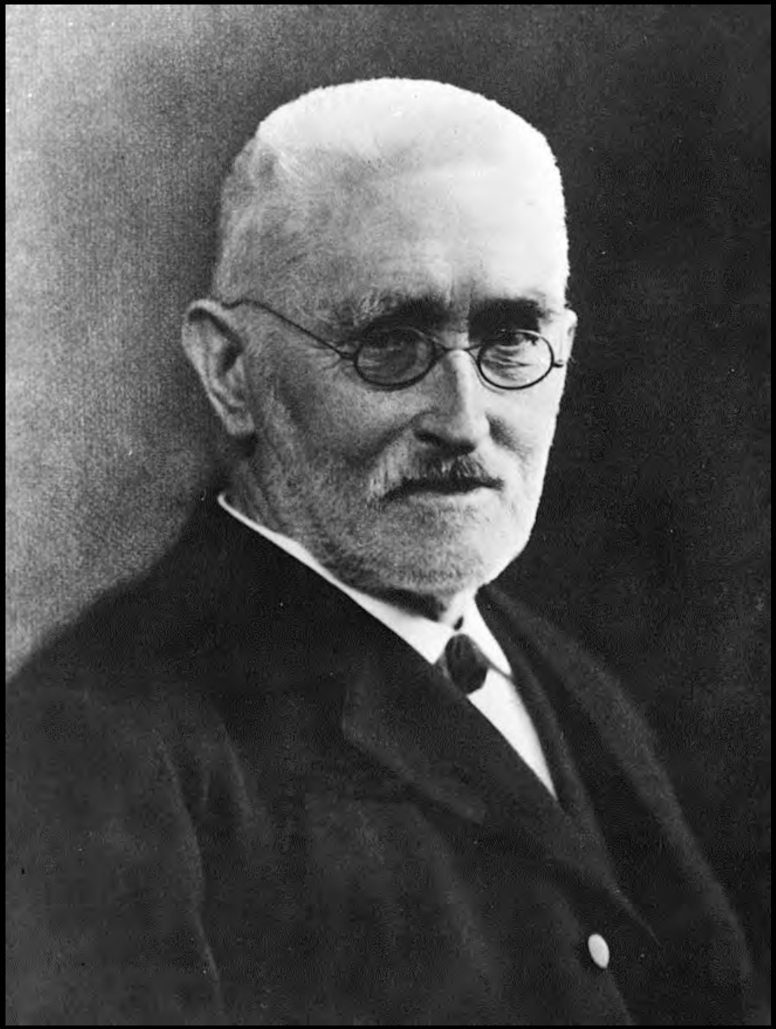
Fact of the Day



Today, October 6, Richard Dedekind would have turned 191 years old

8TH IBERIAN MATHEMATICAL MEETING
Sevilla, Spain

Why does the DESCARTES Solver work?

Alperen A. ERGÜR

Josué TONELLI-CUETO

Elias TSIGARIDAS

The University of Texas at San Antonio™

Photo while working on this project

Real Root Isolation I: The Problem

INPUT:

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

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

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

INPUT SIZE PARAMETERS:

d : degree of f

τ : 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

Portrait by Frans Hal
Source: WikiMedia Commons

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

THM (Descartes' rule of signs)

$$\#Z(g, \mathbb{R}_>) \le V(g)$$

Moreover,

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

COR

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

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

bijection

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:

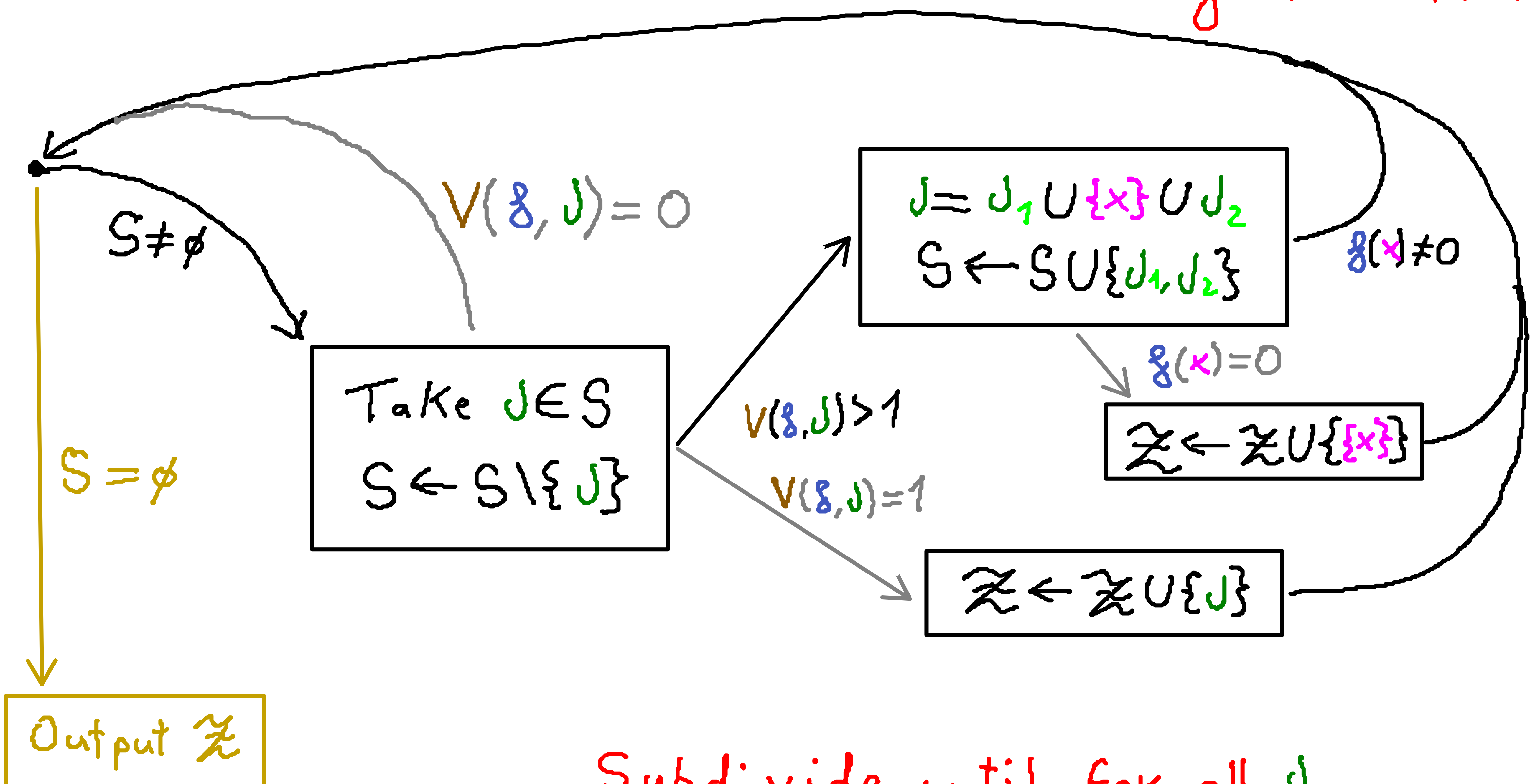
$$\#Z(g, D(m(J), c\,w(J))) \leq K \Rightarrow V(g,J) \leq K$$

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

4) Subadditivity:

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

Descartes Solver III: The Algorithm



Subdivide until for all J,

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

Real Root Isolation IV:

Are we being pessimistic?

Worst-case complexity:

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

Pessimistic in practice

Descartes Solver seems to behave faster in practice!

¿Can we explain this?

Real Root Isolation V: Beyond pessimism

Worst-case complexity:

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

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

(Roughgarden, 2021)

Probabilistic complexity

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

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)

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

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)

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

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

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

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

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

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

Beyond pessimism V:
Examples of Random Bit Polynomials II

- Exact bitsize

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

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

+ 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 τ

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

Then:

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

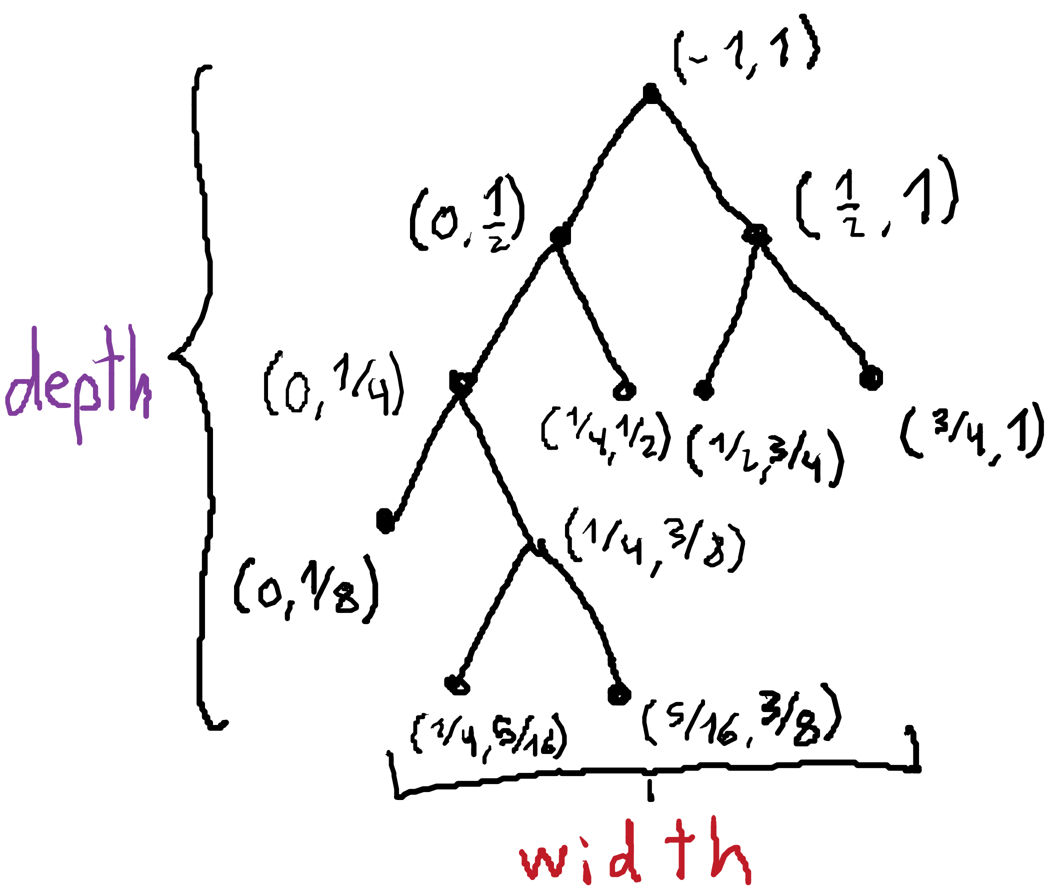
& $u(F_\sigma) \leq 1 + u(F) + \max\{\tau - \tau(F), \tau(\sigma)\}$

Lots of Details

will be Omitted

How to bound the run-time of DESCARTES?

$\mathcal{T}(g) \leftarrow$ DESCARTES' Computation Tree



PROP.

$$\mathrm{cost}(\text{DESCARTES}, g) \leq \mathcal{O}\big(d\tau\,\mathrm{width}\,\mathcal{T}(g)\,\mathrm{depth}\,\mathcal{T}(g) + d^2\,\mathrm{width}\,\mathcal{T}(g)\,\mathrm{depth}^2\,\mathcal{T}(g)\big)$$

I.e. size of $\mathcal{T}(g)$ bounds run-time of DESCARTES!

The Ingredients of the Analysis I: Condition Number

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

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

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

Bounding depth $\mathcal{T}(g)$

Prop.

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

$$\text{sep. between complex roots of } g \text{ nearby } [-1,1] \geq \frac{1}{12\, d\, C(g)}$$

Here no → $\not\wedge$

$$1/2^{\text{depth } \mathcal{T}(g)}$$

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

Bounding width $\tau(g)$

Prop

width $\tau(g)$

$\leq$ # complex roots of g 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

$C(f)$ (& # complex roots of f nearby $[-1,1]$)

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.

$\longrightarrow$ $x + y$ 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!