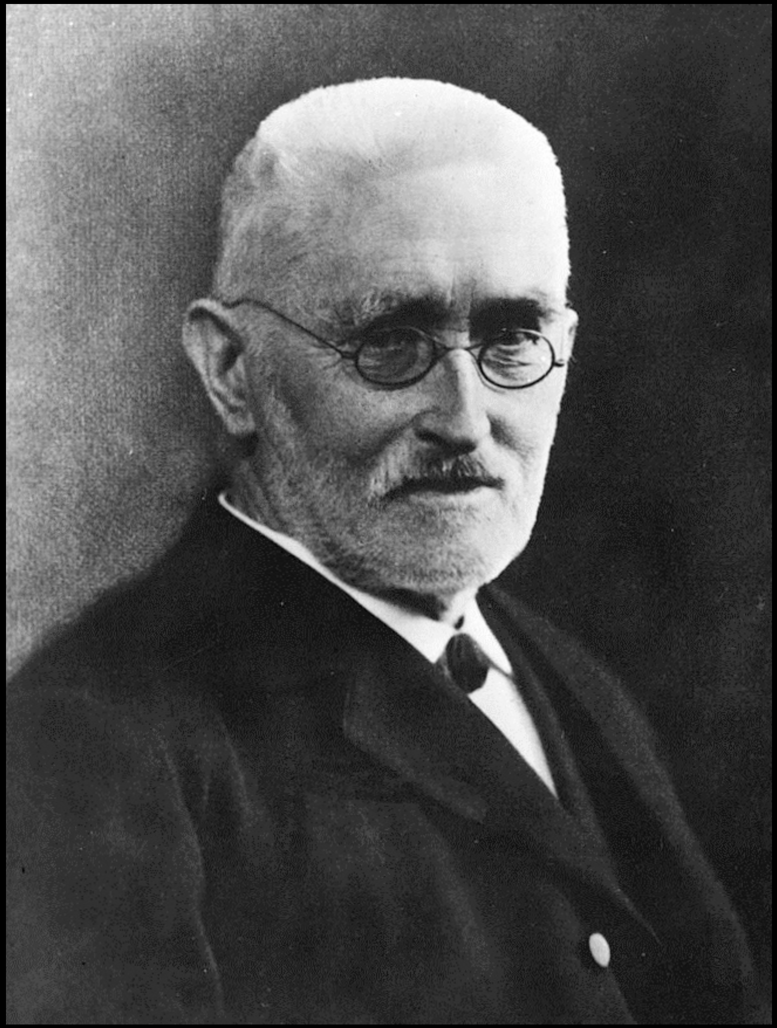
Fact of the Day



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

Slides available at:
tonellicueto.xyz/pdf/8IMM_slides.pdf

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™

Inria

IMJ-PRG

Photo while working on this project

Real Root Isolation I: The Problem

Real Root Isolation I: The Problem

INPUT:

Real Root Isolation I: The Problem

INPUT:

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

Real Root Isolation I: The Problem

INPUT:

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

OUTPUT:

Real Root Isolation I: The Problem

INPUT:

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

OUTPUT:

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

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 $a_i, b_i \in \mathbb{Q}$

Real Root Isolation I: The Problem

INPUT:

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

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

Real Root Isolation I: The Problem

INPUT:

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

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

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

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:

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

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

τ : bit-size of coefficients of f

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

τ : bit-size of coefficients of f

MEASURE OF RUN-TIME

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

τ : bit-size of coefficients of f

MEASURE OF RUN-TIME

Bit complexity

Real Root Isolation II: The State of the Art

Real Root Isolation II: The State of the Art

STURM SOLVER $\qquad \tilde{O}_B(d^4\tau^2)$

Real Root Isolation II: The State of the Art

Sturm Solver $\tilde{O}_B(d^4 \tau^2)$

Descartes Solver $\tilde{O}_B(d^4 \tau^2)$

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

(Sagraloff & Mehlhorn; 2016)

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

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

(Sagraloff & Mehlhorn; 2016)

Pan's Algorithm $\tilde{O}_B(d^2\tau)$

(Pan; 2002)

Q: Can we beat the champion?

Real Root Isolation III: What do we wish?

Real Root Isolation III:

What do we wish?

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

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

Descartes Solver I: Rule of Signs

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

Descartes Solver I: Rule of Signs

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

THM (Descartes' rule of signs)

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

Portrait by Frans Hal
Source: WikiMedia Commons

Descartes Solver I: Rule of Signs

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

THM (Descartes' rule of signs)

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

Moreover,

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

Portrait by Frans Hal
Source: WikiMedia Commons

Descartes Solver I: Rule of Signs

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

Portrait by Frans Hal
Source: WikiMedia Commons

THM (Descartes' rule of signs)

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

Moreover,

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

COR

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

Descartes Solver I: Rule of Signs

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

THM (Descartes' rule of signs)

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

Moreover,

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

Portrait by Frans Hal
Source: WikiMedia Commons

COR

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

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

DESCARTES SOLVER II:

The Descartes' Oracle

DESCARTES SOLVER II:

The Descartes' Oracle

1) Overcounting:

Descartes Solver II:

The Descartes' Oracle

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

Descartes Solver II:

The Descartes' Oracle

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

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

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:

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:

$$\#Z(g, \mathbb{D}(m(J), cw(J))) \leq K \Rightarrow V(g, J) \leq K$$

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:

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

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

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:

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

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

4) Subadditivity:

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:

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

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

4) Subadditivity:

$$\dot{\bigcup} J_i \subseteq J$$

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:

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

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

-

Descartes Solver III:

The Algorithm

$S \neq \emptyset$

Descartes Solver III: The Algorithm

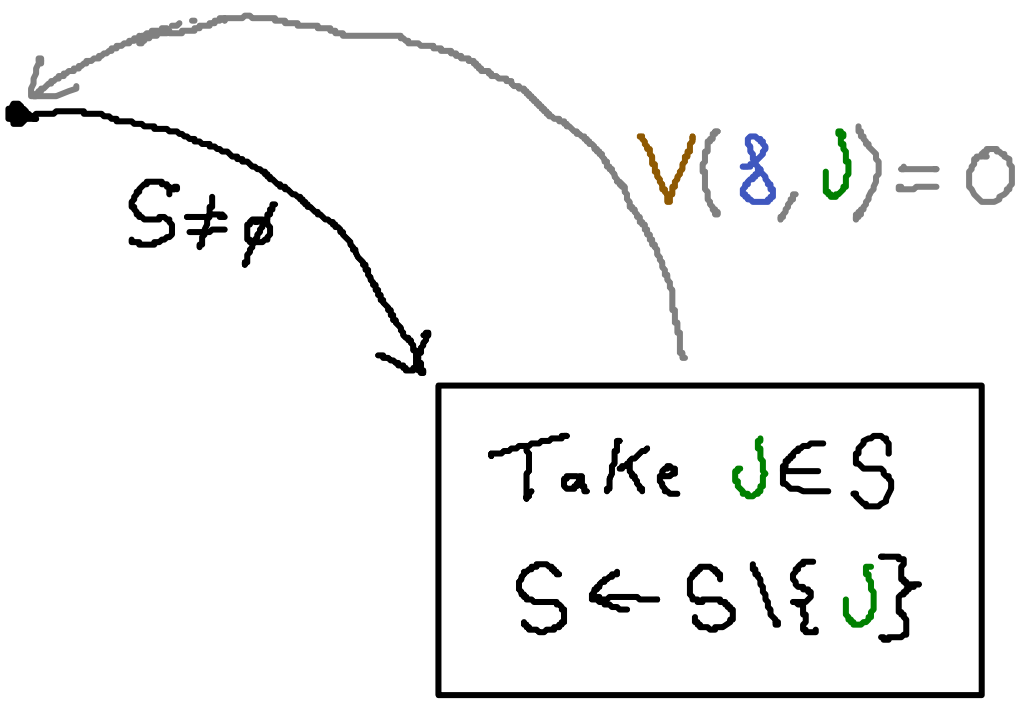
$S \neq \emptyset$

Take $J \in S$

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

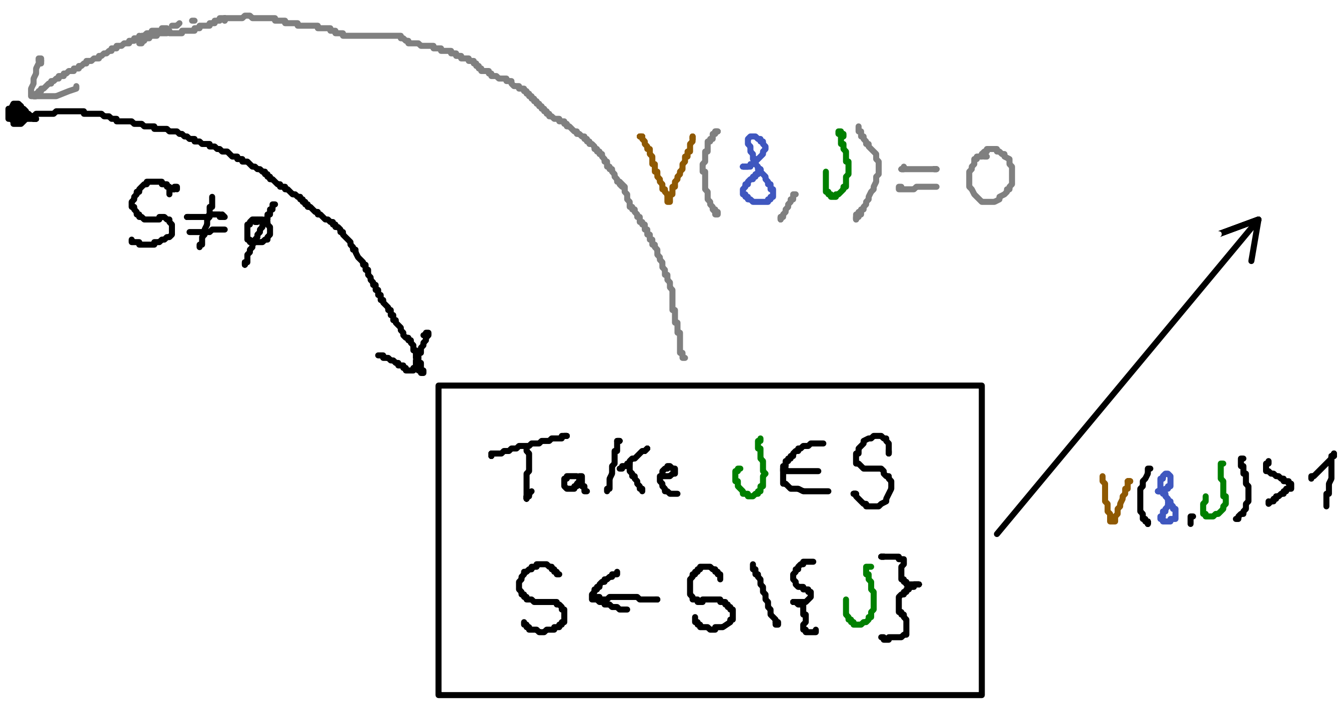
DESCARTES SOLVER III:

The Algorithm

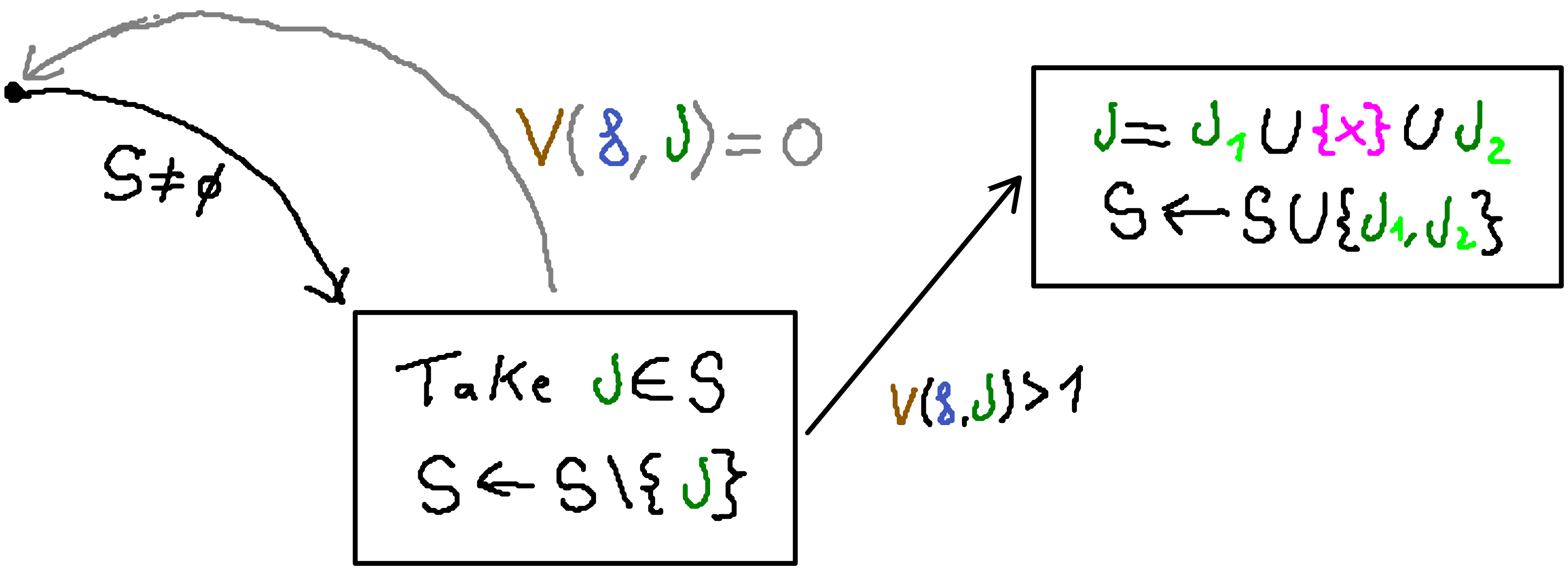


Descartes Solver III:

The Algorithm

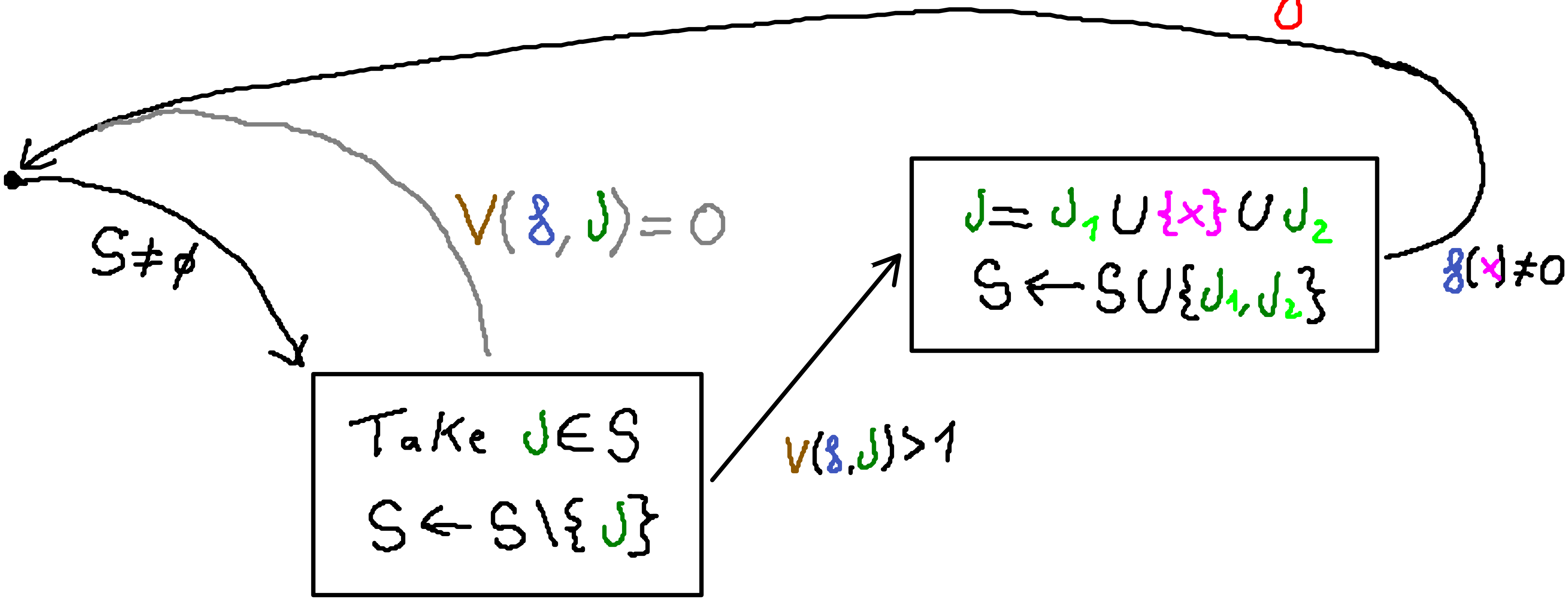


Descartes Solver III: The Algorithm

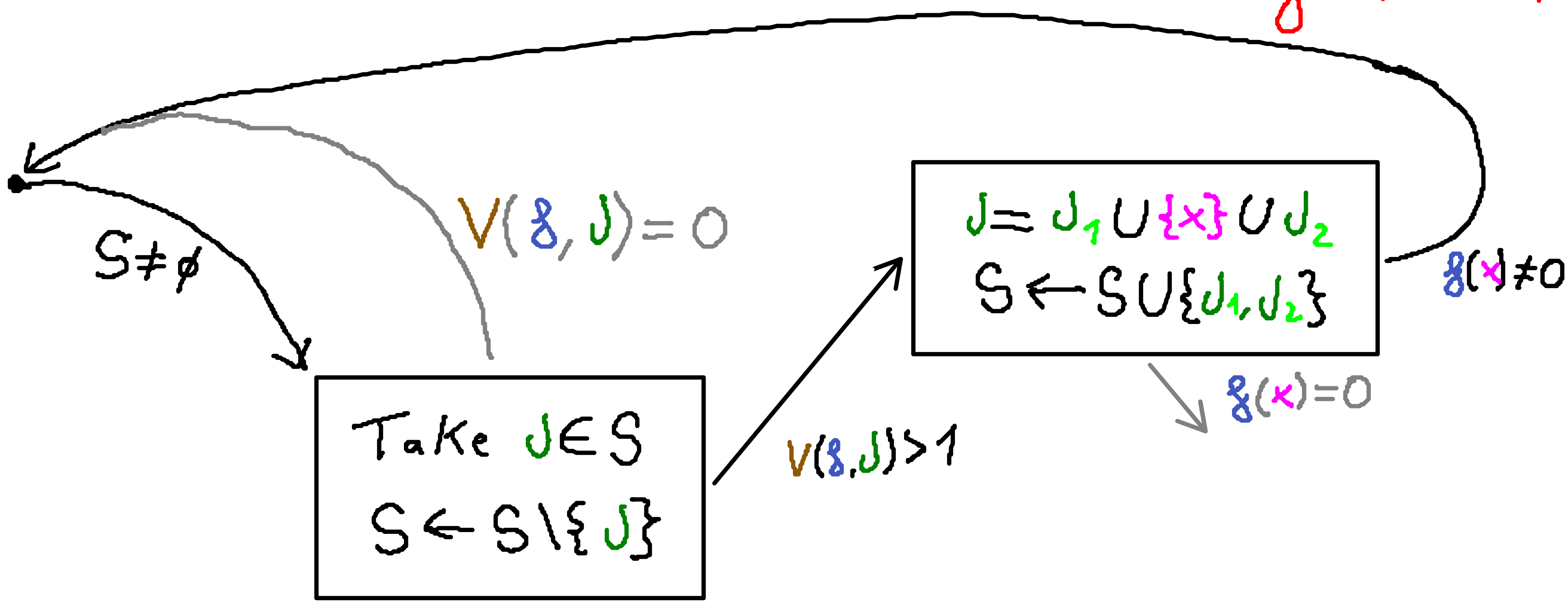


Descartes Solver III:

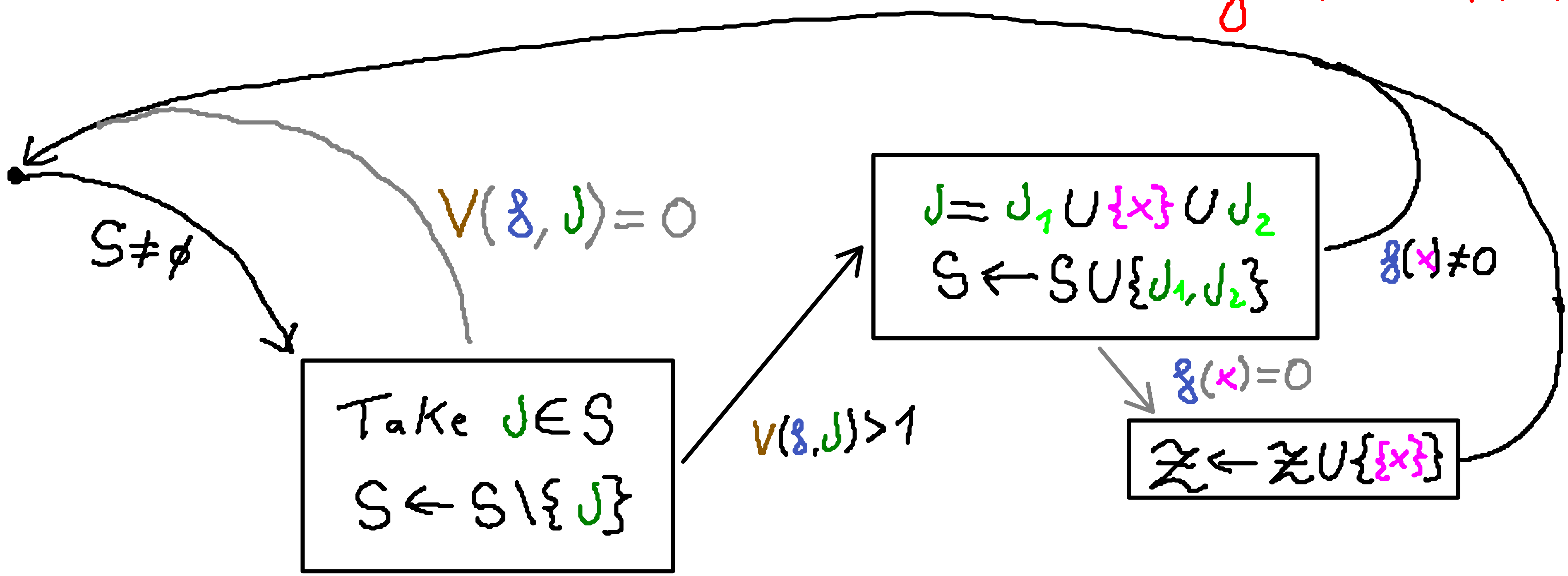
The Algorithm



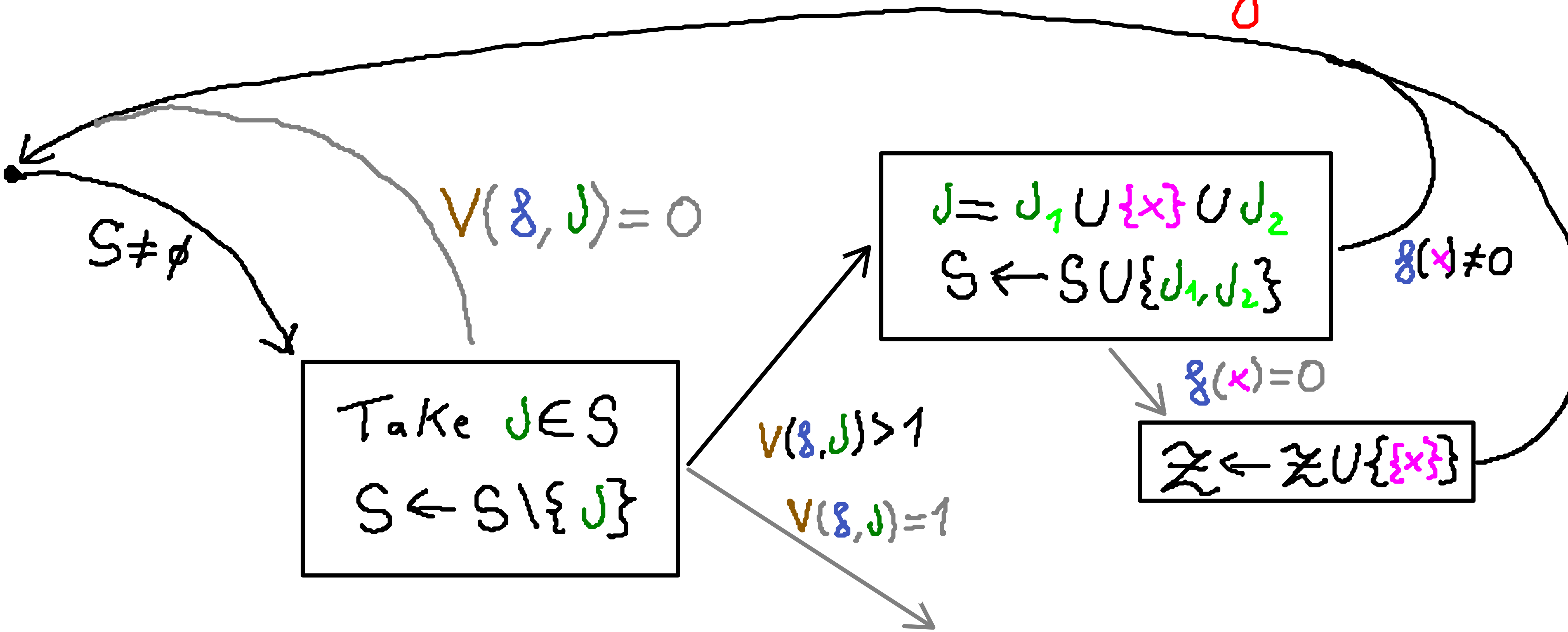
Descartes Solver III: The Algorithm



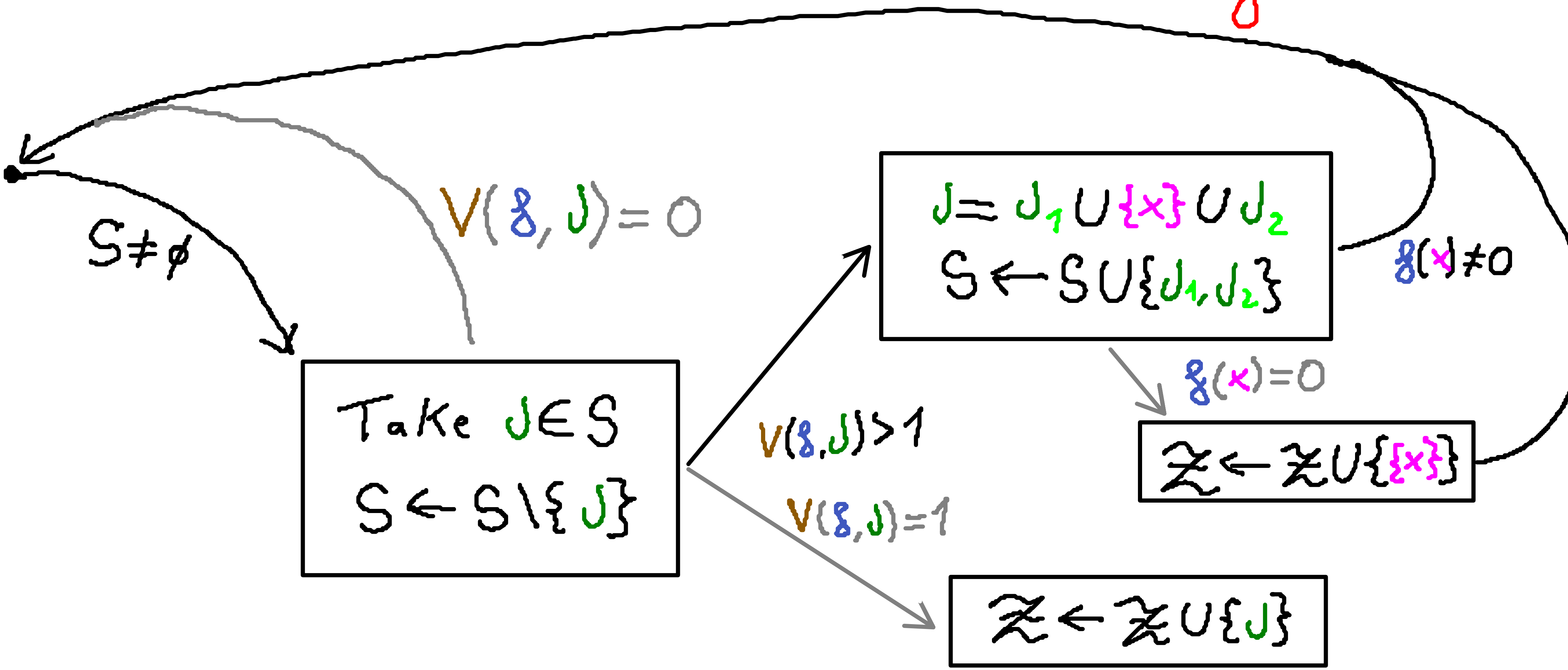
Descartes Solver III: The Algorithm



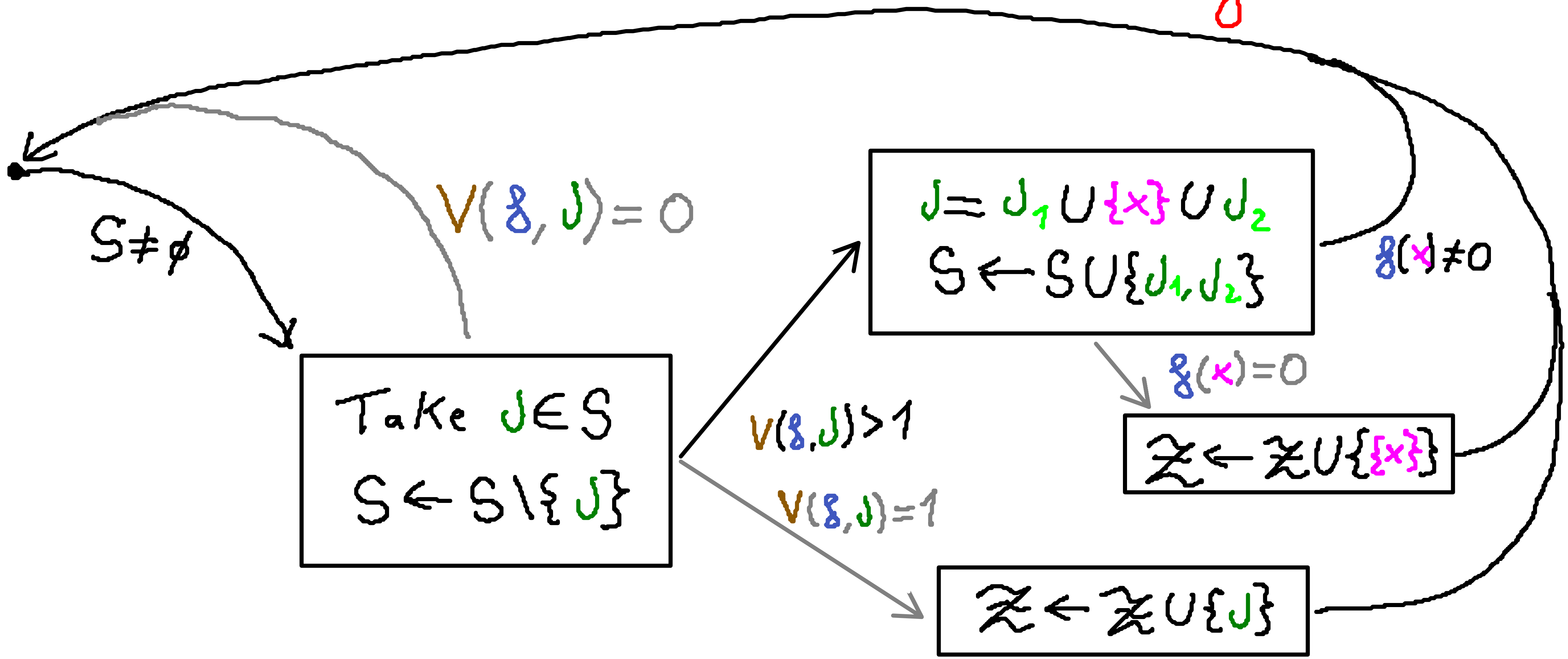
Descartes Solver III: The Algorithm



Descartes Solver II: The Algorithm

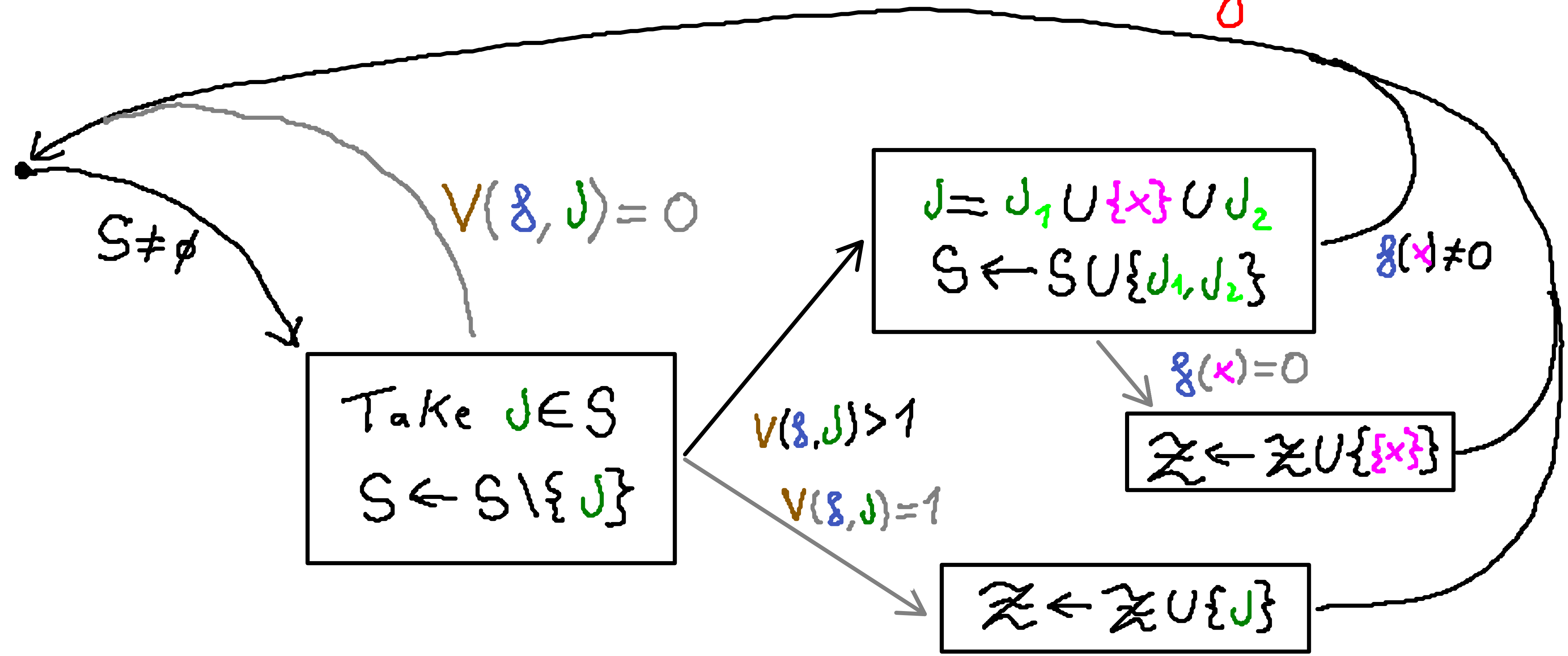


Descartes Solver III: The Algorithm



Descartes Solver III:

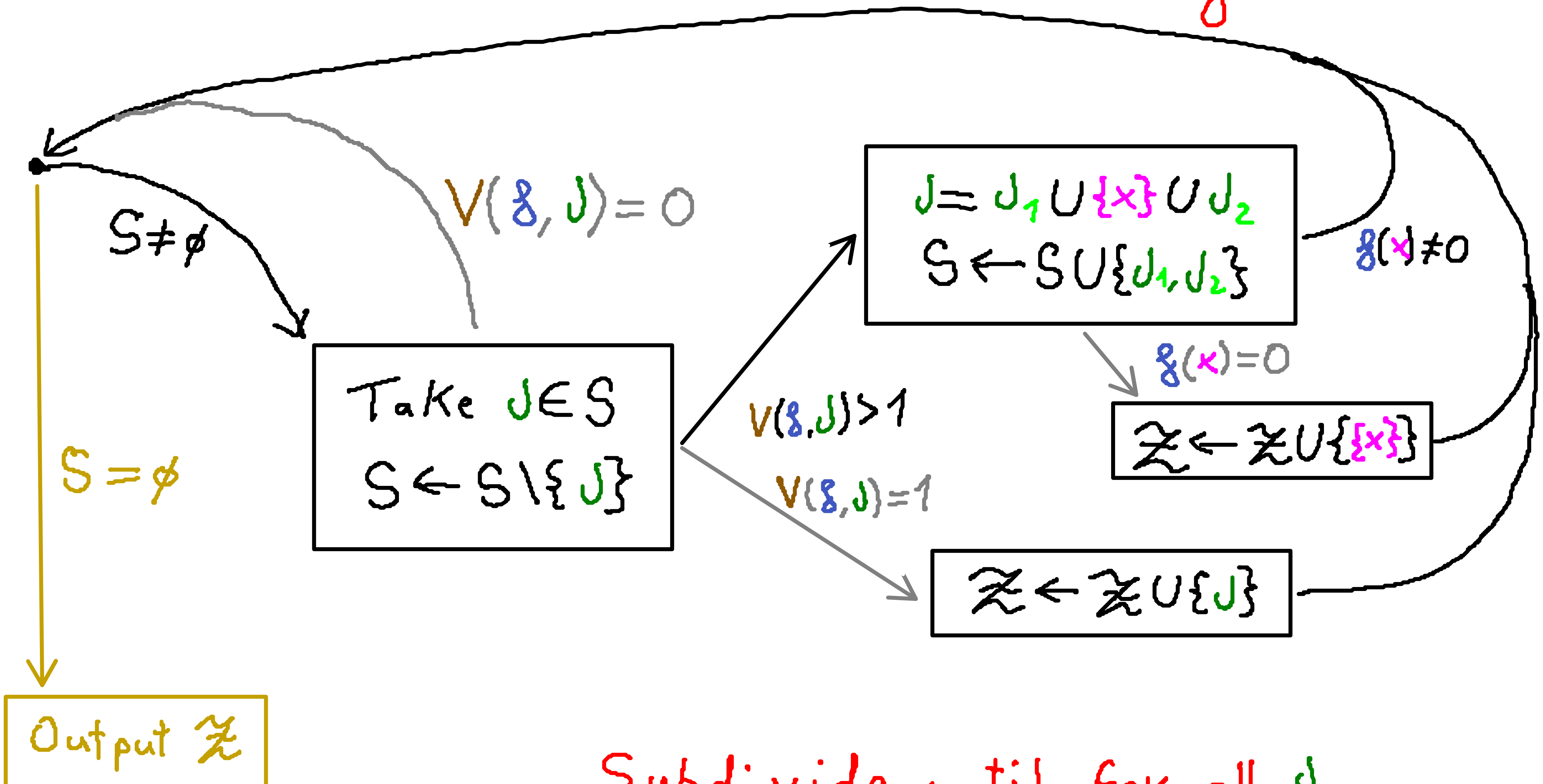
The Algorithm



Subdivide until for all J,

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

Descartes Solver II: The Algorithm



Subdivide until for all J,

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

Real Root Isolation IV:

Are we being pessimistic?

Real Root Isolation IV:
Are we being pessimistic?

Worst-case complexity:

Real Root Isolation IV: Are we being pessimistic?

Worst-case complexity:

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

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

Real Root Isolation IV:

Are we being pessimistic?

Worst-case complexity:

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

Pessimistic in practice

Descartes Solver
seems to behave faster in practice!

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

Real Root Isolation V:
Beyond pessimism

Worst-case complexity:

Real Root Isolation V: Beyond pessimism

Worst-case complexity:

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

Real Root Isolation V: Beyond pessimism

Worst-case complexity:

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

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

(Roughgarden, 2021)

Real Root Isolation V:
Beyond pessimism

Worst-case complexity:

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

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

(Roughgarden, 2021)

Probabilistic complexity

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)

(Roughgarden, 2021)

Probabilistic complexity

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

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)

(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 $\mathfrak{f}$?

Real Root Isolation V: Beyond pessimism

Worst-case complexity:

$$\max\left\{\mathrm{cost}(\mathrm{SOLVER},\mathfrak{f}) \;\middle|\; \text{bit-size}(\mathfrak{f})\leq\tau,\ \deg(\mathfrak{f})\leq d\right\}$$

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

(Roughgarden, 2021)

Probabilistic complexity

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

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

Many choices of randomness 😱

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

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

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

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

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)

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

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

Beyond pessimism II: Random Bit Polynomials

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

Beyond pessimism II: Random Bit Polynomials

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

s.t. f_k independent

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:

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:

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

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:

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:

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

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!

