

Why

does the DESCARTES Solver work?

Alperen A.
ERGÜR

Josué
TONELLI-CUETO

Elias
TSIGARIDAS
Inria





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

γ : bit-size of coefficients of g

MEASURE OF RUN-TIME

Bit complexity

Real Root Isolation II: The State of the Art

STURM SOLVER

$$\tilde{O}_B(d^4 \gamma^2)$$

DESCARTES SOLVER

$$\tilde{O}_B(d^4 \gamma^2)$$

ANewDsc

$$\tilde{O}_B(d^3 + d^2 \gamma)$$

(Sagraloff & Mehlhorn; 2016)

PAN'S ALGORITHM

$$\tilde{O}_B(d^2 \gamma)$$

(Pan; 2002)

Q: Can we beat the champion?

Real Root Isolation III:

What do we wish?

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

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

DESCARTES SOLVER I:

Rule of Signs

$V(g) := \# \text{sign variations of } g_0, g_1, \dots$

THM (Descartes' rule of signs)

$$\#\mathcal{Z}(g, \mathbb{R}_+) \leq V(g)$$

Moreover,

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

COR

$$\#\mathcal{Z}(g, (a, b)) \leq V(g, (a, b)) := V\left((x+1)^d g\left(\frac{bx+a}{x+1}\right)\right)$$

\uparrow
 $(0, \infty) \xrightarrow{\text{bijection}} (a, b)$



Portrait by Frans Hals
Source: Wikimedia Commons

DESCARTES SOLVER II:

The Descartes' Oracle

- 1) Overcounting: $\#Z(g, J) \leq V(g, J)$
- 2) Exactness I: $V(g, J) \leq 1 \Rightarrow$ Equality

3) Exactness II:

$$\#Z(g, D(m(J), c_w(J))) \leq K \Rightarrow V(g, J) \leq K$$

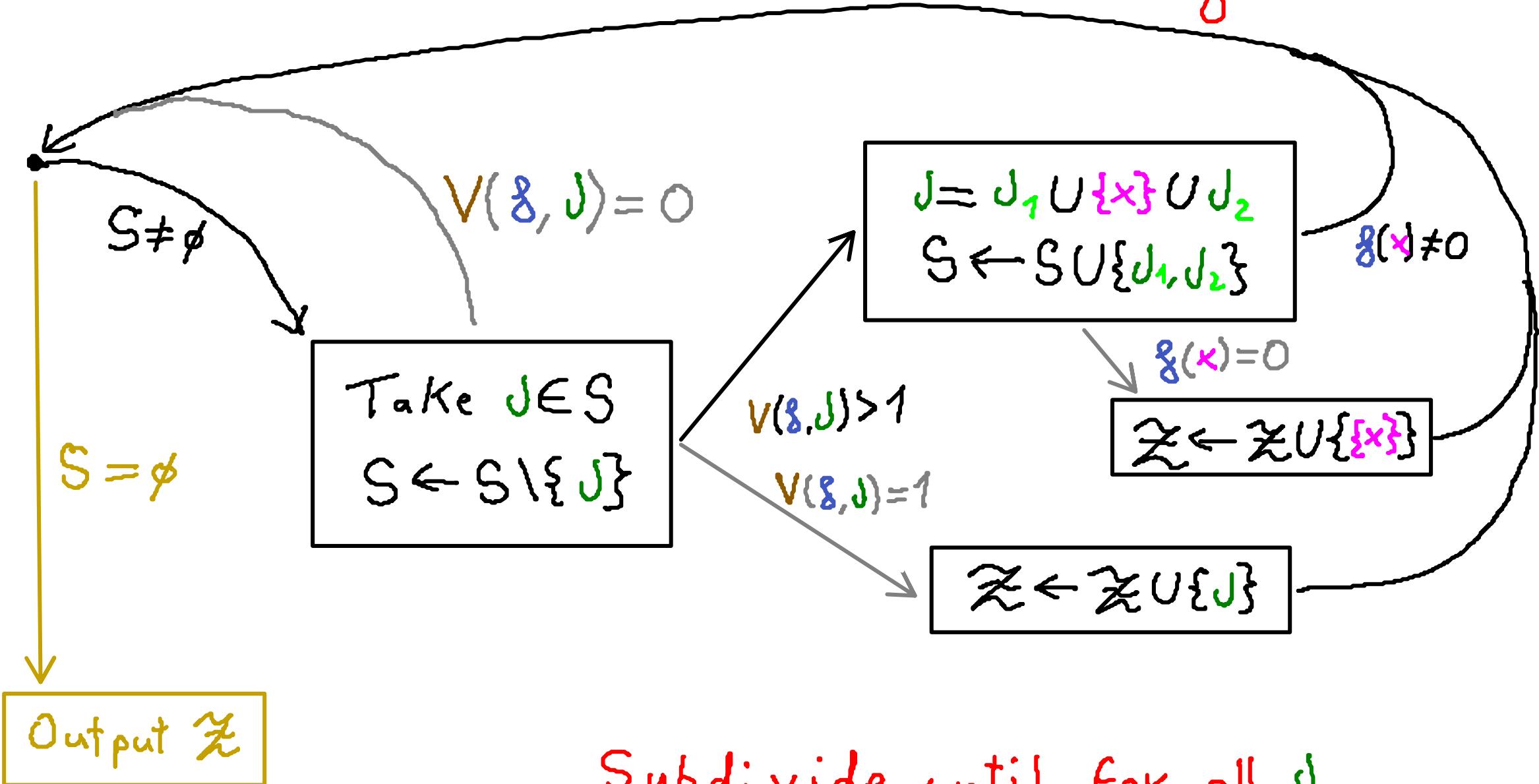
Obreshkoff's Thm: DESCARTES sees the complex roots around!

