Experimental Mathematics, 21(1):69–83, 2012

ISSN: 1058-6458 print / 1944-950X online
DOI: 10.1080/10586458.2011.606184

Taylor & Francis
Taylor & Francis Group

Certified Numerical Homotopy Tracking

Carlos Beltrán and Anton Leykin

CONTENTS

Given a homotopy connecting two polynomial systems, we provide a rigorous algorithm for tracking a regular homotopy path connecting an approximate zero of the start system to an approximate zero of the target system. Our method uses recent results on the complexity of homotopy continuation rooted in the alpha theory of Smale. Experimental results obtained with an implementation in the numerical algebraic geometry package Macaulay2 demonstrate the practicality of the algorithm. In particular, we confirm the theoretical results for random linear homotopies and illustrate the plausibility of a conjecture by Shub and Smale on a good initial pair.

1. INTRODUCTION

Numerical homotopy continuation methods are the backbone of the area of numerical algebraic geometry; while this area has a rigorous theoretical base, its existing software relies on heuristics to perform homotopy tracking.

This paper has two main goals: On the one hand, we intend to provide an overview of some recent developments in the analysis of the complexity of polynomial homotopy continuation methods with a view to a practical implementation. In recent years, there has been much progress in the understanding of this problem. We summarize the main results obtained, writing them in a unified and accessible way.

On the other hand, we present for the first time an implementation of a *certified* homotopy method that does not rely on heuristic considerations. Experiments with this algorithm are also presented, providing for the first time a tool to study deep conjectures on the complexity of homotopy methods (such as Shub and Smale's conjecture discussed below) and illustrating known—yet somehow surprising—features of these methods, such as equiprobability of the output in the case of random linear homotopy and the average polynomial or quasipolynomial time of the algorithms studied by several authors.

Our project constructs a certified homotopy-tracking algorithm and delivers the first practical implementation of a rigorous path-following procedure. In particular, the

2000 AMS Subject Classification: 14Q20, 65H10, 65H20
Keywords: Computational aspects of algebraic geometry, systems of equations, continual methods, homotopy methods, approximate zero, certified algorithms, complexity

case of a *linear homotopy* is addressed in full detail in Algorithm 1.

We begin by fixing some notation. Let $n \geq 1$. For a positive integer $d_0 \geq 1$, let $\mathcal{P}_{d_0} = \mathbb{C}_{d_0}[X_1, \ldots, X_n]$ be the vector space of all polynomials of degree at most d_0 with complex coefficients and unknowns $X_1, \ldots, X_n$. Then for a list of degrees $(d) = (d_1, \ldots, d_n)$, let $\mathcal{P}_{(d)} = \mathcal{P}_{d_1} \times \cdots \times \mathcal{P}_{d_n}$. Note that elements in $\mathcal{P}_{(d)}$ are n-tuples $f = (f_1, \ldots, f_n)$, where f_i is a polynomial of degree d_i. An element $f \in \mathcal{P}_{(d)}$ will be seen both as a vector in some high-dimensional vector space and as a system of n equations in n unknowns. Homotopy methods are among the most successful tools for solving the following problem.

Problem 1.1. Assuming that $f \in \mathcal{P}_{(d)}$ has finitely many zeros, find approximately one, several, or all zeros of f in $\mathbb{C}^n$.

It is helpful to consider the homogeneous version of this problem: For a positive integer $d_0 \geq 1$, let $\mathcal{H}_{d_0}$ be the vector space of all homogeneous polynomials of degree d_0 with complex coefficients and unknowns $X_0, \ldots, X_n$. Then for a list of degrees $(d) = (d_1, \ldots, d_n)$. let $\mathcal{H}_{(d)} = \mathcal{H}_{d_1} \times \cdots \times \mathcal{H}_{d_n}$. Note that elements in $\mathcal{H}_{(d)}$ are n-tuples $h = (h_1, \ldots, h_n)$, where h_i is a homogeneous polynomial of degree d_i. An element $h \in \mathcal{H}_{(d)}$ will be seen both as a vector in some high-dimensional vector space and as a system of n homogeneous equations in $n+1$ unknowns. Note that if $\zeta \in \mathbb{C}^{n+1}$ is a zero of $h \in \mathcal{H}_{(d)}$, then so is $\lambda\zeta$, $\lambda \in \mathbb{C}$. Hence it makes sense to consider zeros of $h \in \mathcal{H}_{(d)}$ as projective points $\zeta \in \mathbb{P}(\mathbb{C}^{n+1})$. Abusing notation, we will denote both a point in $\mathbb{P}(\mathbb{C}^{n+1})$ and a representative of the point in $\mathbb{C}^{n+1}$ by the same symbol. Moreover, if necessary, it is implied that the norm of this representative is 1. The homogeneous version of Problem 1.1 is as follows.

Problem 1.2. Assuming that $h \in \mathcal{H}_{(d)}$ has finitely many zeros, find approximately one, several, or all zeros of h in $\mathbb{P}(\mathbb{C}^{n+1})$.

There is a correspondence between Problems 1.1 and 1.2. Given $f = (f_1, \ldots, f_n) \in \mathcal{P}_{(d)}$,

$$f_i = \sum_{\alpha_1 + \cdots + \alpha_n \leq d_i} a^i_{\alpha_1, \ldots, \alpha_n} X_1^{\alpha_1} \cdots X_n^{\alpha_n},$$

we can consider its homogeneous counterpart $h = (h_1, \ldots, h_n) \in \mathcal{H}_{(d)}$, where

$$h_i = \sum_{\alpha_1 + \cdots + \alpha_n \leq d_i} a^i_{\alpha_1, \ldots, \alpha_n} X_0^{d_i - (\alpha_1 + \cdots + \alpha_n)} X_1^{\alpha_1} \cdots X_n^{\alpha_n}.$$

If $(\eta_1, \ldots, \eta_n)$ is a zero of f, then $(1, \eta_1, \ldots, \eta_n)$ is a zero of h. Conversely, if $(\zeta_0, \ldots, \zeta_n) \in \mathbb{P}(\mathbb{C}^{n+1})$ is a zero of h and $\zeta_0 \neq 0$, then $\left(\frac{\zeta_1}{\zeta_0}, \ldots, \frac{\zeta_n}{\zeta_0}\right)$ is a zero of f.

The general idea of homotopy methods is as follows: Choose some system $g \in \mathcal{H}_{(d)}$ that has a known solution ζ_0. Then consider a path $h_t \subseteq \mathcal{H}_{(d)}$, $0 \leq t \leq T$, such that $h_0 = g$ and $h_T = h$ is the target system (for the time being, the reader may think of the linear path $h_t = (1-t)g + th$). If the homotopy is well posed, the solution ζ_0 can be continuously deformed to a solution ζ_t of h_t. One can try to follow this path ζ_t numerically to get an approximation ζ_T of a zero of h. An important ingredient is how fine the discretization of our numerical method has to be. Depending on a certain geometric property of the path (h_t, ζ_t), its *condition length*, see (3–7) below, we will need finer or coarser discretization. A longstanding conjecture by Shub and Smale is the following (see Section 7.2 for a detailed description): Let[1]

$$g(x) = \begin{cases} d_1^{1/2} x_0^{d_1 - 1} x_1, \\ \vdots \\ d_n^{1/2} x_0^{d_n - 1} x_n, \end{cases} \qquad \zeta_0 = e_0 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}. \qquad (1\text{–}1)$$

Then the running time of a well-designed homotopy method for following linear paths starting at (g, e_0) is polynomial in the size of the input on average (i.e., if h is chosen "randomly," according to a particular probability distribution). In this paper we give experimental data that confirm this conjecture, and we suggest, moreover, a more specific version of it; see (7–3).

The structure of the paper is as follows. In Section 2, we recall the definition of approximate zero, condition number, and Newton's method, and equip the space of polynomial systems with a Hermitian product. In Section 3, we describe a certified algorithm to follow a homotopy path. An overview of approaches to finding all the roots of a system is presented in Section 4. In Section 5, we give an algorithm to construct a random linear homotopy with good average complexity. In Section 6, we explain briefly how to use the software. Section 7 demonstrates the practicality of computation with the developed algorithm and discusses experimental data that could be used to obtain intuition, in particular, with regard to the conjecture of Shub and Smale.

[1] The original pair suggested by Shub and Smale had no $d_i^{1/2}$ factors like those here. As has been done in other papers by several authors, we add these factors here to optimize the condition number $\mu(g, e_0)$.

2. PRELIMINARIES

Let $d = \max\{d_1, \ldots, d_n\}$ and $\mathcal{D} = d_1 \cdots d_n$. Note that d is a small quantity, but in general, $\mathcal{D}$ is an exponential quantity. We denote by $N+1$ the complex dimension of $\mathcal{H}_{(d)}$ and $\mathcal{P}_{(d)}$ as vector spaces. Namely,

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

2.1. Approximate Zeros and Newton's Method

In general, it is hard to describe zeros of $f \in \mathcal{P}_{(d)}$ or $h \in \mathcal{H}_{(d)}$ exactly. One may ask for points that are "ε-close" to some zero, but this is not a very stable concept. The concept of an approximate zero of [Smale 86] fixes that gap.

Given $f \in \mathcal{P}_{(d)}$, consider the Newton operator associated to f,

$$N(f)(x) = x - Df(x)^{-1} f(x),$$

where $Df(x)$ is the $n \times n$ derivative matrix of f at $x \in \mathbb{C}^n$, also often called the Jacobian (matrix). Note that $N(f)(x)$ is defined only if $Df(x)$ is an invertible matrix. We will define

$$N(f)^l(x) = N(f)\overbrace{\circ \cdots \circ}^{l} N(f)(x),$$

the result of l iterations of Newton's method starting at x.

