compact space X such that the pair (X, Y) can be triangulated. That is, there is a homeomorphism h: $(X, Y) \to (K, L)$, where L is a subcomplex of a simplicial complex K. Then there is a neighborhood N of Y such that $X - N$ is a deformation retract of $X - Y$.*

Let $S = \{z \in \mathbb{C}^d \mid \|z\| = 1\}$ using the Hermitian inner product on $\mathbb{C}^d$.

LEMMA 2. *The pair $(\pi(S), \Sigma \cap \pi(S))$ can be triangulated.*

For the proof, see Lojasciewicz (1964).

LEMMA 3. *$\pi(S) - \Sigma \cap \pi(S)$ is a deformation retract of $\mathcal{P}_d - \Sigma$.*

Proof. First define h_t: $\mathbb{C}_d - \Delta \to \mathbb{C}_d - \Delta$ by $h_t(x) = (1 - t)x + tx/\|x\|$. The homotopy is invariant under the group $S(d)$ of covering transformations, hence induces the required homotopy of $\mathcal{P}_d - \Sigma$.

As a consequence of Lemmas 1, 2, and 3, we have:

LEMMA 4. *There is a neighborhood N of $\Sigma \cap \pi(S)$ in $\pi(S)$ such that $\pi(S) - N$ is a deformation retract of $\mathcal{P}_d - \Sigma$.*

Let h_t: $\mathcal{P}_d - \Sigma \to \mathcal{P}_d - \Sigma$ be the retraction. Thus h_0 is the identity, $h_1(\mathcal{P}_d - \Sigma) \subset \pi(S) - N$, and $h_1(y) = y$ for all $y \in \pi(S) - N$. Choose $\eta = \eta(d)$ with this property if $f \in \pi(S) - N$; then the roots of f are separated by at least η.

Next let $P_i = \mathcal{U}_i \cap (\pi(S) - N)$, and suppose $\varepsilon < \eta(d)/2$. Thus for $f \in P_i$, and $\phi_i(f) = (z_1, \ldots, z_d)$, each z_i has a closest root ζ_i of f defined unambiguously. Let $\psi_i(f) = (\zeta_1, \ldots, \zeta_d)$. Then ψ_i: $P_i \to \mathbb{C}^d$ is continuous and $\pi\psi_i(f) = f$. We have found a covering $\{P_i\}$ of $\pi(S) - N$ showing that the covering number of π: $S - \pi^{-1}(N) \to \pi(S) - N$ is at least d. The final step in the proof of Theorem A is to use the deformation retraction to define the appropriate covering $\{Q_i\}$ of $\mathcal{P}_d - \Sigma$. Let $Q_i = h_1^{-1}(P_i)$ and extend ψ_i to Q_i using the covering homotopy property. This finishes the proof of Theorem A.

Remark. It is clear from the proof that Theorem A holds in considerably greater generality.

4

The *cup length* of a ring $\mathcal{R}$ is defined as the maximum number k such that $\gamma_1 \cup \ldots \cup \gamma_k \neq 0$, $\gamma_i \in \mathcal{R}$, where "$\cup$" denotes the product.

For a continuous map f: $X \to Y$, let $K(f)$ be the kernel (an ideal) of

$$f^*\colon H^*(Y) \to H^*(X), \text{ i.e.,}$$

$$K(f) = \{\gamma \in H^*(Y) \mid f^*(\gamma) = 0\}.$$

Here $H^*(X)$ is the singular cohomology ring of X, and f^* is the induced map.

PROPOSITION 1.[1] *The covering number of f is greater than the cup length of $K(f)$.*

The cup length depends on the coefficients in cohomology, but Proposition 1 is true for any coefficients. Later the coefficient ring will be the integers mod 2.

This proposition is related to category theory of Lusternik and Schnirelman; see Schwartz (1967) or Spanier (1966, p. 279).

Proof of Proposition 1. We proceed by supposing the proposition is false. In that case there exist $\gamma_1, \ldots, \gamma_k \in K$ with $\gamma_1 \cup \cdots \cup \gamma_k \neq 0$ and there is an open covering V_i, $i = 1, \ldots, k$ of Y, with associated continuous maps $\sigma_i\colon V_i \to X$ having the property $f(\sigma_i(v)) = v$ for all $v \in V_i$.

Consider a portion of the singular cohomology sequence of the pair (Y, V_i) (see Spanier, 1966).

$$\to H^*(Y, V_i) \xrightarrow{I_i} H^*(Y) \xrightarrow{J_i} H^*(V_i) \to \cdots.$$

Here I_i and J_i are induced by inclusion and the sequence is exact. Consider $\gamma_i \in K(f) \subset H^*(Y)$. Then $J_i(\gamma_i) = \sigma_i^* f^*(\gamma_i) = 0$; thus by exactness, there is some $v_i \in H^*(Y, V_i)$ with $I_i(v_i) = \gamma_i$.

