A deterministic solution to Smale's 17th problem

Algorithms and complexity in algebraic geometry

Simons Institute, Berkeley, December 16, 2015

Pierre Lairez
TU Berlin

Smale 17th problem

> "Can a zero of n complex polynomial equations in n unknowns be found approximately, on the average, in polynomial time with a uniform algorithm?"
>
> *(S. Smale, 1998)*

Approximate root
: A point from which Newton's iteration converges quadratically.

Average polynomial time
: Polynomial w. r. t. input size, on average w. r. t. a reasonable input distribution, typically Gaussian.

Uniform algorithm
: A BSS machine: unit cost arithmetic operations on exact real numbers.

Symbolic vs. numeric

Symbolic
: Knowing one root is knowing them all; the number of root is overpolynomial.

Numeric
: Homotopy methods allow to approximate one root, disregarding the others.
$\rightsquigarrow$ a polynomial complexity is not ruled out.

Typically

- n equations of degree 2 with n unknowns.
- Input size: $N = n\binom{n+2}{2} \sim \frac{1}{2}n^3$.
- Number of roots: $\mathcal{D} = 2^n$, this is overpolynomial in N.

Symbolic vs. numeric

Symbolic

Knowing one root is knowing them all; the number of root is overpolynomial.

Numeric

Homotopy methods allow to approximate one root, disregarding the others.
$\rightsquigarrow$ a polynomial complexity is not ruled out.

Typically

- n equations of degree n with n unknowns.
- Input size: $N = n\binom{2n}{n} \sim Cn^{1/2}4^n$.
- Number of roots: $\mathcal{D} = n^n$, this is overpolynomial in N.

Notations

- n and D, positive integers.
- $\mathcal{H}$, the linear space of all systems of n equations of degree D with n unknowns ; also functions $\mathbb{C}^n \to \mathbb{C}^n$.
- N, the complex dimension of $\mathcal{H}$.

- $\mathcal{H}$ is endowed with a hermitian inner product.
- $\mathbb{S}(\mathcal{H})$, the systems with unit norm.

The homotopy method

Input

$f \in \mathcal{H}$, a system to solve.

Starting point

Choose another $g \in \mathcal{H}$ of which we know a root $\zeta \in \mathbb{C}^n$.

Homotopy

$$
\begin{aligned}
h_0 &= g & h_{k+1} &= h_k + \delta_k \cdot (f - g) \\
z_0 &= \zeta & z_{k+1} &= z_k - (\mathrm{d}_{z_k} h_{k+1})^{-1}(h_{k+1}(z_k)).
\end{aligned}
$$

End point

If $h_K = f$, then z_K is an approximate root of f.

- How to choose the step size δ_k?
- How to choose the starting pair (g, ζ)?

The complexity of the homotopy method

Shub, Smale, 90's

Shub and Smale:

- Gave a method to choose the δ_k in terms of a condition number $\mu(f, z)$;
- For each n and D, proved the existence of a starting point (g, ζ) from which the homotopy method is efficient on the average.
- Gave a bound on the number of iteration in the homotopy method:

$$\text{number of iterations} \leqslant cD^{3/2} \int_g^f \mu(h, \eta)^2 \mathrm{d}h.$$

Random starting points

Beltrán, Pardo, 2009

Beltrán and Pardo:

- Proved that a random starting point (g, ζ) is efficient on the (twofold) average.
- Discovered how to pick a random pair (g, ζ).

For us, Beltrán-Pardo algorithm is a function

$$\mathrm{BP} : \mathbb{S}(\mathcal{H}) \times [0,1]^{\mathbb{N}} \to \mathbb{C}^n$$

such that

- $\mathrm{BP}(f, a)$ is an approximate root of f, for almost all f and a;
- if f and a are uniformly distributed, then $\mathbb{E}(\mathrm{cost}_{\mathrm{BP}}(f, a)) = \mathcal{O}(nD^{3/2}N^2)$.

Smoothed analysis
Bürgisser, Cucker, 2011

Bürgisser and Cucker:

- Proved that the smoothed complexity of Beltrán-Pardo algorithm is polynomial:
$$\sup_{f \in \mathcal{H}} \left[\mathbb{E}\left(\mathrm{cost}_{\mathrm{BP}}(f)\right)\right] = \infty$$
$$\text{but } \sup_{f \in \mathcal{H}} \left[\mathbb{E}\left(\mathrm{cost}_{\mathrm{BP}}(f + \varepsilon)\right)\right] = \mathcal{O}\left(\frac{1}{\sigma} n D^{3/2} N^2\right),$$
where $\varepsilon \in \mathcal{H}$ is a random non centered Gaussian variable with variance σ^2.
- Described a deterministic algorithm with average complexity $N^{\mathcal{O}(\log \log N)}$.

