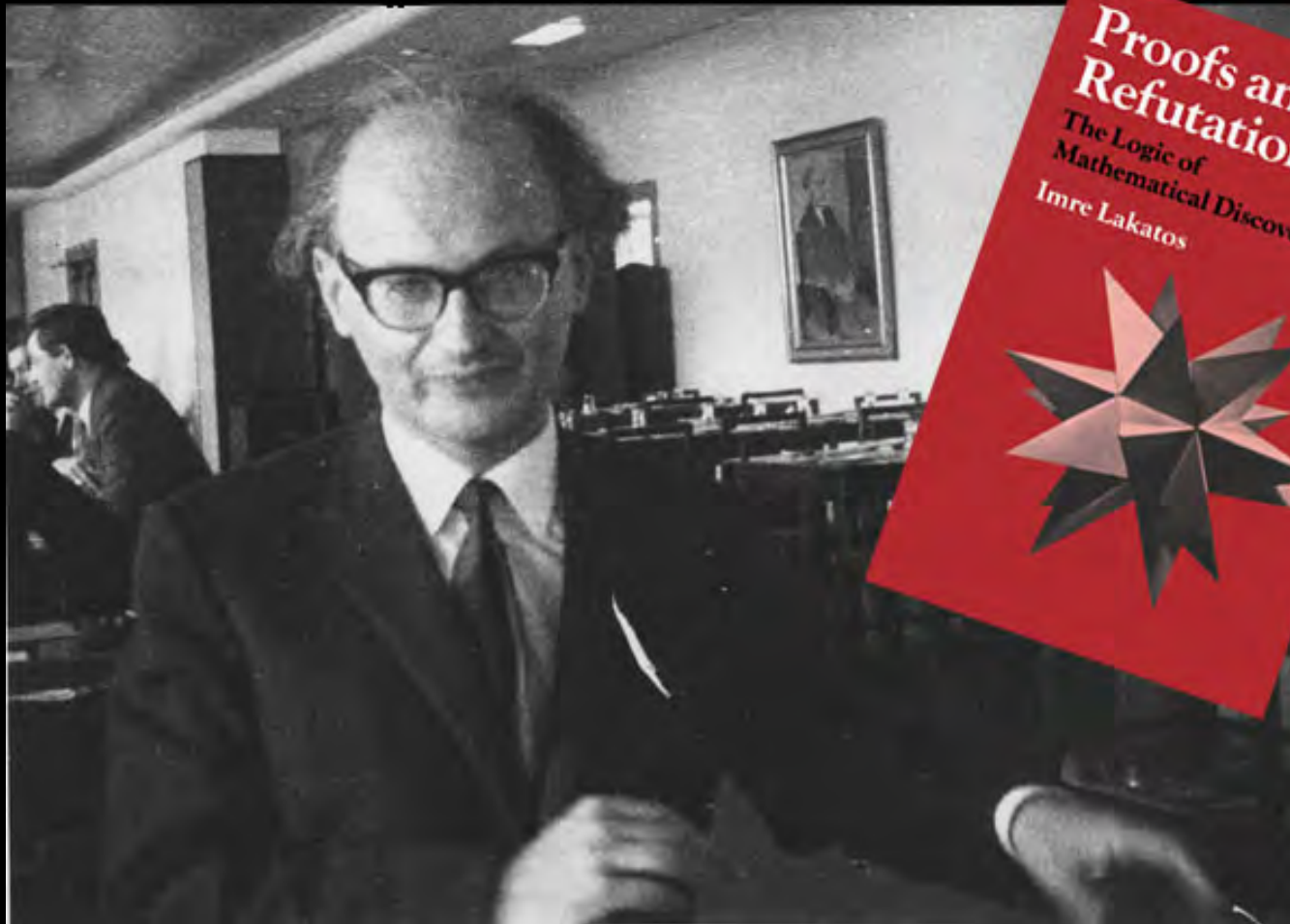


FACT OF THE DAY

Source: LSU library



Fundamental text in philosophy of math!