Definition 2.1. We say that $x \in \mathbb{C}^n$ is an *approximate zero* of $f \in \mathcal{P}_{(d)}$ with associated zero $\eta \in \mathbb{C}^n$ if $N(f)^l(x)$ is defined for all $l \geq 0$ and

$$\left\| N(f)^l(x) - \eta \right\| \leq \frac{\|x - \eta\|}{2^{2^l - 1}}, \quad l \geq 0.$$

The homogeneous version of Newton's method [Shub 93] is defined as follows. Let $h \in \mathcal{H}_{(d)}$ and $z \in \mathbb{P}(\mathbb{C}^{n+1})$. Then

$$N_{\mathbb{P}}(h)(z) = z - (Dh(z)\mid_{z^\perp})^{-1} h(z),$$

where $Dh(z)$ is the $n \times (n+1)$ Jacobian matrix of h at $z \in \mathbb{P}(\mathbb{C}^{n+1})$, and

$$Dh(z)\mid_{z^\perp}$$

is the restriction of the linear operator defined by $Dh(z) : \mathbb{C}^{n+1} \to \mathbb{C}^n$ to the orthogonal complement $z^\perp$ of z. Hence $(Dh(z)\mid_{z^\perp})^{-1}$ is a linear operator from $\mathbb{C}^n$ to $z^\perp$, and $N_{\mathbb{P}}(h)(z)$ is defined if this operator is invertible. The reader may check that $N_{\mathbb{P}}(h)(\lambda z) = \lambda N_{\mathbb{P}}(h)(z)$, namely that $N_{\mathbb{P}}(h)$ is a well-defined projective operator. Note that $N_{\mathbb{P}}(h)$ may be written in a matrix form

$$N_{\mathbb{P}}(h)(z) = z - \begin{pmatrix} Dh(z) \\ z^* \end{pmatrix}^{-1} \begin{pmatrix} h(z) \\ 0 \end{pmatrix},$$

which is more convenient for computations. As before, we denote by $N_{\mathbb{P}}(h)^l(z)$ the result of l consecutive applications of $N_{\mathbb{P}}(h)$ with the initial point z.

Definition 2.2. We say that $z \in \mathbb{P}(\mathbb{C}^{n+1})$ is an *approximate zero* of $h \in \mathcal{H}_{(d)}$ with associated zero $\zeta \in \mathbb{P}(\mathbb{C}^{n+1})$ if $N_{\mathbb{P}}(h)^l(z)$ is defined for all $l \geq 0$ and

$$d_R(N_{\mathbb{P}}(h)^l(z), \zeta) \leq \frac{d_R(z, \zeta)}{2^{2^l - 1}}, \quad l \geq 0.$$

Here d_R is the Riemann distance in $\mathbb{P}(\mathbb{C}^{n+1})$, namely

$$d_R(z, z') = \arccos \frac{|\langle z, z' \rangle|}{\|z\| \, \|z'\|} \in [0, \pi/2],$$

where $\langle \cdot, \cdot \rangle$ and $\| \cdot \|$ are the usual Hermitian product and norm in $\mathbb{C}^{n+1}$. Note that $d_R(z, z') = d_R(\lambda z, \lambda' z')$ for $\lambda, \lambda' \in \mathbb{C}$; namely d_R is well defined in $\mathbb{P}(\mathbb{C}^{n+1}) \times \mathbb{P}(\mathbb{C}^{n+1})$.

The reader familiar with Riemannian geometry may check that $d_R(z, z')$ is the length of the shortest C^1 curve with extremes $z, z' \in \mathbb{P}(\mathbb{C}^{n+1})$ when $\mathbb{P}(\mathbb{C}^{n+1})$ is endowed with the usual Hermitian structure (see [Blum et al. 98, p. 226]).

Let $f \in \mathcal{P}_{(d)}$ and let $h \in \mathcal{H}_{(d)}$ be the homogeneous counterpart of f. In contrast to the case of exact zeros, it may happen that $z = (z_0, \ldots, z_n)$ is an approximate zero of h but still $\left(\frac{z_1}{z_0}, \ldots, \frac{z_n}{z_0}\right)$ is not an approximate zero of f. In Proposition 2.5 we explain how to fix that gap.

2.2. The Bombieri–Weyl Hermitian Product

In studying Problems 1.1 and 1.2, it is very helpful to introduce some geometric and metric properties in the vector spaces $\mathcal{P}_{(d)}$ and $\mathcal{H}_{(d)}$. We recall now the unitarily invariant Hermitian product in $\mathcal{H}_{(d)}$, sometimes called the Kostlan Hermitian product [Blum et al. 98] or Bombieri–Weyl Hermitian product [Beltrán and Shub 10]. Given $d_0 \in \mathbb{N}$ and two polynomials $v, w \in \mathcal{H}_{d_0}$,

$$v = \sum_{\alpha_0 + \cdots + \alpha_n = d_0} a_{\alpha_0, \ldots, \alpha_n} X_0^{\alpha_0} \cdots X_n^{\alpha_n},$$

and

$$w = \sum_{\alpha_0 + \cdots + \alpha_n = d_0} b_{\alpha_0, \ldots, \alpha_n} X_0^{\alpha_0} \cdots X_n^{\alpha_n},$$

we consider their (Bombieri–Weyl) product

$$\langle v, w\rangle = \sum_{\alpha_0+\alpha_1+\cdots+\alpha_n=d_0} \binom{d_0}{(\alpha_0,\ldots,\alpha_n)}^{-1} \times a_{\alpha_0,\ldots,\alpha_n}\overline{b_{\alpha_0,\ldots,\alpha_n}},$$

where $\overline{\cdot}$ is complex conjugation and

$$\binom{d_0}{(\alpha_0,\ldots,\alpha_n)} = \frac{d_0!}{\alpha_0!\cdots\alpha_n!}$$

is the multinomial coefficient.

Then, given two elements $h = (h_1,\ldots,h_n)$ and $h' = (h'_1,\ldots,h'_n)$ of $\mathcal{H}_{(d)}$, we define

$$\langle h, h'\rangle = \langle h_1, h'_1\rangle + \cdots + \langle h_n, h'_n\rangle, \quad \|h\| = \langle h, h\rangle^{1/2}.$$

This Hermitian product defines a real inner product in $\mathcal{H}_{(d)}$ as usual,

$$\langle h, h'\rangle_{\mathbb{R}} = \operatorname{Re}\left(\langle h, h'\rangle\right).$$

We also define a Hermitian product and the associated norm in $\mathcal{P}_{(d)}$ as follows: Given $f, f' \in \mathcal{P}_{(d)}$, let $h, h' \in \mathcal{H}_{(d)}$ be the homogeneous counterparts of f, f'. Then define

$$\langle f, f'\rangle = \langle h, h'\rangle, \quad \|f\| = \|h\|.$$

From now on, we will denote by $\mathbb{S}$ the unit sphere in $\mathcal{H}_{(d)}$ for this norm, namely

$$\mathbb{S} = \{h \in \mathcal{H}_{(d)} : \|h\| = 1\}.$$

Note that for solving Problem 1.2, we may restrict our input systems $h \in \mathcal{H}_{(d)}$ to $h \in \mathbb{S}$, for zeros of a system of equations do not change if the system is multiplied by a nonzero scalar number.

2.3. The Condition Number

The condition number at $(h, z) \in \mathcal{H}_{(d)} \times \mathbb{P}(\mathbb{C}^{n+1})$ is defined as follows:

$$\mu(h, z) = \|h\| \left\|(Dh(z)\mid_{z^\perp})^{-1}\operatorname{Diag}\left(\|z\|^{d_i-1}d_i^{1/2}\right)\right\|,$$

or $\mu(h, z) = \infty$ if $Dh(\zeta)\mid_{z^\perp}$ is not invertible. Here, $\|h\|$ is the Bombieri–Weyl norm of h, and the second norm in the product is the operator norm of that linear operator. Note that $\mu(h, z)$ is essentially equal to the operator norm of the inverse of the Jacobian $Dh(\zeta)$, restricted to the orthogonal complement of z. The rest of the factors in this definition are normalizing factors that make results look nicer and allow projective computations. See [Shub and Smale 93] for more details. Sometimes μ is denoted by μ_{norm} or μ_{proj}, but we keep the simpler notation here.

The two following results are versions of Smale's γ-theorem, and follow from the study of the condition number in [Shub and Smale 93, Shub 09].

Proposition 2.3. [Beltrán and Pardo 09, Proposition 4.1] *Let $f \in \mathcal{P}_{(d)}$ and let $h \in \mathcal{H}_{(d)}$ be its homogeneous counterpart. Let $\eta = (\eta_1,\ldots,\eta_n) \in \mathbb{C}^n$ be a zero of f, and let $\zeta = (1, \eta_1,\ldots,\eta_n) \in \mathbb{P}(\mathbb{C}^{n+1})$ be the associated zero of h. Let $x \in \mathbb{C}^n$ satisfy*

$$\|x - \eta\| \le \frac{3-\sqrt{7}}{d^{3/2}\mu(h,\zeta)}.$$

Then x is an affine approximate zero of f, with associated zero η.

Proposition 2.4. [Beltrán 11] *Let $\zeta \in \mathbb{P}(\mathbb{C}^{n+1})$ be a zero of $h \in \mathcal{H}_{(d)}$ and let $z \in \mathbb{P}(\mathbb{C}^{n+1})$ be such that*

$$d_R(z,\zeta) \le \frac{u_0}{d^{3/2}\mu(h,\zeta)}, \quad \text{where } u_0 = 0.17586.$$

Then z is an approximate zero of h with associated zero ζ.

The following result gives a tool to obtain affine approximate zeros from projective ones.

