A deterministic algorithm to compute approximate roots of polynomial systems in polynomial average time

Pierre Lairez

A deterministic algorithm to compute approximate roots of polynomial systems in polynomial average time

Pierre Lairez

Abstract

We describe a deterministic algorithm that computes an approximate root of n complex polynomial equations in n unknowns in average polynomial time with respect to the size of the input, in the Blum-Shub-Smale model with square root. It rests upon a derandomization of an algorithm of Beltrán and Pardo and gives a deterministic affirmative answer to Smale's 17^{th} problem. The main idea is to make use of the randomness contained in the input itself.

Introduction

Shub and Smale provided an extensive theory of Newton's iteration and homotopy continuation which aims at studying the complexity of computing approximate roots of complex polynomial systems of equations with as many unknowns as equations.[1] In their theory, an *approximate root* of a polynomial system refers to a point from which Newton's iteration converges quadratically to an exact zero of the system—see Definition 1. This article answers by a deterministic algorithm the following question that they left open:

Problem (Smale[2])**.** *Can a zero of n complex polynomial equations in n unknowns be found approximately, on the average, in polynomial time with a uniform algorithm?*

The term *algorithm* refers a machine *à la* Blum-Shub-Smale[3] (BSS): a random access machine whose registers can store arbitrary real numbers, that can compute elementary arithmetic operations in the real field at unit cost and that can branch according to the sign of a given register. To avoid vain technical argumentation, I consider the BSS model extended with the possibility of computing

Technische Universität Berlin, Germany — DFG research grant BU 1371/2-2

Date. July 20, 2015.

Keywords. Polynomial system, homotopy continuation, complexity, Smale's 17th problem, derandomization.

2010 Mathematics subject classification. Primary 68Q25; Secondary 65H10, 65H20, 65Y20.

[1] Smale, "Newton's method estimates from data at one point"; Shub and Smale, "Complexity of Bézout's theorem. I. Geometric aspects", "Complexity of Bezout's theorem. II. Volumes and probabilities", "Complexity of Bezout's theorem. IV. Probability of success; extensions", "Complexity of Bezout's theorem. V. Polynomial time"; Shub, "Complexity of Bezout's theorem. VI. Geodesics in the condition (number) metric".

[2] Smale, "Mathematical problems for the next century", 17^{th} problem.

[3] Blum, Shub, and Smale, "On a theory of computation and complexity over the real numbers: NP-completeness, recursive functions and universal machines".

the square root of a positive real number at unit cost. The wording *uniform algorithm* emphasizes the requirement that a single finite machine should solve all the polynomial systems whatever the degree or the dimension. The complexity should be measured with respect to the size of the input, that is the number of real coefficients in a dense representation of the system to be solved. An important characteristic of a root of a polynomial system is its *conditioning*. Because of the feeling that approximating a root with arbitrarily large condition number requires arbitrarily many steps, the problem only asks for a complexity that is polynomial *on the average* when the input is supposed to be sampled from a certain probability distribution that we choose. The relevance of the average-case complexity is arguable, for the input distribution may not reflect actual inputs arising from applications. Though, average-case complexity sets a mark with which any other result should be compared.

The problem of solving polynomial systems is a matter of numerical analysis just as much as it is a matter of symbolic computation. Nevertheless, the reaches of these approaches differ in a fundamental way. In an exact setting, having one root of a generic polynomial system is having them all because of Galois' indeterminacy, and it turns out that the number of solutions of a generic polynomial system is the product of the degrees of the equations, Bézout's bound, and is not polynomially bounded by the number of coefficients in the input. This is why achieving a polynomial complexity is only possible in a numeric setting.

The main numerical method to solve a polynomial system f is homotopy continuation. The principle is to start from another polynomial system g of which we know a root η and to move g toward f step by step while tracking all the way to f an approximate root of the deformed system by Newton's iteration. The choice of the step size and the complexity of this procedure is well understood in terms of the condition number along the homotopy path.[4] Most of the theory so far is exposed in the book *Condition*.[5] The main difficulty is to choose the starting pair (g, η). Shub and Smale[6] showed that there exists good starting pairs but without providing a way to compute them efficiently. Beltrán and Pardo[7] discovered how to pick a starting pair at random and showed that, on average, this is a good choice. This led to a non-deterministic polynomial average-time algorithm which answers Smale's question. Bürgisser and Cucker[8] performed a smoothed analysis of the Beltrán-Pardo algorithm and described a deterministic algorithm with complexity $N^{O(\log\log N)}$, where N is the input size. The question of the existence of a deterministic algorithm with polynomial average complexity it still considered open.

This work provides, with Theorem 22, a complete deterministic answer to Smale's problem, even though, as we will see, it enriches the theory of homotopy continuation itself only marginally. The answer is based on a derandomization of the non-deterministic Beltrán and Pardo's algorithm according to two basic observations. Firstly, an approximate root of a system f is also an approximate root of a slight pertubation of f. Therefore, to compute an approximate root of f, one can only consider the most significant digits of the coefficients of f. Secondly, the remaining least significant digits, or noise, of a continuous random variable are practically independent from the most significant

[4] Beltrán and Pardo, "Fast linear homotopy to find approximate zeros of polynomial systems"; Bürgisser and Cucker, "On a problem posed by Steve Smale"; Shub, "Complexity of Bezout's theorem. VI. Geodesics in the condition (number) metric".
[5] Bürgisser and Cucker, *Condition*.
[6] Shub and Smale, "Complexity of Bezout's theorem. V. Polynomial time".
[7] Beltrán and Pardo, "Fast linear homotopy to find approximate zeros of polynomial systems", "Smale's 17th problem: average polynomial time to compute affine and projective solutions".
[8] Bürgisser and Cucker, "On a problem posed by Steve Smale".

digits and almost uniformly distributed. In the BSS model, where the input is given with infinite precision, this noise can be extracted and can be used in place of a genuine source of randomness. This answer shows that for Smale's problem, the deterministic model and the non-deterministic are essentially equivalent: randomness is part of the question from its very formulation asking for an average analysis. It is worth noting that the idea that the input is subject to noise that does not affect the result is what makes the smoothed analysis of algorithms relevant.[9] Also, the study of the resolution of a system f given only the most significant digits of f is somewhat related to recent works in the setting of machines with finite precision.[10]

The derandomization proposed here is different in nature from the derandomization theorem $\mathrm{BPP}_{\mathbb{R}} = \mathrm{P}_{\mathbb{R}}$,[11] which states that a decision problem that can be solved over the reals in polynomial time (worst-case complexity) with randomization and bounded error probability can also be solved deterministically in polynomial time. Contrary to this work, the derandomization theorem above relies on the ability of a BSS machine to hold arbitrary constants in its definition, even hardly computable ones or worse, not computable ones which may lead to unlikely statements. For example, one can decide the termination of Turing machines with a BSS machine insofar Chaitin's Ω constant is built in the machine.

Acknowledgment I am very grateful to Peter Bürgisser for his help and constant support. This work is partially funded by the research grant BU 1371/2-2 of the Deutsche Forschungsgemeinschaft.

Contents

1 The method of homotopy continuation

This part exposes the principles of Newton's iterations and homotopy continuation upon which rests Beltrán and Pardo's algorithm. It mostly contains known results and variations of known results that will be used in the next part. For Smale's problem, the affine setting and the projective setting are known to be equivalent,[12] so we only focus on the latter.

[9] Spielman and Teng, "Smoothed analysis of algorithms: why the simplex algorithm usually takes polynomial time".
[10] Briquel, Cucker, Peña, and Roshchina, "Fast computation of zeros of polynomial systems with bounded degree under finite-precision".
[11] Blum, Cucker, Shub, and Smale, *Complexity and real computation*, §17.6.
[12] Beltrán and Pardo, "Smale's 17th problem: average polynomial time to compute affine and projective solutions".

1.1 Approximate root

(Symbols in the margin mark the place where they are defined.)

Let n be a positive integer. The space $\mathbb{C}^{n+1}$ is endowed with the usual Hermitian inner product. For $d \in \mathbb{N}$, let H_d denote the vector space of homogeneous polynomials of degree d in the variables $x_0, \dots, x_n$. It is endowed with an Hermitian inner product, called *Weyl's inner product*, for which the monomial basis is an orthogonal basis and $\|x_0^{a_0} \cdots x_n^{a_n}\|^2 = \frac{a_0! \cdots a_n!}{(a_1+\cdots+a_n)!}$. Let $d_1, \dots, d_n$ be positive integers and let $\mathcal{H}$ denote $H_{d_1} \times \cdots \times H_{d_n}$, the space of all systems of homogeneous equations in $n+1$ variables and of degree $d_1, \dots, d_n$. This space is endowed with the Hermitian inner product induced by the inner product of each factor. The dimension n and the d_i's are fixed throughout this article. Let D be the maximum of all d_i's and let N denote the complex dimension of $\mathcal{H}$, namely

$\mathcal{H}$

D

N

$$N = \binom{n+d_1}{n} + \cdots + \binom{n+d_n}{n}.$$

Elements of $\mathcal{H}$ are polynomial systems to be solved, and $2N$ is the *input size*. Note that $2 \leqslant N$, $n^2 \leqslant N$ and $D \leqslant N$.

For all Hermitian space V, we endow the set $\mathbb{S}(V)$ of elements of norm 1 with the induced Riemannian metric $d_{\mathbb{S}}$: the distance between two points $x, y \in \mathbb{S}(V)$ is the angle between them, namely $\cos d_{\mathbb{S}}(x,y) = \mathrm{Re}\langle x, y\rangle$. The projective space $\mathbb{P}(V)$ is endowed with the quotient Riemannian metric $d_{\mathbb{P}}$ defined by

$$d_{\mathbb{P}}([x],[y]) \stackrel{\text{def}}{=} \min_{\lambda \in \mathbb{S}(\mathbb{C})} d_{\mathbb{S}}(x, \lambda y).$$

An element of $f \in \mathcal{H}$ is regarded as a homogeneous polynomial function $\mathbb{C}^{n+1} \to \mathbb{C}^n$. A *root*—or *solution*, or *zero*—of f is a point $\zeta \in \mathbb{P}^n$ such that $f(\zeta) = 0$. Let V be the *solution variety* $\{(f,\zeta) \in \mathcal{H} \times \mathbb{P}^n \mid f(z) = 0\}$. For $z \in \mathbb{C}^{n+1} \setminus \{0\}$, let $\mathrm{d}f(z) : \mathbb{C}^{n+1} \to \mathbb{C}^n$ denote the differential of f at z. Let $z^\perp$ be the orthogonal complement of $\mathbb{C}z$ in $\mathbb{C}^{n+1}$. If the restriction $\mathrm{d}f(z)|_{z^\perp} : z^\perp \to \mathbb{C}^n$ is invertible, we define the *projective Newton operator* $\mathcal{N}$ by

V

$\mathcal{N}(f,z)$

$$\mathcal{N}(f,z) \stackrel{\text{def}}{=} z - \mathrm{d}f(z)|_{z^\perp}^{-1}(f(z)).$$

It is clear that $\mathcal{N}(f, \lambda z) = \lambda \mathcal{N}(f,z)$, so $\mathcal{N}(f,-)$ defines a partial function $\mathbb{P}^n \to \mathbb{P}^n$.

Definition 1. A point $z \in \mathbb{P}^n$ is an *approximate root* of f if the sequence defined by $z_0 = z$ and $z_{k+1} = \mathcal{N}(f, z_k)$ is well defined and if there exists $\zeta \in \mathbb{P}^n$ such that $f(\zeta) = 0$ and $d_{\mathbb{P}}(z_k, \zeta) \leqslant 2^{1-2^k} d_{\mathbb{P}}(z, \zeta)$ for all $k \geqslant 0$. The point ζ is the *associated root* of z and we say that z *approximates* ζ *as a root of* f.