Today
Lairez, 2015

Deterministic algorithm with complexity $\mathcal{O}(nD^{3/2}N^2)$.

Duplication of the uniform dist. on $[0,1]$

- $q > 0$ an integer.
- $x \in [0,1]$ a uniformly distributed random variable.

- $\lfloor x \rfloor_q \overset{\text{def}}{=} 2^{-q} \lfloor 2^q x \rfloor \in [0,1]$, the truncature of x to precision q.
- $\{x\}_q \overset{\text{def}}{=} 2^q x - \lfloor 2^q x \rfloor \in [0,1]$, the fractionary part.

Proposition

- The probability distribution of $\lfloor x \rfloor_q$ converges to the uniform distribution $[0,1]$ when $q \to \infty$.
- $\{x\}_q$ is uniformly distributed on $[0,1]$.
- $\lfloor x \rfloor_q$ and $\{x\}_q$ are independent.

Duplication of the uniform dist. on $\mathbb{S}(\mathcal{H})$

- $q > 0$ an integer.
- $x \in \mathbb{S}(\mathcal{H})$ a uniformly distributed random variable.

- $\lfloor x \rfloor_q \stackrel{\text{def}}{=} [\ldots] \in \mathbb{S}(\mathcal{H})$, the truncature of x to precision q.
- $\{x\}_q \stackrel{\text{def}}{=} [\ldots] \in \mathbb{S}(\mathcal{H})$, the fractionary part.

Proposition

- The probability distribution of $\lfloor x \rfloor_q$ converges to the uniform distribution $\mathbb{S}(\mathcal{H})$ when $q \to \infty$.
- $\{x\}_q$ is *almost* uniformly distributed on $\mathbb{S}(\mathcal{H})$.
- $\lfloor x \rfloor_q$ and $\{x\}_q$ are *almost* independent.

A deterministic algorithm

Derandomization of Beltrán-Pardo algorithm

Beltrán-Pardo algorithm

$$\mathrm{BP} : \mathbb{S}(\mathcal{H}) \times [0,1]^{\mathbb{N}} \to \mathbb{C}^n.$$

A deterministic algorithm

Derandomization of Beltrán-Pardo algorithm

Modified Beltrán-Pardo algorithm

$$\mathrm{BP} : \mathbb{S}(\mathcal{H}) \times \mathbb{S}(\mathcal{H}) \to \mathbb{C}^n.$$

A deterministic algorithm

Derandomization of Beltrán-Pardo algorithm

Modified Beltrán-Pardo algorithm

$$\mathrm{BP} : \mathbb{S}(\mathcal{H}) \times \mathbb{S}(\mathcal{H}) \to \mathbb{C}^n.$$

A deterministic algorithm

Derandomization of Beltrán-Pardo algorithm

Modified Beltrán-Pardo algorithm

$$\mathrm{BP} : \mathbb{S}(\mathcal{H}) \times \mathbb{S}(\mathcal{H}) \to \mathbb{C}^n.$$

The algorithm, 1st try

procedure DBP(f)
  $q \leftarrow$ a large enough integer
  return BP $\left(\lfloor f \rfloor_q, \{f\}_q\right)$
end procedure

A deterministic algorithm

Derandomization of Beltrán-Pardo algorithm

Modified Beltrán-Pardo algorithm

$$\mathrm{BP} : \mathbb{S}(\mathcal{H}) \times \mathbb{S}(\mathcal{H}) \to \mathbb{C}^n.$$

The algorithm, 2nd try

procedure DBP(f)
  $q \leftarrow \lfloor \log_2 N \rfloor$
  repeat
    $q \leftarrow 2q$
    $z \leftarrow \mathrm{BP}\left(\lfloor f \rfloor_q, \{f\}_q\right)$
  until z is an approximate root of f
  return z
end procedure

A deterministic algorithm

Derandomization of Beltrán-Pardo algorithm

Modified Beltrán-Pardo algorithm

$$\mathrm{BP} : \mathbb{S}(\mathcal{H}) \times \mathbb{S}(\mathcal{H}) \to \mathbb{C}^n.$$

The algorithm, final version

procedure DBP(f)
  $q \leftarrow \lfloor \log_2 N \rfloor$
  repeat
    $q \leftarrow 2q$
    $z \leftarrow \mathrm{BP}\left(\lfloor f \rfloor_q, \{f\}_q\right)$ with early abort
  until z is an approximate root of f
  return z
end procedure