Proposition 2.5. [Beltrán and Pardo 09, Proposition 4.5] *Let $f \in \mathcal{P}_{(d)}$ and let $h \in \mathcal{H}_{(d)}$ be its homogeneous counterpart. Let $\eta = (\eta_1,\ldots,\eta_n) \in \mathbb{C}^n$ be a zero of f, and let $\zeta = (1, \eta_1,\ldots,\eta_n) \in \mathbb{P}(\mathbb{C}^{n+1})$ be the associated zero of h. Let $z = (z_0,\ldots,z_n) \in \mathbb{P}(\mathbb{C}^{n+1})$ be a projective approximate zero of h with associated zero ζ such that*

$$d_R(z,\zeta) \le \arctan\left(\frac{3-\sqrt{7}}{d^{3/2}\mu(h,\zeta)}\right)$$

($d_R(z,\zeta) \le \frac{u_0}{d^{3/2}\mu(h,\zeta)}$ suffices).

Let $z^l = \mathbb{N}_{\mathbb{P}}(h)^l(z)$, where $l \in \mathbb{N}$ is such that

$$l \ge \log_2\log_2\left(4\left(1+\|\eta\|^2\right)\right).$$

Let $x^l = \left(\frac{z_1^l}{z_0^l},\ldots,\frac{z_n^l}{z_0^l}\right)$. Then

$$\left\|x^l - \eta\right\| \le \frac{3-\sqrt{7}}{d^{3/2}\mu(h,\zeta)}.$$

In particular, x^l is an affine approximate zero of f with associated zero η by Proposition 2.3.

Thus, if we have a bound on $\|\eta\|$ and a projective approximate zero of h with associated zero the projective solution ζ, we just need to apply the projective Newton operator $N_{\mathbb{P}}(h)$ a few times $\lceil \log_2\log_2(4(1+\|\eta\|^2))\rceil$ to get an affine approximate zero of f with associated zero

η. Here by $\lceil\lambda\rceil$, we mean the smallest integer greater than λ, $\lambda \in \mathbb{R}$. Thus, a solution to Problem 1.1 follows from a solution to Problem 1.2 and a control on the norm of the affine solutions of $f \in \mathcal{P}_{(d)}$. The latter can be done either on per case basis or via a probabilistic argument as in [Beltrán and Pardo 09, Corollary 4.9], where it is proved that for f such that $\|f\| = 1$ and $\delta \in (0,1)$, we have $\|\eta\| \leq \mathcal{D}\sqrt{\pi n}/\delta$ with probability greater than $1-\delta$.

From now on, we center our attention on Problem 1.2, and we will assume that all the input systems h have unit norm, namely $h \in \mathbb{S}$.

3. THE HOMOTOPY METHOD: AN ALGORITHM FOR FINDING ONE ROOT

Let $V = \{(f,\zeta) \in \mathbb{S} \times \mathbb{P}(\mathbb{C}^{n+1}) : f(\zeta) = 0\}$ be the so-called *solution variety*. Elements in V are pairs (system, solution). Consider the projection on the first coordinate $\pi : V \to \mathbb{S}$. The condition number defined above is an upper bound for the norm of the derivative of the local inverse of π near $\pi(f,\zeta)$; see, for example, [Blum et al. 98, Chapter 12]. In particular, π is locally invertible near (f,ζ) if $\mu(f,\zeta) < \infty$.

Let $t \to h_t \in \mathbb{S}$, $0 \leq t \leq T$, be a C^1 curve, and let ζ_0 be a solution of h_0. If $\mu(h_0,\zeta_0) < \infty$, then π is locally invertible near h_0. Thus, there exists some $\varepsilon > 0$ such that for $0 \leq t < \varepsilon$, the zero ζ_0 can be continued to a zero ζ_t of h_t in such a way that $t \to \zeta_t$ is a C^1 curve. We call the curve $t \to (h_t, \zeta_t)$ the *lifted curve* of $t \to h_t$. There are two possible scenarios:

Regular: The whole curve $t \to h_t$, $0 \leq t \leq T$, can be lifted to $t \to (h_t, \zeta_t)$.

Singular: There is some $\varepsilon \leq T$ such that $t \to h_t$ can be lifted for $0 \leq t < \varepsilon$, but $\mu(h_t,\zeta_t) \to \infty$ as $t \to \varepsilon$.

Problem 3.1. Create a *homotopy continuation algorithm*, a numerical procedure that follows closely the lifted curve. Namely, in the regular case, the goal of such an algorithm is to construct a sequence $0 = t_0 < t_1 < \cdots < t_k = T$ and pairs $(g_i, z_i) \in \mathbb{S} \times \mathbb{P}(\mathbb{C}^{n+1})$ such that for all $i = 0, \ldots, k$ we have $g_i = h_{t_i}$ and z_i is an approximate zero associated with the zero ζ_i of g_i with (g_0,ζ_0) and (g_i,ζ_i) lying on the same lifted curve.

The homotopy method that we have in mind solves the problem above (in the regular case) and creates an infinite sequence $\{t_i\}$ converging to the first singularity on the curve in the singular case.

Remark 3.2. A homotopy algorithm still may be useful in a singular case in which the curve can be lifted for $t \in [0,T)$, which is the scenario, for example, of a homotopy curve leading to a singular solution. One may use z_i for t_i close to T as an empirical approximation of the singular zero. Approximate zeros (defined before) associated to a singular zero might not exist, since Newton's method loses its quadratic convergence near a singularity.

Given a C^1 curve $t \to h_t$, we define $\dot{h}_t = \frac{d}{dt}h_t$. Namely, $\dot{h}_t$ is the tangent vector to the curve at t. Note that $\dot{h}_t$ depends on the parameterization of the curve, not only on the geometric object (the arc defined by the curve).

A continuous curve $t \to h_t \in \mathbb{S}$, $0 \leq t \leq T$, is of class $C^{1+\mathrm{Lip}}$ if it is of class C^1 in $[0,T]$ (i.e., it has a continuous derivative in $(0,T)$ and one-sided derivatives at $t = 0$ and $t = T$, making $\dot{h}(t)$ continuous in $[0,T]$), and if the mapping $t \to \dot{h}_t$ is a Lipschitz map, namely if there exists a constant $K > 0$ such that

$$\|\dot{h}_t - \dot{h}_s\| \leq K|t-s|, \quad \forall\, t,s \in [0,T].$$

By Rademacher's theorem, this implies that the second derivative $\ddot{h}_t$ exists almost everywhere and is bounded by $\|\ddot{h}_t\| \leq K$.

3.1. Explicit Construction of the Homotopy Method

A certified homotopy method and its complexity was shown for the first time in [Shub and Smale 93, Shub and Smale 94], at least for the case of linear homotopy. In a recent work [Shub 09], the theoretical complexity of such methods was greatly improved, although no specific algorithm was shown because the choice of the step size was not specified. This last piece can be done in several ways; see [Beltrán 11, Bürgisser and Cucker 12, Dedieu et al. 12]. We now recall the homotopy method of [Beltrán 11], designed to follow a $C^{1+\mathrm{Lip}}$ curve $t \to h_t \in \mathbb{S}$, $t \in [0,T]$. We make the following assumptions:

1. We know an approximate zero z_0, $\|z_0\| = 1$, of $g_0 = h_0$, satisfying
$$d_R(z_0,\zeta_0) \leq \frac{u_0}{2d^{3/2}\mu(h_0,\zeta_0)}, \tag{3–1}$$
where $u_0 = 0.17586$, for some exact zero ζ_0 of h_0.
2. Given $t \in [0,T]$, it is possible to compute h_t and $\dot{h}_t = \frac{dh_t}{dt}$.
3. We know some real number $H \geq 0$ satisfying
$$\|\ddot{h}_t\| \leq d^{3/2}H\|\dot{h}_t\|^2, \tag{3–2}$$

for almost every $t \in [0,T]$. From now on, we define

$$P = \sqrt{2} + \sqrt{4+5H^2} \in \mathbb{R}\,.$$

For $i \geq 1$, define (g_{i+1}, z_{i+1}) inductively as follows. Let a representative of z_i be chosen such that $\|z_i\| = 1$. Let $s \in [0,T]$ be such that $h_s = g_i$ and let $\dot{g}_i = \dot{h}_s \in \mathcal{H}_{(d)}$ be the tangent vector to the curve $t \to h_t$ at $t = s$. Let

$$\chi_{i,1} = \left\| \begin{pmatrix} Dg_i(z_i) \\ z_i^* \end{pmatrix}^{-1} \begin{pmatrix} \sqrt{d_1} & & & \\ & \ddots & & \\ & & \sqrt{d_n} & \\ & & & 1 \end{pmatrix} \right\| \tag{3–3}$$

and

$$\chi_{i,2} = \left(\|\dot{g}_i\|^2 + \left\| \begin{pmatrix} Dg_i(z_i) \\ z_i^* \end{pmatrix}^{-1} \begin{pmatrix} \dot{g}_i(z_i) \\ 0 \end{pmatrix} \right\|^2 \right)^{1/2}, \tag{3–4}$$

and consider

$$\varphi_i = \chi_{i,1}\chi_{i,2}. \tag{3–5}$$

Let

$$c = \frac{(1-\sqrt{2}u_0/2)^{\sqrt{2}}}{1+\sqrt{2}u_0/2} \left(1 - \left(1 - \frac{u_0}{\sqrt{2}+2u_0} \right)^{P/\sqrt{2}} \right),$$

and let t_i be chosen in such a way that

$$\frac{c}{2Pd^{3/2}\varphi_i} \leq t_i \leq \frac{c}{Pd^{3/2}\varphi_i}, \tag{3–6}$$

or $t_i = T - s$ if

$$\frac{c}{2Pd^{3/2}\varphi_i} \geq T - s.$$

Note that this last case occurs when the step t_i chosen with the formula above takes us beyond the limits of the interval $[0,T]$. The lower bound on (3–6) is used to guarantee that the homotopy step is not too small (and thus the total number of steps is not too big).