For $f \in \mathcal{H}$ and $z \in \mathbb{C}^{n+1} \setminus \{0\}$, we consider the linear map

$$\Theta(f,z) : (u_1, \dots, u_n) \in \mathbb{C}^n \mapsto \mathrm{d}f(z)|_{z^\perp}^{-1} \left(\sqrt{d_1}\|z\|^{d_1-1} u_1, \dots, \sqrt{d_n}\|z\|^{d_n-1} u_n \right) \in z^\perp$$

and the *condition number*[13] *of* f *at* z is defined to be $\mu(f,z) \stackrel{\text{def}}{=} \|f\| \, \|\Theta(f,z)\|$, where $\|\Theta(f,z)\|$ is the operator norm. When $\mathrm{d}f(z)|_{z^\perp}$ is not invertible, we set $\mu(f,z) = \infty$. For all $\lambda, \mu \in \mathbb{C}^\times$ we check that $\mu(\lambda f, \mu z) = \mu(f,z)$. The projective γ-theorem relates the condition number and the notion of approximate root:

$\mu(f,z)$

Theorem 2 (Shub, Smale[14])**.** *For any* $(f,\zeta) \in V$ *and* $z \in \mathbb{P}^n$*, if* $D^{3/2}\mu(f,\zeta) d_{\mathbb{P}}(z,\zeta) \leqslant \frac{1}{3}$*, then* z *is an approximate root of* f *with associated root* ζ*.*

[13] See Bürgisser and Cucker, *Condition*, §16, for more details about the condition number. What is denoted μ here is denoted μ_{norm} in this reference.

[14] Shub and Smale, "Complexity of Bézout's theorem. I. Geometric aspects".

Remark. The classical form of the result,[15] requires $D^{3/2}\mu(f,\zeta)\tan(d_{\mathbb{P}}(z,\zeta)) \leqslant 3-\sqrt{7}$. The hypothesis required here is stronger: since $D^{3/2}\mu(f,\zeta) \geqslant 1$, if $D^{3/2}\mu(f,\zeta)d_{\mathbb{P}}(z,\zeta) \leqslant \frac{1}{3}$ then $d_{\mathbb{P}}(z,\zeta) \leqslant \frac{1}{3}$ and then $\tan(d_{\mathbb{P}}(z,\zeta)) \leqslant 3\tan(\frac{1}{3})d_{\mathbb{P}}(z,\zeta) \leqslant \frac{3-\sqrt{7}}{D^{3/2}\mu(f,\zeta)}$ because $\tan(\frac{1}{3}) \leqslant_{\boxplus} 3-\sqrt{7}$. The symbol $\leqslant_{\boxplus}$ indicates an inequality that is easily checked using a calculator. $\leqslant_{\boxplus}$

The algorithmic use of the condition number heavily relies on this explicit Lipschitz estimate:

Proposition 3 (Shub[16])**.** *Let $0 \leqslant \varepsilon \leqslant \frac{1}{7}$. For any $f,g \in \mathbb{P}(\mathcal{H})$ and $x,y \in \mathbb{P}^n$, if*

$$\mu(f,x)\max\left(D^{1/2}d_{\mathbb{P}}(f,g), D^{3/2}d_{\mathbb{P}}(x,y)\right) \leqslant \frac{\varepsilon}{4}$$

then $(1+\varepsilon)^{-1}\mu(f,x) \leqslant \mu(g,y) \leqslant (1+\varepsilon)\mu(f,x)$.

1.2 Homotopy continuation algorithm

Let $I \subset \mathbb{R}$ be an interval containing 0 and let $t \in I \mapsto f_t \in \mathbb{P}(\mathcal{H})$ be a continuous function. Let ζ be a root of f_0 such that $\mathrm{d}f_0(\zeta)_{|\zeta^\perp}$ is invertible. There is a subinterval $J \subset I$ containing 0 and open in I, and a continuous function $t \in J \mapsto \zeta_t \in \mathbb{P}^n$ such that $\zeta_0 = \zeta$ and $f_t(\zeta_t) = 0$ for all $t \in J$. We choose J to be the largest such interval.

Lemma 4. *If $\mu(f_t,\zeta_t)$ is bounded on J, then $J = I$.*

Proof. Let M be the supremum of $\mu(f_t,\zeta_t)$ on J. From the construction of ζ_t with the implicit function theorem we see that $t \in J \mapsto \zeta_t$ is M-Lipschitz continuous. Hence the map $t \in J \mapsto \zeta_t$ extends to a continous map on $\overline{J}$. Thus J is closed in I, and $I = J$ because J is also open. □

Proposition 5. *Let $(f,\zeta) \in V$, $g \in \mathbb{P}(\mathcal{H})$ and $0 < \varepsilon \leqslant \frac{1}{7}$. If $D^{3/2}\mu(f,\zeta)^2 d_{\mathbb{P}}(f,g) \leqslant \frac{\varepsilon}{4(1+\varepsilon)}$, then*

(i) there exists a unique root η of g such that $d_{\mathbb{P}}(\zeta,\eta) \leqslant (1+\varepsilon)\mu(f,\zeta)d_{\mathbb{P}}(f,g)$;

(ii) $(1+\varepsilon)^{-1}\mu(f,\zeta) \leqslant \mu(g,\eta) \leqslant (1+\varepsilon)\mu(f,\zeta)$.

(iii) ζ approximates η as a root of g and η approximates ζ as a root of f;

Proof. Let $t \in [0,1] \mapsto f_t \in \mathbb{P}(\mathcal{H})$ be a geodesic path such that $f_0 = f$, $f_1 = g$ and $\|\dot{f}_t\| = d_{\mathbb{P}}(f,g)$. Let $t \in J \mapsto \zeta_t$ be the homotopy continuation associated to this path starting from the root ζ and defined as above on a maximal interval $J \subset [0,1]$. Let μ_t denote $\mu(f_t,\zeta_t)$.

For all $t \in J$ we know that $\|\dot{\zeta}_t\| \leqslant \mu_t\|\dot{f}_t\|$,[17] so that

$$d_{\mathbb{P}}(\zeta_0,\zeta_t) \leqslant \int_0^t \|\dot{\zeta}_u\|du \leqslant d_{\mathbb{P}}(f,g)\int_0^t \mu_u du. \tag{1}$$

Let J' be the closed subinterval of J defined by $J' = \left\{t \in J \;\middle|\; \forall t' \leqslant t, D^{3/2}\mu_0 d_{\mathbb{P}}(\zeta_0,\zeta_{t'}) \leqslant \frac{\varepsilon}{4}\right\}$. For all $t \in J'$ we have $D^{3/2}\mu_0 d_{\mathbb{P}}(\zeta_0,\zeta_t) \leqslant \frac{\varepsilon}{4}$, by definition and $D^{1/2}\mu_0 d_{\mathbb{P}}(f_0,f_t) \leqslant D^{3/2}\mu_0^2 d_{\mathbb{P}}(f,g) \leqslant \frac{\varepsilon}{4}$, by hypothesis. Thus, Proposition 3 ensures that

$$(1+\varepsilon)^{-1}\mu_0 \leqslant \mu_t \leqslant (1+\varepsilon)\mu_0, \text{ for all } t \in J'. \tag{2}$$

[15] Blum, Cucker, Shub, and Smale, *Complexity and real computation*, §14, Theorems 1 and 2.

[16] Shub, "Complexity of Bezout's theorem. VI. Geodesics in the condition (number) metric", Theorem 1; see also Bürgisser and Cucker, *Condition*, Theorem 16.2.

[17] Bürgisser and Cucker, *Condition*, Corollary 16.14 and Inequality (16.12).

Thanks to Inequality (1) we conclude that $d_{\mathbb{P}}(\zeta_0,\zeta_t) \leqslant (1+\varepsilon)t\, d_{\mathbb{P}}(f,g)\mu_0$, for all $t \in J'$, so that $D^{3/2}\mu_0 d_{\mathbb{P}}(\zeta_0,\zeta_t) \leqslant \frac{t\varepsilon}{4}$. This proves that J' is open in J. Since it is also closed, we have $J' = J$. Since μ_t is bounded on J', by Inequality (2), Lemma 4 implies that $J' = J = [0,1]$. Now, Inequalities (1) and (2) imply that $d_{\mathbb{P}}(\zeta_0,\zeta_1) \leqslant (1+\varepsilon)d_{\mathbb{P}}(f,g)\mu_0$. This proves (i) and (ii) follows from (2) for $t = 1$.

To prove that η approximates ζ as a root of f, it is enough to check that

$$D^{3/2}\mu(f,\zeta)d_{\mathbb{P}}(\zeta,\eta) \leqslant (1+\varepsilon)D^{3/2}\mu(f,\zeta)^2 d_{\mathbb{P}}(f,g) \leqslant \frac{\varepsilon}{4} \leqslant_{\text{▦}} \frac{1}{3},$$

by Theorem 2. To prove that ζ approximates η as a root of g, we check that

$$D^{3/2}\mu(g,\eta)d_{\mathbb{P}}(\zeta,\eta) \leqslant (1+\varepsilon)^2 D^{3/2}\mu(f,\zeta)^2 d_{\mathbb{P}}(f,g) \leqslant \frac{\varepsilon(1+\varepsilon)}{4} \leqslant_{\text{▦}} \frac{1}{3}.$$

This proves (iii) and the lemma. □

Throughout this article, let $\varepsilon = \frac{1}{13}$, $A = \frac{1}{52}$, $B = \frac{1}{101}$ and $B' = \frac{1}{65}$. The main result that allows to compute a homotopy continutation with discrete jumps is the following:

Lemma 6. *For any $(f,\zeta) \in V$ and $g \in \mathcal{H}$ and for any $z \in \mathbb{P}^n$, if $D^{3/2}\mu(f,z)d_{\mathbb{P}}(z,\zeta) \leqslant A$ and $D^{3/2}\mu(f,z)^2 d_{\mathbb{P}}(f,g) \leqslant B'$ then:*

(i) z is an approximate root of g with some associated root η;

(ii) $(1+\varepsilon)^{-2}\mu(f,z) \leqslant \mu(g,\eta) \leqslant (1+\varepsilon)^2\mu(f,z)$.

(iii) $D^{3/2}\mu(g,\eta)d_{\mathbb{P}}(z,\eta) \leqslant \frac{1}{23}$;

If moreover $D^{3/2}\mu(f,z)^2 d_{\mathbb{P}}(f,g) \leqslant B$ then

(iv) $D^{3/2}\mu(g,z')d_{\mathbb{P}}(z',\eta) \leqslant A$, where $z' = \mathcal{N}(g,z)$.

Proof. Firstly, we bound $\mu(f,\zeta)$. Since $D^{3/2}\mu(f,z)d_{\mathbb{P}}(z,\zeta) \leqslant A = \frac{\varepsilon}{4}$, Proposition 3 gives

$$(1+\varepsilon)^{-1}\mu(f,\zeta) \leqslant \mu(f,z) \leqslant (1+\varepsilon)\mu(f,\zeta).$$

Next, we have $D^{3/2}\mu(f,\zeta)^2 d_{\mathbb{P}}(f,g) \leqslant (1+\varepsilon)^2 B' \leqslant_{\text{▦}} \frac{\varepsilon}{4(1+\varepsilon)}$, thus Proposition 5 applies and ζ is an approximate root of g with some associated root η such that $d_{\mathbb{P}}(\zeta,\eta) \leqslant (1+\varepsilon)\mu(f,\zeta)d_{\mathbb{P}}(f,g)$ and $(1+\varepsilon)^{-1}\mu(f,\zeta) \leqslant \mu(g,\eta) \leqslant (1+\varepsilon)\mu(f,\zeta)$ and this gives (ii).

