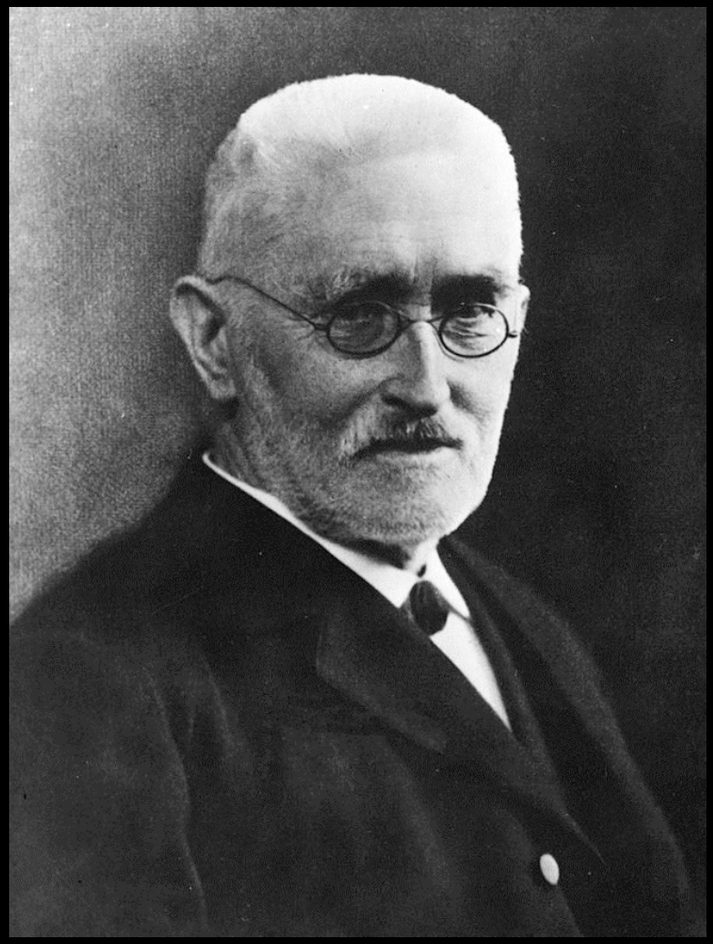
Fact of the Day



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

UTSA 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:

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

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:

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

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

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

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:

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

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	$\tilde{\mathcal{O}}_B(d^4\tau^2)$
Descartes Solver	$\tilde{\mathcal{O}}_B(d^4\tau^2)$
ANewDsc (Sagraloff & Mehlhorn; 2016)	$\tilde{\mathcal{O}}_B(d^3+d^2\tau)$

Real Root Isolation II: The State of the Art

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

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 (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?

Real Root Isolation III:

What do we wish?

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

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

$V(\&) :=$ # sign variations of $\&_0, \&_1, \ldots$

Descartes Solver I: Rule of Signs

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

THM (Descartes' rule of signs)

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

Portrait by Frans Hal
Source: WikiMedia Commons

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

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

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

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

Descartes Solver II:

The Descartes' Oracle

1) Overcounting:

Descartes Solver II:

The Descartes' Oracle

1) Overcounting: $\#Z(\mathcal{S}, J) \leq V(\mathcal{S}, J)$

Descartes Solver II:

The Descartes' Oracle

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

Descartes Solver II:

The Descartes' Oracle

1) Overcounting: $\#Z(\mathcal{S}, J) \leq V(\mathcal{S}, J)$

2) Exactness I: $V(\mathcal{S}, J) \leq 1 \Rightarrow$ Equality

Descartes Solver II:

The Descartes' Oracle

1) Overcounting: $\#Z(\mathcal{S}, J) \leq V(\mathcal{S}, J)$

2) Exactness I: $V(\mathcal{S}, J) \leq 1 \Rightarrow$ Equality

3) Exactness II:

Descartes Solver II:

The Descartes' Oracle

1) Overcounting: $\#Z(\mathfrak{F}, J) \leq V(\mathfrak{F}, J)$

2) Exactness I: $V(\mathfrak{F}, J) \leq 1 \Rightarrow$ Equality

3) Exactness II:

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

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!

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:

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:

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

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:

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

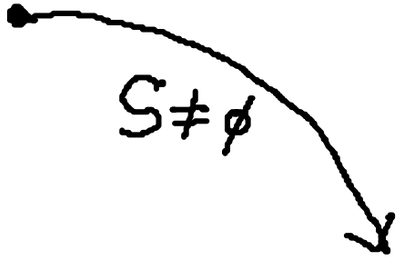
Descartes Solver III:

The Algorithm

•

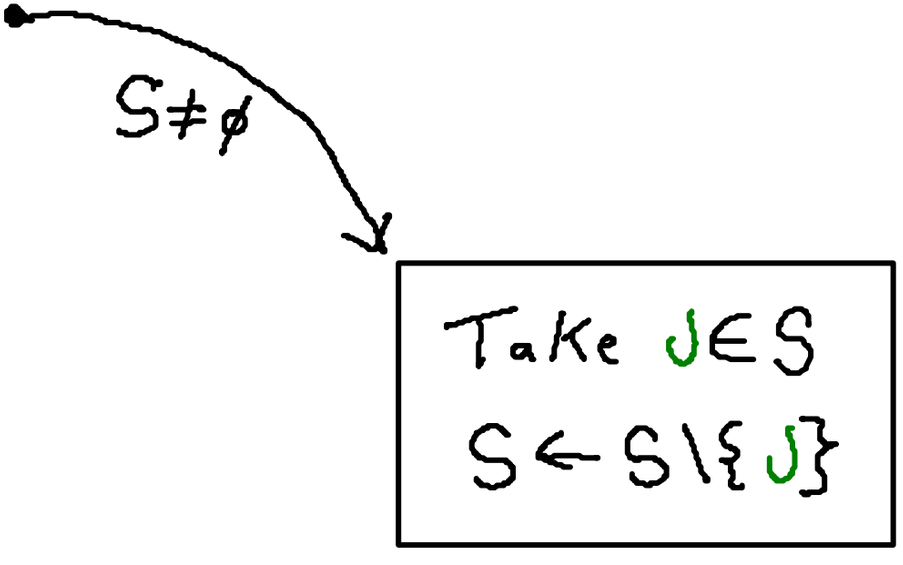
Descartes Solver III:

The Algorithm



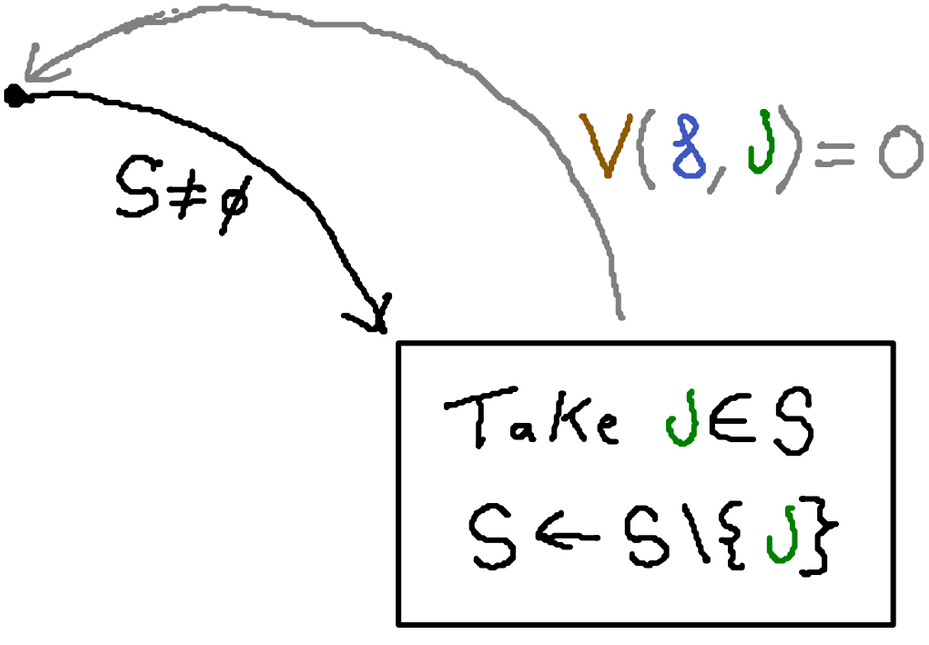
Descartes Solver III:

The Algorithm



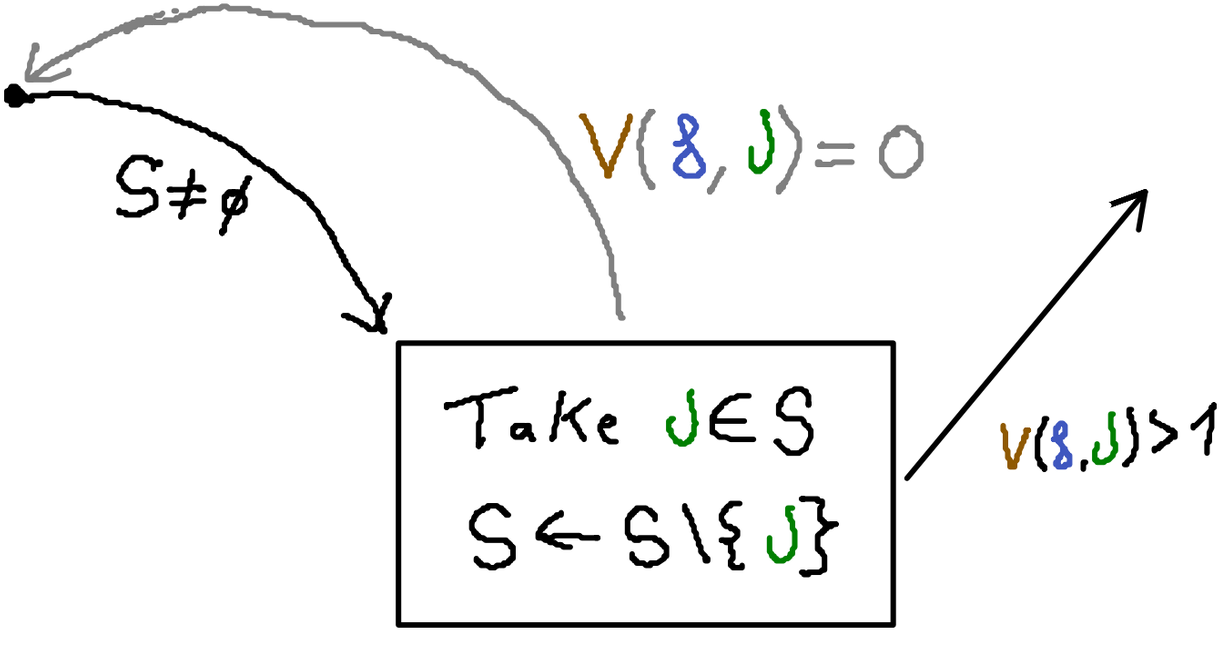
Descartes Solver III:

The Algorithm



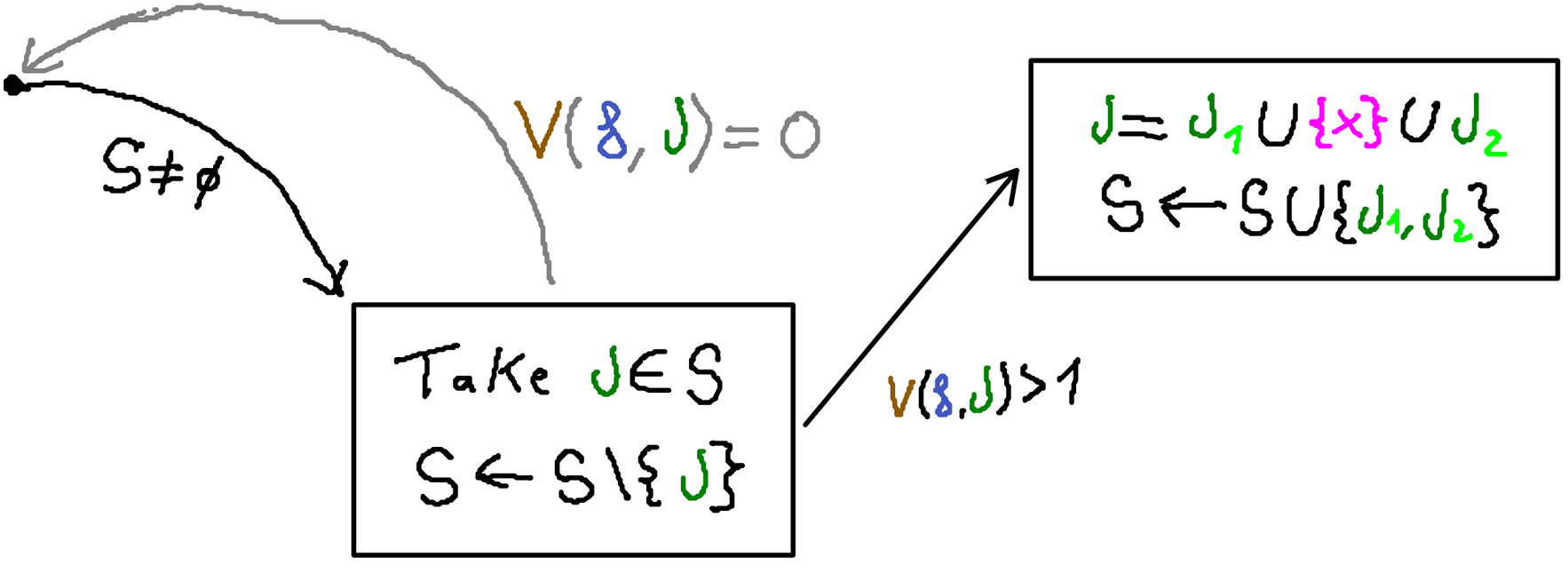
Descartes Solver III:

The Algorithm



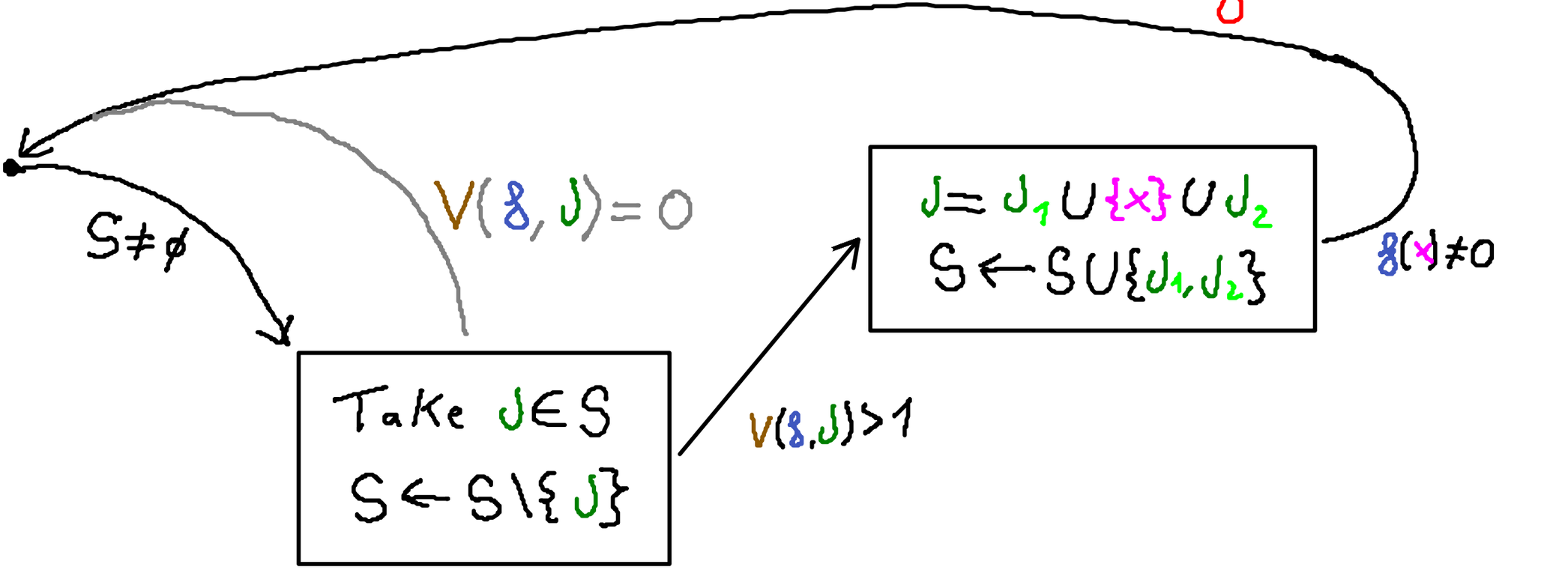
Descartes Solver III:

The Algorithm



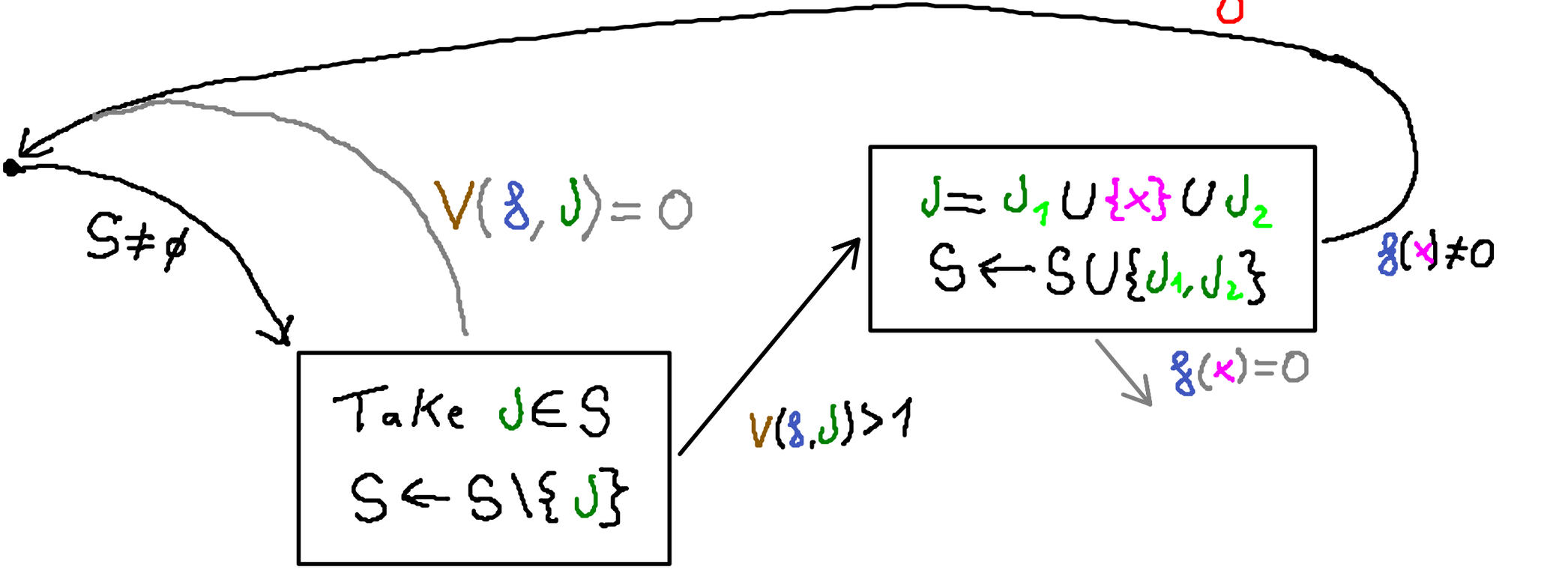
Descartes Solver III:

The Algorithm



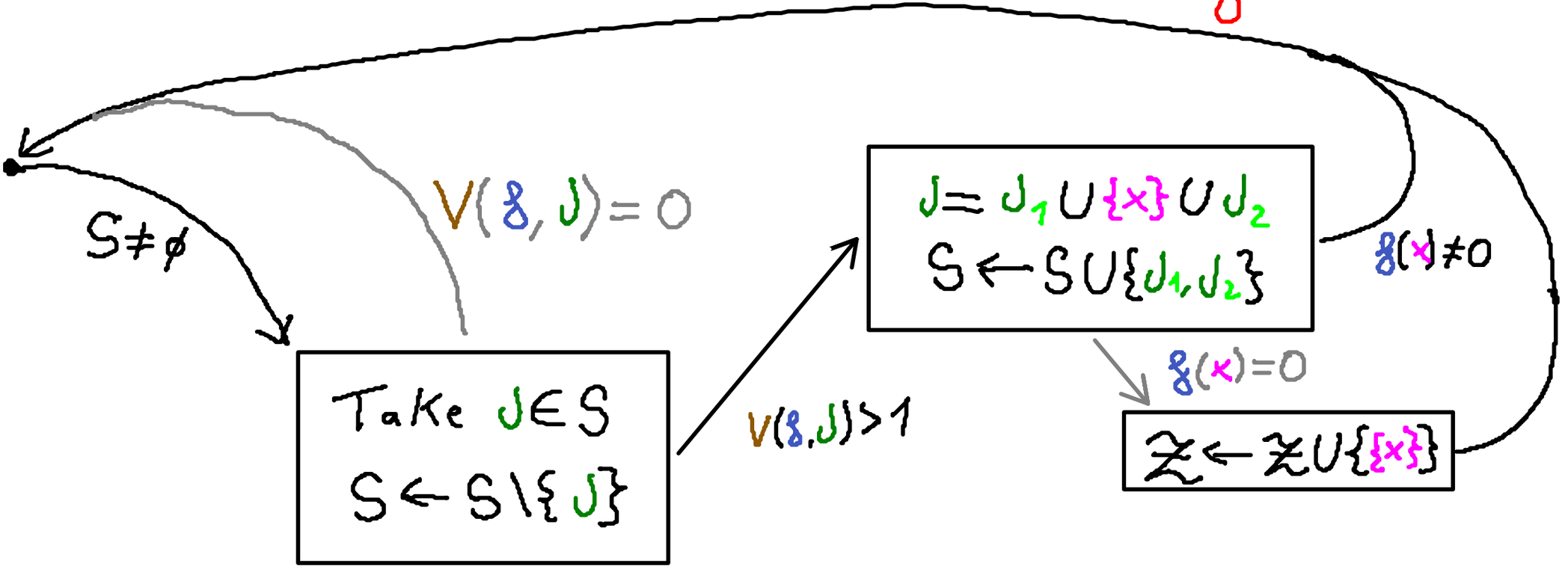
Descartes Solver III:

The Algorithm



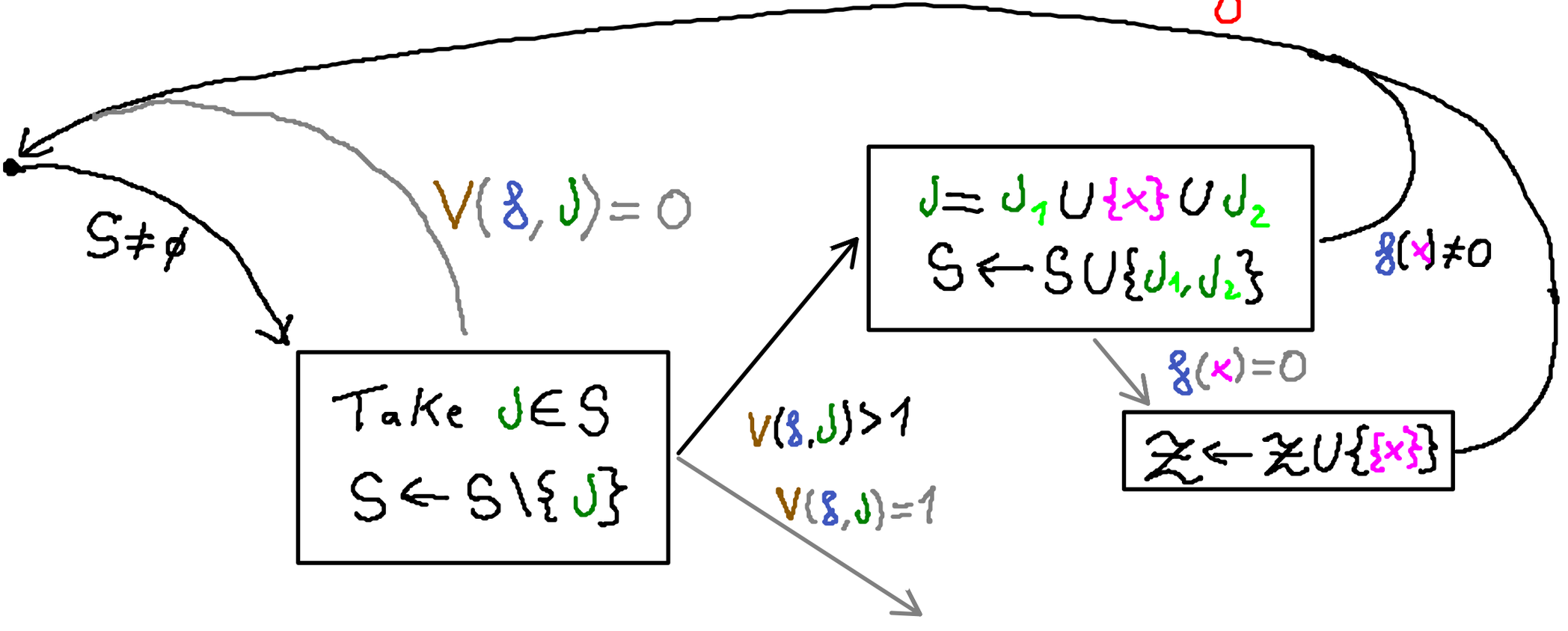
Descartes Solver III:

The Algorithm



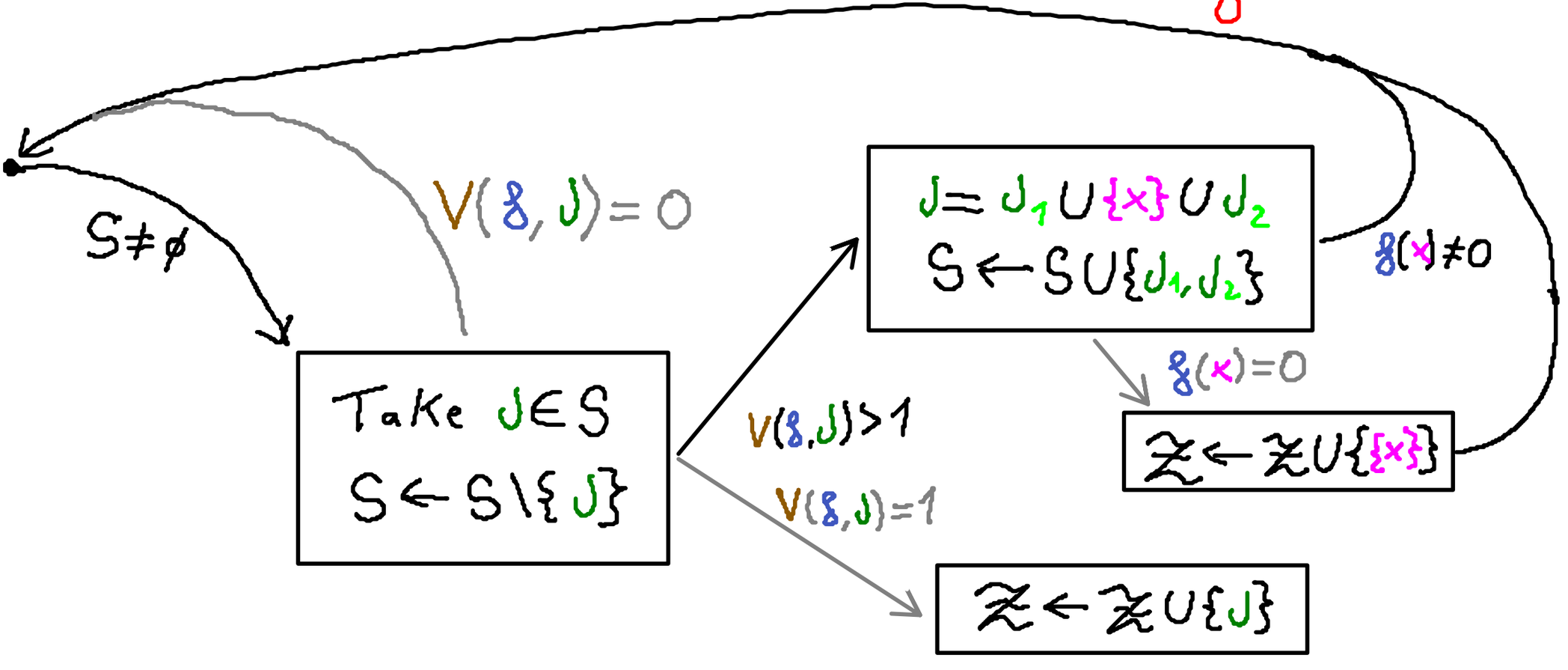
Descartes Solver III:

The Algorithm



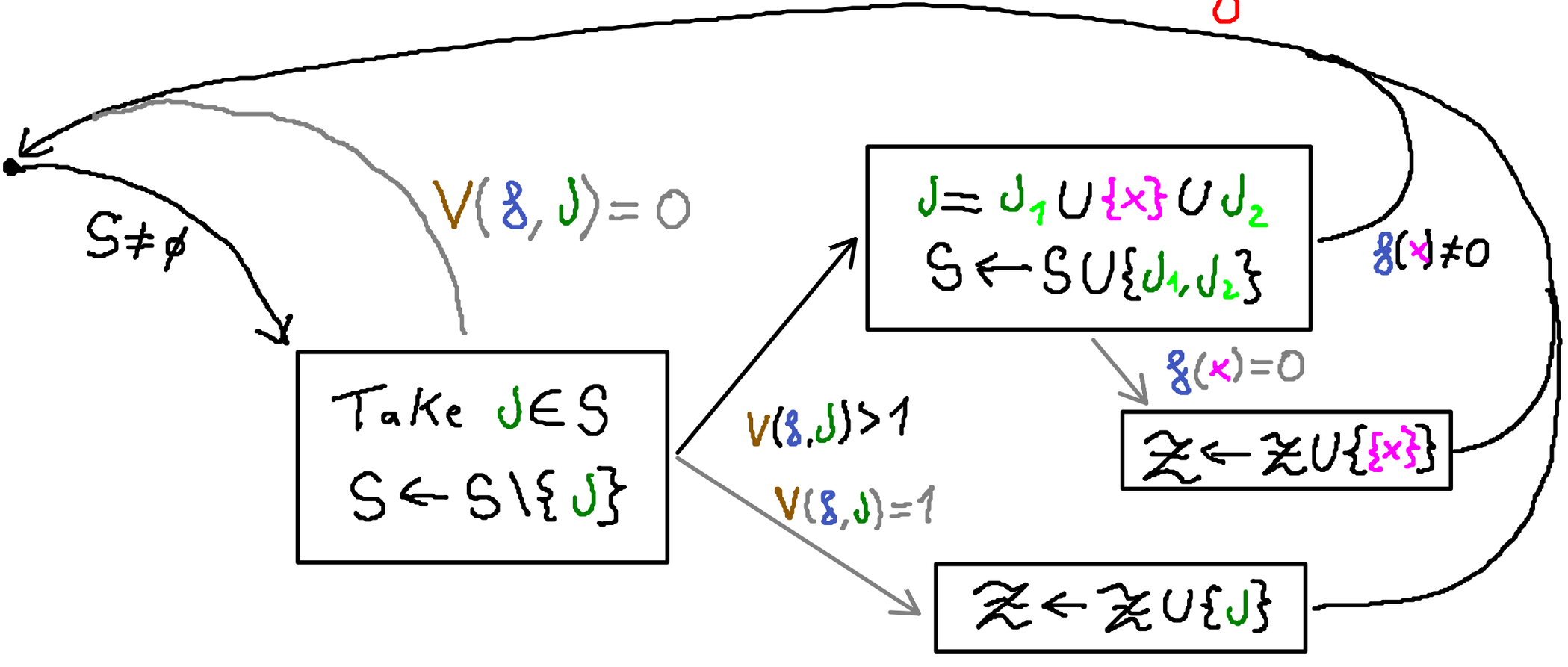
Descartes Solver III:

The Algorithm



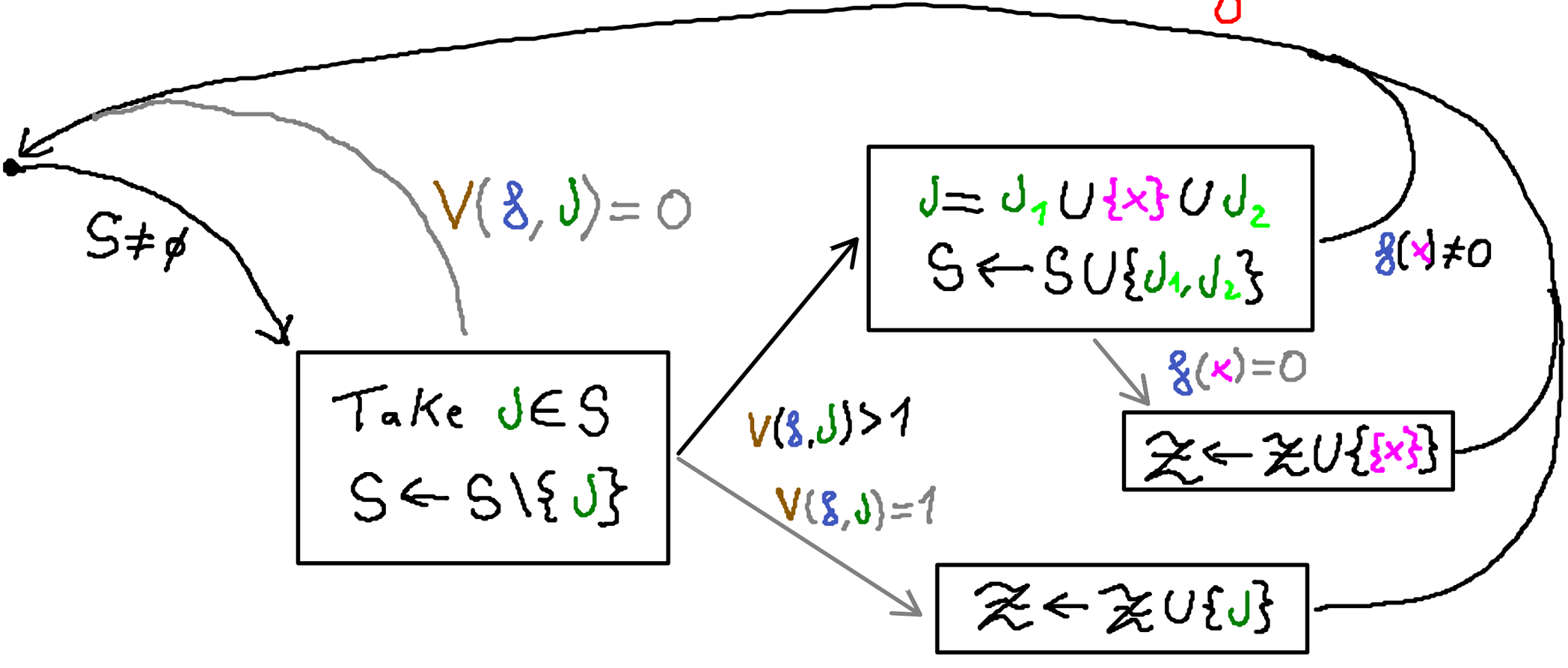
Descartes Solver III:

The Algorithm



Descartes Solver III:

The Algorithm

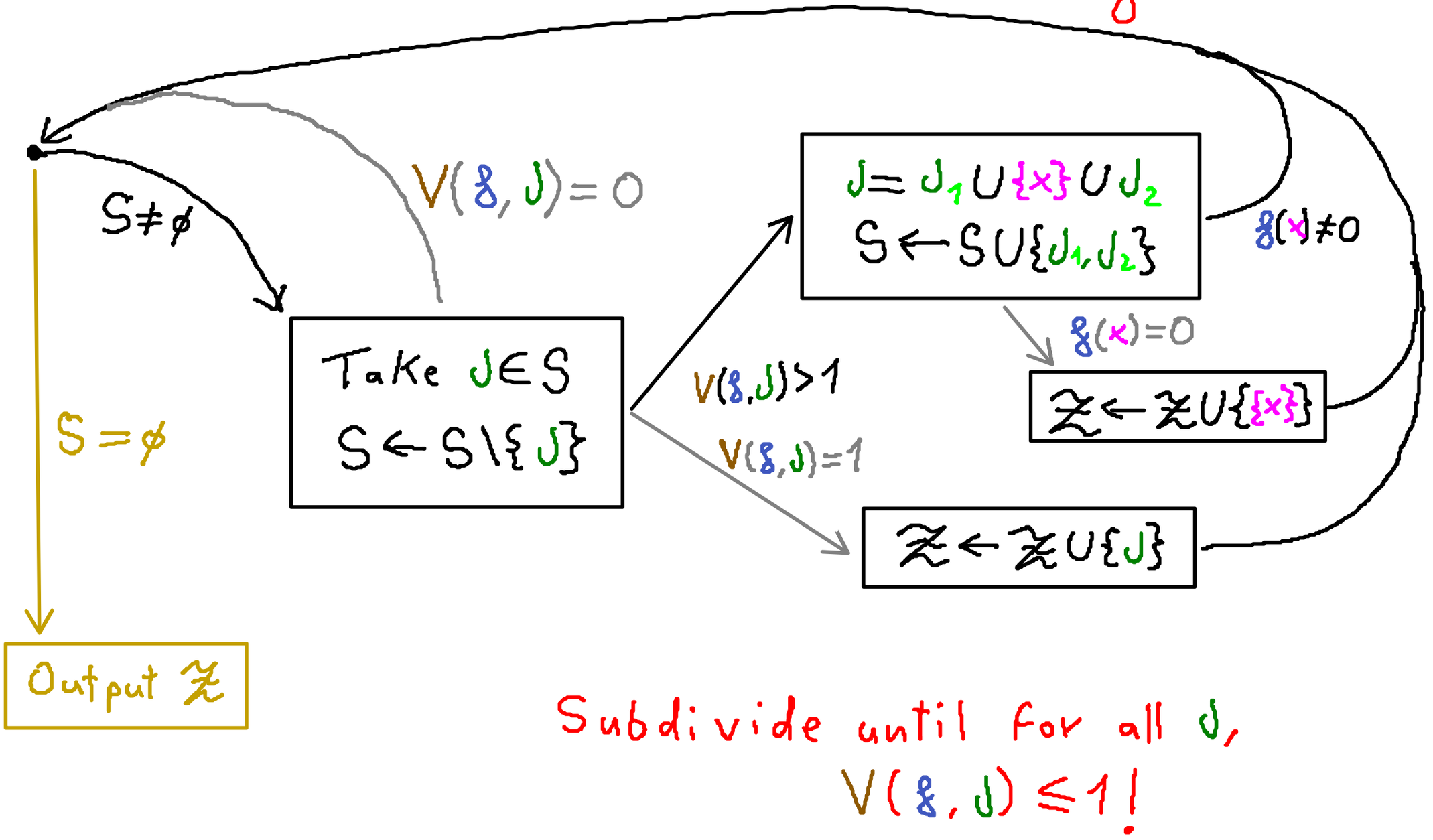


Subdivide until for all J,

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

Descartes Solver III:

The Algorithm



Subdivide until for all J,

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

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:

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

Real Root Isolation IV:

Are we being pessimistic?

Worst-case complexity:

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

↑

Pessimistic in practice

Real Root Isolation IV:

Are we being pessimistic?

Worst-case complexity:

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

↑

Pessimistic in practice

DESCARTES SOLVER seems to behave faster in practice!

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

Real Root Isolation V:

Beyond pessimism

Worst-case complexity:

Real Root Isolation V:

Beyond pessimism

Worst-case complexity:

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

Real Root Isolation V:

Beyond pessimism

Worst-case complexity:

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

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

(Roughgarden, 2021)

Real Root Isolation V:

Beyond pessimism

Worst-case complexity:

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

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

(Roughgarden, 2021)

Probabilistic complexity

Real Root Isolation V:

Beyond pessimism

Worst-case complexity:

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

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

(Roughgarden, 2021)

Probabilistic complexity

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

Real Root Isolation V:

Beyond pessimism

Worst-case complexity:

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

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

(Roughgarden, 2021)

Probabilistic complexity

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

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

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

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

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

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

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

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

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

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

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:

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

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:

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:

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

weight of f:

No middle indexes!

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

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:

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

Beyond pessimism III:

Main Theorem

Main Thm (Ergür, T-C, Tsigaridas)

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

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 $\Rightarrow u(f) = 0$

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, $u(f) = O(1)$

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!

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

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

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

Beyond pessimism IV: Examples of Random Bit Polynomials I

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

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

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

Beyond pessimism IV: Examples of Random Bit Polynomials I

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

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

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

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

Beyond pessimism IV: Examples of Random Bit Polynomials I

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

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

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

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

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

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

Beyond pessimism V: Examples of Random Bit Polynomials II

- Exact bitsize

Beyond pessimism V: Examples of Random Bit Polynomials II

- Exact bitsize

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

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 $u(F) \leqslant \ln 3$

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

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!

LOTS OF DETAILS
WILL BE OMITED

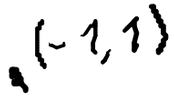
How to bound the run-time of DESCARTES?

How to bound the run-time of DESCARTES?

$\Upsilon(\mathcal{S})$ ← DESCARTES' Computation Tree

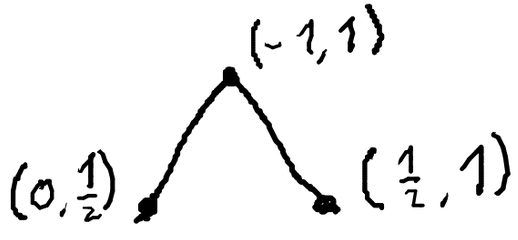
How to bound the run-time of DESCARTES?

$\Upsilon(\mathcal{S}) \leftarrow$ DESCARTES' Computation Tree



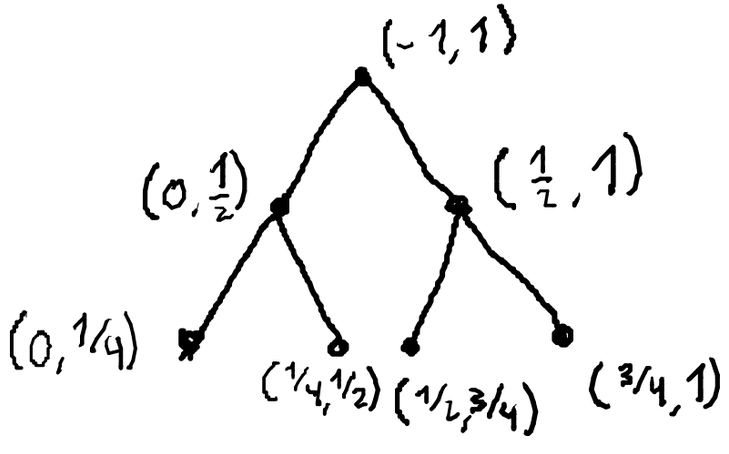
How to bound the run-time of DESCARTES?

$\Upsilon(\mathcal{S}) \leftarrow$ DESCARTES' Computation Tree



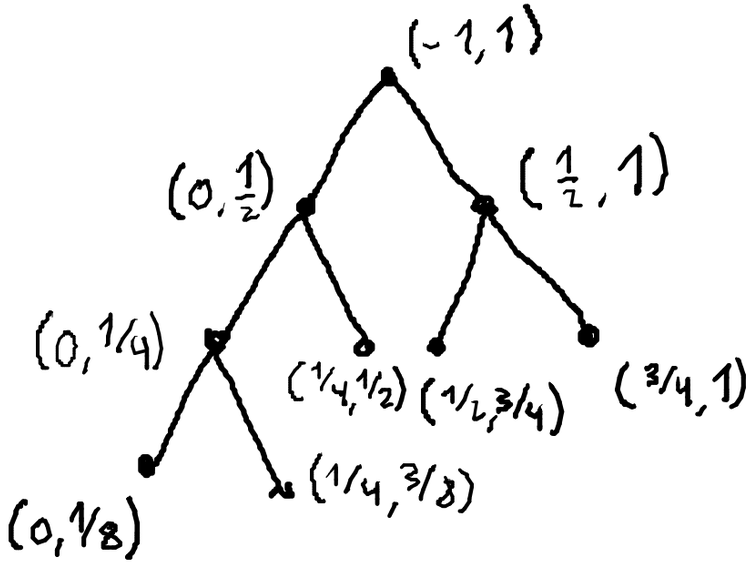
How to bound the run-time of DESCARTES?

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



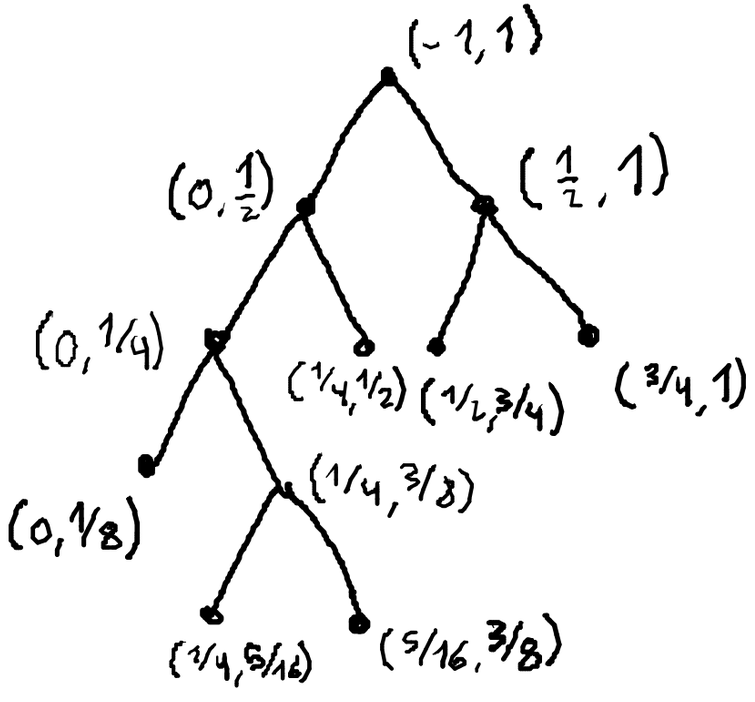
How to bound the run-time of DESCARTES?

