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
INRIA Paris & IMJ-PRJ

Photo while working on this project

# Real Root Isolation I: The Problem

INPUT:

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

OUTPUT:

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

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

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

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

INPUT SIZE PARAMETERS:

$d$ : degree of $f$

$\tau$ : bit-size of coefficients of $f$

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

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

THM (Descartes' rule of signs)

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

Moreover,

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

Portrait by Frans Hal
Source: WikiMedia Commons

COR

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

$(0,\infty) \to (a,b)$ 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:

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

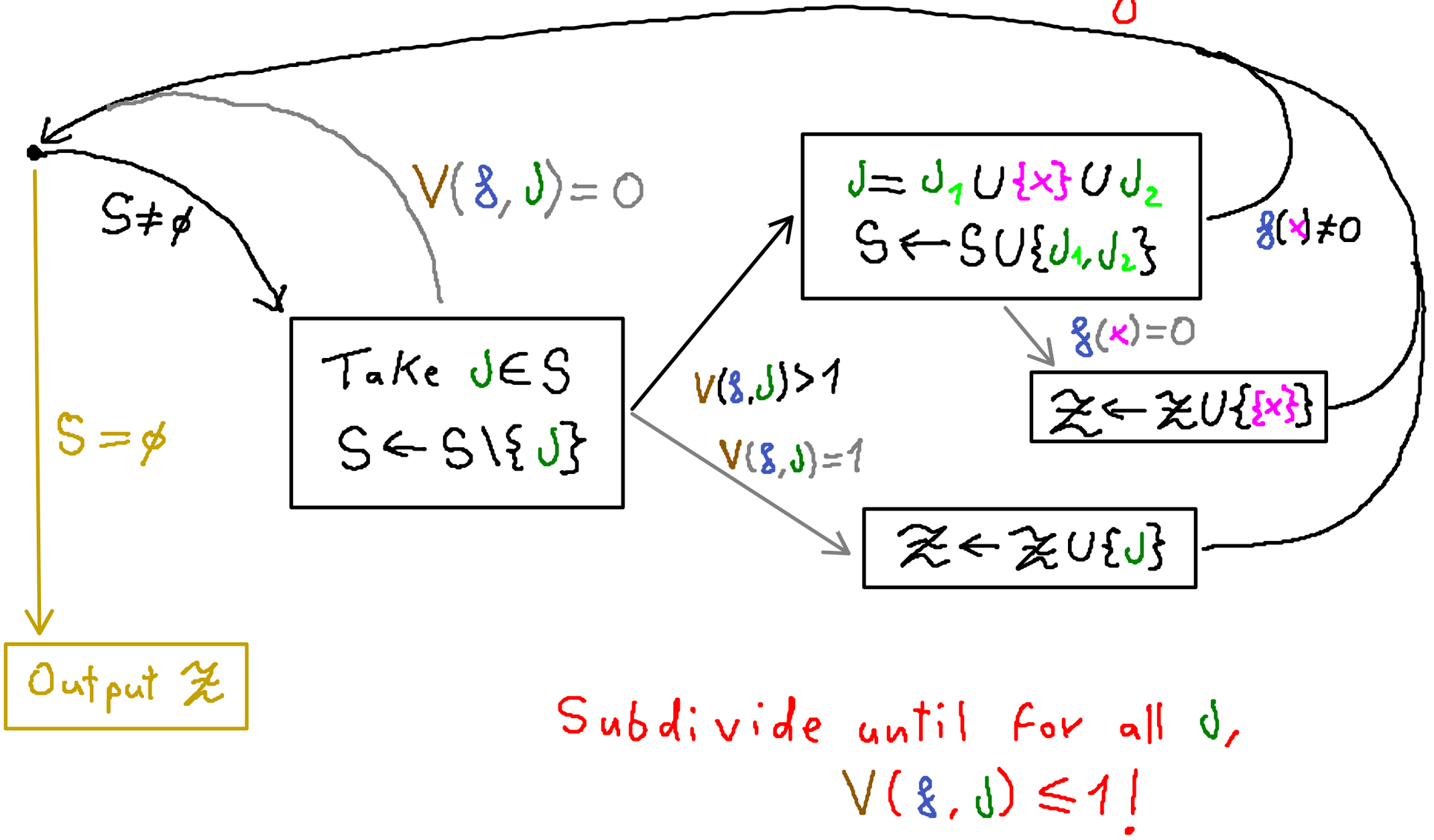
Obreshkoff's Thm: Descartes sees the complex roots around!