Then, we check that z approximates η as a root of g. Indeed

$$d_{\mathbb{P}}(z,\eta) \leqslant d_{\mathbb{P}}(z,\zeta) + d_{\mathbb{P}}(\zeta,\eta) \leqslant \frac{A + (1+\varepsilon)^2 B'}{D^{3/2}\mu(f,z)} \leqslant \frac{(1+\varepsilon)^2(A + (1+\varepsilon)^2 B')}{D^{3/2}\mu(g,\eta)}.$$

And $(1+\varepsilon)^2(A + (1+\varepsilon)^2 B') \leqslant_{\text{▦}} \frac{1}{23} < \frac{1}{3}$, so Theorem 2 applies and we obtain (i) and (iii).

We assume now that $D^{3/2}\mu(f,z)^2 d_{\mathbb{P}}(f,g) \leqslant B$. All the inequalities above are valid with B' replaced by B. By definition of an approximate root $d_{\mathbb{P}}(z',\eta) \leqslant \frac{1}{2}d_{\mathbb{P}}(z,\eta)$, so that

$$D^{3/2}\mu(g,\eta)d_{\mathbb{P}}(z',\eta) \leqslant \frac{1}{2}(1+\varepsilon)^2(A + (1+\varepsilon)^2 B) \leqslant_{\text{▦}} \frac{\varepsilon}{4}.$$

Thus $(1+\varepsilon)^{-1}\mu(g,\eta) \leqslant \mu(g,z') \leqslant (1+\varepsilon)\mu(g,\eta)$.

To conclude, we have $D^{3/2}\mu(g,z')d(z',\eta) \leqslant \frac{1}{2}(1+\varepsilon)^3(A + (1+\varepsilon)^2 B) \leqslant_{\text{▦}} A$. □

Algorithm 1. Homotopy continuation

Input. $f, g \in \mathbb{S}(\mathcal{H})$ and $z \in \mathbb{P}^n$.

Precondition. There exists a root η of g such that $52\, D^{3/2}\mu(g,z)d_{\mathbb{P}}(z,\eta) \leqslant 1$.

Output. $w \in \mathbb{P}^n$

Postcondition. w is an approximate root of f.

function HC(f, g, z)
  $t \leftarrow 1/\left(101D^{3/2}\mu(g,z)^2 d_{\mathbb{S}}(f,g)\right)$
  while $1 > t$ **do**
    $h \leftarrow \Gamma(g,f,t)$
    $z \leftarrow \mathcal{N}(h,z)$
    $t \leftarrow t + 1/\left(101D^{3/2}\mu(h,z)^2 d_{\mathbb{S}}(f,g)\right)$
  end while
  return z
end function

Let $f,g \in \mathbb{S}(\mathcal{H})$, with $f \neq -g$. Let $t \in [0,1] \mapsto \Gamma(g,f,t)$ be the geodesic path from g to f in $\mathbb{S}(\mathcal{H})$. The condition $f \neq -g$ guarantees that the geodesic path is uniquely determined. Namely

$$\Gamma(g,f,t) = \frac{\sin\left((1-t)\alpha\right)}{\sin(\alpha)}g + \frac{\sin(t\alpha)}{\sin(\alpha)}f, \tag{3}$$

where $\alpha = d_{\mathbb{S}}(f,g) \in [0,\pi[$ is the angle between f and g.

Let $z \in \mathbb{P}^n$ such that $D^{3/2}\mu(g,z)d_{\mathbb{P}}(z,\eta) \leqslant A$, for some root η of g. By Lemma 6(i), applied with $g = f$ and $\eta = \zeta$, the point z is an approximate root of g, with associated root η. Given g and z, we can compute an approximate root of f in the following way. Let $g_0 = g$, $t_0 = 0$ and by induction on k we define

$$\mu_k = \mu(g_k,z_k),\ t_{k+1} = t_k + \frac{B}{D^{3/2}\mu_k^2 d_{\mathbb{S}}(f,g)},\ g_{k+1} = \Gamma(g,f,t_{k+1}) \text{ and } z_{k+1} = \mathcal{N}(g_{k+1},z_k).$$

Let $K(f,g,z)$, or simply K, be the least integer such that $t_{K+1} > 1$, if any, and $K(f,g,z) = \infty$ otherwise. Let $\tilde{M}(f,g,z)$ denote the maximum of all μ_k with $0 \leqslant k \leqslant K$. Let HC be the procedure that takes as input f, g and z and outputs z_K. Algorithm 1 recapitulates the definition. It terminates if and only if $K < \infty$, in which case K is the number of iterations. For simplicity, we assume that we can compute exactly the square root function, the trigonometric functions and the operator norm required for the computation of $\mu(f,z)$. Section §2.5 shows how to implement things in the BSS model extended with the square root only.

$K(f,g,z)$
$\tilde{M}(f,g,z)$
$\mathrm{HC}(f,g,z)$

Let $h_t = \Gamma(f,g,t)$ and let $t \in J \mapsto \zeta_t$ be the homotopy continuation associated to $t \in [0,1] \mapsto h_t$, where η_0 is the associated root of z, defined on a maximal subinterval $J \subset [0,1]$. Let

$$M(f,g,z) \stackrel{\text{def}}{=} \max_{t\in J}\mu(f_t,\zeta_t) \quad \text{and} \quad I_p(f,g,z) \stackrel{\text{def}}{=} \int_J \mu(h_t,\eta_t)^p \mathrm{d}t.$$

$I_p(f,g,z)$,
$M(f,g,z)$

The behavior of the procedure HC can be controlled in terms of the integrals $I_p(f,g,z)$. It is one of the corner stone of the complexity theory of hotopy continuation methods. The following estimation of the maximum of the condition number, along a homotopy path, in terms of the third moment of the condition number seems to be original. It will be important for the average complexity analysis.

Proposition 7. *If $J = [0,1]$ then $M(f,g,z) \leqslant 151\, D^{3/2} I_3(f,g,z)$.*

Proof. Let $\varepsilon = \frac{1}{7}$ and let $s \in [0,1]$ such that $\mu(f_s,\zeta_s)$ is maximal. For all $t \in [0,1]$, $d_{\mathbb{S}}(f_s,f_t) \leqslant |t-s| d_{\mathbb{S}}(f,g)$. Thus, if

$$|t-s| \leqslant \frac{\varepsilon}{4(1+\varepsilon)D^{3/2}\mu(f_s,\zeta_s)^2 d_{\mathbb{S}}(f,g)}, \tag{4}$$

then $\mu(f_t,\zeta_t) \geqslant (1+\varepsilon)^{-1}\mu(f_s,\zeta_s)$, by Proposition 5. Since $d_{\mathbb{S}}(f,g) \leqslant \pi$, the diameter of the interval H of all $t \in [0,1]$ satisfying Inequality (4) is at least $\frac{\varepsilon}{4\pi(1+\varepsilon)D^{3/2}\mu(f_s,\zeta_s)^2}$. Thus

$$\int_0^1 \mu(f_t,\zeta_t)^3 \mathrm{d}t \geqslant \int_H \frac{\mu(f_s,\zeta_s)^3}{(1+\varepsilon)^3}\mathrm{d}t \geqslant \frac{\varepsilon\,\mu(f_s,\zeta_s)}{4\pi(1+\varepsilon)^4 D^{3/2}} \geqslant \frac{1}{151}\frac{\mu(f_s,\zeta_s)}{D^{3/2}}. \qquad \square$$

Theorem 8 (Shub[18])**.** *With the notations above, if $D^{3/2}\mu(g,z)d_{\mathbb{P}}(z,\eta) \leqslant A$ then:*

(i) $\mathrm{HC}(f,g,z)$ *terminates if and only if $I_2(f,g,z)$ is finite, in which case $J = [0,1]$;*

If moreover $\mathrm{HC}(f,g,z)$ *terminates then:*

(ii) $(1+\varepsilon)^{-2}M(f,g,z) \leqslant \tilde{M}(f,g,z) \leqslant (1+\varepsilon)^2 M(f,g,z)$.

(iii) $K(f,g,z) \leqslant 136\, D^{3/2} d_{\mathbb{S}}(f,g) I_2(f,g,z)$;

(iv) $\mathrm{HC}(f,g,z)$ *is an approximate root of f;*

(v) $D^{3/2}\mu(f,\zeta)d_{\mathbb{P}}(\mathrm{HC}(f,g,z),\zeta) \leqslant \frac{1}{23}$, *where ζ is the associated root of* $\mathrm{HC}(f,g,z)$.

Proof. Let η_k denote ζ_{t_k}. Since $D^{3/2}\mu_k^2 d_{\mathbb{P}}(g_k,g_{k+1}) \leqslant B$ for all $k \geqslant 0$, Lemma 6(iv) proves, by induction on k that $D^{3/2}\mu_k d_{\mathbb{P}}(z_k,\eta_k) \leqslant A$ for any $k \geqslant 0$

Assume that $[0,t_k] \subset J$ for some $k \geqslant 0$ and let $t \in [t_k,t_{k+1}] \cap J$ so that

$$D^{3/2}\mu_k^2 d(g_k,h_t) \leqslant D^{3/2}\mu_k^2 d(g_k,g_{k+1}) \leqslant B.$$

Moreover $D^{3/2}\mu_k d(z_k,\eta_k) \leqslant A$, so Lemma 6(ii) applies to (g_k,η_k), h_t and z_k and asserts that

$$(1+\varepsilon)^{-2}\mu_k \leqslant \mu(h_t,\zeta_t) \leqslant (1+\varepsilon)^2\mu_k. \tag{5}$$

By definition $\mu_k^2(t_{k+1}-t_k) = \frac{B}{D^{3/2}d_{\mathbb{S}}(f,g)}$, so integrating over t leads to

$$\int_0^{t_k} \mu(h_t,\zeta_t)^2 \mathrm{d}t \geqslant (1+\varepsilon)^{-4}\sum_{j=0}^{k-1}\mu_j^2(t_{j+1}-t_j) = \frac{kB}{(1+\varepsilon)^4 D^{3/2} d_{\mathbb{S}}(f,g)}, \tag{6}$$

$$\text{and} \quad \int_0^{\sup J} \mu(h_t,\zeta_t)^2 \leqslant (1+\varepsilon)^4 \sum_{j=0}^{k}\mu_j^2(t_{j+1}-t_j) = \frac{(1+\varepsilon)^4(k+1)B}{D^{3/2}d_{\mathbb{S}}(f,g)}. \tag{7}$$

Assume now that $I_2(f,g,z)$ is finite. The left-hand side of Inequality (6) is finite so there exists a k such that $t_{k+1} \notin J$. But then Inequalities (5) shows that μ_t is bounded on J which implies, Lemma 4 that $J = [0,1]$. And since $t_{k+1} \notin J$, this proves that K is finite.

Conversely, assume that K is finite, *i.e.* $\mathrm{HC}(f,g,z)$ terminates. Then there exists a maximal k such that $[0,t_k] \subset J$ and thus for all $t \in J$

$$\mu(h_t,\zeta_t) \leqslant (1+\varepsilon)^2 \max_{j\leqslant k}\mu(g_k,z_k).$$

[18] Shub, "Complexity of Bezout's theorem. VI. Geodesics in the condition (number) metric".