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

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:

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

Beyond pessimism III:

Main Theorem

Main Thm (Ergür, T-C, Tsigaridas)

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

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 $\Rightarrow$ $u(f) = 0$

Beyond pessimism III:

Main Theorem

Main Thm (Ergür, T-C, Tsigaridas)

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

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

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

Beyond pessimism III: MAIN THEOREM

MAIN THM (Ergür, T-C, Tsigaridas)

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

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

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

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

Beyond pessimism III: Main Theorem

Main Thm (Ergür, T-C, Tsigaridas)

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

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

Beyond pessimism IV: Examples of Random Bit Polynomials I

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

Beyond pessimism IV: Examples of Random Bit Polynomials I

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

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

Beyond pessimism IV: Examples of Random Bit Polynomials I

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

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

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

Beyond pessimism IV: Examples of Random Bit Polynomials I

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

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

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

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

Beyond pessimism IV: Examples of Random Bit Polynomials I

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

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

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

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

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

Beyond pessimism IV: Examples of Random Bit Polynomials I

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

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

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

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

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

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

Beyond pessimism V:

Examples of Random Bit Polynomials II

Beyond pessimism V: Examples of Random Bit Polynomials II

- Exact bitsize

Beyond pessimism V: Examples of Random Bit Polynomials II

- Exact bitsize

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

Beyond pessimism V: Examples of Random Bit Polynomials II

- Exact bitsize

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

... 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

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!

Lots of Details
will be Omited

How to bound
the run-time of DESCARTES?

How to bound the run-time of DESCARTES?

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

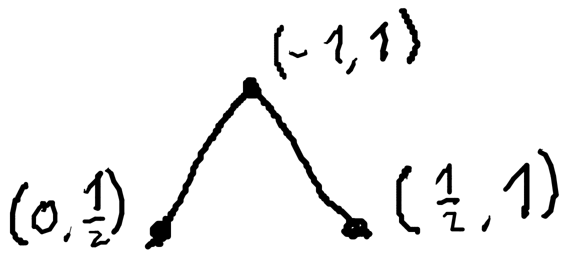
How to bound the run-time of DESCARTES?

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

$\bullet\ (-1,1)$

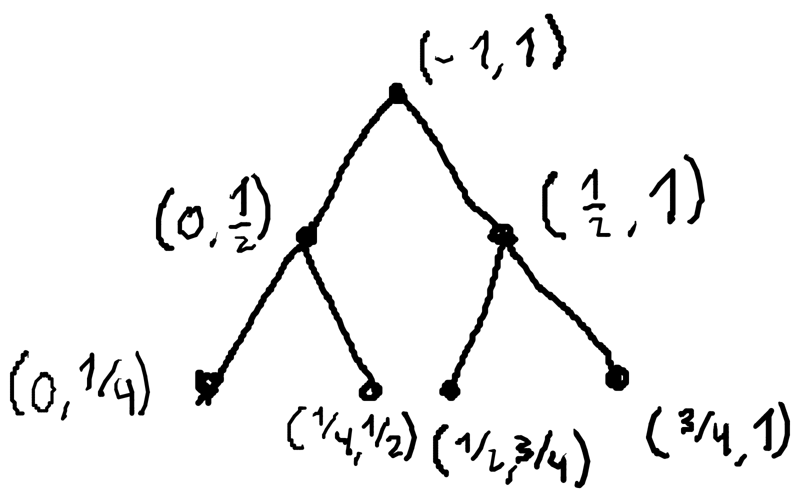
How to bound the run-time of Descartes?

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



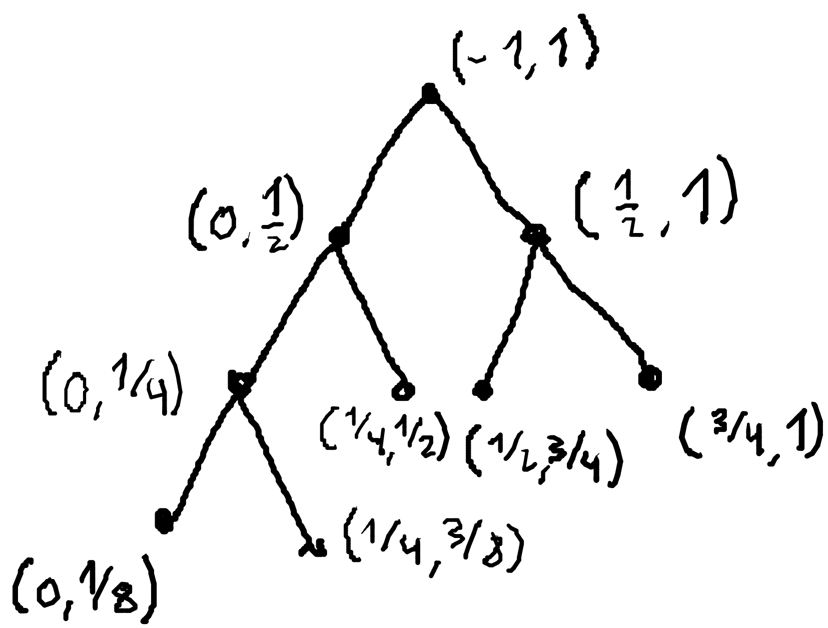
How to bound the run-time of DESCARTES?

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



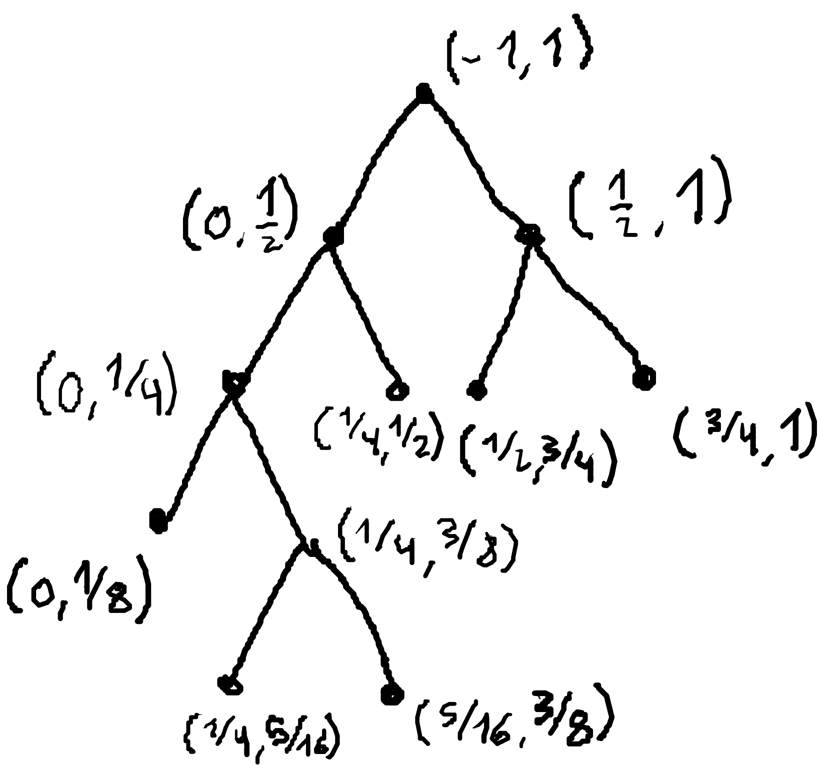
How to bound the run-time of DESCARTES?