Note that in order to compute φ_i, we must compute the norm of a vector (for $\chi_{i,2}$) and the norm of a matrix (for $\chi_{i,1}$). However, we need to do these tasks only approximately, for we just need to compute a number in $[\varphi_i, 2\varphi_i]$.

In Section 3.3 below, we describe the value of the constants to be taken in the case of linear homotopy.

Let $g_{i+1} = h_{s+t_i}$ and let

$$z_{i+1} = \frac{N_{\mathbb{P}}(g_{i+1})(z_i)}{\|N_{\mathbb{P}}(g_{i+1})(z_i)\|}.$$

In this way, we generate (g_1, z_1), (g_2, z_2), etc. We stop at k such that $g_k = h_T$, and we output $z_k \in \mathbb{P}(\mathbb{C}^{n+1})$.

3.2. Convergence and Complexity of the Homotopy Method

The homotopy method is guaranteed to produce an approximate zero of the target system $h = h_T$ if we are in the regular scenario. Moreover, its complexity (number of projective Newton's method steps) is also well understood and attains the theoretical result of [Shub 09]. With the notation above, let

$$\mathcal{C}_0 = \int_0^T \mu(h_t, \zeta_t) \left\| (\dot{h}_t, \dot{\zeta}_t) \right\| dt. \tag{3–7}$$

The reader may observe that $\mathcal{C}_0$ (called the *condition length* of the path (h_t, ζ_t) in $\mathbb{S} \times \mathbb{P}(\mathbb{C}^{n+1})$) is the length of the path (h_t, ζ_t) in the condition metric, which is the metric in the solution variety V obtained by pointwise multiplying the usual metric inherited from that of the product $\mathbb{S} \times \mathbb{P}(\mathbb{C}^{n+1})$ by the condition number μ.

Theorem 3.3. [Beltrán 11] *With the notation and hypotheses above, assume that*

$$d_R(z_0, \zeta_0) \leq \frac{u_0}{2d^{3/2}\mu(h_0, \zeta_0)}, \quad u_0 = 0.17586.$$

Then for every $i \geq 0$, z_i is an approximate zero of g_i, with associated zero ζ_i, the unique zero of g_i that lies in the lifted path (h_t, ζ_t). Moreover,

$$d_R(z_i, \zeta_i) \leq \frac{u_0}{2d^{3/2}\mu(h_i, \zeta_i)}, \quad i \geq 1.$$

If $\mathcal{C}_0 < \infty$, there exists $k \geq 0$ such that $h_T = g_k$. Namely, the number of homotopy steps is at most k. Moreover,

$$k \leq \lceil Cd^{3/2}\mathcal{C}_0 \rceil,$$

where

$$C = \frac{2P}{(1-\sqrt{2}u_0/2)^{1+\sqrt{2}}} \left(\frac{1}{c} + \frac{1+\sqrt{2}u_0/2}{\left(1-\sqrt{2}u_0/2\right)^{\sqrt{2}}} \right).$$

In particular, if $\mathcal{C}_0 < \infty$, the algorithm finishes and outputs z_k, an approximate zero of $h_T = g_k$ with associated zero ζ_k, the unique zero of h_T that lies in the lifted path (h_t, ζ_t).

Remark 3.4. Since $\lceil \lambda \rceil \leq \lambda + 1$ for $\lambda \in \mathbb{R}$, we have that the number of steps is at most

$$1 + Cd^{3/2}\mathcal{C}_0.$$

Remark 3.5. If the curve $t \to h_t$ is piecewise $C^{1+\mathrm{Lip}}$, we may divide the curve into L pieces, each of them of class $C^{1+\mathrm{Lip}}$ and satisfying a.e. $\|\ddot{h}_t\| \leq d^{3/2}H\|\dot{h}_t\|^2$ for a suitable $H \geq 0$. The algorithm may then be applied to each

of these pieces, and an upper bound on the total number of steps is at most

$$L + Cd^{3/2}\mathcal{C}_0.$$

Remark 3.6. If more than one approximate zero of $g = h_0$ is known, the algorithm described above may be used to follow each of the homotopy paths starting at those zeros. From Theorem 3.3, if the approximate zeros of g correspond to different exact zeros of g, and if $\mathcal{C}_0$ is finite for all the paths (i.e., if the algorithm finishes for every initial input), then the exact zeros associated with the output of the algorithm correspond to different exact zeros of h_T.

3.3. Linear Homotopy

Note that given $g, h \in \mathbb{S}$, the segment joining g, h is not contained in $\mathbb{S}$. One can still follow the (short) portion of the great circle in $\mathbb{S}$ containing those two systems. We refer to such "great circle homotopy" as linear homotopy, because it is the projection of linear homotopies on $\mathbb{S}$. The arc-length parameterization of the path is

$$t \to h_t = g\cos(t) + \frac{h - \mathrm{Re}(\langle h, g\rangle)g}{\sqrt{1 - \mathrm{Re}(\langle h, g\rangle)^2}}\sin(t), \quad t \in [0, T], \tag{3–8}$$

where

$$T = \arcsin\sqrt{1 - \mathrm{Re}\langle h, g\rangle^2} = \mathrm{distance}(g, h) \in [0, \pi].$$

Note that this is a C^∞ parameterization, so in particular, it is $C^{1+\mathrm{Lip}}$. From [Beltrán 11, Section 2.2], in this case we may take the following value of c/P in the description of the algorithm:

$$\frac{c}{P} = 0.04804448\ldots.$$

The procedure of certified tracking for a linear homotopy is presented by Algorithm 1.

The bound on the number of steps in Algorithm 1 given by Theorem 3.3 is

$$k \le \left\lceil 71d^{3/2}\mathcal{C}_0 \right\rceil. \tag{3–9}$$

Algorithm 1 Certified tracking for a linear homotopy, $z_* = \mathrm{TrackLinearHomotopy}(h, g, z_0)$.

Require: $h, g \in \mathbb{S}$; z_0 is an approximate zero of g satisfying (3–1).

Ensure: z_* is an approximate zero of h associated with the end of the homotopy path starting at the zero of g associated with z_0 and defined by the homotopy (3–8).

1: $i \leftarrow 0$; $s_i = 0$.
2: **while** $s_i \neq T$ **do**
3: Compute
$$\dot{g}_i \leftarrow \dot{h}_s = -g\sin(s) + \frac{f - \mathrm{Re}(\langle f, g\rangle)g}{\sqrt{1 - \mathrm{Re}(\langle f, g\rangle)^2}}\cos(s)$$
at $s = s_i$.
4: Determine φ_i using (3–3), (3–4), and (3–5).
5: Let t_i be any number satisfying
$$\frac{0.04804448}{2d^{3/2}\varphi_i} \le t_i \le \frac{0.04804448}{d^{3/2}\varphi_i}.$$
6: **if** $t_i > T - s$ **then**
7: $t_i \leftarrow T - s$.
8: **end if**
9: $s_{i+1} \leftarrow s_i + t_i$; $g_{i+1} \leftarrow h_{s_{i+1}}$; $z_{i+1} \leftarrow \frac{N_{\mathbb{P}}(g_{i+1})(z_i)}{\|N_{\mathbb{P}}(g_{i+1})(z_i)\|}$.
10: $i \leftarrow i + 1$.
11: **end while**
12: $z_* \leftarrow z_T$.

4. FINDING ALL ROOTS

Let us consider polynomial functions in $\mathcal{O}_{(d)}$, where $\mathcal{O}_{(d)}$ is one of $\{\mathcal{P}_{(d)}, \mathcal{H}_{(d)}, \mathbb{S}\}$ with zeros in $\mathbb{O}^n$, where $\mathbb{O}^n$ is either $\mathbb{C}^n$ or $\mathbb{P}(\mathbb{C}^{n+1})$.

Consider a homotopy $t \to h_t \in \mathcal{O}_{(d)}$, $t \in [0, T]$, connecting the *target system* h_T and the *start system* h_0 along with a set of *start solutions* $Z_0 \subset h_0^{-1}(0) \subset \mathbb{O}^n$.

Suppose the homotopy curve $t \to h_t$ can be lifted to $t \to (h_t, \zeta_t) \in \mathcal{O}_{(d)} \times \mathbb{O}^n$, $t \in [0, T]$, such that the projection map $\pi : \mathcal{O}_{(d)} \times \mathbb{O}^n \to \mathcal{O}_{(d)}$ is locally invertible at any $t \in [0, T)$. A *homotopy path* is defined as the projection of such a lifted curve onto the second coordinate. If the map π is locally invertible at $t = T$ as well, then the path is called *regular*.

The homotopy $t \to h_t$ is called *optimal* if every $\zeta_0 \in Z_0$ is the beginning of a regular homotopy path. If every solution of h_T is the (other) end of the homotopy path beginning at some $\zeta_0 \in Z_0$, then we call the homotopy *total*.

The field of *numerical algebraic geometry* (see, e.g., [Sommese and Wampler 05]) relies on the ability to reliably track optimal homotopies and find *all* roots of a given 0-dimensional polynomial system of equations in $\mathcal{O}_{(d)}$. One way to accomplish this is to arrange a total-degree homotopy.

4.1. Total-Degree Homotopy

For a target system $f \in \mathcal{P}_{(d)}$, $(d) = (d_1, \ldots, d_n)$, define a *total-degree linear homotopy* to be

$$t \to f_t = (T-t)f_0 + \gamma t f_T,\ \gamma \in \mathbb{C}^*,\ t \in [0,T], \quad (4\text{–}1)$$

where the start system is

$$f_0 = \left(x_1^{d_1} - 1, \ldots, x_n^{d_n} - 1\right) \in \mathcal{P}_{(d)}. \quad (4\text{–}2)$$

One can readily write down the zeros of f_0, the number of which equals the *total degree*, i.e., $d_1 \cdots d_n$.