So $\mu(h_t,\zeta_t)$ is bounded on J, which implies that $J = [0,1]$, and thus $k = K$. Inequality (6) then shows that $I_2(f,g,z)$ is finite, which concludes the proof of (i). We keep assuming that K is finite. Inequality (5) shows (ii). Since $[0,t_K] \subset [0,1]$, by definition, Inequalities (6) and (7) shows that

$$\frac{1}{B(1+\varepsilon)^4} D^{3/2} d_{\mathbb{S}}(f,g) I_2(f,g,z) - 1 \leqslant K \leqslant \frac{(1+\varepsilon)^4}{B} D^{3/2} d_{\mathbb{S}}(f,g) I_2(f,g,z).$$

We check that $\frac{(1+\varepsilon)^4}{B} \leqslant_{\blacksquare} 136$, which gives (iii). Finally, Lemmas 6(i) and 6(iii) show that z_K approximates ζ_1 as a root of f and that $D^{3/2}\mu(f,\zeta_1) d_{\mathbb{P}}(z_K,\zeta_1) \leqslant \frac{1}{23}$, which gives (iv) and (v). □

1.3 Beltrán-Pardo randomization and average complexity analysis

An important discovery of Beltrán and Pardo is a procedure to pick a random system and one of its root simultaneously without actually solving any polynomial system. And from the complexity point of view, it turns out that a random pair $(g,\eta) \in V$ is a good starting point to perform the homotopy continuation. Let $g \in \mathbb{S}(\mathcal{H})$ be a uniform random variable, where the uniform measure is relative to the Riemannian metric on $\mathbb{S}(\mathcal{H})$. Almost surely g has finitely many roots in $\mathbb{P}^n$. Let η be one of them, randomly chosen with the uniform distribution. The probability distribution of the random variable $(g,\eta) \in V$ is denoted ρ_{std}. ρ_{std}

Let us assume that $f = (f_1,\dots,f_n) \in \mathbb{S}(\mathcal{H})$ is a uniform random variable and write f as

$$f_i = c_i x_0^{d_i} + \sqrt{d_i} x_0^{d_i-1} \sum_{j=1}^{n} a_{i,j} x_i + f_i'(x_0,\dots,x_n),$$

for some $c_i, a_{i,j} \in \mathbb{C}$ and $f_i' \in H_{d_i}$. Let $f' = (f_1',\dots,f_n') \in \mathcal{H}$. It lies in the subspace $R \subset \mathcal{H}$ of all h such that $h(e_0) = 0$ and $\mathrm{d}h(e_0) = 0$. Let

$$M = \begin{pmatrix} a_{1,1} & \cdots & a_{1,n} & c_1 \\ \vdots & \ddots & \vdots & \vdots \\ a_{n,1} & \cdots & a_{n,n} & c_n \end{pmatrix} \in \mathbb{C}^{n\times(n+1)}.$$

$M/\|M\|$ and $f'/\|f'\|$ are independent uniform random variables in $\mathbb{S}(\mathbb{C}^{n\times(n+1)})$ and $\mathbb{S}(R)$ respectively and $\|f\|^2 = \|M\|^2 + \|f'\|^2$. Almost surely, $\ker M$ has dimension 1. Let $\zeta \in \mathbb{S}(\mathbb{C}^{n+1})$ be the unique element of $\ker M \cap \mathbb{S}(\mathbb{C}^{n+1})$ whose first non-zero coordinate is a real positive number. Let $h = (h_1,\dots,h_n) \in \mathcal{H}$ be defined by

$$h_i = \sqrt{d_i} \left(\sum_{i=0}^{n} x_i \overline{\zeta_i} \right)^{d_i-1} \sum_{j=0}^{n} m_{i,j} x_j.$$

By construction $h(\zeta) = 0$. Let $u \in U(n+1)$, the unitary group of $\mathbb{C}^{n+1}$, such that $u(e_0) = \zeta$. The choice of u is arbitrary but should depend only on ζ. For example, we can choose u, for almost all ζ, to be the unique element of $U(n+1)$ with determinant 1 that is the identity on the orthogonal complement of $\{e_0,\zeta\}$ and that sends e_0 to ζ. Finally, let $g = f' \circ u^{-1} + h \in \mathcal{H}$. By construction $g(\zeta) = 0$ and we may check that $\|g\| = 1$. We define $\mathrm{BP}(f) = (g,\zeta)$ which is a point in the solution variety V. $\mathrm{BP}(f)$

Theorem 9 (Beltrán, Pardo[19]). *If $f \in \mathbb{S}(\mathcal{H})$ is a uniform random variable, then $\mathrm{BP}(f) \sim \rho_{std}$.*

[19] Beltrán and Pardo, "Fast linear homotopy to find approximate zeros of polynomial systems", §2.3; Bürgisser and Cucker,

Given $f \in \mathbb{S}(\mathcal{H})$, Beltrán and Pardo's algorithm proceeds in sampling a system $g \in \mathbb{S}(\mathcal{H})$ from the uniform distribution and then computing $\mathrm{HC}(f, \mathrm{BP}(g))$. If the input f is a uniform random variable then we can evaluate the expected number of homotopy steps $\mathbb{E}(K(f, \mathrm{BP}(g)))$. Indeed, let η be root of g, uniformly chosen, the theorem above asserts that $\mathrm{BP}(g)$ has the same probability distribution as (g, η) so $\mathbb{E}(K(f, \mathrm{BP}(g))) = \mathbb{E}(K(f, g, \eta))$. Thanks to Theorem 8(iii), it is not difficult to see that $\mathbb{E}(K(f, g, \eta)) \leqslant 214\, D^{3/2}\mathbb{E}(\mu(g, \eta)^2)$. This is why the estimation of $\mathbb{E}(\mu(g, \eta)^2)$ is another corner stone of the average complexity analysis of homotopy methods. Deriving from a identity of Beltrán and Pardo, we obtain the following:

Theorem 10. *If $(g, \eta) \sim \rho$, then $\mathbb{E}(\mu(g, \eta)^p) \leqslant \frac{3}{4-p}(nN)^{p/2}$ for any $2 \leqslant p < 4$.*

Proof. Let $s = p/2 - 1$. Beltrán and Pardo[20] state that

$$\mathbb{E}(\mu(g, \eta)^{2+2s}) = \frac{\Gamma(N+1)}{\Gamma(N-s)} \sum_{k=1}^{n} \binom{n+1}{k+1} \frac{\Gamma(k-s)}{\Gamma(k)} n^{-k+s}.$$

We use the inequality $x^{-y}\Gamma(x) \leqslant \Gamma(x-y) \leqslant (x-1)^{-y}\Gamma(x)$, for $x \in [1, \infty)$ and $y \in (-1, 1)$, which comes from the log-convexity of Γ. In particular

$$\Gamma(N+1)/\Gamma(N-s) \leqslant N^{1+s} \quad \text{and} \quad \Gamma(k-s) \leqslant (k-1)^{-s}\Gamma(k).$$

Thus

$$\mathbb{E}(\mu(g, \eta)^{2+2s}) \leqslant N^{1+s}\left(\binom{n+1}{2}\frac{\Gamma(1-s)}{\Gamma(1)} n^{s-1} + \sum_{k=2}^{n} \binom{n+1}{k+1}(k-1)^{-s} n^{-k+s}\right)$$

On the one hand $(1-s)\Gamma(1-s) = \Gamma(2-s) \leqslant \Gamma(2) = \Gamma(1)$, so

$$\binom{n+1}{2}\frac{\Gamma(1-s)}{\Gamma(1)} n^{s-1} \leqslant \frac{(n+1)n}{2}\frac{1}{1-s} n^{s-1} \leqslant \frac{n^{1+s}}{1-s}.$$

On the other hand,

$$\begin{aligned}
\sum_{k=2}^{n} \binom{n+1}{k+1}(k-1)^{-s} n^{-k+s} &\leqslant n^{1+s} \sum_{k=3}^{n+1} \binom{n+1}{k} n^{-k} \\
&= n^{1+s}\left(\left(1 + \frac{1}{n}\right)^{n+1} - 1 - \frac{n+1}{n} - \frac{1}{n^2}\binom{n+1}{2}\right) \\
&\leqslant_{\blacksquare} \frac{n^{1+s}}{4} \leqslant \frac{n^{1+s}}{4(1-s)}.
\end{aligned}$$

Putting together all above, we obtain the claim. □

2 Derandomization of the Beltrán-Pardo algorithm

2.1 Duplication of the uniform distribution on the sphere

An important argument of the construction is the ability to produce approximations of two independent uniform random variables in $\mathbb{S}^{2N-1}$ from a single uniform random variable in $\mathbb{S}^{2N-1}$ given with infinite precision. More precisely, let Q be a positive integer. This section is dedicated to the

Condition, Chap. 17.

[20] Beltrán and Pardo, "Fast linear homotopy to find approximate zeros of polynomial systems", Theorem 23.

contruction of two functions $\lfloor - \rfloor_Q$ and $\{-\}_Q$ from the sphere $\mathbb{S}^{2N-1}$ to itself, respectively called the *truncation* and the *fractional part* of x at precision Q, such that $\lfloor x \rfloor_Q$ is close to x and such that if $x \in \mathbb{S}^{2N-1}$ is uniformly distributed then $\{x\}_Q$ is *nearly* uniformly distributed in $\mathbb{S}^{2N-1}$ and *nearly* independent from $\lfloor x \rfloor_Q$ in the following sense:

Lemma 11. *For any $x \in \mathbb{S}^{2N-1}$, $d_{\mathbb{S}}\left(\lfloor x \rfloor_Q, x\right) \leqslant (2N)^{1/2}/Q$. Moreover, for any continuous non-negative function $\Theta : \mathbb{S}^{2N-1} \times \mathbb{S}^{2N-1} \to \mathbb{R}$,*

$$\frac{1}{|\mathbb{S}^{2N-1}|} \int_{\mathbb{S}^{2N-1}} \Theta\left(\lfloor x \rfloor_Q, \{x\}_Q\right) \mathrm{d}x \leqslant \frac{\exp\left(\frac{2N^{3/2}}{Q}\right)}{|\mathbb{S}^{2N-1}|^2} \int_{\mathbb{S}^{2N-1}} \int_{\mathbb{S}^{2N-1}} \Theta\left(\lfloor x \rfloor_Q, y\right) \mathrm{d}x\mathrm{d}y.$$

For $x \in \mathbb{R}$, let $A(x)$ denote the integral part of a and let $A_Q(a) = Q^{-1}A(Qa)$ be the truncation at precision Q. For $x \in \mathbb{R}^{2N-1}$, let $A_Q(x) \in \mathbb{R}^{2N-1}$ be the vector $(A_Q(x_1), \ldots, A_Q(x_{2N-1}))$ and let $B_Q(x) = Q(x - A_Q(x))$, it is a vector in $[0,1]^{2N-1}$. We note that $\|A_Q(x) - x\|^2 \leqslant (2N-1)/Q^2$, because the difference is bounded componentwise by $1/Q$.

Let C denote $[-1,1)^{2N-1}$ and C_+ denote $[0,1)^{2N-1}$ and let $F(x) = (1 + \|x\|^2)^{-N}$. We first show that if $x \in C$ is a random variable with probability density function F (divided by the appropriate normalization constant) then $B_Q(x)$ is *nearly* uniformly distributed in C_+ and *nearly* independent from $A_Q(x)$.