4) Subadditivity:

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

# Descartes Solver III:

## The Algorithm



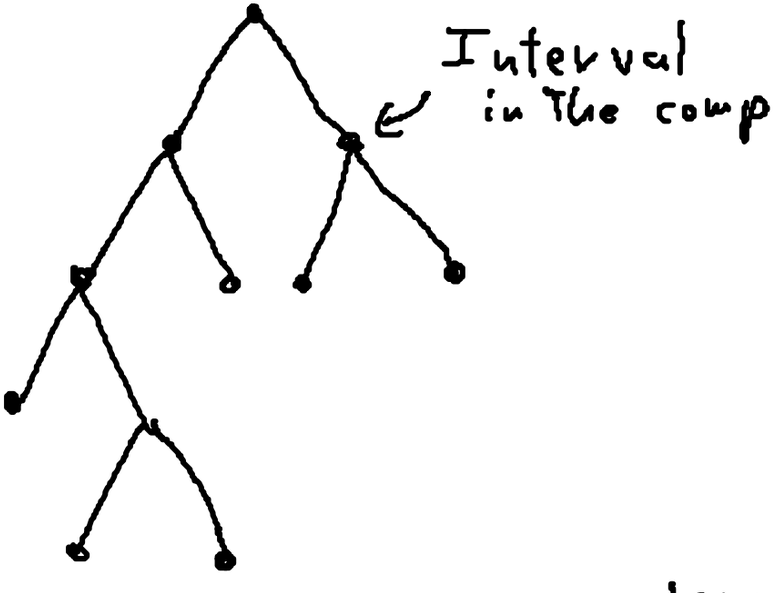

Subdivide until for all $J$,

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

# Descartes Solver IV:

## Descartes' tree

$\Upsilon(f, I)$




size of $\Upsilon(f, I)$

$\updownarrow$

run-time of DESCARTES$(f, I)$

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

# Real Root Isolation IV:

## Are we being pessimistic?

Worst-case complexity:

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

↑

Pessimistic in practice

DESCARTES SOLVER seems to behave faster in practice!

¿Can we explain this?

# Real Root Isolation V:

## Beyond pessimism

## Worst-case complexity:

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

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

(Roughgarden, 2021)

## Probabilistic complexity

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

What's a 'good' random model for $f$?

↑

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

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

$$\mathbb{E}\, \text{cost}(\text{DESCARTES}, F) = \tilde{O}_B(d^2 + dr)$$

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 $F$:

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

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 $F$:

$$u(F) := \ln\left(w(F)\left(1 + 2^{r(F)+1}\right)\right)$$

# Beyond pessimism III:

## Main Theorem

### Main Thm (Ergür, T-C, Tsigaridas)

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

Note: $f$ uniform $\Rightarrow u(f) = 0$

Claim: For many cases, $u(f) = O(1)$

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

On average, Descartes is almost optimal!

# Beyond pessimism IV: Examples of Random Bit Polynomials I

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

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

$$\ldots \text{ then } u(f) = 0$$

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

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

$$\ldots \text{ then } u(f) \leqslant \ln 3$$

# Beyond pessimism V:
# Examples of Random Bit Polynomials II

- Exact bitsize

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

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

+ their combinations

Our random model is flexible!

# Beyond pessimism V: 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 $\tau$

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

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

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

$C(f) = \infty \Leftrightarrow f$ 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

Upper bounds for

We only care about nearby roots!

# complex roots of $f$ around $[-1,1]$

$\longrightarrow$ 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!)