Proposition 4.1. *Assume that f_T has a finite number of zeros, and let Z_0 be the set of zeros of f_0 above. Then for all but finitely many values of the constant γ, the homotopy (4–1) is total.*

If the number of solutions to the target system $f_T \in \mathcal{P}_{(d)}$ equals the total degree, then (for a generic γ) this homotopy is optimal.

If the target system $f_T \in \mathcal{P}_{(d)}$ has fewer solutions than the total degree, then:

- Some solutions of the target system may be multiple (singular).
- If $\mathbb{O}^n = \mathbb{C}^n$, some of the homotopy paths may diverge (to infinity) when approaching $t = T$.

To compute singular solutions, one may track regular homotopy paths to $t = T - \varepsilon$ for a small $\varepsilon > 0$ (as in Remark 3.2) and then use either *singular endgames* [Sommese and Wampler 05, Section 10.3] or *deflation* [Leykin et al. 06, Leykin et al. 08]. To avoid diverging paths, one may homogenize the homotopy passing from $\mathcal{P}_{(d)}$ to $\mathcal{H}_{(d)}$. The start system of the total homotopy is then the homogenized version of (4–2), that is,

$$g = \left(x_1^{d_1} - x_0^{d_1}, \ldots, x_n^{d_n} - x_0^{d_n}\right) \in \mathcal{H}_{(d)}. \quad (4\text{–}3)$$

4.2. Other Homotopy Methods

There are other ways to obtain all solutions with homotopy continuation that exploit either sparseness or the special structure of a given polynomial system. Here we list a few:

- Polyhedral homotopy continuation based on [Huber and Sturmfels 95] allows one to recover all solutions of a sparse polynomial system in the torus $(\mathbb{C}^*)^n$.
- In many cases presented with a parametric family of polynomial systems, it is enough to solve one system given by a generic choice of parameters. Then, given another system in the family, the chosen generic system may be used as a start system in the so-called *coefficient-parameter* or *cheater's* homotopy [Sommese and Wampler 05, Chapter 7] to recover all solutions of the latter.
- Special homotopies, such as *Pieri homotopies* arising in the Schubert calculus [Huber et al. 98], are total and optimal by design.

5. RANDOM LINEAR HOMOTOPY AND POLYNOMIAL TIME

Suppose we are given a system $h \in \mathcal{H}_{(d)}$ all of whose solutions are regular, and we would like to construct an initial pair (g, ζ_0) in a random fashion such that every root of h is equally likely to be at the end of the linear homotopy path determined by this initial pair. A simple solution to this problem would be to take g to be the start system (4–3) of the total-degree homotopy and pick ζ_0 from the start solutions with uniform probability distribution on the latter. It has been very recently proved [Bürgisser and Cucker 12] that this is a fairly good candidate for the linear homotopy starting pair, since the total average number of steps for each path is $O(d^3 N n^{d+1})$, that is, $O(N^{\log(\log(N))})$, hence close to polynomial in the input size, mainly when $n \gg d$.

In [Beltrán and Pardo 08, Beltrán and Pardo 09, Beltrán and Pardo 11], a probabilistic way to choose the initial pair was proposed. We now center our attention on the last and most recent of these works, where it is proved that if the initial pair (g, ζ_0) is chosen at random (with a certain probability distribution), then the average number of steps performed by the algorithm described in Section 3 is $O(d^{3/2} n N)$, thus almost linear in the size of the input. It is also proved that in this way, we obtain an approximation of a zero of h, so that all the zeros of h are equiprobable if h has no singular solution. In [Beltrán and Shub 10], it is seen that some higher moments (in particular, the variance) of that algorithm are also polynomial in the size of the input. In this section, we describe in detail how the process of randomly choosing (g, ζ_0) works, and we recall the main results of [Beltrán and Pardo 11, Beltrán and Shub 10].

Given $\zeta \in \mathbb{P}(\mathbb{C}^{n+1})$, we consider the set

$$R_\zeta = \left\{\tilde{h} \in \mathcal{H}_{(d)} : \tilde{h}(\zeta) = 0, D\tilde{h}(\zeta) = 0\right\}.$$

Note that R_ζ is defined as the set of polynomials in $\mathcal{H}_{(d)}$ whose coefficients (in the usual monomial basis)

satisfy n^2+2n linear homogeneous equalities. Thus, R_ζ is a vector subspace of $\mathcal{H}_{(d)}$. Moreover, let $e_0 = (1,0,\dots,0)^T$. Then R_{e_0} is the set of polynomial systems $\tilde{h} = (\tilde{h}_1,\dots,\tilde{h}_n) \in \mathcal{H}_{(d)}$ such that all the coefficients of $\tilde{h}_i$ containing $X_0^{d_i}$ or $X_0^{d_i-1}$ are zero, namely

$$\tilde{h}_i = X_0^{d_i-2} p_{2,i}(X_1,\dots,X_n) + X_0^{d_i-3} p_{3,i}(X_1,\dots,X_n) + \cdots,$$

where $p_{k,i}$ is a homogeneous polynomial of degree k with unknowns $X_1,\dots,X_n$.

Recall that $N+1$ is the (complex) dimension of $\mathcal{H}_{(d)}$. The process of choosing (g,ζ_0) at random is as follows:

1. Let $(M,\ell) \in \mathbb{C}^{n^2+n} \times \mathbb{C}^{N+1-n^2-n} = \mathbb{C}^{N+1}$ be chosen at random with the uniform distribution in

$$B(\mathbb{C}^{N+1}) = \left\{ r \in \mathbb{C}^{N+1} : \|r\|_2 \le 1 \right\},$$

where $\|\cdot\|_2$ is the usual Euclidean norm in $\mathbb{C}^{N+1}$. Thus, M is an (n^2+n)-dimensional complex vector, which we consider as an $n \times (n+1)$ complex matrix. Note that choosing $\|(M,\ell)\|_2 \le 1$ implies that $\|M\|_F \le 1$, and indeed, the expected value of $\|M\|_F^2$ is

$$\frac{n^2+n}{N+2}.$$

At this point, we can discard ℓ and just keep M. Note that this procedure is different from just choosing a random matrix, since it induces a certain distribution in the norm of the matrix that is precisely the one in which we are interested. Hence, choosing (M,ℓ) in the unit ball and then discarding ℓ is not a fool's errand!

2. With probability 1, the choice above has produced a matrix M whose kernel has complex dimension 1. Let ζ_0 be a unit norm element of $\ker(M)$, randomly chosen in $\ker(M)$ with the uniform distribution (we may obtain any such ζ_0 simply by solving $M\zeta_0 = 0$ with our preferred method, and then multiplying ζ_0 by a uniformly chosen random complex number of modulus 1). Let V be any unitary matrix such that $V^*\zeta_0 = e_0$. Choose a system $\tilde{h}$ at random in the unit ball (for the Bombieri–Weyl norm) of R_{e_0}. Then consider $h = \tilde{h} \circ V^*$. (This last procedure is equivalent to choosing a system at random with the uniform distribution in $B(R_{\zeta_0}) = \{h \in R_{\zeta_0} : \|h\| \le 1\}$.)

3. Let $\hat{g} \in \mathcal{H}_{(d)}$ be the polynomial system defined by

$$\hat{g}(z) = \sqrt{1-\|M\|_F^2}\, h(z) + \begin{pmatrix} \langle z,\zeta_0\rangle^{d_1-1}\sqrt{d_1} & & \\ & \ddots & \\ & & \langle z,\zeta_0\rangle^{d_n-1}\sqrt{d_n} \end{pmatrix} Mz.$$

4. Let

$$g = \frac{\hat{g}}{\|\hat{g}\|}.$$

Then we have chosen (g,ζ_0), and the reader may check that $g(\zeta_0) = 0$, so ζ_0 is an exact zero of g.

Consider the randomized algorithm defined as follows:

1. Input $h \in \mathbb{S}$.
2. Choose (g,ζ_0) at random with the process described above.
3. Consider the path

$$t \to h_t = g\cos(t) + \frac{h - \mathrm{Re}(\langle h,g\rangle)g}{\sqrt{1-\mathrm{Re}(\langle h,g\rangle)^2}}\sin(t),$$

$t \in [0,T]$, where $T = \arcsin\sqrt{1-\mathrm{Re}\langle h,g\rangle^2}$, and note that $h_0 = g$, $h_T = h$. Use Algorithm 1 to follow the path h_t and output an approximate zero of h.

For given $h \in \mathbb{S}$, let $NS(h)$ be the expected number of homotopy steps performed by this algorithm on input $h \in \mathbb{S}$. We have seen in (3–9) that

$$NS(h) \le \left\lceil 71 d^{3/2} \mathcal{C}_0 \right\rceil.$$

The main theorems of [Beltrán and Pardo 11, Beltrán and Shub 10] are now summarized as follows.

Theorem 5.1. *If $h \in \mathbb{S}$ is such that every zero of h is nonsingular (thus h has exactly $\mathcal{D} = d_1\cdots d_n$ projective zeros), then:*

- *The algorithm above finishes with probability 1 on the choice of (g,ζ_0).*
- *Every zero of h is equally probable as the exact zero associated with the output of the algorithm (which is an approximate zero of h).*

Assuming that $h \in \mathbb{S}$ is chosen at random with the uniform distribution on $\mathbb{S}$, the expected value and variance of $NS(h)$ satisfy

$$\mathrm{E}(NS(h)) \le C_1 n N d^{3/2},$$
$$\mathrm{Var}(NS(h)) \le C_2 n^2 N^2 d^3 \ln(\mathcal{D}),$$

where C_1 and C_2 are universal constants. One may choose $C_1 = 71\pi/\sqrt{2}$.

Note that this theorem gives not only a uniform distribution of the probability of producing any given root of a regular system, but also a good expected running time with the number of steps almost linear in the size of the input.

