ISSAC 2022
Lille, France

Beyond Worst-Case Analysis for Root Isolation Algorithms

Alperen A. ERGÜR
UTSA

Josué TONELLI-CUETO
INRIA Paris & IMJ-PRJ

Elias TSIGARIDAS

Photo while working on this project

Real Root Isolation I: The Problem

INPUT:

$g \in \mathbb{Z}[X]$

OUTPUT:

Intervals $J_1, \dots, J_k$ s.t.

0) $J_i = (a_i, b_i)$ with $a_i, b_i \in \mathbb{Q}$

1) $Z(g) \cap \mathbb{R} \subseteq \bigcup_{i=1}^{k} J_i$

2) $\forall i,\ \# Z(g) \cap J_i = 1$

INPUT SIZE PARAMETERS:

d : degree of g

τ : bit-size of coefficients of g

MEASURE OF RUN-TIME

Bit complexity

Real Root Isolation II: The State of the Art

Sturm Solver	$\tilde{O}_B(d^4\tau^2)$
Descartes Solver	$\tilde{O}_B(d^4\tau^2)$
ANewDsc (Sagraloff & Mehlhorn; 2016)	$\tilde{O}_B(d^3+d^2\tau)$
Pan's Algorithm (Pan; 2002)	$\tilde{O}_B(d^2\tau)$

Q: Can we beat the champion?

Real Root Isolation III: What do we wish?

$$\tilde{O}_B(d\tau)$$

We wish to find real roots almost as fast as we read the polynomial!

Descartes Solver I: Rule of Signs

Portrait by Frans Hal
Source: WikiMedia Commons

$V(f) :=$ # sign variations of $f_0, f_1, \ldots$

THM (Descartes' rule of signs)

$$\#Z(f,\mathbb{R}_>) \leq V(f)$$

Moreover,

$$V(f) \leq 1 \Rightarrow \text{Equality}$$

COR

$$\#Z(f,(a,b)) \leq V(f,(a,b)) := V\left((X+1)^d f\left(\frac{bX+a}{X+1}\right)\right)$$

$\uparrow$

$(0,\infty) \longrightarrow (a,b)$
bijection

Descartes Solver II:

The Descartes' Oracle

1) Overcounting: $\#Z(f,J) \leq V(f,J)$

2) Exactness I: $V(f,J) \leq 1 \Rightarrow$ Equality

3) Exactness II:

$$\#Z(f, D(m(J), cw(J))) \leq K \Rightarrow V(f,J) \leq K$$

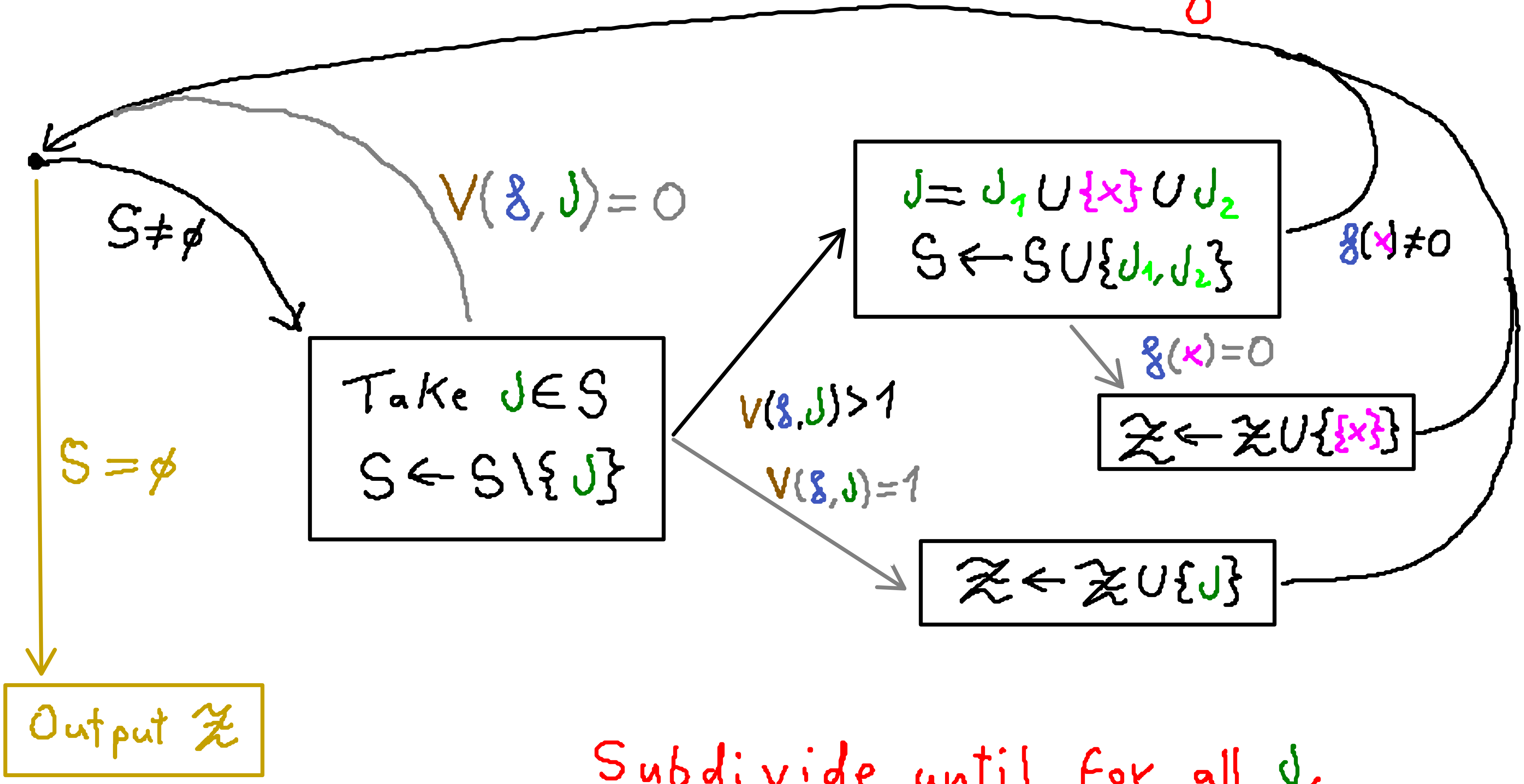
Obreshkoff's Thm: Descartes sees the complex roots around!