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



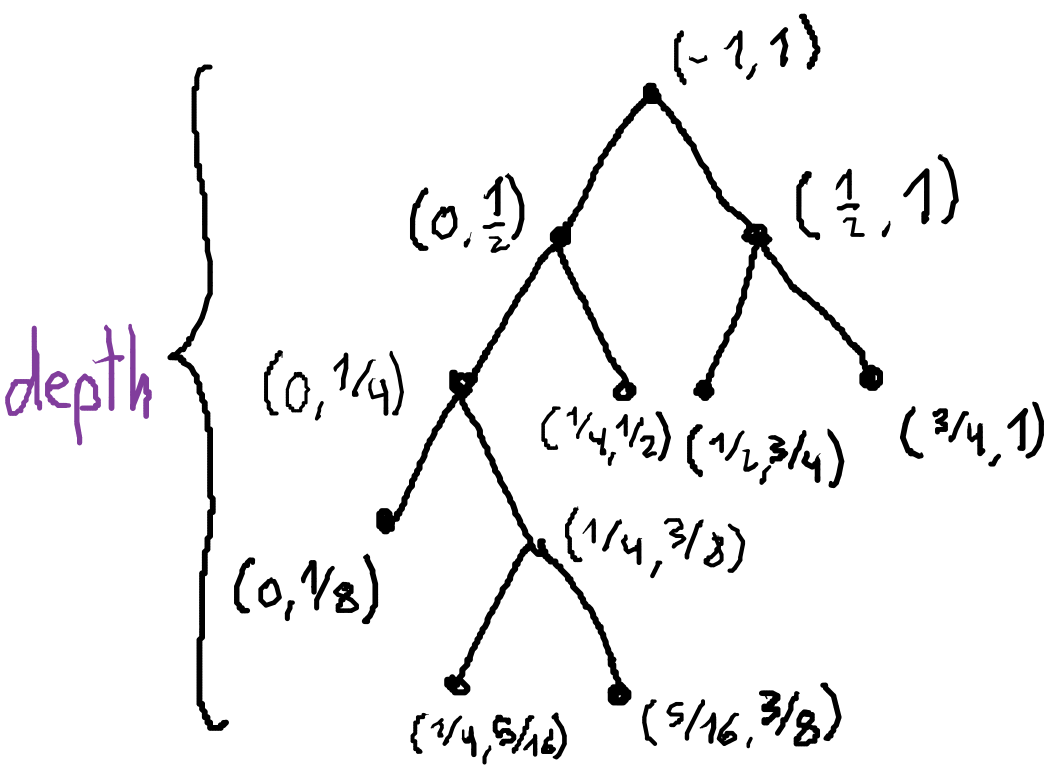
How to bound the run-time of Descartes?

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



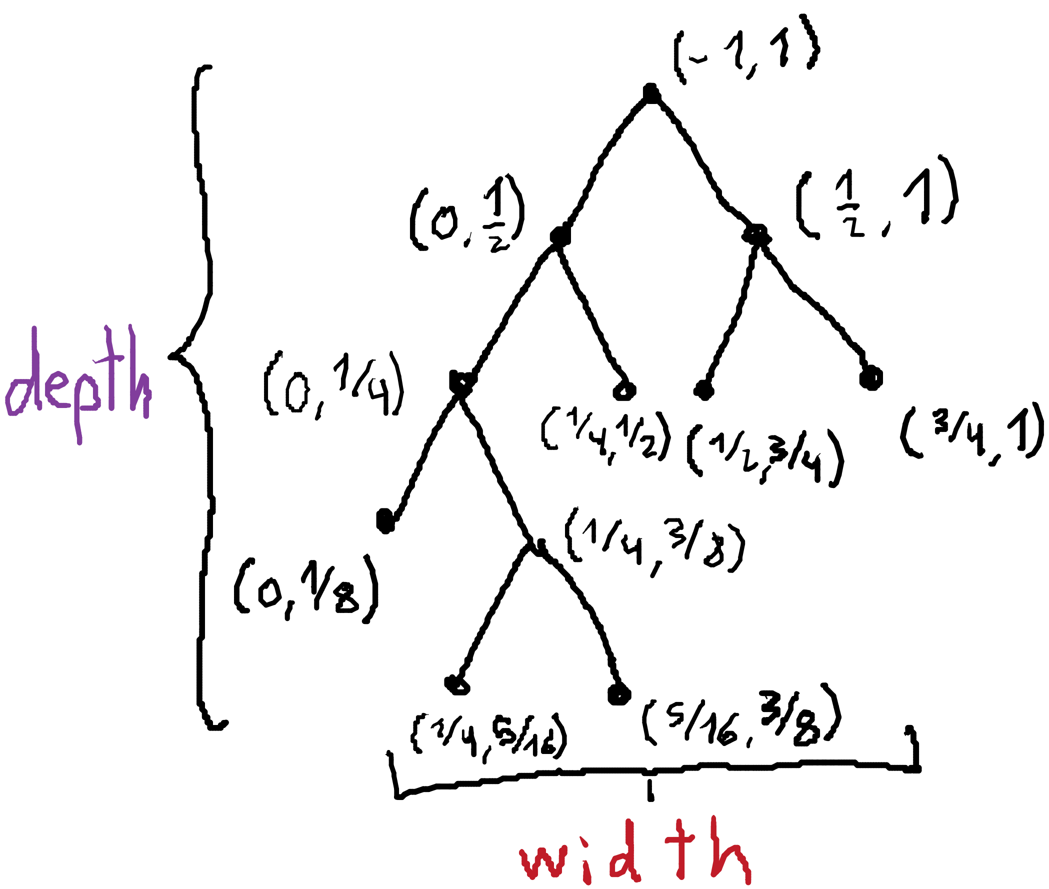
How to bound the run-time of Descartes?

$\Upsilon(g) \leftarrow$ Descartes' Computation Tree



How to bound the run-time of DESCARTES?

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

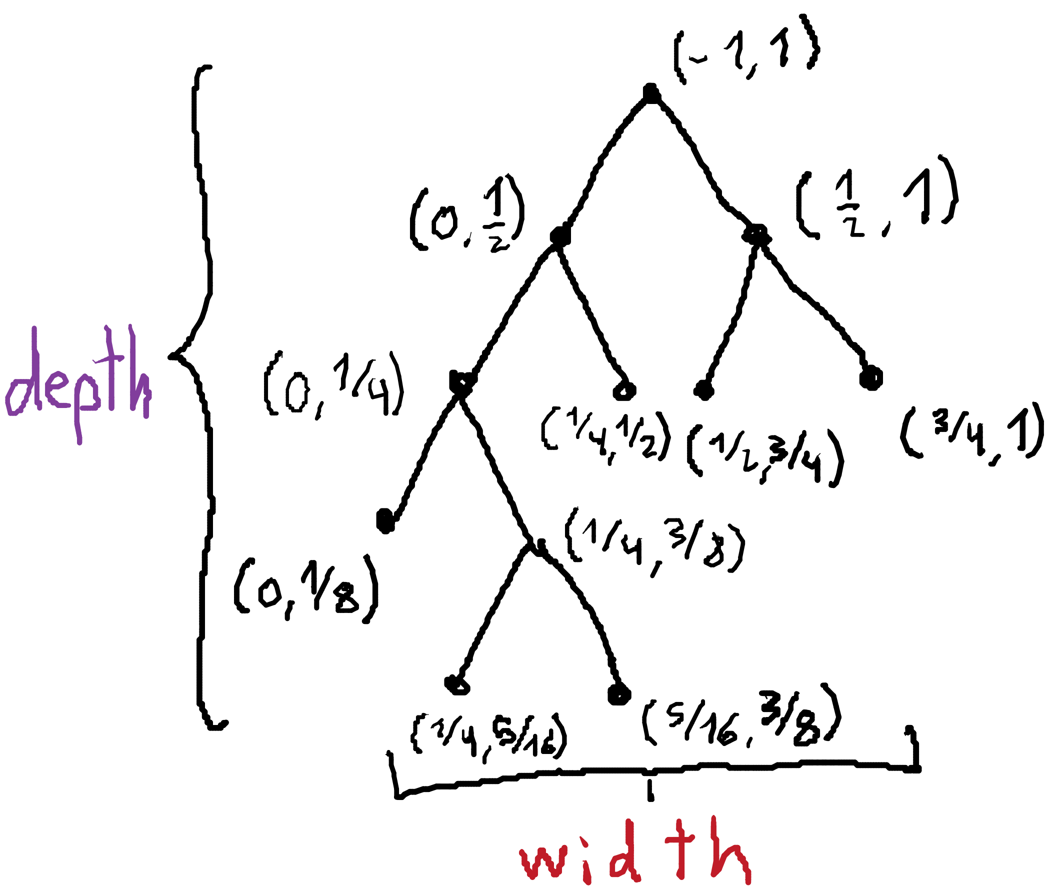


How to bound the run-time of Descartes?