An algorithm for finding all solutions of a system h with regular zeros follows from Theorem 5.1: repeatedly create and follow random homotopies to find one root of the system until the number of roots found equals the total degree. Tracking $\lceil 2\mathcal{D}\log\mathcal{D}\rceil$ such random homotopies, one finds all zeros of h with (high) probability $1 - 1/\mathcal{D}$ (see [Beltrán and Pardo 11, Corollary 27]). Thus, the expected number of steps of the proposed procedure is $O(d^{3/2}nN\mathcal{D}\log\mathcal{D})$, which grows fast as the total degree of the system increases. This fast growth is necessary if we are attempting to find all $\mathcal{D}$ solutions of the system. The bound $O(d^{3/2}nN\mathcal{D}\log\mathcal{D})$ is the smallest proven value for the complexity of finding all roots of a system. However, this algorithm may not be the most practical one. Using the naive start system (4–3) should require, according to [Bürgisser and Cucker 12], an average number of steps $O(d^{3/2}n^{d+1}N\mathcal{D})$, which is a bigger bound than $O(d^{3/2}nN\mathcal{D}\log\mathcal{D})$ but guarantees that just $\mathcal{D}$ homotopy paths have to be followed.

6. IMPLEMENTATION OF THE METHOD

The computer algebra system Macaulay2—to be more precise, the NAG4M2 (internal name `NumericalAlgebraicGeometry`) package [Leykin 11]—hosts the implementation of Algorithm 1, which is the first implementation of certified homotopy tracking in numerical polynomial homotopy continuation software. The current implementation is carried out with standard double-precision floating-point arithmetic without analyzing effects of round-off errors. For a variant of the algorithm that facilitates rigorous error control, see [Beltrán and Leykin 12].

6.1. NAG4M2: User Manual

There are several functions that we would like to describe here. First, let us give an example of launching the `track` procedure with the certified homotopy tracker:

```
i1 : loadPackage "NumericalAlgebraicGeometry";
i2 : R = CC[x,y,z];
i3 : T = {x^2+y^2-z^2, x*y};
i4 : (S,x0) = totalDegreeStartSystem T;
i5 : x1 = first track(S,T,x0,
          Predictor=>Certified,Normalize=>true)
o5 = {.00000207617, -.706804, .70744}
o5 : Point
i6 : x1.NumberOfSteps
o6 = 129
```

The values for the optional arguments `Predictor` and `Normalize` specify that the certified homotopy tracking is performed and the polynomial systems are normalized to the unit sphere $\mathbb{S}$. In this particular example, `totalDegreeStartSystem` creates an initial pair based on the system described in (4–3), and `track` follows the linear homotopy starting at this initial pair and finishing at the given target system.

The user can also get a good initial pair (1–1) discussed below with the function `goodInitialPair` as well as a random pair of start system and solution as described in Section 5 with `randomInitialPair`.

It is possible for `track` to return a solution marked as *failure*. This happens when the step size becomes smaller than the threshold set by the optional parameter `tStepMin`, which has the default value 10^{-6}.

6.2. Uncertified Homotopy Continuation

All existing software, such as HOM4PS2 [Lee et al 11], Bertini [Bates et al. 11], and PHCpack [Verschelde 99], utilize algorithms based on alternating *predictor* and *corrector* steps. Here is a summary of operations performed at a point of continuation sequence $t \in [0, T]$ starting with a pair (h_t, x_t), where x_t approximates some zero η_t of h_t:

1. Decide heuristically on the step size Δt that the predictor should take.
2. Use a predictor method, i.e., one of the methods for numerical integration of the system of ODEs
$$\dot{z} = -(Dh_t)^{-1}\,\dot{h}_t$$
to produce an approximation of $\zeta_{t+\Delta t}$, a solution of $h_{t+\Delta t}$.
3. Apply the corrector: perform a fixed number l of iterations of Newton's method to obtain a refined approximation $x_{t+\Delta t} = N(h_{t+\Delta t})^l(x_{t+\Delta t})$.
4. If the estimated error bound in step 3 is larger than a predefined tolerance, decrease Δt and go to step 1.

After the parameters, e.g., tolerance values, have been tuned, the application of the described heuristics often produces correct solutions.

System	Number of Solutions	Number of Steps per Path (C)	(H)
$\text{Random}_{(2,2)}$	4	198.5	31
$\text{Random}_{(2,2,2)}$	8	370.125	23
$\text{Random}_{(2,2,2,2)}$	16	813.812	44.375
$\text{Random}_{(2,2,2,2,2)}$	32	1542.5	48.5312
$\text{Random}_{(2,2,2,2,2,2)}$	64	2211.58	58.5312
Katsura_3	4	569.5	25.75
Katsura_4	8	1149.88	41.5
Katsura_5	16	1498.38	39.0625
Katsura_6	32	2361.81	55.5625

TABLE 1. Comparison of the number of steps in the certified and a heuristic algorithm.

We can imagine several "unfortunate" scenarios in which two distinct homotopy paths come too close to each other. Consider sequences $z_0, z_{t_1}, \ldots, z_{t_k}$ and $z'_0, z'_{t'_1}, \ldots, z'_{t'_{k'}}$ created by an uncertified algorithm in an attempt to approximate these two paths:

- If there are subsequences in two sequences that approximate a part of the same path, then this is referred to as *path jumping*.
- *Path swapping* occurs when the sequences jump from one path to the other, but there is no common path segment that they approximate.

While path jumping can in principle be detected a posteriori and the continuation rerun with tighter tolerances and smaller step sizes, path swapping cannot be determined easily.

Path swapping does not result in an incorrect set of target solutions; however, for certain homotopy-based algorithms such as *numerical irreducible decomposition* [Sommese et al. 01] and applications relying on *monodromy* computation such as [Leykin and Sottile 09], the order of the target solutions is crucial. Therefore, one needs not only to certify the endpoints of homotopy paths, but also to show that the approximating sequences follow the same path from start to finish. The certification of the sequence produced in Section 3 provided by Theorem 3.3 gives such a guarantee.

In certain cases, the target solutions obtained by means of uncertified homotopy continuation can be rigorously certified after all of them have been obtained. For instance, suppose a target system $h_T \in \mathcal{H}_{(d)}$ has distinct regular solutions in $\mathbb{P}(\mathbb{C}^{n+1})$. Then their number is equal to the total degree. Suppose some procedure provides that many approximations to the solutions. If a bound on $\max\{\mu(h_T, \zeta) \mid \zeta \in h_T^{-1}(0)\}$ is known, then using Proposition 2.4, these approximations may be certified as distinct numerical zeros, thus certifying that all solutions have been found. If no such bound is known, one may still try to prove that the zeros are different by means of Smale's α-theorem [Smale 86] (see [Hauenstein and Sottile 10]). As discussed above, these procedures cannot determine whether path swapping has occurred.

7. EXPERIMENTAL RESULTS

The algorithm that we developed and implemented gave us a chance to conduct experiments that illuminated several aspects of the complexity analysis of solving polynomial systems via homotopy continuation.

7.1. Certified versus Heuristic tracking

Our experiments in this section were designed to explore how well the certified tracking provided by Algorithm 1 scales in comparison with heuristic approaches. Needless to say, it was expected that running a certified nonheuristic method like the one we propose would require more computational time. As was already mentioned, the proposed certified procedure makes sense only for a regular homotopy. In nearly singular examples, the certified homotopy (like any other method) is bound to show bad performance due to steps being minuscule at the end of paths, which is mandated by (3–6).

In Table 1 we give the data produced by the tracking of total-degree homotopy that are optimal for the chosen examples:

- $\text{Random}_{(d_1,\ldots,d_n)}$: a random system in $\mathbb{S} \subset \mathcal{H}_{(d)}$ with uniform distribution.
- Katsura_n: a classical benchmark with one linear and $n-1$ quadratic equations in n variables.

n	$\mathrm{E}_{\mathrm{good}}$	$\mathrm{Var}_{\mathrm{good}}$	$\mathrm{E}_{\mathrm{total}}$	$\mathrm{Var}_{\mathrm{total}}$	$\mathrm{E}_{\mathrm{rand}}$	$\mathrm{Var}_{\mathrm{rand}}$	$B(n,d,N)$
4	962.051	$3.2 \cdot 10^5$	1263.72	$4.3 \cdot 10^5$	1622.29	$6.8 \cdot 10^5$	$1.0 \cdot 10^5$
5	1524.6	$6.9 \cdot 10^5$	2130.54	$1.2 \cdot 10^6$	2728.3	$1.7 \cdot 10^6$	$2.3 \cdot 10^5$
6	2258.33	$1.3 \cdot 10^6$	3129.56	$2.2 \cdot 10^6$	4137.16	$3.5 \cdot 10^6$	$4.5 \cdot 10^5$
7	3130.83	$2.3 \cdot 10^6$	4530.55	$4.5 \cdot 10^6$	5743.32	$5.5 \cdot 10^6$	$7.8 \cdot 10^5$
8	4154.38	$3.9 \cdot 10^6$	5967.57	$6.7 \cdot 10^6$	8048.94	$1.0 \cdot 10^7$	$1.2 \cdot 10^6$
9	5488.93	$7.0 \cdot 10^6$	8013.71	$1.1 \cdot 10^7$	10482.1	$1.6 \cdot 10^7$	$1.9 \cdot 10^6$
10	6871.35	$1.0 \cdot 10^7$	10071	$1.4 \cdot 10^7$	13477.5	$2.2 \cdot 10^7$	$2.9 \cdot 10^6$
11	8622	$1.2 \cdot 10^7$	12996.1	$2.8 \cdot 10^7$	17193.3	$3.5 \cdot 10^7$	$4.2 \cdot 10^6$
12	10413.3	$2.0 \cdot 10^7$	15115.4	$2.8 \cdot 10^7$	20761.3	$4.6 \cdot 10^7$	$5.8 \cdot 10^6$
13	12447.1	$2.6 \cdot 10^7$	18744.5	$4.3 \cdot 10^7$	25646.5	$6.3 \cdot 10^7$	$7.9 \cdot 10^6$
14	14769.9	$3.3 \cdot 10^7$	22317.1	$6.1 \cdot 10^7$	29596.7	$9.1 \cdot 10^7$	$1.0 \cdot 10^7$
15	17255.7	$4.4 \cdot 10^7$	26017.7	$7.3 \cdot 10^7$	35582.6	$1.2 \cdot 10^8$	$1.4 \cdot 10^7$
16	20959.7	$5.9 \cdot 10^7$	30063.9	$1.0 \cdot 10^8$	42098.9	$1.5 \cdot 10^8$	$1.7 \cdot 10^7$
17	23589.4	$7.5 \cdot 10^7$	35403.1	$1.3 \cdot 10^8$	48024.5	$1.7 \cdot 10^8$	$2.2 \cdot 10^7$
18	27400.9	$9.6 \cdot 10^7$	40242.5	$1.5 \cdot 10^8$	54955.4	$2.3 \cdot 10^8$	$2.7 \cdot 10^7$
19	29930.3	$1.0 \cdot 10^8$	46502.2	$2.3 \cdot 10^8$	62855.2	$2.9 \cdot 10^8$	$3.4 \cdot 10^7$
20	34374.2	$1.4 \cdot 10^8$	51730.2	$2.3 \cdot 10^8$	71242.5	$3.5 \cdot 10^8$	$4.1 \cdot 10^7$