4) Subadditivity:

$$\bigcup_{i=1}^n J_i \subseteq J \Rightarrow \sum V(g, J_i) \leq V(g, J)$$

DESCARTES SOLVER III:

The Algorithm



Subdivide until for all J ,
 $V(g, J) \leq 1!$

Real Root Isolation IV:

Are we being pessimistic?

Worst-case complexity:

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



Pessimistic in practice

DESCARTES SOLVER

seems to behave faster in practice!

Can we explain this?

Real Root Isolation V:

Beyond pessimism

Worst-case complexity:

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

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

(Roughgarden, 2021)

Probabilistic complexity

$$\mathbb{E} \{ \text{cost}(\text{SOLVER}, g)^l \mid \text{bit-size}(g) \leq \tau, \deg(g) \leq d \}$$

What's a 'good' random model for g ?

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

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

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

On average, DESCARTES is almost optimal!

Beyond pessimism II:

Random Bit Polynomials

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

bit-size of F : s.t. f_k independent

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

weight of F : No middle indexes!

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

uniformity of F : $u(F) := \ln(w(F)(1 + 2^{\gamma(F)+1}))$

Beyond pessimism III:

MAIN THEOREM

MAIN THM (Ergür, T-C, Tsigaridas)

$$\mathbb{E} \text{cost}(\text{DESCARTES}, F) = \tilde{O}_B(d^2 + d\gamma)(1 + u(F))^4$$

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

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

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

On average, DESCARTES is almost optimal!

Beyond pessimism IV:

Examples of Random Bit Polynomials I

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

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

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

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

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

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

Beyond pessimism V:

Examples of Random Bit Polynomials II

- Exact bitsize

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

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

+ their combinations

Our random model is flexible!

Beyond pessimism VI:

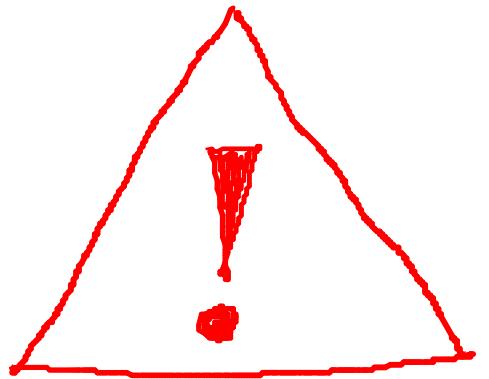
Smoothed case included!

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

$$g = \sum_{k=1}^d g_k X^k$$
 fix polynomial
 $\sigma \in \mathbb{Z} \setminus \{0\}$ of entries of size γ

Then:

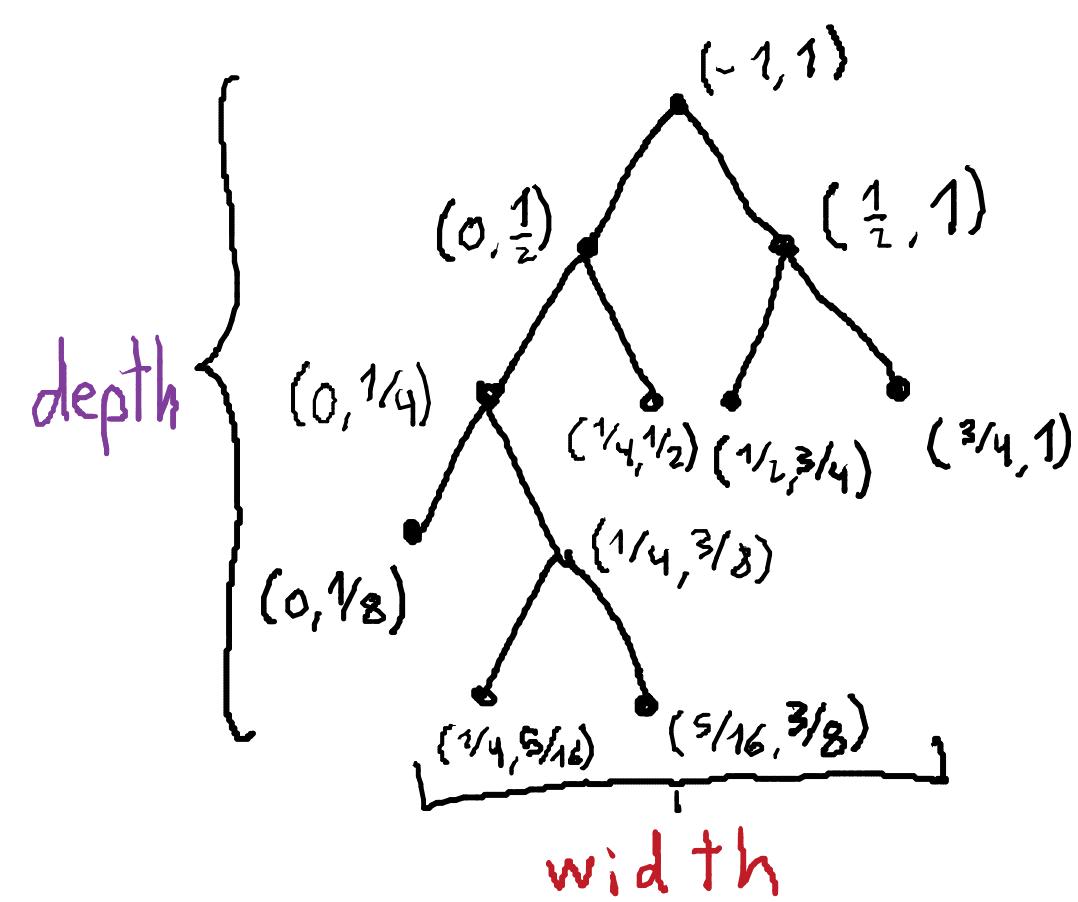
$$f_\sigma = g + \sigma f$$
 random bit polynomial
 $\& u(f_\sigma) \leq 1 + u(f) + \max\{\gamma - \gamma(f), \gamma(\sigma)\}$



LOTS OF DETAILS
WILL BE OMITTED

How to bound the run-time of DESCARTES?

$\gamma(g) \leftarrow$ DESCARTES' Computation Tree



PROP.
 $\text{cost}(\text{DESCARTES}, g)$
 \propto
 $O(d \gamma \text{width} \gamma(g) \text{depth} \gamma(g))$
 $+ d^2 \text{width} \gamma(g) \text{depth}^2 \gamma(g))$

I.e. size of $\gamma(g)$ bounds
run-time of DESCARTES!

The Ingredients of the Analysis I: Condition Number

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

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

$\frac{1}{C(g)} \sim \left\{ \begin{array}{l} \text{How much I have to perturb} \\ \text{the coefficients of } g \text{ so that} \\ \tilde{g} \text{ has a singular root in } [-1,1] \end{array} \right.$

Bounding depth $\gamma(g)$

PROP.

$$\text{depth } \gamma(g) \leq 5 + \log d + \log C(g)$$



$$\text{sep. between complex roots of } g \geq \frac{1}{12dC(g)}$$

Here $\rightarrow 1/\lambda$
no.
 $\frac{1}{2}$ $\text{depth } \gamma(g)$

Here it is
essential for
roots being near $[-1, 1]$!

Bounding width $\gamma(8)$

PROP

width $\gamma(8)$

$\leq \#$ complex roots of f nearby $[-1, 1]$



Important
For good bound
of the RHS!

Secret tool to bound RHS:

Titchmarsh's thm.

The Ingredients of the Analysis II: Cont. Probabilistic Toolbox

We can handle

$$C(F) \left(\text{ & # complex roots of } F \text{ nearby } [-1, 1] \right)$$

for a wide class of random F
as long as continuous distribution
— using geometric functional analysis

... but we don't have a continuous dist.

The Ingredients of the Analysis III: Ball's Smoothing Trick

$x \in \mathbb{Z}^N$ discrete random variable
 $y \in \mathbb{R}^N$ s.t. $y_i \sim \mathcal{U}(-\frac{1}{2}, \frac{1}{2})$ i.i.d.

→ $x + y$ continuous random var.

We can use our old cont. toolbox!

SUMMING UP:

DESCARTES' SOLVER

IS ALMOST OPTIMAL ON AVERAGE!

... AND THAT'S WHY DESCARTES WORKS SO WELL

Muito Obrigado

pela Atenção!

¡Muchas Gracias

por su Atención!