Lemma 12. *For any continuous non-negative function $\Theta : [-1,1]^{2N-1} \times [0,1]^{2N-1} \to \mathbb{R}$,*

$$\int_C \Theta\left(A_Q(x), B_Q(x)\right) F(x)\mathrm{d}x \leqslant \exp\left(\tfrac{2N^{3/2}}{Q}\right) \int_{C_+} \int_C \Theta\left(A_Q(x), y\right) F(x)\mathrm{d}x\mathrm{d}y.$$

Proof. For any integers $-Q \leqslant k_i < Q$, for $1 \leqslant i \leqslant 2N-1$, the function A_Q is constant on the set $\prod_{i=1}^{2N-1} \left[\frac{k_i}{Q}, \frac{k_i+1}{Q}\right)$, and these sets form a partition of X. Let $U_1, \ldots, U_{(2Q)^{2N-1}}$ denote an enumeration of these sets and let a_k denote the unique value of A_Q on U_k. The diameter of U_k is $\sqrt{2N-1}/Q$. Since the function $x \in [0,\infty) \mapsto -N\log(1+x^2)$ is N-Lipschitz continuous, we derive that

$$\max_{U_k} F \leqslant e^{N\sqrt{2N-1}/Q} \min_{U_k} F. \tag{8}$$

For any $1 \leqslant k \leqslant (2Q)^{2N-1}$ we have

$$\int_{U_k} \Theta\left(A_Q(x), B_Q(x)\right) F(x)\mathrm{d}x \leqslant \max_{U_k} F \int_{U_k} \Theta\left(a_k, Q(x-a_k)\right) \mathrm{d}x,$$

because $A_Q(x) = a_k$ on U_k and by definition of $B_Q(x)$. A simple change of variable shows that

$$\int_{U_k} \Theta\left(b_k, Q(x-b_k)\right) \mathrm{d}x = |U_k| \int_{C_+} \Theta(b_k, y)\mathrm{d}y,$$

where $|U_k|$ is the volume of U_k, namely Q^{-2N+1}. Besides,

$$\Theta(b_k, y) \leqslant \frac{1}{|U_k| \min_{U_k} F} \int_{U_k} \Theta\left(A_Q(x), y\right) F(x)\mathrm{d}x.$$

Putting together all above and summing over k gives the claim. □

Thanks to a method due to Sibuya, we may transform a uniform random variable of C_+ into a uniform random variable in $\mathbb{S}^{2N-1}$. Let $x = (x_1, \ldots, x_{2N-1}) \in C_+$, let $u_1, \ldots, u_{N-1}$ be $x_{N+1}, \ldots, x_{2N-1}$

arranged in ascending order, and let $u_0 = 0$ and $u_N = 1$. Let $S(x) \in \mathbb{R}^{2N}$ denote the vector such that for any $1 \leqslant i \leqslant N$

$$S(x)_{2i-1} = \sqrt{u_i - u_{i-1}}\cos(2\pi x_i) \quad \text{and} \quad S(x)_{2i} = \sqrt{u_i - u_{i-1}}\sin(2\pi x_i). \tag{9}$$

Proposition 13 (Sibuya[21]). *If x a uniformly distributed random variable in C_+, then $S(x)$ is uniformly distributed in $\mathbb{S}^{2N-1}$.*

We now define $\lfloor - \rfloor_Q$ and $\{-\}_Q$. Let $\Sigma \in \mathbb{R}^{2N}$ be the set of all $x \in \mathbb{R}^{2N}$ such that $\|x\|_\infty = 1$. This hypersurface is divided into $4N$ faces that are isometric to C: they are the sets $\Sigma_i^\varepsilon = \{x \in \Sigma \mid x_i = \varepsilon\}$, for $\varepsilon \in \{-1, 1\}$ and $1 \leqslant i \leqslant 2N$ and the isometry is given by the map

$$t_{i,\varepsilon} : \Sigma_i^\varepsilon \to C, \quad x \mapsto (x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n).$$

Through these isometries, we define the functions A'_Q and B'_Q on Σ in the following way: for $x \in \Sigma_i^\varepsilon$ we set $A'_Q(x) = t_{i,\varepsilon}^{-1}(A_Q(t_{i,\varepsilon}(x))) \in \Sigma_i^\varepsilon$ and $B'_Q(x) = B_Q(t_{i,\varepsilon}(x)) \in C_+$. Let $\nu_\infty : x \in \mathbb{S}^{2N-1} \mapsto x/\|x\|_\infty \in \Sigma$ and its inverse $\nu_2 : x \in \Sigma \mapsto x/\|x\| \in \mathbb{S}^{2N-1}$. Finally, we define, for $x \in \mathbb{S}^{2N-1}$ $\lfloor x \rfloor_Q$, $\{x\}_Q$

$$\lfloor x \rfloor_Q \stackrel{\text{def}}{=} \nu_2\left(A'_Q(\nu_\infty(x))\right) \quad \text{and} \quad \{x\}_Q \stackrel{\text{def}}{=} S\left(B'_Q(\nu_\infty(x))\right). \tag{10}$$

We may now prove Lemma 11.

Proof of Lemma 11. Let $x \in \mathbb{S}^{2N-1}$. It is well-known that $d_{\mathbb{S}}(\lfloor x \rfloor_Q, x) \leqslant \frac{\pi}{2}\|\lfloor x \rfloor_Q - x\|$. Furthermore the map ν_2 is clearly 1-Lipschitz continuous so $\|\lfloor x \rfloor_Q - x\| \leqslant \|A'_Q(\nu_\infty(x)) - \nu_\infty(x)\|$ and we already remarked that this is at most $\sqrt{2N-1}/Q$.

Concerning the second claim, we consider partition of the sphere by the sets $\nu_2(\Sigma_i^\varepsilon)$. The determinant of the Jacobian of the differentiable map $t_{i,\varepsilon} \circ \nu_\infty : \nu_2(\Sigma_i^\varepsilon) \to C$ at $\nu_2(t_{i,\varepsilon}^{-1}(x))$, for some $x \in C$, is precisely $F(x)$. Thus

$$\int_{\nu_2(\Sigma_i^\varepsilon)} \Theta\left(\lfloor u \rfloor_Q, \{u\}_Q\right) \mathrm{d}u = \int_C \Theta\left(\nu_2\left(t_{i,\varepsilon}^{-1}(A_Q(x))\right), S(B_Q(x))\right) F(x)\mathrm{d}x,$$

and then Lemma 12 implies

$$\leqslant \exp\left(\tfrac{2N^{3/2}}{Q}\right) \int_C \int_{C_+} \Theta\left(\nu_2\left(t_{i,\varepsilon}^{-1}(A_Q(x))\right), S(y)\right) \mathrm{d}y\, F(x)\mathrm{d}x$$

and Proposition 13 gives the equality

$$= \frac{\exp\left(\frac{2N^{3/2}}{Q}\right)}{|\mathbb{S}^{2N-1}|} \int_C \int_{\mathbb{S}^{2N-1}} \Theta\left(\nu_2\left(t_{i,\varepsilon}^{-1}(A_Q(x))\right), y\right) \mathrm{d}y\, F(x)\mathrm{d}x,$$

and applying the inverse change of variable $\nu_2 \circ t_{i,\varepsilon}^{-1}$ gives the claim. □

The orthogonal monomial basis of $\mathcal{H}$ gives an identification $\mathcal{H} \simeq \mathbb{R}^{2N}$ and we define this way the truncation $\lfloor f \rfloor_Q$ and the fractional part $\{f\}_Q$ of a polynomial system $f \in \mathbb{S}(\mathcal{H})$. The derandomization relies on finding a approximate root of $\lfloor f \rfloor_Q$, for some Q large enough, and using $\{f\}_Q$ as the source of randomness for the Beltrán-Pardo procedure. Namely, we compute $\mathrm{HC}(\lfloor f \rfloor_Q, \mathrm{BP}(\{f\}_Q))$. Almost surely, this computation produces an approximate root of $\lfloor f \rfloor_Q$. If Q is large enough, it is also an approximate root of f. The main technical difficulty is to choose a precision and to ensure that the result is correct while keeping the complexity under control.

[21] Sibuya, "A method for generating uniformly distributed points on N-dimensional spheres".

2.2 Homotopy continuation with precision check

Let f, f', $g \in \mathbb{S}(\mathcal{H})$ and let $\eta \in \mathbb{P}^n$ be a root of g. Throughout this section, we assume that $d_{\mathbb{S}}(f,f') \leqslant \rho$, for some $\rho > 0$, that $I_2(f,g,\zeta) < \infty$ and that $d_{\mathbb{S}}(f,g) \leqslant \pi/2$. Up to changing g into $-g$, the latter is always true, since $d_{\mathbb{S}}(f,-g) = \pi - d_{\mathbb{S}}(f,g)$. The notations I_2, M and $\tilde{M}$ used in this section have been introduced in §1.2. If ρ is small enough, then $\mathrm{HC}(f',g,\eta)$ is an approximate root not only of f' but also of f. But if ρ fails to be small enough, $\mathrm{HC}(f',g,\eta)$ may not even terminate or, to say the least, $\mathrm{HC}(f',g,\eta)$ may take arbitrarily long to compute something that is not an approximate root of f. To control the complexity of the new algorithm, it is important to be able to recognize this situation at least as fast as $\mathrm{HC}(f,g,\eta)$ would terminate.

As in §1.2, let $f_t = \Gamma(g,f,t)$ and $f'_t = \Gamma(g,f',t)$. Let $t \in [0,1] \to \zeta_t \in \mathbb{P}^n$ be the homotopy continuation associated to f_t, on $[0,1]$, and $t \in J \to \zeta'_t \in \mathbb{P}^n$ be the one associated to f'_t, defined on some maximal interval $0 \in J \subset [0,1]$. Let $\mu_t = \mu(f_t,\zeta_t)$ and $\mu'_t = \mu(f'_t,\zeta'_t)$.

Lemma 14. *$d_{\mathbb{S}}(f_t,f'_t) \leqslant 2d_{\mathbb{S}}(f,f')$ for any $t \in [0,1]$.*

Proof. Let $\alpha_t = d_{\mathbb{S}}(f_t,f'_t)$, $\beta = d_{\mathbb{S}}(f,g) \leqslant \pi/2$ and $\gamma = d_{\mathbb{S}}(f',g)$. Without loss of generality we may assume that $\beta \leqslant \gamma$. The spherical law of cosines applied to the spherical triangle $\{g,f_t,f'_t\}$ gives the equality

$$\cos\alpha_t = \cos(t\beta)\cos(t\gamma) + \sin(t\beta)\sin(t\gamma)\cos A,$$

where A is the angle at g of the spherical triangle $\{f,f',g\}$. Thus

$$\frac{\mathrm{d}\cos\alpha_t}{\mathrm{d}t} = -\frac{1}{2}(1+\cos A)(\gamma-\beta)\sin(t\gamma-t\beta) - \frac{1}{2}(1-\cos A)(\beta+\gamma)\sin(t\beta+t\gamma).$$

If $\gamma \leqslant \pi/2$, then $t\beta + t\gamma \leqslant \pi$ and thus $\frac{\mathrm{d}\cos\alpha_t}{\mathrm{d}t} \leqslant 0$, so in that case $\alpha_t \leqslant \alpha_1$ for all $t \in [0,1]$. In the general case, let h be the the unique point on the spherical segment $[f',g]$ such that $d_{\mathbb{S}}(g,h) = \beta$. Since f', g and h lie on the same geodesic path $d_{\mathbb{S}}(\Gamma(g,h,t),f'_t) = td_{\mathbb{S}}(f',h)$. Moreover $d_{\mathbb{S}}(f,h) \leqslant \alpha_1$. Since $d_{\mathbb{S}}(g,h) \leqslant \pi/2$, the argument above shows that $d_{\mathbb{S}}(f_t,\Gamma(g,h,t)) \leqslant d_{\mathbb{S}}(g,h)$. In the end, we obtain

$$\begin{aligned} d_{\mathbb{S}}(f_t,f'_t) &\leqslant d_{\mathbb{S}}(f_t,\Gamma(g,h,t)) + d_{\mathbb{S}}(\Gamma(g,h,t),f'_t) \\ &\leqslant \alpha_1 + td_{\mathbb{S}}(f',h) \leqslant 2d_{\mathbb{S}}(f,f'). \end{aligned}$$

□

Lemma 15. *If $D^{3/2}M(f,g,\zeta)^2\rho \leqslant \frac{1}{112}$ then for any $t \in [0,1]$:*

(i) $(1+\varepsilon)^{-1}\mu'_t \leqslant \mu_t \leqslant (1+\varepsilon)\mu'_t$;

(ii) $D^{3/2}\mu_t d_{\mathbb{P}}(\zeta_t,\zeta'_t) \leqslant \frac{1}{51}$.