Since the V_i are open in Y (see Spanier, 1966) we may take the cup product of the v_i, $v_1 \cup \cdots \cup v_k$ in $H^*(Y, \cup_{i=1}^k V_i) = H^*(Y, Y) = 0$. On the other hand, by naturality $v_1 \cup \cdots \cup v_k$ maps into $\gamma_1 \cup \cdots \cup \gamma_k \neq 0$. This is a contradiction and Proposition 1 is proved.

PROPOSITION 2. *Let $\pi\colon \mathbb{C}^d - \Delta \to \mathcal{P}_d - \Sigma$ be as in Theorem A. Then the induced map in cohomology, coefficients Z_2,*

$$\pi^*\colon H_i^*(\mathcal{P}_d - \Sigma, Z_2) \to H_i^*(\mathbb{C}^d - \Delta, Z_2)$$

is trivial for $i > 0$ (and an isomorphism for $i = 0$, of course).

For this and the next proposition, we use the work of Fuchs (1970), but also the works of Arnold (1968), Birman (1974), Brieskorn (1973), Cohen in Cohen *et al.* (1976), and Fadell and Newwirth (1962) are also quite

[1] *Note added in proof.* Moe Hirsch pointed out to me that by taking X as the path space of Y, Proposition 1 contains the Lusternik–Schnirelman result.

pertinent. One definition of the braid group is the fundamental group of $\mathcal{P}_d - \Sigma$ and these papers all deal with the topology of the braid group. The cohomology of the braid group is the same thing as the cohomology of $\mathcal{P}_d - \Sigma$.

Proof of Proposition 2. Consider certain spaces as follows. Let $O(d)$ be the orthogonal group and $B_{O(d)}$ the corresponding classifying space (see Husemoller, 1966). Let $S(d)$ be the symmetric group on d elements and let $B_{S(d)}$ be the Eilenberg–MacLane space $K(S(d), 1)$ let $u_d \to B_{S(d)}$ be the universal covering (see Spanier, 1966).

According to Fadell and Newwirth (1962) $\mathcal{P} - \Sigma$ is an Eilenberg–MacLane space, $K(\Pi_1(\mathcal{P} - \Sigma), 1)$. The map π: $\mathbb{C}^d - \Delta \to \mathcal{P} - \Sigma$ is a regular covering (see Spanier, 1966) with group $S(d)$ since the map π is given by the symmetric functions. Thus there is a natural map from covering space theory

$$\Pi_1(\mathcal{P} - \Sigma) \to S(d).$$

This map can also be given by interpreting geometrically $\Pi_1(\mathcal{P} - \Sigma)$ as the braid group; each braid gives a permutation. There is also a natural map

$$S(d) \to O(d)$$

by the symmetric group permuting the coordinates.

Ring homomorphisms in cohomology over Z_2 are induced by the group homomorphisms, so we have $H^*(\mathcal{P}_d - \Sigma) \leftarrow H^*(B_{S(d)}) \leftarrow H^*(B_{O(d)})$. According to Fuchs (1970) the map $H^*(B_{O(d)}, Z_2) \to H^*(\mathcal{P}_d - \Sigma, Z_2)$ is surjective.

Thus

LEMMA. *The map* $H^*(B_{S(d)}, Z_2) \to H^*(\mathcal{P}_d - \Sigma, Z_2)$ *is surjective.*

Since the composition $\Pi_1(\mathbb{C}^d - \Delta) \to \Pi_1(\mathcal{P}_d - \Sigma) \to \Pi_1(B_{S(d)}) \simeq S(d)$ is zero, by covering space theory (Spanier, 1966), there is a map h with the cummutative diagram:

$$\begin{array}{ccc} \mathbb{C}^d - \Delta & \xrightarrow{h} & \mathcal{U}_d \\ \downarrow & & \downarrow \\ \mathcal{P}_d - \Sigma & \to & B_{S(d)}. \end{array}$$

Since $H^*(\mathcal{U}_d, Z_2) \simeq H^0(\mathcal{U}_d, Z_2)$, $H_i^*(B_{S(d)}, Z_2) \to H_i^*(\mathbb{C}^d - \Delta)$ is trivial for $i > 0$ (either way around the diagram). Proposition 2 follows, using the lemma.

Let $H_a^*(\mathcal{P}_d - \Sigma, Z_2)$ be the ring $\sum_{i=1}^{2d} H^i(\mathcal{P}_d - \Sigma, Z_2)$.