4) Subadditivity:

$$\dot{\bigcup} J_i \subseteq J \Rightarrow \sum V(f,J_i) \leq V(f,J)$$

Descartes Solver III:

The Algorithm



$S \neq \emptyset$

Take $J \in S$

$S \leftarrow S \setminus \{J\}$

$V(g, J) = 0$

$V(g,J) > 1$

$J = J_1 \cup \{x\} \cup J_2$

$S \leftarrow S \cup \{J_1, J_2\}$

$g(x) \neq 0$

$g(x) = 0$

$\mathcal{Z} \leftarrow \mathcal{Z} \cup \{\{x\}\}$

$V(g,J) = 1$

$\mathcal{Z} \leftarrow \mathcal{Z} \cup \{J\}$

$S = \emptyset$

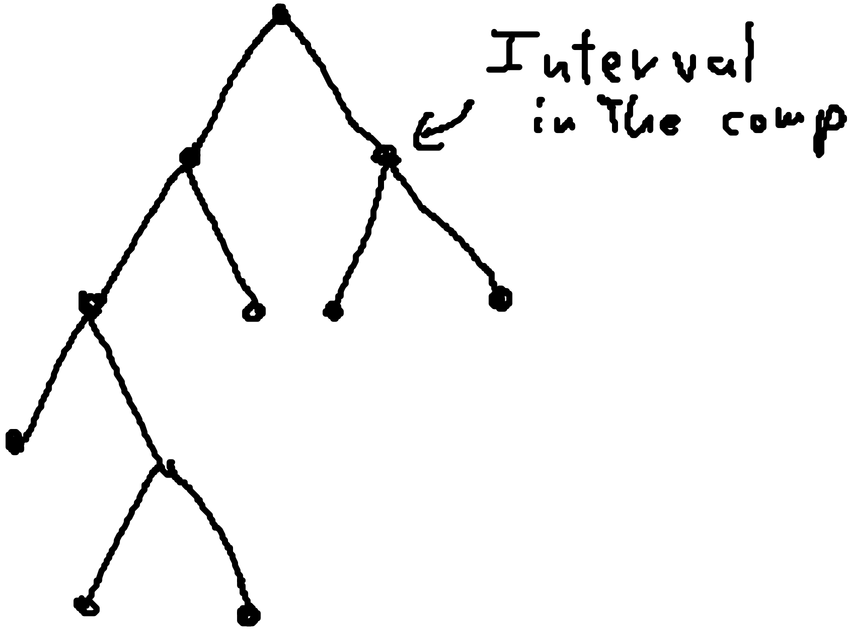
Output $\mathcal{Z}$

Subdivide until for all J,

$V(g, J) \leq 1$!

DESCARTES SOLVER IV:
Descartes' tree

$\mathcal{T}(g, I)$



size of $\mathcal{T}(g, I)$

$\updownarrow$

run-time of DESCARTES(g, I)

We only need to control the size of subdiv. tree!

Real Root Isolation IV:

Are we being pessimistic?

Worst-case complexity:

$$\max\{\mathrm{cost}(\mathrm{SOLVER}, f) \mid \text{bit-size}(f) \leq \tau, \deg(f) \leq d\}$$

↑

Pessimistic in practice

DESCARTES SOLVER

seems to behave faster in practice!

¿Can we explain this?