Proof. Let S the set of all $t \in [0,1]$ such that $D^{3/2}\mu_t d_{\mathbb{P}}(\zeta_t,\zeta'_t) \leqslant \frac{1}{51}$. It is a non empty closed subset of I. Let $t \in S$. By Lemma 14, we have $d_{\mathbb{P}}(f_t,f'_t) \leqslant 2\rho$, so

$$D^{3/2}\mu_t^2 d_{\mathbb{P}}(f_t,f'_t) \leqslant \frac{2}{112} = \frac{\varepsilon}{4(1+\varepsilon)}.$$

Proposition 5 implies that there exists a root η of f'_t such that $d_{\mathbb{P}}(\eta,\zeta_t) \leqslant 2(1+\varepsilon)\mu_t\rho$ and $(1+\varepsilon)^{-1}\mu_t \leqslant \mu(f'_t,\eta) \leqslant (1+\varepsilon)\mu_t$. Because $d(\eta,\zeta'_t) \leqslant d(\eta,\zeta_t) + d(\zeta_t,\zeta'_t)$ and $t \in S$ we obtain

$$D^{3/2}\mu(f'_t,\eta)d(\eta,\zeta'_t) \leqslant D^{3/2}(1+\varepsilon)\mu_t\left(2(1+\varepsilon)\mu_t\rho + \frac{1}{51D^{3/2}\mu_t}\right) \leqslant (1+\varepsilon)^2\frac{2}{112} + (1+\varepsilon)\frac{1}{51} \leqslant_{\blacksquare} \frac{1}{3}.$$

Algorithm 2. Homotopy continuation with precision check

Input. $f, g \in \mathbb{S}(\mathcal{H})$, $z \in \mathbb{P}^n$ and $\rho > 0$.

Output. $w \in \mathbb{P}^n$ or FAIL.

Specifications. See Proposition 16.

function HC′(f, g, z, ρ)
  $t \leftarrow 1/\left(101D^{3/2}\mu(g,z)^2 d_{\mathbb{S}}(f,g)\right)$
  $h \leftarrow g$
  while $1 > t$ and $D^{3/2}\mu(h,z)^2\rho \leqslant \frac{1}{151}$ **do**
    $h \leftarrow \Gamma(g,f,t)$
    $z \leftarrow \mathcal{N}(h,z)$
    $t \leftarrow t + 1/\left(101D^{3/2}\mu(h,z)^2 d_{\mathbb{S}}(f,g)\right)$
  end while
  if $D^{3/2}\mu(h,z)^2\rho > \frac{1}{151}$ **then**
    return FAIL
  else
    return z
  end if
end function

and Theorem 2 implies that ζ_t' approximates η as a root of f_t'. Since it is also an exact root of f_t', this implies $\zeta_t' = \eta$. In particular $D^{3/2}\mu_t d_{\mathbb{P}}(\zeta_t', \zeta_t) \leqslant 2(1+\varepsilon)D^{3/2}\mu_t^2\rho <_{\blacksquare} \frac{1}{51}$. Thus t is in the interior of S, which proves that S is open and finally that $S = [0,1]$. □

This leads to the procedure HC′, see Algorithm 2. It modifies procedure HC, Algorithm 1, in only one respect: each iteration checks up on the failure condition $D^{3/2}\mu(h,z)^2\rho > \frac{1}{151}$. If the failure condition is never met, then HC′ computes exactly the same thing as HC.

Proposition 16. *If $d_{\mathbb{S}}(f,g) \leqslant \pi/2$ and $d(f,f') \leqslant \rho$, then the procedure* HC′(f',g,η,ρ)*:*

(i) terminates and performs at most $158\, D^{3/2} d_{\mathbb{S}}(f,g) I_2(f,g,\eta) + 2$ *steps;*

(ii) outputs an approximate root of f, or fails ;

(iii) succeeds if and only if $D^{3/2}\tilde{M}(f',g,\eta)^2\rho \leqslant \frac{1}{151}$;

(iv) succeeds if $D^{3/2}M(f,g,\eta)^2\rho \leqslant \frac{1}{235}$.

Proof. At each iteration, the value of t increases by at most $151\rho/(101 d_{\mathbb{S}}(f',g))$, thus there are at most $101 d_{\mathbb{S}}(f',g)/(151\rho)$ iterations before termination.

By construction, the procedure HC′(f',g,η,ρ) fails if and only if at some point of the procedure HC(f',g,η,ρ) it happens that $D^{3/2}\mu(h,z)^2\rho > \frac{1}{151}$. In other words, the procedure HC′(f',g,η,ρ) fails if and only if $D^{3/2}\tilde{M}(f',g,\eta)^2\rho \leqslant \frac{1}{151}$, by definition of $\tilde{M}$. And since the procedure terminates, it succeeds if and only if it does not fail. This proves (iii).

Let us bound the number $K'(f',g,\eta,\rho)$ of iterations of the procedure HC′(f',g,η,ρ) before termination. If HC′(f',g,η,ρ) succeeds, then $K'(f',g,\eta,\rho) = K(f',g,\eta)$. Furthermore

$$K'(f',g,\eta,\rho) = \sup\left\{K(f_s',g,\eta) \mid s \in [0,1],\ \text{HC}'(f_s',g,\eta,\rho) \text{ succeeds}\right\}. \tag{11}$$

Let $s \in [0,1]$ such that $\mathrm{HC}'(f'_s, g, \eta, \rho)$ succeeds, that is to say $D^{3/2}\tilde{M}(f'_s, g, \eta)^2\rho \leqslant \frac{1}{151}$. We note that $\frac{1}{151} \leqslant \frac{1}{112(1+\varepsilon)^4}$. Theorem 8(ii) shows that

$$(1+\varepsilon)^{-2}M(f'_s, g, \eta) \leqslant \tilde{M}(f'_s, g, \eta) \leqslant (1+\varepsilon)^2 M(f'_s, g, \eta).$$

In particular $D^{3/2}M(f'_s, g, \zeta)^2\rho \leqslant \frac{1}{112}$ and Lemma 15 shows that $\mu_t \leqslant (1+\varepsilon)\mu_t$ for all $t \leqslant s$. In particular $I_2(f'_s, g, \eta) \leqslant (1+\varepsilon)^2 I_2(f_s, g, \eta)$.

$$\begin{aligned}
K(f'_s, g, \eta) &\leqslant 136\, D^{3/2} d_{\mathbb{S}}(f'_s, g) I_2(f'_s, g, \eta) && \text{by Theorem 8(iii)}\\
&\leqslant 136(1+\varepsilon)^2 D^{3/2}\left(d_{\mathbb{S}}(f_s, g) + 2\rho\right) I_2(f_s, g, \eta) && \text{by Lemma 14}\\
&\leqslant 158 D^{3/2} d_{\mathbb{S}}(f_s, g) I_2(f_s, g, \eta) + 2 && \text{using } I_2(f_s, g, \eta) \leqslant M(f_s, g, \eta)^2\\
&\leqslant 158 D^{3/2} d_{\mathbb{S}}(f, g) I_2(f, g, \eta) + 2.
\end{aligned}$$

Together with Equation (11), this completes the proof of (i).

Let us assume that the procedure $\mathrm{HC}'(f', g, \eta, \rho)$ succeeds and let z be its output, which is nothing but $\mathrm{HC}(f', g, \eta)$. Theorem 8(v) shows that $D^{3/2}\mu'_1 d_{\mathbb{P}}(z, \zeta'_1) \leqslant \frac{1}{23}$. As above, with $s = 1$, we check that $\mu_1 \leqslant (1+\varepsilon)\mu'_1$ and $D^{3/2}\mu'_1 d_{\mathbb{P}}(\zeta_1, \zeta'_1) \leqslant \frac{1}{51}$ using Lemma 15. Thus

$$D^{3/2}\mu_1 d_{\mathbb{P}}(z, \zeta_1) \leqslant (1+\varepsilon)\left(\frac{1}{23} + \frac{1}{51}\right) < \frac{1}{3}.$$

Then z approximates ζ_1 as a root of f_1, by Theorem 2. This proves (ii).

Lastly, let us assume that $D^{3/2}M(f, g, \eta)^2\rho \leqslant \frac{1}{235} \leqslant \frac{1}{112(1+\varepsilon)^{10}}$. Lemma 15 implies that $M(f, g, \eta) \geqslant (1+\varepsilon)^{-1}M(f', g, \eta)$ and Theorem 8(ii) shows that $M(f', g, \eta) \leqslant (1+\varepsilon)^{-2}\tilde{M}(f', g, \eta)$. Thus

$$D^{3/2}\tilde{M}(f', g, \eta)^2\rho \leqslant (1+\varepsilon)^6 D^{3/2} M(f, g, \eta)^2\rho \leqslant \frac{1}{112(1+\varepsilon)^4} \leqslant_{\blacksquare} \frac{1}{151}$$

and $\mathrm{HC}'(f', g, \eta, \rho)$ succeeds. This proves (iv). □

2.3 A deterministic algorithm

Let $f \in \mathbb{S}(\mathcal{H})$ be the input system to be solved and let $Q \geqslant 1$ be a given precision. We compute

$$f' = \lfloor f \rfloor_Q,\ (g, \eta) = \mathrm{BP}(\{f\}_Q),\ \varepsilon = \mathrm{sign}(\pi/2 - d_{\mathbb{S}}(f, g)) \text{ and } \rho = (2N)^{1/2}/Q.$$

Lemma 14 shows that $d_{\mathbb{S}}(f, f') \leqslant \rho$. Then we run the homotopy continuation procedure with precision check $\mathrm{HC}'(f', \varepsilon g, \eta, \rho)$, which may fail or output a point $z \in \mathbb{P}^n$. If it does succeed, then Proposition 16 ensures that z is an approximate root of f. If the homotopy continuation fails, then we replace Q by Q^2 and we start again, until the call to HC′ succeeds. This leads to the deterministic procedure DBP, Algorithm 3. If the computation of $\mathrm{DBP}(f)$ terminates then the result is an approximate root of f. Section 2.4 studies the average number of homotopy steps performed by $\mathrm{DBP}(f)$ while Section 2.5 studies the average total cost of an implementation of DBP in the BSS model extended with the square root.

2.4 Average analysis

Let $f \in \mathbb{S}(\mathcal{H})$ be the input system, a uniform random variable, and we consider a run of the procedure $\mathrm{DBP}(f)$. Let Q_k be the precision at the k^{th} iteration, namely $Q_k = N^{2^k}$. We set also

$$f_k = \lfloor f \rfloor_{Q_k},\ (g_k, \eta_k) = \mathrm{BP}(\{f\}_{Q_k}),\ \varepsilon_k = \mathrm{sign}(\pi/2 - d_{\mathbb{S}}(f, g_k)) \text{ and } \rho_k = (2N)^{1/2}/Q_k.$$

Q_k

$f_k, g_k, \eta_k, \varepsilon_k, \rho_k$

Algorithm 3. Deterministic variant of Beltrán-Pardo algorithm

Input. $f \in \mathcal{H}$

Output. $z \in \mathbb{P}^n$

Postcondition. z is an approximate root of f

function DBP(f)
  $Q \leftarrow N$
  repeat
    $Q \leftarrow Q^2$
    $f' \leftarrow \lfloor f \rfloor_Q$
    $(g, \eta) \leftarrow \mathrm{BP}(\{f\}_Q)$
    $\varepsilon \leftarrow \mathrm{sign}(\mathrm{Re}\langle f, g\rangle)$ ▷ $\varepsilon = \mathrm{sign}(d_{\mathbb{S}}(f,g) - \pi/2)$
    $\rho \leftarrow (2N)^{1/2}/Q$
    $z \leftarrow \mathrm{HC}'(f', \varepsilon g, \eta, \rho)$
  until HC′ succeeds
  return z
end function