Homotopy continuation with early abort

procedure HC'(f, g, z, q)
  $t \leftarrow 1/\left(101 D^{3/2} \mu(g,z)^2 d_{\mathbb{S}}(f,g)\right)$
  while $1 > t$ **do**
    $h \leftarrow \Gamma(g, f, t)$ ▷ "$tf + (1-t)g$" on the sphere
    $z \leftarrow \mathrm{Newton}(h, z)$
    $t \leftarrow t + 1/\left(101 D^{3/2} \mu(h,z)^2 d_{\mathbb{S}}(f,g)\right)$
    abort if $151 D^{3/2} \mu(h,z)^2 > 2^q$
  end while
  return z
end procedure

- If $\|f - \tilde{f}\| \leqslant 2^{-q}$, then HC'$(f, g, z, q)$ fails or returns an approximate root of $\tilde{f}$.
- In any case, it performs at most $cD^{3/2} \int_g^{\tilde{f}} \mu(h,z)^2 \mathrm{d}h$ steps.

Complexity analysis

- Let $f \in \mathbb{S}(\mathcal{H})$ be a uniformly distributed random variable.
- Let Ω be the number of iterations in $\mathrm{DBP}(f)$.

Proposition — $\mathbb{E}(\Omega) \leqslant 7$. (And the distribution is very light-tailed.)

$\rightsquigarrow$ The precision q is typically no more than $128 \log N$.

Complexity analysis

- Let $f \in \mathbb{S}(\mathcal{H})$ be a uniformly distributed random variable.
- Let Ω be the number of iterations in DBP(f).

Proposition — $\mathbb{E}(\Omega) \leqslant 7$. (And the distribution is very light-tailed.)

$\rightsquigarrow$ The precision q is typically no more than $128 \log N$.

Complexity analysis

- $\mathrm{cost}_{\mathrm{DBP}}(f) = \sum_{k=1}^{\Omega} \left(\mathcal{O}(N q_k) + \mathrm{cost}_{\mathrm{BP'}} \left(\lfloor f \rfloor_{q_k}, \{f\}_{q_k} \right) \right)$

Complexity analysis

- Let $f \in \mathbb{S}(\mathcal{H})$ be a uniformly distributed random variable.
- Let Ω be the number of iterations in $\mathrm{DBP}(f)$.

Proposition — $\mathbb{E}(\Omega) \leqslant 7$. (And the distribution is very light-tailed.)

$\rightsquigarrow$ The precision q is typically no more than $128 \log N$.

Complexity analysis

- $\mathrm{cost}_{\mathrm{DBP}}(f) = \sum_{k=1}^{\Omega} \left(\mathcal{O}(N q_k) + \mathrm{cost}_{\mathrm{BP'}} \left(\lfloor f \rceil_{q_k}, \{f\}_{q_k} \right) \right)$
- $\mathrm{cost}_{\mathrm{BP'}} \left(\lfloor f \rceil_{q_k}, \{f\}_{q_k} \right) \sim \mathrm{cost}_{\mathrm{BP}}(\lfloor f \rceil_{q_k}, g) \sim \mathrm{cost}_{\mathrm{BP}}(f, g)$

Complexity analysis

- Let $f \in \mathbb{S}(\mathcal{H})$ be a uniformly distributed random variable.
- Let Ω be the number of iterations in $\mathrm{DBP}(f)$.

Proposition — $\mathbb{E}(\Omega) \leqslant 7$. (And the distribution is very light-tailed.)

$\rightsquigarrow$ The precision q is typically no more than $128 \log N$.

Complexity analysis

- $\mathrm{cost}_{\mathrm{DBP}}(f) = \sum_{k=1}^{\Omega} \left(\mathcal{O}(Nq_k) + \mathrm{cost}_{\mathrm{BP'}} \left(\lfloor f \rfloor_{q_k}, \{f\}_{q_k} \right) \right)$
- $\mathrm{cost}_{\mathrm{BP'}} \left(\lfloor f \rfloor_{q_k}, \{f\}_{q_k} \right) \sim \mathrm{cost}_{\mathrm{BP}}(\lfloor f \rfloor_{q_k}, g) \sim \mathrm{cost}_{\mathrm{BP}}(f, g)$
- $\boxed{\mathbb{E}(\mathrm{cout}_{\mathrm{BPD}}(f)) = \mathcal{O}(nD^{3/2}N^2)}$

Conclusion

Randomness is part of Smale's 17th problem from its very formulation asking for an average analysis.

Problème no. 17bis — Can a zero of n complex polynomial equations in n unknowns be found approximately in polynomial time with respect to the evaluation complexity of the input and the logarithm of its conditionning?

Conclusion

Randomness is part of Smale's 17th problem from its very formulation asking for an average analysis.

Problème no. 17bis — Can a zero of n complex polynomial equations in n unknowns be found approximately in polynomial time with respect to the evaluation complexity of the input and the logarithm of its conditionning?

Thank you!