TABLE 2. The number of steps of the certified homotopy continuation algorithm for good, total degree, and random initial pairs on average and its variance; $B(n,d,n)$ is the bound in Theorem 5.1.

For every experiment, we provide the number of solutions and the average number of steps per homotopy path both for the certified algorithm (C) and for one of the best heuristic procedures (H) implemented in Macaulay2. Note that we used the default settings for the parameters that control heuristics without tightening them for larger (worse-conditioned) problems.

One step in a heuristic algorithm involves more basic operations than in the certified tracker: there is a predictor and several corrector steps performed, and if unsuccessful, a new step size is chosen and the procedure is repeated. Even though the heuristic approach leads to much smaller computational time for larger systems, this means that one should expect heuristics to enjoy better *practical* complexity for most examples (there is no sense in talking about the theoretical complexity of such methods).

7.2. A Conjecture of Shub and Smale

In [Shub and Smale 94], the pair described in (1–1) was conjectured to be a good starting pair for the linear homotopy. More precisely, let

$$\mathrm{E}_{\mathrm{good}} = \mathrm{E}\big(\sharp(\textit{steps}) \text{ to solve } h \text{ with linear homotopy starting at } (g, e_0)\big),$$

where the expectation is taken for random $h \in \mathbb{S}$. Then the conjecture in [Shub and Smale 94] can be written as

$$\mathrm{E}_{\mathrm{good}} \leq \text{ a small quantity, polynomial in } N. \qquad (7\text{–}1)$$

The experimental data displayed in Table 2 (see also Figure 1) were obtained by running a linear homotopy connecting the pair (g, e_0) as in (1–1) to a random system in $\mathbb{S} \subset \mathcal{H}_{(d)}$ with $d_i = 2$ for $i = 1, \ldots, n$. We compare the values to that of $B(n,d,N) = 71\pi d^{3/2} nN/\sqrt{2}$, which according to Theorem 5.1 is a bound on the average number of steps of random linear homotopy.

For each value of n, we have generated 1000 random systems in $\mathbb{S}$ with a uniform probability distribution. The values $\mathrm{E}_{\mathrm{good}}$ and $\mathrm{Var}_{\mathrm{good}}$ are estimated expected value and variance of the number of steps taken by Algorithm 1 for the initial pair in (1–1); $\mathrm{E}_{\mathrm{rand}}$ and $\mathrm{Var}_{\mathrm{rand}}$ refer to values for the *random* initial pair; $\mathrm{E}_{\mathrm{total}}$ and $\mathrm{Var}_{\mathrm{total}}$ refer to those for the homogeneous version of the total-degree homotopy system of Section 4.1 containing all the roots of unity (the choice of the root is irrelevant for symmetry reasons), namely, the pair

$$h_0 = \left(X_1^{d_1} - X_0^{d_1}, \ldots, X_n^{d_n} - X_0^{d_n}\right), \quad \zeta_0 = (1, \ldots, 1). \qquad (7\text{–}2)$$

Table 2 and Figure 1 suggest two conclusions for the case of degree-two polynomials:

- The random homotopy seems to take approximately double the number of steps as the homotopy with initial pair (1–1). The total-degree homotopy lies somewhere in between.
- The average number of steps in the three cases appears to grow as $C \cdot N/\sqrt{n}$ with C a constant,

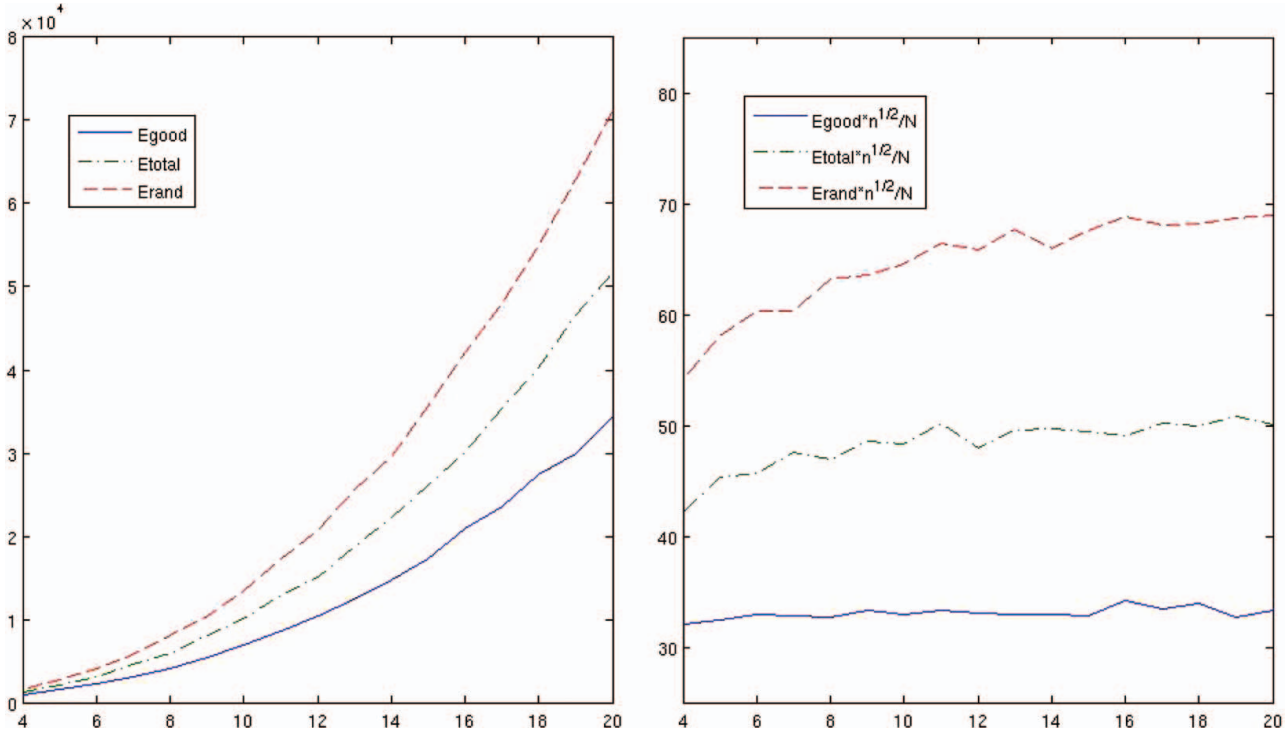

FIGURE 1. In the first figure, we have plotted the experimental values obtained for $\mathrm{E}_{\mathrm{good}}$, $\mathrm{E}_{\mathrm{rand}}$, and $\mathrm{E}_{\mathrm{total}}$ for $n = 4, \ldots, 20$. In the second one we plot $\mathrm{E}_{\mathrm{good}} n^{1/2}/N$, $\mathrm{E}_{\mathrm{total}} n^{1/2}/N$, and $\mathrm{E}_{\mathrm{rand}} n^{1/2}/N$ for $n = 4, \ldots, 20$ (color figure available online).

$C \approx 35, 50, 70$, for $\mathrm{E}_{\mathrm{good}}$, $\mathrm{E}_{\mathrm{total}}$, and $\mathrm{E}_{\mathrm{rand}}$, respectively.

This experiment thus confirms the conjecture of Shub and Smale, and moreover, it suggests a more specific form, suggesting that the same bound given for random homotopy should hold for the conjectured pair:

$$\mathrm{E}_{\mathrm{good}} \leq CnNd^{3/2}, \tag{7–3}$$

with C a constant. We also extend this conjecture to the case of the initial total-degree homotopy pair (h_0, ζ_0) of (7–2):

$$\mathrm{E}_{\mathrm{total}} \leq CnNd^{3/2}.$$

Moreover, as pointed out above, in the case of degree-2 systems, our experiments suggest the existence of a much better bound, since $\mathrm{E}_{\mathrm{good}}$, $\mathrm{E}_{\mathrm{total}}$, and $\mathrm{E}_{\mathrm{rand}}$ all appear to behave as $CN/\sqrt{n}$, where C is a constant. The difference between the experimentally observed value and the theoretical bound in the case of randomly chosen initial pairs, respectively $O(N/\sqrt{n})$ and $O(nN)$ for $(d) = (2, \ldots, 2)$, can be explained as follows. The proof of the theoretical bound starts by bounding

$$\begin{aligned} \mathcal{C}_0 &= \int_0^T \mu(h_t, \zeta_t) \|(\dot{h}_t, \dot{\zeta}_t)\| \, dt \\ &\leq \sqrt{2} \int_0^T \mu(h_t, \zeta_t)^2 \|\dot{h}_t\| \, dt, \end{aligned}$$

which follows from the fact that $\|\dot{\zeta}_t\| \leq \mu(h_t, \zeta_t)\|\dot{h}_t\|$ by the geometric interpretation of the condition number. This last inequality is not sharp in general, and hence one may expect better behavior of the random linear homotopy method than that given by the theoretical bound.