Let Ω be the least k such that the homotopy continuation with precision check $\mathrm{HC}'(f_k, \varepsilon_k g_k, \eta_k, \rho_k)$ succeeds. Note that Ω is a random variable. Let $(g, \eta) \in V$ be a random variable with distribution ρ_{std} and independent of f and let ε be the sign of $\pi/2 - d_{\mathbb{S}}(f, g_k)$. Ω g, η, ε

Lemma 17. *Let $\Theta : \mathcal{H} \times V \to \mathbb{R}$ be any non-negative measurable function. For any $k \geqslant 1$,*

$$\mathbb{E}\left(\Theta(f_k, g_k, \eta_k)\right) \leqslant 5\mathbb{E}\left(\Theta(f_k, g, \eta)\right).$$

Proof. It is an application of Lemma 11:

$$\begin{aligned}
\mathbb{E}\left(\Theta(f_k, g_k, \eta_k)\right) &= \frac{1}{|\mathbb{S}(\mathcal{H})|} \int_{\mathbb{S}(\mathcal{H})} \Theta\left(\lfloor f \rfloor_{Q_k}, \mathrm{BP}(\{f\}_{Q_k})\right) \mathrm{d}f \\
&\leqslant \frac{\exp\left(\frac{2N^{3/2}}{Q_k}\right)}{|\mathbb{S}(\mathcal{H})|^2} \int_{\mathbb{S}(\mathcal{H}) \times \mathbb{S}(\mathcal{H})} \Theta\left(\lfloor f \rfloor_{Q_k}, \mathrm{BP}(g)\right) \mathrm{d}f \mathrm{d}g \\
&= \frac{\exp\left(\frac{2N^{3/2}}{Q_k}\right)}{|\mathbb{S}(\mathcal{H})|} \int_{\mathcal{H}} \int_V \Theta\left(\lfloor f \rfloor_{Q_k}, g, \eta\right) \mathrm{d}f \mathrm{d}\rho_{\mathrm{std}}(g, \eta) \\
&= \exp\left(\tfrac{2N^{3/2}}{Q_k}\right) \mathbb{E}\left(\Theta(f_k, g, \eta)\right),
\end{aligned}$$

where the second last equality comes from Theorem 9. Since $Q_k \geqslant N^2$ and $e^{\sqrt{2}} \leqslant 5$, this gives the lemma. □

Lemma 18. $\mathbb{E}(I_p(f, \varepsilon g, \zeta)) = \mathbb{E}(\mu(g, \eta)^p)$ *for any $p \geqslant 1$.*

Proof. Let $h_t = \Gamma(\varepsilon g, f, t)$, for $t \in [0,1]$, and let ζ_t be the associated homotopy continuation. Let $\tau \in [0,1]$ be a uniform random variable independent from f and (g, η). Clearly $\mathbb{E}(I_p(f, \varepsilon g, \zeta)) = \mathbb{E}(\mu(h_\tau, \zeta_\tau)^p)$, so it is enough to prove that $(h_\tau, \zeta_\tau) \sim \rho_{\mathrm{std}}$. The systems f and g are independent and uniformly distributed on $\mathbb{S}(\mathcal{H})$. So their probability distributions is invariant under any unitary transformation of $\mathcal{H}$. Then so is the probability distribution of h_t for any $t \in [0,1]$, and

there is a unique such probability distribution: the uniform distribution on $\mathbb{S}(\mathcal{H})$. The homotopy continuation makes a bijection between the roots of g and those of h_t. Since η is uniformly chosen among the roots of g, so is ζ_t among the roots of h_t. That is, $(h_t, \zeta_t) \sim \rho_{\mathrm{std}}$ for all $t \in [0,1]$, and then $(h_\tau, \zeta_\tau) \sim \rho_{\mathrm{std}}$. □

Lemma 19. $\mathbb{P}(\Omega > k) \leqslant 10^5\, D^{9/4} n^{3/2} N^{7/4} Q_k^{-1/2}$.

Proof. The probability that $\Omega > k$ is no more than the probability that $\mathrm{HC}'(f_k, g_k, \eta_k, \rho_k)$ fails. By Lemma 17, $\mathbb{P}\left(\mathrm{HC}'(f_k, \varepsilon_k g_k, \eta_k, \rho_k) \text{ fails}\right) \leqslant 5\mathbb{P}\left(\mathrm{HC}'(f_k, \varepsilon g, \eta, \rho_k) \text{ fails}\right)$. Given that $d_{\mathbb{S}}(f, f_k) \leqslant \rho_k$,

$$\begin{aligned}
\mathbb{P}\left(\mathrm{HC}'(f_k, \varepsilon g, \eta, \rho_k) \text{ fails}\right) &\leqslant \mathbb{P}\left(D^{3/2} M(f, \varepsilon g, \eta)^2 \rho_k \geqslant \frac{1}{235}\right) && \text{by Proposition 16(iv)} \\
&\leqslant \mathbb{P}\left(D^{9/2} I_3(f, \varepsilon g, \eta)^2 \rho_k \geqslant \frac{1}{235 \cdot 151^2}\right) && \text{by Proposition 7} \\
&\leqslant 151\sqrt{235}\, D^{9/4} \rho_k^{1/2}\, \mathbb{E}\left(I_3(f, \varepsilon g, \eta)\right) && \text{by Markov's inequality.}
\end{aligned}$$

Lemma 18 and Theorem 10 imply then

$$\mathbb{E}\left(I_3(f, \varepsilon g, \eta)\right) \leqslant \mathbb{E}\left(\mu(g, \eta)^3\right) \leqslant 3(nN)^{3/2}.$$

All in all, and since $\rho_k = (2N)^{1/2}/Q_k$,

$$\mathbb{P}(\Omega > k) \leqslant 5 \cdot 151\sqrt{235}\, D^{9/4} \cdot 2^{1/4} N^{1/4} Q_k^{-1/2} \cdot 3n^{3/2} N^{3/2} \leqslant_{\blacksquare} 10^5\, D^{9/4} n^{3/2} N^{7/4} Q_k^{-1/2} \qquad \square$$

Lemma 20. *For $p = \log N/(\log N - 1)$ and for any sequence $(X_k)_{k \geqslant 1}$ of non-negative random variables*

$$\mathbb{E}\Big(\sum_{k=1}^{\Omega} X_k\Big) \leqslant 7 \max_{k \geqslant 1} \mathbb{E}(X_k^p)^{1/p}.$$

In particular, $\mathbb{E}(\Omega) \leqslant 7$.

Proof. We first write the expectation as

$$\mathbb{E}\Big(\sum_{k=1}^{\Omega} X_k\Big) = \sum_{k=1}^{\infty} \mathbb{E}(X_k \mathbb{1}_{\Omega \geqslant k}).$$

Let $q = 1/\log N$, so that $\frac{1}{p} + \frac{1}{q} = 1$. From Hölder's inequality

$$\mathbb{E}(X_k \mathbb{1}_{\Omega \geqslant k}) \leqslant \mathbb{E}(X_k^p)^{1/p} \mathbb{P}(\Omega \geqslant k)^{1/q}$$

By Lemma 19

$$\mathbb{P}(\Omega \geqslant k)^{1/q} \leqslant \left(10^5\, D^{9/4} n^{3/2} N^{7/4} N^{-2^{k-2}}\right)^{\frac{1}{\log N}} = \left(10^5\, D^{9/4} n^{3/2} N^{7/4}\right)^{\frac{1}{\log N}} e^{-2^{k-2}}.$$

Since $D^{9/4} n^{3/2} N^{7/4} \leqslant N^5$, we have $\left(10^5\, D^{9/4} n^{3/2} N^{7/4}\right)^{\frac{1}{\log N}} \leqslant 10^{5/\log N} e^5 \leqslant_{\blacksquare} 10^9$. Besides the probability $\mathbb{P}(\Omega \geqslant k)$ is at most one. Thus, for any integer $A \geqslant 1$,

$$\mathbb{E}\Big(\sum_{k=1}^{\Omega} X_k\Big) \leqslant \left(\max_{k \geqslant 1} \mathbb{E}(X_k^p)^{1/p}\right)\left(A - 1 + 10^9 \sum_{k \geqslant A} \exp(-2^{k-2})\right).$$

Since $\left\{2^{k-2} \;\middle|\; k \geqslant A\right\} \subset \left\{k2^{A-2} \;\middle|\; k \geqslant 1\right\}$,

$$\sum_{k \geqslant A} \exp(-2^{k-2}) \leqslant \sum_{k \geqslant 1} \exp(-2^{A-2}k) = \frac{\exp(-2^{A-2})}{1 - \exp(-2^{A-2})}.$$

With $A = 6$, we compute that

$$A - 1 + 10^9 \frac{\exp(-2^{A-2})}{1 - \exp(-2^{A-2})} \leqslant_{\blacksquare} 7,$$

and this concludes the proof. □

Let $K(f)$ be the total number of homotopy steps performed by procedure DBP(f) and let the number of homotopy steps performed by procedure HC$'(f_k, \varepsilon_k g_k, \eta_k, \rho_k)$ be denoted by $K'(f_k, \varepsilon_k g_k, \eta_k, \rho_k)$, so that $K(f)$

$$K(f) = \sum_{k=1}^{\Omega} K'(f_k, \varepsilon_k g_k, \eta_k, \rho_k),$$

Theorem 21. *If $N \geqslant 21$ then $\mathbb{E}(K(f)) \leqslant 10^4\, nD^{3/2}N$.*

Proof. Let $p = \log N/(\log N - 1)$. If $N \geqslant 21$ then $2p \leqslant 3$. By Lemma 17 and Proposition 16(i),

$$\mathbb{E}\left(K'(f_k, \varepsilon_k g_k, \eta_k, \rho_k)^p\right)^{1/p} \leqslant 5\mathbb{E}\left(\left(158\, D^{3/2} d_{\mathbb{S}}(f, \varepsilon g) I_2(f, \varepsilon g, \eta) + 2\right)^p\right)^{1/p},$$

and because $d_{\mathbb{S}}(f, \varepsilon g) \leqslant \frac{\pi}{2}$ and by Minkowski's inequality, we obtain

$$\leqslant 5\left(79\, D^{3/2}\pi \mathbb{E}\left(I_2(f, \varepsilon g, \eta)^p\right)^{1/p} + 2\right).$$

Jensen's inequality implies that $I_2(f, \varepsilon g, \eta)^p \leqslant I_{2p}(f, \varepsilon g, \eta)$. Then $\mathbb{E}\left(I_{2p}(f, \varepsilon g, \eta)\right) \leqslant (nN)^p$, by Lemma 18 and Theorem 10. In the end,

$$\mathbb{E}\left(K'(f_k, \varepsilon_k g_k, \eta_k, \rho_k)^p\right)^{1/p} \leqslant_{\blacksquare} 1251\, nD^{3/2}N.$$

Lemma 20 applies to the expectation of the sum $K(f)$ and gives the result, with $7 \cdot 1251 \leqslant_{\blacksquare} 10^4$. □

2.5 Implementation in the BSS model with square root

Algorithms HC′ and DBP (Algorithms 2 and 3 respectively) have been described assuming the possibility to compute exactly certain non rational functions: the square root, the trigonometric functions cos and sin and the operator norm of a linear map. A BSS machine can only approximate them, but it can do it efficiently. I propose here an implementation in the BSS model extended with the ability of computing the square root of a positive real number at unit cost. We could reduce further to the plain BSS model at the cost of some lengthy and nearly irrelevant technical argumentation. We now prove the main result of this article:

Theorem 22. *There exists a BSS machine A with square root and a constant $c > 0$ such that for any positive integer n and any positive integers $d_1, \ldots, d_n$:*

(i) $A(f)$ computes an approximate root of f for almost all $f \in \mathcal{H}$;

(ii) if $f \in \mathbb{S}(\mathcal{H})$ is a uniform random variable, then the average number of operations performed by $A(f)$ is at most $cn^2D^{3/2}N(N + n^3)$.