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



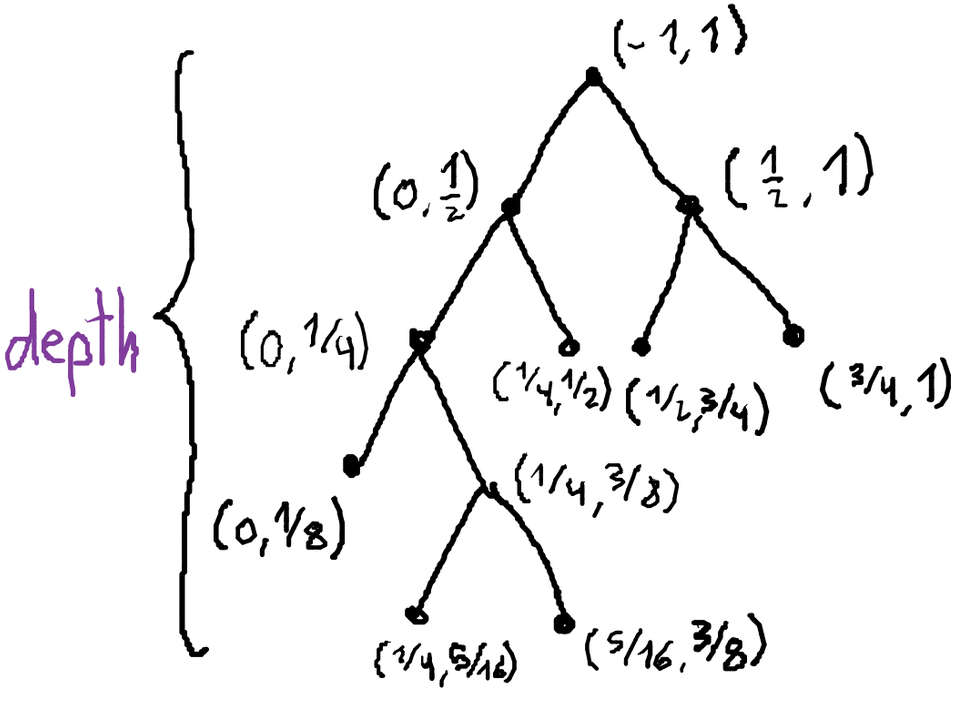
How to bound the run-time of DESCARTES?

$T(8) \leftarrow$ DESCARTES' Computation Tree



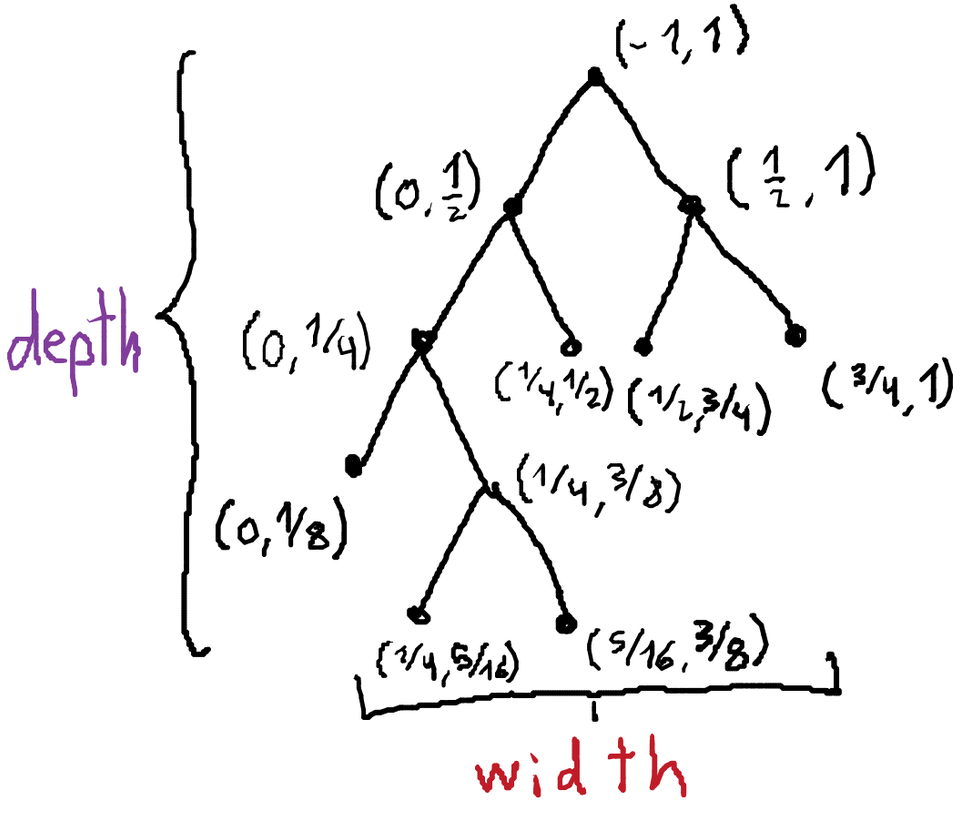
How to bound the run-time of DESCARTES?

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



How to bound the run-time of DESCARTES?

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

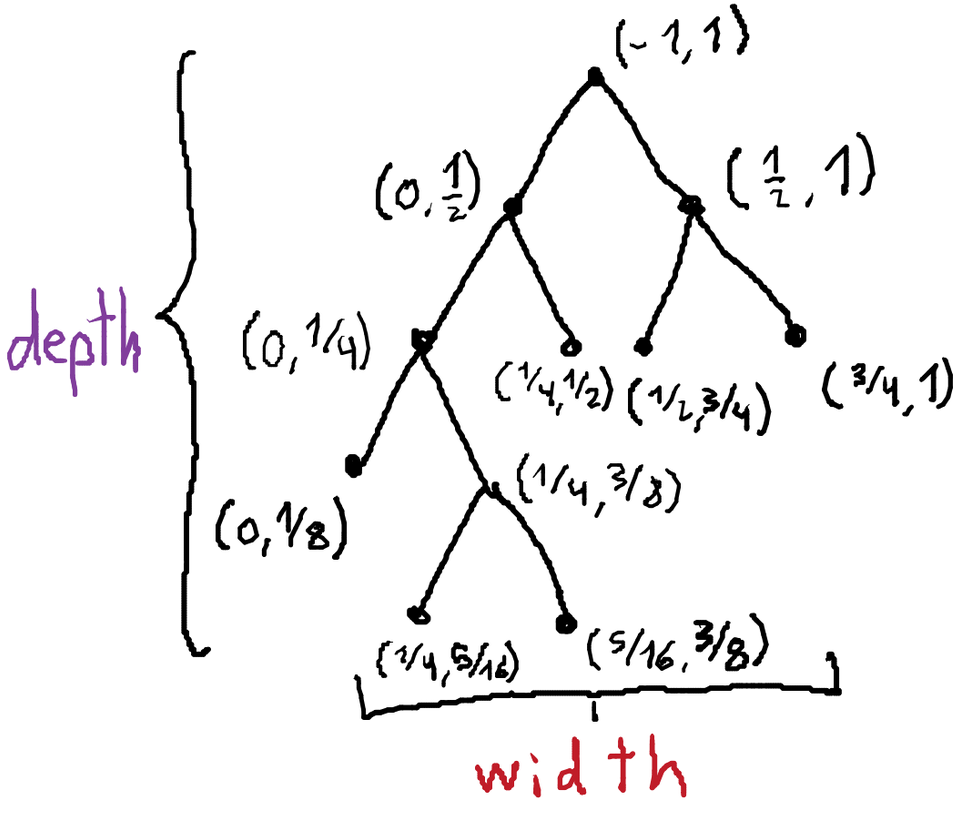


How to bound the run-time of DESCARTES?