7.3. Equiprobable Roots via Random Homotopy

The algorithm constructing a random homotopy has been implemented in two variants:

1. It is implemented as described in Section 5.
2. The initial pair for the linear homotopy is built by taking (g, e_0) in (1–1) and performing a random unitary coordinate transformation (see [Mezzadri 07] for a stable and efficient algorithm that chooses such a random unitary matrix).

Then the following experiment was conjured to show the equiprobability of the roots at the end of a random

homotopy promised by Theorem 5.1: As the target system we take $h = g + \varepsilon\tilde{h}$, where g is as in (1–1), $\tilde{h}$ is chosen randomly in $\mathbb{S}$, and ε is small. Note that g has a unique nonsingular solution, which is very well conditioned, but it also has a whole subspace of degenerate solutions. Hence h also has a rather well conditioned solution, and then $\mathcal{D} - 1$ isolated but poorly conditioned ones. One might expect that the random homotopy (2) we have just described (for such a fixed h) would be biased toward discovering the well-conditioned root. However, we obtained numerical evidence that this is not the case: all the solutions seem to be equiprobable.

For h with the degrees $d = (2, 2, 2)$ and $\varepsilon = 0.1$ and several random choices of g, we have carried out experiments with the certified tracking procedure making 8000 runs. We experimented with both variants (1) and (2) of choosing the random initial pair. Each experiment resulted in close to 1000 hits for each of eight roots, in both variants (1) and (2). This appears to support the conclusion of Theorem 5.1, valid for variant (1), and moreover extend it to the case of variant (2).

We can state this experimental result in a more precise way, using Shannon's entropy as suggested in [Beltrán and Pardo 11]. Assume that we have an algorithm that involves some random choice in its input and that can produce different outputs $x_1, \ldots, x_l$. Shannon's entropy is by definition the number

$$H = -\sum_{i=1}^{l} p_i \log_2(p_i),$$

where p_i is the probability that the output is x_i. It is easy to see that Shannon's entropy of an algorithm is maximal, and equal to $\log_2(l)$, if and only if every output is equally probable. The experimental value of Shannon's entropy for the random algorithm in all experiments described above is in the interval $[2.99, 3]$; the maximum, in this case, is $\log_2 8 = 3$.

The exact reason for the modified algorithm (variant (2)) to produce equiprobability of the roots is not understood. This poses a very interesting mathematical question, which together with proving (7–3) would yield great progress in the understanding of homotopy methods for solving systems of polynomial equations.

ACKNOWLEDGMENTS

The authors would like to thank Mike Shub for insightful comments. The second author is grateful to Jan Verschelde for early discussions of practical certification issues. This work was partially done while the authors were attending a workshop on the complexity of numerical computation as part of the FoCM thematic program hosted by the Fields Institute, Toronto. We thank that institution for their kind support. We are also thankful to the referees for their helpful comments. Carlos Beltrán's research was partially supported by MTM2007-62799 and MTM2010-16051, Spanish Ministry of Science (MICINN). Anton Leykin's research was partially supported by NSF grant DMS-0914802.

REFERENCES

[Bates et al. 11] D. J. Bates, J. D. Hauenstein, A. J. Sommese, and C. W. Wampler. "Bertini: Software for Numerical Algebraic Geometry." Available online (http://www.nd.edu/~sommese/bertini), 2011.

[Beltrán 11] C. Beltrán. "A Continuation Method to Solve Polynomial Systems, and Its Complexity." *Numerische Mathematik* 117:1 (2011), 89–113.

[Beltrán and Leykin 12] C. Beltrán and A. Leykin. "Robust Certified Numerical Homotopy Tracking." arXiv: 1105.5992, 2012.

[Beltrán and Pardo 08] C. Beltrán and L. M. Pardo. "On Smale's 17th Problem: A Probabilistic Positive Solution." *Found. Comput. Math.* 8:1 (2008), 1–43.

[Beltrán and Pardo 09] C. Beltrán and L. M. Pardo. "Smale's 17th Problem: Average Polynomial Time to Compute Affine and Projective Solutions." *J. Amer. Math. Soc.* 22 (2009), 363–385.

[Beltrán and Pardo 11] C. Beltrán and L. M. Pardo. "Fast Linear Homotopy to Find Approximate Zeros of Polynomial Systems." *Foundations of Computational Mathematics* 11:1 (2011), 95–129.

[Beltrán and Shub 10] C. Beltrán and M. Shub. "A Note on the Finite Variance of the Averaging Function for Polynomial System Solving." *Found. Comput. Math.* 10 (2010), 115–125.

[Blum et al. 98] L. Blum, F. Cucker, M. Shub, and S. Smale. *Complexity and Real Computation*. Springer, 1998.

[Bürgisser and Cucker 12] P. Bürgisser and F. Cucker. "On a Problem Posed by Steve Smale." To appear in *Annals of Mathematics*, 2012.

[Dedieu et al. 12] J.-P. Dedieu, G. Malajovich, and M. Shub. "Adaptative Step Size Selection for Homotopy Methods to Solve Polynomial Equations," To appear, 2012.

[Hauenstein and Sottile 10] J. D. Hauenstein and F. Sottile. "alphaCertified: Certifying Solutions to Polynomial Systems." To appear in *ACM Transactions on Mathematical Software*.

[Huber and Sturmfels 95] B. Huber and B. Sturmfels. "A Polyhedral Method for Solving Sparse Polynomial Systems." *Math. Comp.*, 64:212 (1995), 1541–1555.

[Huber et al. 98] B. Huber, F. Sottile, and B. Sturmfels. "Numerical Schubert Calculus." *J. Symbolic Comput.* 26:6 (1998), 767–788.

[Lee et al 11] T. L. Lee, T. Y. Li, and C. H. Tsai. "Hom4ps-2.0: A Software Package for Solving Polynomial Systems by the Polyhedral Homotopy Continuation Method." Available online (http://hom4ps.math.msu.edu/HOM4PS_soft.htm), 2011.

[Leykin 11] A. Leykin. "Numerical Algebraic Geometry." *JSAG* 3 (2011), 5–10.

[Leykin and Sottile 09] A. Leykin and F. Sottile. "Galois Groups of Schubert Problems via Homotopy Computation." *Math. Comp.* 78:267 (2009), 1749–1765.

[Leykin et al. 06] A. Leykin, J. Verschelde, and A. Zhao. "Newton's Method with Deflation for Isolated Singularities of Polynomial Systems." *Theoretical Computer Science* 359:1-3 (2006), 111–122.

[Leykin et al. 08] A. Leykin, J. Verschelde, and A. Zhao. "Higher-Order Deflation for Polynomial Systems with Isolated Singular Solutions." In *Algorithms in Algebraic Geometry*, IMA Vol. Math. Appl. 146, pp. 79–97. Springer, 2008.

[Mezzadri 07] F. Mezzadri. "How to Generate Random Matrices from the Classical Compact Groups." *Notices of the American Mathematical Society* 54:5 (2007), 592–604.

[Shub 93] M. Shub. "Some Remarks on Bézout's Theorem and Complexity Theory." In *From Topology to Computation: Proceedings of the Smalefest (Berkeley, CA, 1990)*, pp. 443–455. Springer, 1993.

[Shub 09] M. Shub. "Complexity of Bézout's Theorem. VI: Geodesics in the Condition (Number) Metric." *Found. Comput. Math.* 9:2 (2009), 171–178.

[Shub and Smale 93] M. Shub and S. Smale. "Complexity of Bézout's Theorem. I. Geometric Aspects." *J. Amer. Math. Soc.* 6:2 (1993), 459–501.

[Shub and Smale 94] M. Shub and S. Smale. "Complexity of Bézout's Theorem. V. Polynomial Time." *Theoret. Comput. Sci.* 133:1 (1994), Selected papers of the Workshop on Continuous Algorithms and Complexity (Barcelona, 1993), 141–164.

[Smale 86] S. Smale. "Newton's Method Estimates from Data at One Point." In *The Merging of Disciplines: New Directions in Pure, Applied, and Computational Mathematics (Laramie, Wyo., 1985)*, pp. 185–196. Springer, 1986.

[Sommese and Wampler 05] A. J. Sommese and C. W. Wampler. *The Numerical Solution of Systems of Polynomials.* World Scientific, 2005.

[Sommese et al. 01] A. J. Sommese, J. Verschelde, and C. W. Wampler. "Numerical Decomposition of the Solution Sets of Polynomial Systems into Irreducible Components." *SIAM J. Numer. Anal.* 38:6 (2001), 2022–2046.

[Verschelde 99] J. Verschelde. "Algorithm 795: PHCpack: A General-Purpose Solver for Polynomial Systems by Homotopy Continuation." *ACM Trans. Math. Softw.* 25:2 (1999), 251–276.

[Zyczkowski and Kus 94] K. Zyczkowski and M. Kus. "Random Unitary Matrices" (English summary). *J. Phys. A* 133:27 (1994), 4235–4245.

Carlos Beltrán, Departamento de Matemáticas, Estadística y Computación, Universidad de Cantabria, Spain (carlos.beltran@unican.es)

Anton Leykin, School of Mathematics, Georgia Tech, Atlanta, GA, USA (leykin@math.gatech.edu)

Received December 20, 2010; accepted June 21, 2011.