Real Root Isolation V: Beyond pessimism

Worst-case complexity:

$$\max\{\mathrm{cost}(\mathrm{SOLVER}, \mathfrak{f}) \mid \text{bit-size}(\mathfrak{f}) \leq \tau, \deg(\mathfrak{f}) \leq d\}$$

(Goldstine & von Neumann, 1951)
(Demmel, 1988) (Smale; 1985, 1997)

$\rightsquigarrow$ (Roughgarden, 2021)

Probabilistic complexity

$$\mathbb{E}\{\mathrm{cost}(\mathrm{SOLVER}, \mathfrak{f})^{\ell} \mid \text{bit-size}(\mathfrak{f}) \leq \tau, \deg(\mathfrak{f}) \leq d\}$$

What's a 'good' random model for $\mathfrak{f}$?

↑ Many choices of randomness 😱

Beyond pessimism I: Uniform Random Bit Polynomials & a Simple Main Theorem

$$f = \sum_{k=0}^{d} f_k X^k$$

s.t. $f_k \sim \mathcal{U}([-2^\tau, 2^\tau] \cap \mathbb{Z})$ independent

SIMPLE MAIN THM (Ergür, T-C, Tsigaridas)

$$\mathbb{E}\,\mathrm{cost}(\text{DESCARTES}, f) = \widetilde{\mathcal{O}}_B(d^2 + d\tau)$$

On average, DESCARTES is almost optimal!

Beyond pessimism II: Random Bit Polynomials

$$f = \sum_{k=0}^{d} f_k X^k \in \mathbb{Z}[X]$$

s.t. f_k independent

bit-size of f:

$$\tau(f) := \min\{\tau \mid \forall k, \mathbb{P}(|f_k| \leq 2^{\tau}) = 1\}$$

weight of f:

No middle indexes!

$$w(f) := \max\{\mathbb{P}(f_k = c) \mid c \in \mathbb{R}, k \in \{0, 1, d-1, d\}\}$$

uniformity of f: $u(f) := \ln\left(w(f)\left(1 + 2^{\tau(f)+1}\right)\right)$

Beyond pessimism III: MAIN THEOREM

MAIN THM (Ergür, T-C, Tsigaridas)

$$\mathbb{E}\,\mathrm{cost}(\mathrm{DESCARTES}, f) = \widetilde{\mathcal{O}}_B(d^2 + d\tau)(1+u(f))^4$$

Note: f uniform ⇒ $u(f) = 0$

Claim: For many cases, $u(f) = \mathcal{O}(1)$

IF $\tau = \Omega(d)$, almost like reading!

On average, DESCARTES is almost optimal!

Beyond pessimism IV: Examples of Random Bit Polynomials I

- Support control $\{0, 1, d-1, d\} \subseteq A$

$$f = \sum_{k \in A} f_k X^k \text{ with } f_k \sim \mathcal{U}([-2^\tau, 2^\tau] \cap \mathbb{Z})$$

... then $u(f) = 0$

- Sign control $\sigma \in \{-1, +1\}^{\{0, \dots, d\}}$

$$f = \sum_{k=1}^{d} f_k X^k \text{ with } f_k \sim \mathcal{U}(\sigma_k([1, 2^\tau] \cap \mathbb{N}))$$

... then $u(f) \leq \ln 3$

Beyond pessimism V:
Examples of Random Bit Polynomials II

- Exact bitsize

$$F = \sum_{k=1}^{d} f_k X^k \quad \text{with} \quad f_k \sim \mathcal{U}\left(\{n \in \mathbb{Z} \mid \lfloor \log n \rfloor = \tau\}\right)$$

... then $u(F) \leq \ln 3$

+ their combinations

Our random model is flexible!

Beyond pessimism VI:

Smoothed case included!

$F=\sum_{k=1}^{d} f_k X^k$ random bit polynomial

$g=\sum_{k=1}^{d} g_k X^k$ fix polynomial of entries of size τ

$\sigma \in \mathbb{Z}\setminus\{0\}$

Then:

$F_\sigma = g + \sigma F$ random bit polynomial

& $u(F_\sigma) \leq 1 + u(F) + \max\{\tau - \tau(F), \tau(\sigma)\}$

The Ingredients of the Analysis I: Condition Numbers

$$C(f) := \max_{x \in [-1,1]} \frac{\sum_{k=0}^{d} |f_k|}{\max\{|f(x)|, |f'(x)|/d\}}$$

$C(f) = \infty \iff f$ has a singular root in $[-1,1]$

Upper bounds on $C(f)$

→ Lower bounds for root separation of f

→ Upper bounds for depth of DESCARTES' tree

The Ingredients of the Analysis II: Bounds for Number of Complex Roots

We only care about nearby roots!

Upper bounds for # complex roots of g around $[-1,1]$

→ Upper bounds for width of Descartes' tree

Complex analysis!

Tichmarsh thm

The Ingredients of the Analysis III: Probabilistic Toolbox

Ball's smoothing:

$x \in \mathbb{Z}^N$ discrete random variable

$y \in \mathbb{R}^N$ s.t. $y_i \sim \mathcal{U}((-1/2, 1/2))$ i.i.d.

Then: $x + y$ continuous random var.

We can use our old cont. toolbox!

⚠ I am omitting a lot of technical details.

SUMMING UP:

DESCARTES' SOLVER IS ALMOST OPTIMAL ON AVERAGE!

Eskerrik asko!

(Thank you!)