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

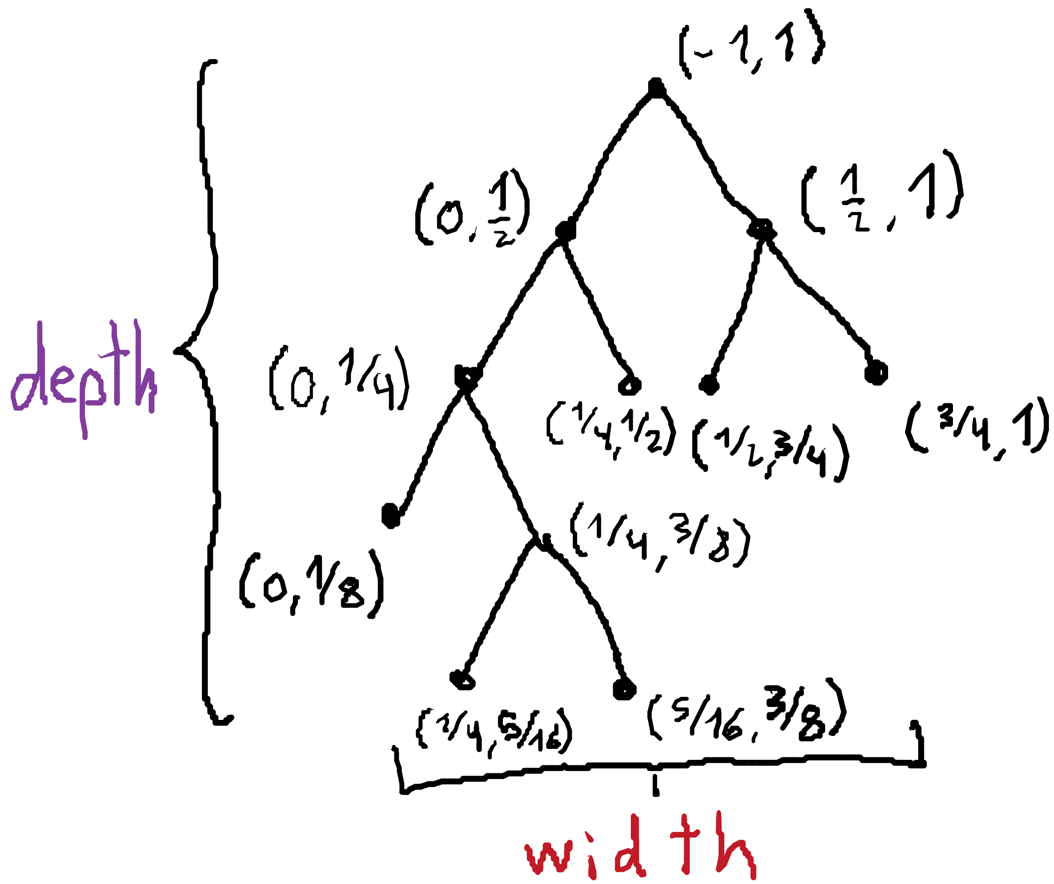
Prop.

$\mathrm{cost}(\text{Descartes}, g)$



How to bound the run-time of Descartes?

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

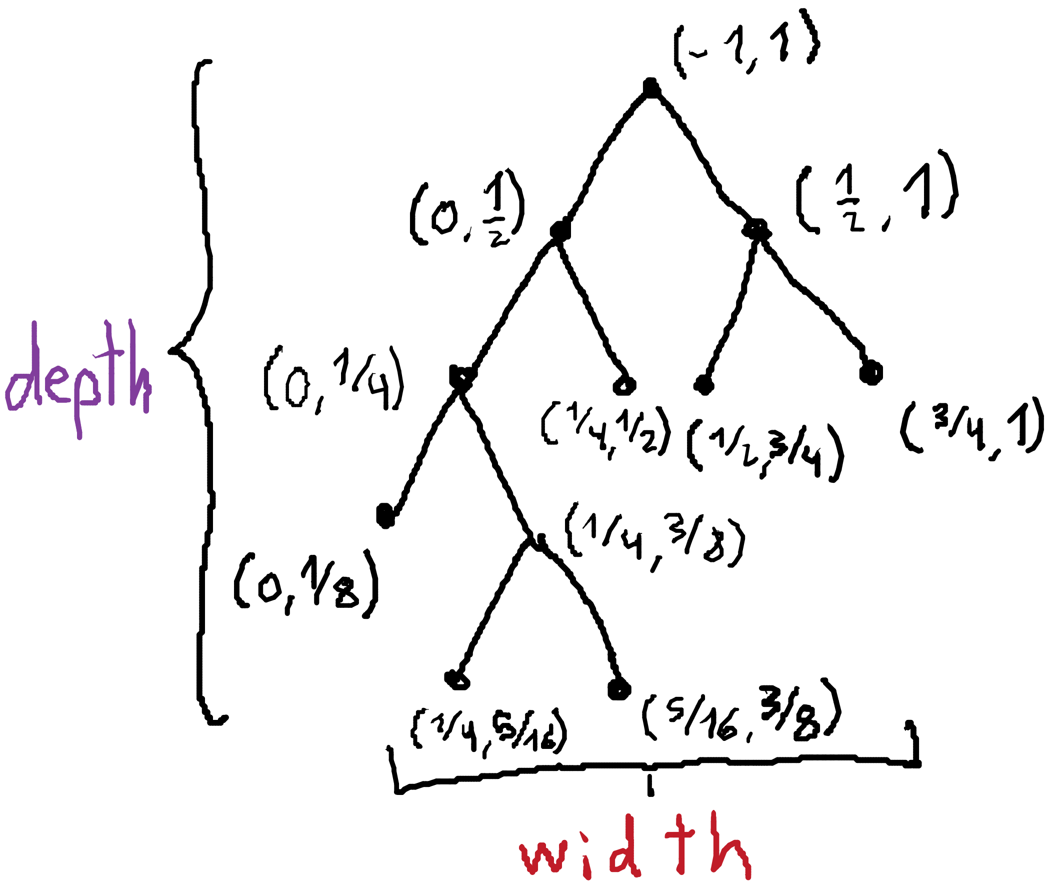


Prop.

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

How to bound the run-time of DESCARTES?

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



Prop.

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

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

The Ingredients of the Analysis I: Condition Number

The Ingredients of the Analysis I: Condition Number

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

The Ingredients of the Analysis I: Condition Number

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

$$C(g) = \infty$$

The Ingredients of the Analysis I: Condition Number

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

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

The Ingredients of the Analysis I: Condition Number

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

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

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

Bounding depth $\Upsilon(g)$

Bounding depth $\Upsilon(\delta)$

PROP.

$$\operatorname{depth} \Upsilon(\delta) \leq 5 + \log d + \log C(\delta)$$

Bounding depth $\Upsilon(g)$

PROP.

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

sep. between complex roots of g nearby $[-1, 1]$

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

PROP.

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

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

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

Prop.

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

sep. between complex roots of g near by $[-1,1]$ $\geq \dfrac{1}{12\, d\, C(g)}$

$$\text{sep.} \geq 1/2^{\operatorname{depth} \mathcal{T}(g)}$$

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

Prop.

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

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

$$\text{sep. between complex roots of } g \text{ near by } [-1,1] \geq 1/2^{\text{depth } \mathcal{T}(g)}$$

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

Bounding depth $\gamma(g)$

Prop.

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

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

$$\text{sep. between complex roots of } g \text{ nearby } [-1,1] \gg 1/2^{\text{depth}\,\gamma(g)}$$

Here no

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

Bounding width $\Upsilon(8)$

Bounding width $\tau(8)$

PROP

width $\tau(8)$

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

Prop

width $\mathcal{T}(g)$

$$\leq \#\text{complex roots of } g \text{ nearby } [-1,1]$$

Bounding width $\gamma(g)$

Prop

width $\gamma(g)$

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

Important for good bound of the RHS!

Bounding $\operatorname{width} \mathcal{T}(g)$

PROP
$\operatorname{width} \mathcal{T}(g)$

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

Important for good bound of the RHS!

Secret tool to bound RHS:

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

The Ingredients of the Analysis II: Cont. Probabilistic Toolbox

We can handle

$C(f)$

for a wide class of random f

The Ingredients of the Analysis II: Cont. Probabilistic Toolbox

We can handle

$C(f)$

for a wide class of random f

as long as continuous distribution

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

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

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

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

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

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. $y_i \sim \mathcal{U}((-1/2, 1/2))$ i.i.d.

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. $y_i \sim \mathcal{U}\left(\left(-\tfrac{1}{2}, \tfrac{1}{2}\right)\right)$ i.i.d.

$\longrightarrow x + y$ continuous random var.

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:

Summing Up:

Descartes' Solver

is almost optimal on average!

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!