Firstly, we describe an implementation of Algorithms HC′ and DBP in the extended BSS model. The first difficulty is the condition number $\mu(f,z)$: it rests upon the operator norm for the Euclidean distance which is not computable with rational operations. While there are efficient numerical algorithms to compute such an operator norm in practice, it is not so easy to give an algorithm that approximates it in good complexity in the BSS model. [22] The simplest workaround is to replace the operator norm $\|A\|$, for $A \in \mathbb{C}^{n\times n}$ by the Frobenius norm $\|A\|_F = \left(\sum_{ij} |a_{ij}|^2\right)^{1/2}$, which satisfies $n^{-1/2}\|A\|_F \leqslant \|A\|_2 \leqslant \|A\|_F$. Instead of computing $\mu(f,z)$, we compute

$$\mu_F(f,z) \stackrel{\text{def}}{=} \|f\|\|\Theta(f,z)\|_F,$$

with the notations of §1.1, which we can do in the exended BSS model. The factor $n^{-1/2}$ is responsible for a extra factor n in the estimated number of homotopy steps, and thus in the overall complexity.

The second difficulty lies in the use of the trigonometric functions sin and cos. They first appear in the definition of the geodesic path Γ, Equation (3), which is used in Algorithm 2. In the case where $d_{\mathbb{S}}(f,g) \leqslant \pi/2$, it is good enough to replace $\Gamma(g,f,\delta)$ by

$$\frac{\delta f + (1-\delta)g}{\|\delta f + (1-\delta)g\|}.$$

This is classical and implies modifications in the constants only.[23] The trigonometric functions also appear in Sibuya's function S, see Equation (9).

Lemma 23. *There is a BSS machine with square root that computes, for any N and any $x \in [0,1]^{2N-1}$, a point $\tilde{S}(x) \in \mathbb{S}^{2N-1}$ such that*

$$\int_{[0,1]^{2N-1}} \Theta(\tilde{S}(x))\mathrm{d}x \leqslant \frac{2}{|\mathbb{S}^{2N-1}|}\int_{\mathbb{S}^{2N-1}} \Theta(y)\mathrm{d}y,$$

with $O(N\log N)$ operations.

Sketch of the proof. For any positive integer Q, let $F_Q(x)$ be the Taylor series expansion, truncated at x^Q, of the entire function $(\exp(2i\pi x)-1)/(x-1)$. It is a polynomial of degree Q that can be computed $O(Q)$ operations, assuming that that π is a constant of the machine, by using the linear recurrence $(n+2)u_{n+2} = (2i\pi + n + 2)u_{n+1} + 2i\pi u_n$ satisfied by the coefficients of F_Q. Let $\mathrm{Cos}_Q(x)$ and $\mathrm{Sin}_Q(x)$ be the real and imaginary parts of $(1+(x-1)F_Q(x))/|(1+(x-1)F_Q(x))|$ respectively.

The function $x \in [0,1] \to (\mathrm{Cos}_Q(x), \mathrm{Sin}_Q(x))$ gives a parametrization of the circle $\mathbb{S}^1$ whose Jacobian is almost constant: we can check that there is a constant $C > 0$ such that

$$\left|\mathrm{Cos}'_Q(x)^2 + \mathrm{Sin}'_Q(x)^2 - 2\pi\right| \leqslant Ce^{-Q}.$$

Thus for any continuous function $\theta : \mathbb{S}^1 \to \mathbb{R}$

$$\int_0^1 \theta(\mathrm{Cos}_Q(x), \mathrm{Sin}_Q(x))\mathrm{d}x \leqslant \frac{1+Ce^{-Q}}{2\pi}\int_{\mathbb{S}^1}\theta(y)\mathrm{d}y.$$

Let $\tilde{S}$ be the function $[0,1]^{2N-1} \to \mathbb{S}^{2N-1}$ defined in the same way as S, Equation (9), but with Cos_Q and Sin_Q in place of sin and cos repectively, with some $Q \sim \log N$ such that $(1+Ce^{-Q})^N \leqslant 2$. It is easy to check that $\tilde{S}$ satisfies the desired properties. □

[22] See for example Armentano, Beltrán, Bürgisser, Cucker, and Shub, *A stable, polynomial-time algorithm for the eigenpair problem* or Armentano and Cucker, "A randomized homotopy for the Hermitian eigenpair problem"; unfortunately the Gaussian distribution that they assume does not fit the situation here.

[23] See for example Bürgisser and Cucker, *Condition*, §17.1.

In Algorithm DBP, there is no harm in using $\tilde{S}$ in place of S. We obtain this way variants of Algorithms HC′ and DBP that fit in the BSS model with square root. It only remains to evaluate the overall number of operations. Concerning the computational cost of Newton's iteration $\mathcal{N}(f,z)$, it is clear that this can be done in $O(nN)$ operation for the computation of $\mathrm{d}f(z)$ and $f(z)$ and $O(n^3)$ operations more for the computation of $\mathrm{d}f(z)|_{z^\perp}^{-1}(f(z))$. It is also well known that this can be significantly improved, as a consequence of a theorem of Baur and Strassen.[24] It applies to the computation of $\mu_F(f,z)$ too.

Lemma 24. *There exists a BSS machine that compute $\mu_F(f,z)^2$ and $\mathcal{N}(f,z)$, for any $f \in \mathcal{H}$ and $z \in \mathbb{P}^n$, in $O(N+n^3)$ operations.*

The expected total number of homotopy steps is $O(n^2D^{3/2}N)$. The extra factor n, in comparison with Theorem 21, comes from the use of μ_F instead of μ. Each homotopy step costs $O(N+n^3)$, by Lemma 24. The k^{th} iteration in Algorithm DBP performs $O(N\log Q_k)$ operations, excluding the call to HC′: it is dominated by the computation of $\mathrm{BP}(\lfloor f\rfloor_Q)$. Naturally, the integral part $\lfloor x\rfloor$ of a real number x is not a rational function of x but it can be computed in the BSS model in $O(\log(1+|x|))$ operations using the recursive formula, say for $x \geqslant 0$,

$$\lfloor x\rfloor = \begin{cases} 0 & \text{if } x < 1 \\ 2\lfloor x/2\rfloor & \text{if } x < 2\lfloor x/2\rfloor + 1 \\ 2\lfloor x/2\rfloor + 1 & \text{else.} \end{cases}$$

Therefore, for $f \in \mathbb{S}(\mathcal{H})$, one can compute $\lfloor f\rfloor_Q$ in $O(N\log Q)$ operations. From $\lfloor f\rfloor_Q$, one computes $\{f\}_Q$ in $O(N\log N)$ operations, by Lemma 23, using $\tilde{S}$ in place of S. Finally, one computes $\mathrm{BP}(\{f\}_Q)$ in $O(N^2)$ operations. Thus, the overall expected cost of the algorithm is

$$O\left(n^2D^{3/2}N(N+n^3) + \mathbb{E}\Big(\sum_{k=0}^{\Omega} N^2 + N\log Q_k\Big)\right).$$

Lemma 25. $\mathbb{E}\left(\sum_{k=1}^{\Omega}\log Q_k\right) = O(\log N)$

Proof. Because $Q_k = N^{2^k}$,

$$\mathbb{E}\Big(\sum_{k=1}^{\Omega}\log Q_k\Big) = \sum_{k=1}^{\infty}\log Q_k\,\mathbb{P}(\Omega \geqslant k) = \log N\sum_{k=1}^{\infty}2^k\,\mathbb{P}(\Omega\geqslant k).$$

We proceed in the same fashion as for Lemma 20 and split the sum at $A=5$, so that $5 < 2^{A-2}$. Lemma 19 and the inequality $D^{9/4}n^{3/2}N^{7/4} \leqslant N^5$ imply

$$\sum_{k=1}^{\infty}2^k\,\mathbb{P}(\Omega\geqslant k) \leqslant 2^A + 10^5N^5\sum_{k=A}^{\infty}2^k\,N^{-2^{k-2}} = 2^A + O\left(N^{5-2^{A-2}}\right) = O(1). \qquad \square$$

This concludes the proof of Theorem 22.

[24] Baur and Strassen, "The complexity of partial derivatives".

References

Diego Armentano, Carlos Beltrán, Peter Bürgisser, Felipe Cucker, and Michael Shub. *A stable, polynomial-time algorithm for the eigenpair problem.* 2015. arXiv: 1505.03290.

Diego Armentano and Felipe Cucker. "A randomized homotopy for the Hermitian eigenpair problem". In: *Found. Comput. Math.* 15.1 (2015), pp. 281–312.

Walter Baur and Volker Strassen. "The complexity of partial derivatives". In: *Theoretical Computer Science* 22.3 (1983), pp. 317–330.

Carlos Beltrán and Luis Miguel Pardo. "Fast linear homotopy to find approximate zeros of polynomial systems". In: *Found. Comput. Math.* 11.1 (2011), pp. 95–129.

– "Smale's 17th problem: average polynomial time to compute affine and projective solutions". In: *J. Amer. Math. Soc.* 22.2 (2009), pp. 363–385.

Lenore Blum, Felipe Cucker, Michael Shub, and Steve Smale. *Complexity and real computation.* Springer-Verlag, New York, 1998.

Lenore Blum, Michael Shub, and Steve Smale. "On a theory of computation and complexity over the real numbers: NP-completeness, recursive functions and universal machines". In: *Bull. Amer. Math. Soc. (N.S.)* 21.1 (1989), pp. 1–46.

Irénée Briquel, Felipe Cucker, Javier Peña, and Vera Roshchina. "Fast computation of zeros of polynomial systems with bounded degree under finite-precision". In: *Math. Comp.* 83.287 (2014), pp. 1279–1317.

Peter Bürgisser and Felipe Cucker. *Condition.* Vol. 349. Grundlehren der Mathematischen Wissenschaften. The geometry of numerical algorithms. Springer, Heidelberg, 2013.

– "On a problem posed by Steve Smale". In: *Ann. of Math. (2)* 174.3 (2011), pp. 1785–1836.

Michael Shub. "Complexity of Bezout's theorem. VI. Geodesics in the condition (number) metric". In: *Found. Comput. Math.* 9.2 (2009), pp. 171–178.

Michael Shub and Steve Smale. "Complexity of Bézout's theorem. I. Geometric aspects". In: *J. Amer. Math. Soc.* 6.2 (1993), pp. 459–501.

– "Complexity of Bezout's theorem. II. Volumes and probabilities". In: *Computational algebraic geometry (Nice, 1992).* Vol. 109. Progr. Math. Birkhäuser Boston, Boston, MA, 1993, pp. 267–285.

– "Complexity of Bezout's theorem. IV. Probability of success; extensions". In: *SIAM J. Numer. Anal.* 33.1 (1996), pp. 128–148.

– "Complexity of Bezout's theorem. V. Polynomial time". In: *Theoret. Comput. Sci.* 133.1 (1994). Selected papers of the Workshop on Continuous Algorithms and Complexity (Barcelona, 1993), pp. 141–164.

Masaaki Sibuya. "A method for generating uniformly distributed points on N-dimensional spheres". In: *Ann. Inst. Statist. Math.* 14 (1962), pp. 81–85.

Steve Smale. "Mathematical problems for the next century". English. In: *The Mathematical Intelligencer* 20.2 (1998), pp. 7–15.

Steve 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)*. Springer, New York, 1986, pp. 185–196.

Daniel Spielman and Shang-Hua Teng. “Smoothed analysis of algorithms: why the simplex algorithm usually takes polynomial time”. In: *Proceedings of the Thirty-Third Annual ACM Symposium on Theory of Computing*. ACM, New York, 2001, 296–305 (electronic).

Technische Universität Berlin
Institut für Mathematik
Sekretariat MA 3-2
Straße des 17. Juni 136
10623 Berlin
Deutschland

E-mail address: pierre@lairez.fr
URL: pierre.lairez.fr