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

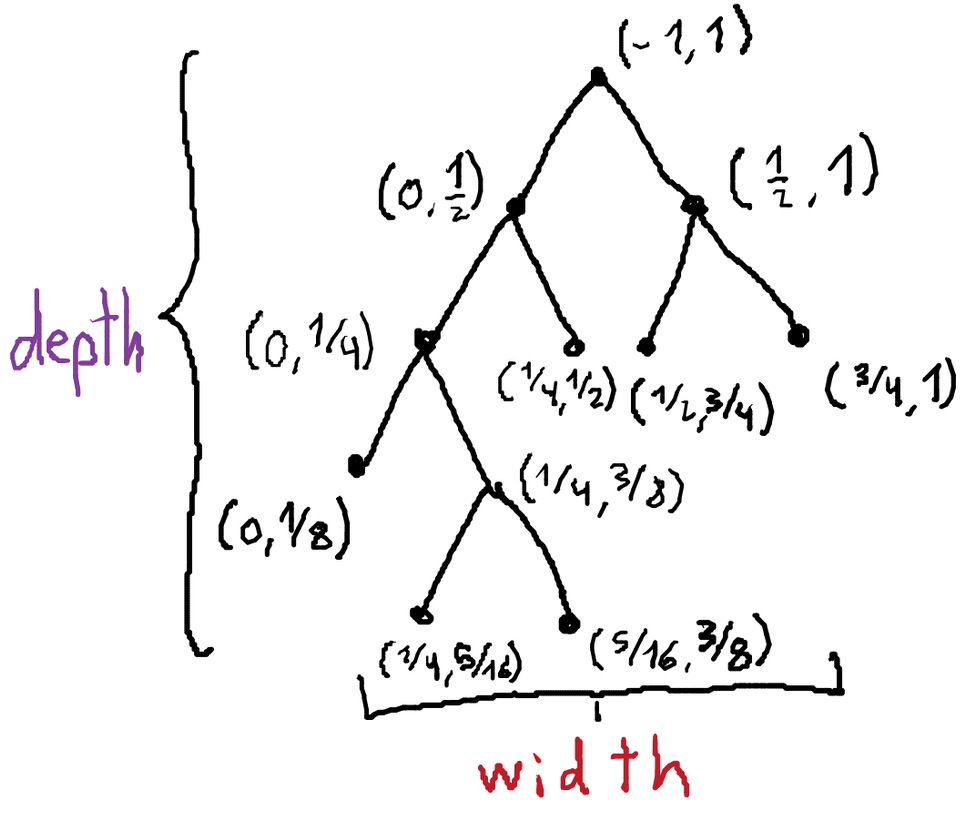
PROP.

cost(DESCARTES, δ)



How to bound the run-time of DESCARTES?

$\mathcal{T}(\mathcal{S})$ ← DESCARTES' Computation Tree

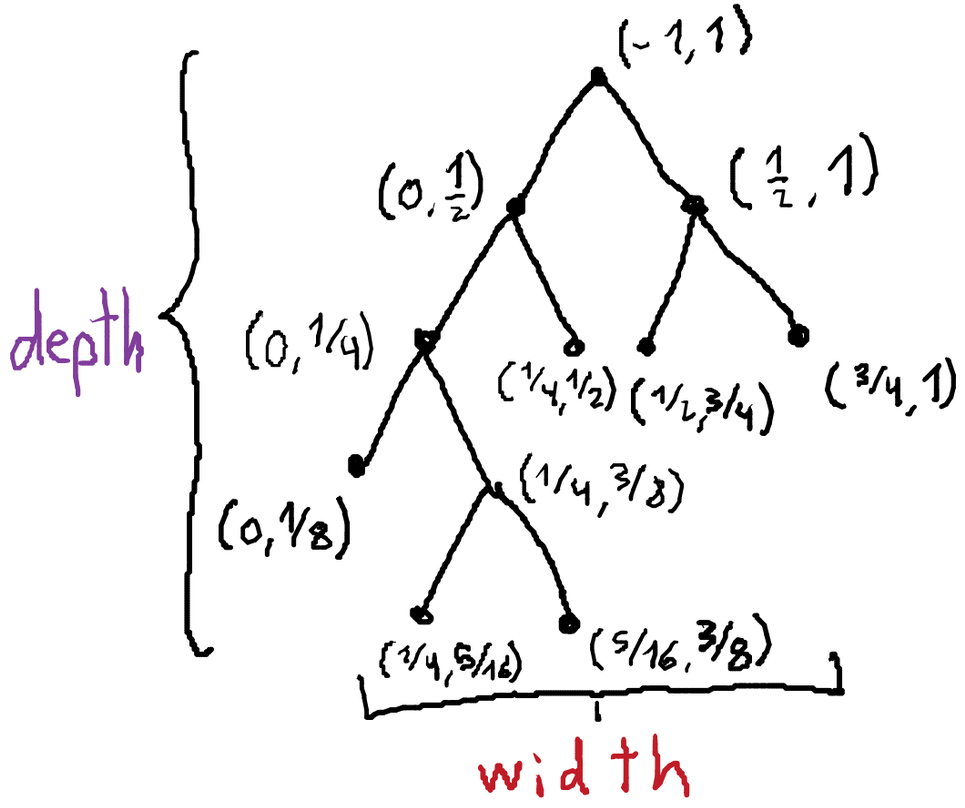


PROP.

$$\text{cost}(\text{DESCARTES}, \mathcal{S}) \;/\!/\; O(d\,\mathrm{width}\,\mathcal{T}(\mathcal{S})\,\mathrm{depth}\,\mathcal{T}(\mathcal{S}) + d^2\,\mathrm{width}\,\mathcal{T}(\mathcal{S})\,\mathrm{depth}^2\,\mathcal{T}(\mathcal{S}))$$

How to bound the run-time of DESCARTES?

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



PROP.

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

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

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

$C(g) = \infty \iff g$ 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 $[-1,1]$

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

Bounding depth $\gamma(g)$

Bounding depth $\gamma(g)$

Prop.

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

Bounding depth $T(g)$

Prop.

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

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

Bounding depth $\gamma(g)$

PROP.

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

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

Bounding depth $\gamma(g)$

PROP.

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

$\uparrow$

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

$\uparrow\uparrow$

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

Bounding depth $\gamma(g)$

Prop.

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

$\uparrow$

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

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

$\wedge\!\wedge$

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

Bounding depth $\gamma(g)$

Prop.

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

$\uparrow$

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

$\uparrow$

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

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

Bounding width $\gamma(8)$

Bounding width $\gamma(\delta)$

PROP

width $\gamma(\delta)$

Bounding width $\gamma(\delta)$

PROP

width $\gamma(\delta)$

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

Bounding width $\gamma(\delta)$

PROP

width $\gamma(\delta)$

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

↑

Important for good bound of the RHS!

Bounding width $\gamma(\delta)$

PROP

width $\gamma(\delta)$

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

↑

Important for good bound of the RHS!

Secret tool to bound RHS:

Bounding width $\gamma(\delta)$

PROP

width $\gamma(\delta) \leq$ # complex roots of δ 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. $y_i \sim \mathcal{U}((-1/2, 1/2))$ 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. $y_i \sim \mathcal{U}((-1/2, 1/2))$ 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!