PROPOSITION 3. *The cup length of* $H_a^*(\mathcal{P}_d - \Sigma, Z_2)$ *is greater than* $(\log_2 d)^{2/3}$.

Proof. According to Fuchs (1970), the generators of $H_a^*(\mathcal{P}_d - \Sigma, Z_2)$ are $a_{m,k}$, $k = 0, 1, 2, \ldots$, $m = 1, 2, 3, \ldots$, degree $a_{m,k} = 2^k(2^{m-1})$, relations $a_{m,k}^2 = 0$ and otherwise, $a_{m_1,k_1} \cdot \ldots \cdot a_{m_t,k_t} = 0$ just when $2^{m_1+\cdots+m_t+k_1+\cdots+k_t} > d$.

So we want to find a sequence of distinct pairs, $(m_1, k_1), \ldots, (m_t, k_t)$ with t as large as possible and

$$\sum_1^t m_i + \sum_1^t k_i \leq \log_2 d. \tag{*}$$

Consider now the set of all distinct pairs (m_i, k_i) such that $m_i + k_i \leq M$. An easy counting shows that there are $t = M(M + 1)/2$ of these pairs.

A second easy counting shows that (*) will be satisfied provided $\sum_1^M j^2 = M(M + 1)(2M + 1)/6 \leq \log_2 d$.

It is not difficult to check that $t = (\log_2 d)^{2/3}$ satisfies these conditions. Actually there is a universal $\varepsilon > 0$ with $t = (1 + \varepsilon)(\log_2 d)^{2/3}$ satisfactory. This proves Proposition 3.

The proof of the Main Theorem now follows:

Topological complexity Poly(d)	
$\geq$ Covering Number (π: $\mathbb{C}^d - \Delta \to \mathcal{P}_d - Z$)	Theorem A
$>$ Cup length ker π^*	Proposition 1
$=$ Cup length $H_a^*(\mathcal{P}_d - \Sigma, Z_2)$	Proposition 2
$> (\log_2 d)^{2/3}$	Proposition 3.

REFERENCES

ARNOLD, V. I. (1968), On braids of algebraic functions and cohomologies of swallowtails, *Uspekhi Mat. Nauk* **23**, 247–248.

BEN-OR, M. (1983), Lower bounds for algebraic computation trees, *in* "Proceedings, 15th ACM STOC," pp. 80–86.

BIRMAN, J. (1974), "Braids, Links, and Mapping Class Groups," Annals of Math. Studies, Princeton Univ. Press, Princeton, NJ.

BRIESKORN, E. (1973), Sur les groupes de tresses (d'apres V. I. Arnold), *in* "Seminaire Bourbaki," Lecture Notes in Mathematics, Vol. 1971/72, No. 317, Springer-Verlag, New York.

COHEN, F., LADA, T., AND MAY, P. (1976), The homology of iterated loop spaces, *in* "Lecture Notes in Mathematics, Vol. 533," Springer-Verlag, New York.

FADELL, E., AND NEWWIRTH, L. (1962), Configuration spaces, *Math. Scand.* **10**, 111–118.

FUCHS, D. (1970), Cohomologies of the braid groups mod 2, *Functional Anal. Appl.* **4**, 143–151.

HUSEMOLLER, D. (1966), "Fibre Bundles," 2nd ed., Graduate Texts in Mathematics, No. 20, Springer-Verlag, New York.

LANG, S. (1984), "Algebra," 2nd ed., Addison-Wesley, Reading, MA.

LOJASCIEWICZ, S. (1964), Triangulation of semi-analytic sets, *Ann. Scuola Norm. Sup. Pisa Cl. Sci.* (3) **18,** 449–474.

MANNA, Z. (1974), "Mathematical Theory of Computation," McGraw-Hill, New York.

MCMULLEN, C. (1985), Families of rational maps and iterative root-finding algorithms, preprint.

MCMULLEN, C. (1986a), Automorphisms of rational maps. I. Nielson realization and dynamics on the ideal boundary, MSRI, Berkeley.

MCMULLEN, C. (1986b), Automorphisms of rational maps. II. Braiding of the attractor and the failure of iterative algorithms, MSRI, Berkeley.

MUNKRES, J. (1975), "Topology," Prentice-Hall, Englewood Cliffs, N.J.

PURDOM, P., AND BROWN, C. (1985), "The Analysis of Algorithms," Holt, Rinehart & Winston, New York.

SCHWARTZ, J. (1967), "Non-linear Functional Analysis," Gordon & Breach, New York.

SPANIER, E. (1966), "Algebraic Topology," McGraw-Hill, New York.

STEELE, M., AND YAO, A. (1982), Lower bounds for algebraic decision trees, *J. Algorithms* **3,** 1–8.