Today, November 9, the philosopher **Imre Lakatos** was born 100 years ago

slides available at:

https://tonellicueto.xyz/pdf/4BYMAT_slides.pdf

Average
Almost-Optimality
of DESCARTES Solver

Alperen A.
ERGÜR

Josué
TONELLI-CUETO

Elias
TSIGARIDAS
Inria



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

n : bit-size of coefficients of f

MEASURE OF RUN-TIME

Bit complexity

Real Root Isolation II:

The State of the Art

STURM SOLVER

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

DESCARTES SOLVER

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

ANewDsc

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

(Sagraloff & Mehlhorn; 2016)

PAN'S ALGORITHM

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

(Pan; 2002)

Q: Can we beat the champion?

Real Root Isolation III:

What do we wish?

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

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, \dots

THM (Descartes' rule of signs)

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

Moreover,

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

COR

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

\uparrow
 $(0, \infty) \rightarrow (a, b)$
bijection



Portrait by Frans Hals
Source: Wikimedia Commons

DESCARTES SOLVER II:

The Descartes' Oracle

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

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

3) Exactness II:

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

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

4) Subadditivity:

$$\dot{\cup} J_i \subseteq J \Rightarrow \sum V(\delta, J_i) \leq V(\delta, J)$$

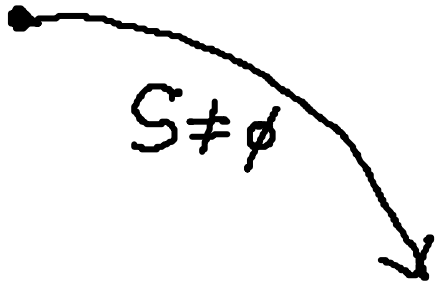
DESCARTES SOLVER III:

The Algorithm

•

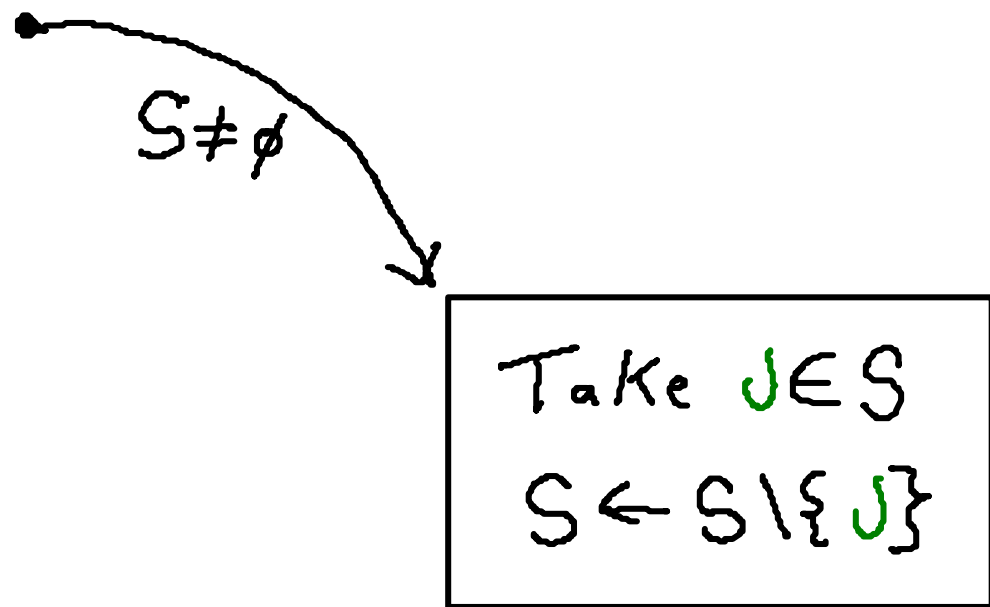
DESCARTES SOLVER III:

The Algorithm



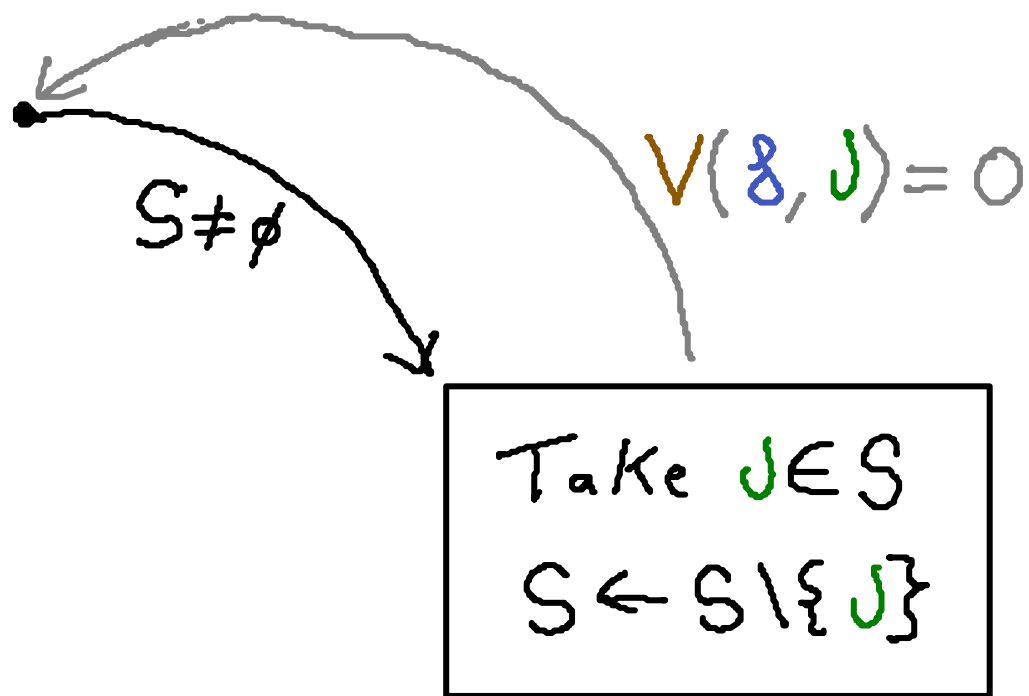
DESCARTES SOLVER III:

The Algorithm



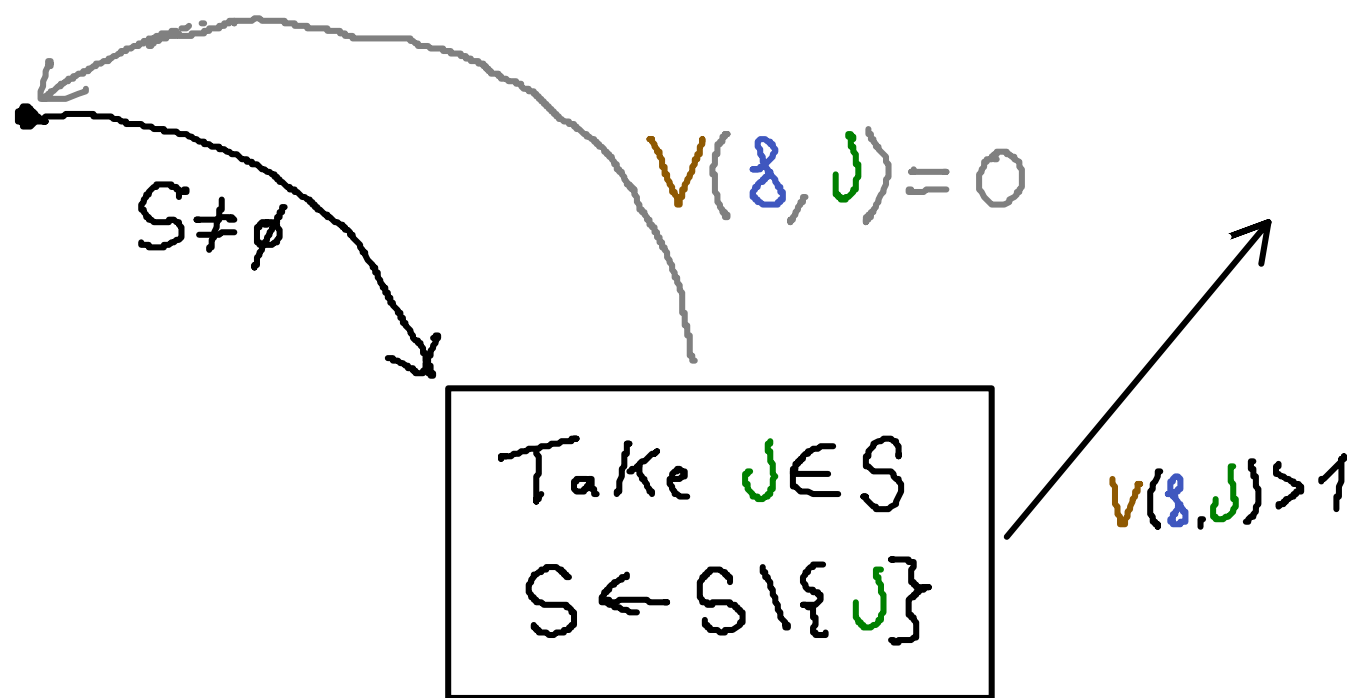
DESCARTES SOLVER III:

The Algorithm



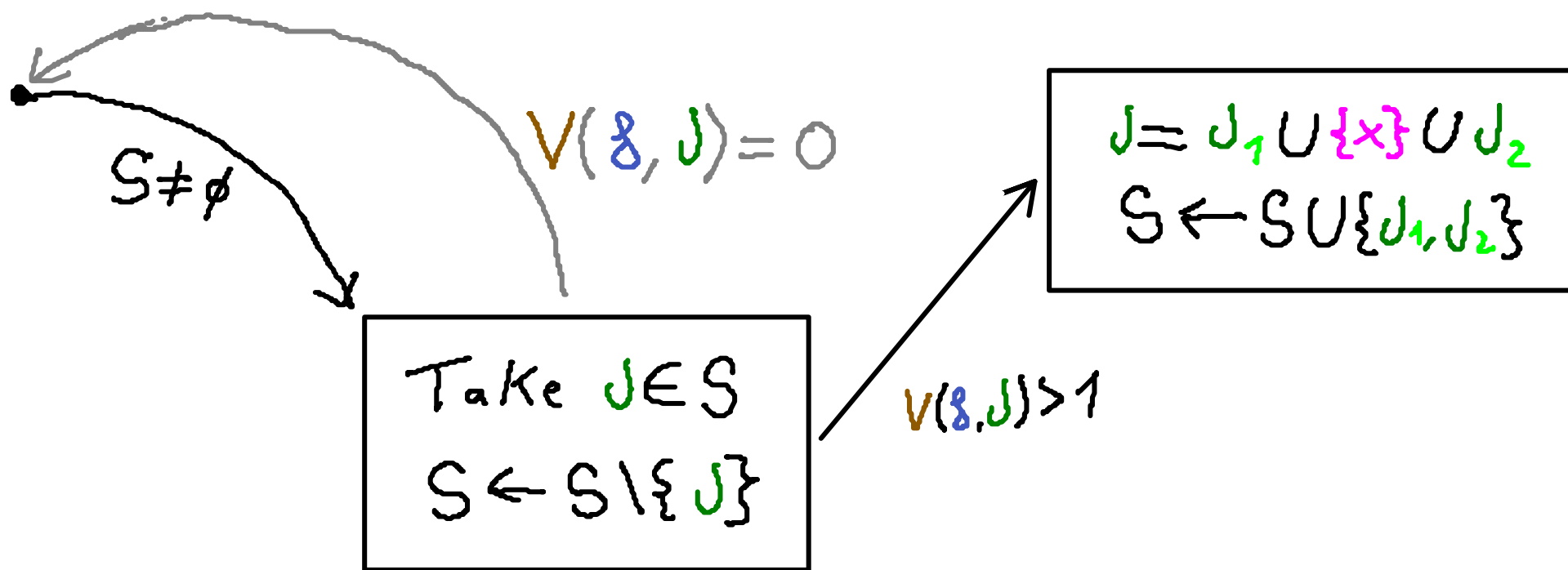
DESCARTES SOLVER III:

The Algorithm



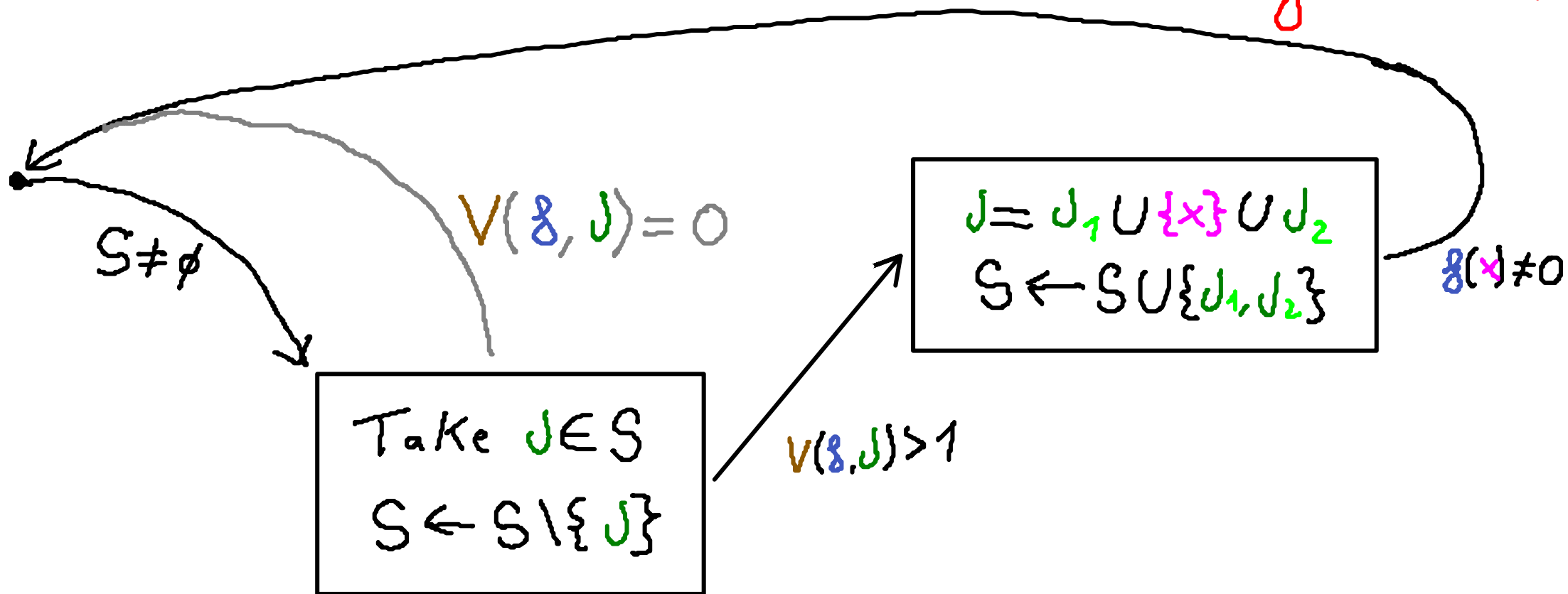
DESCARTES SOLVER III:

The Algorithm



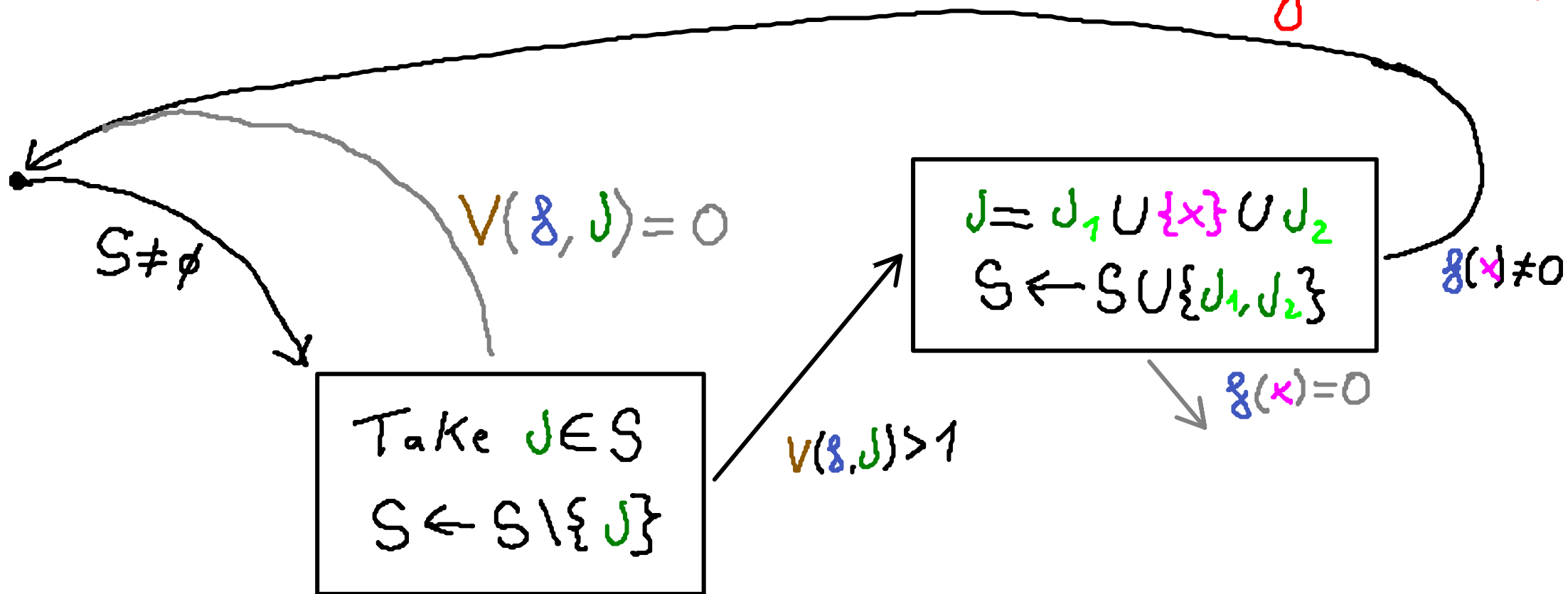
DESCARTES SOLVER III:

The Algorithm



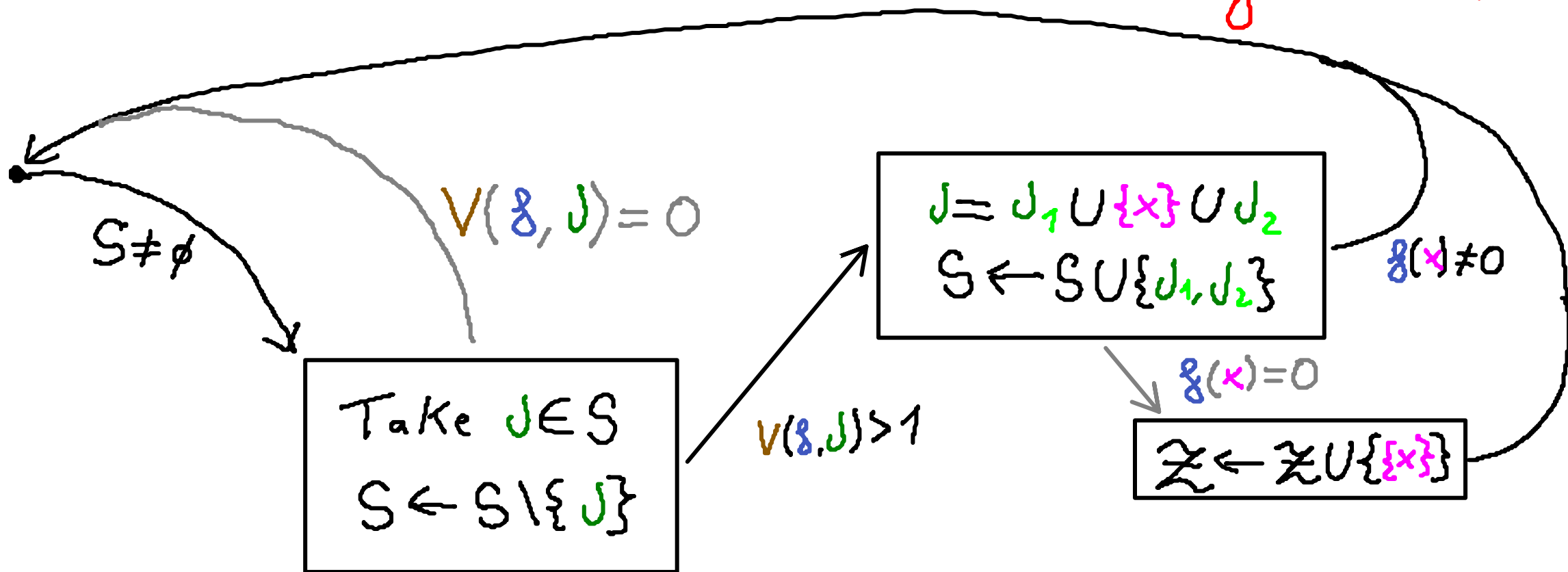
DESCARTES SOLVER III:

The Algorithm



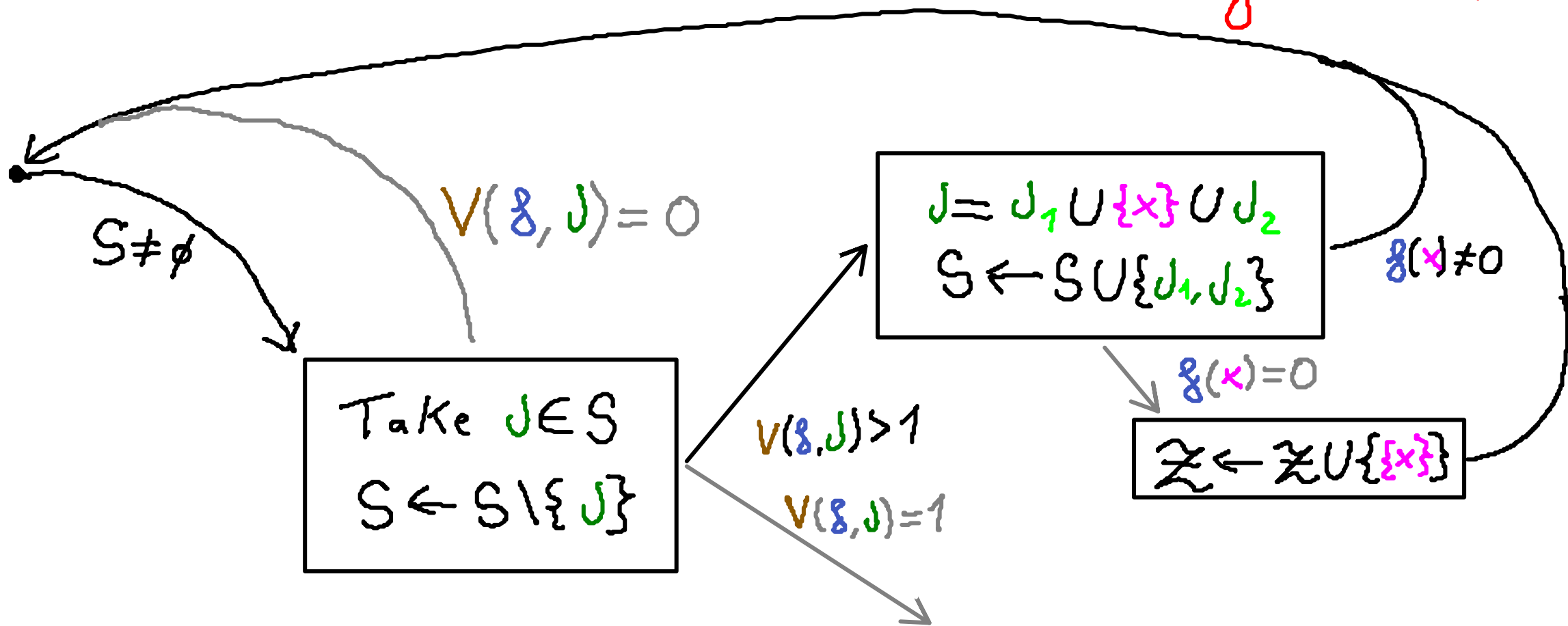
DESCARTES SOLVER III:

The Algorithm



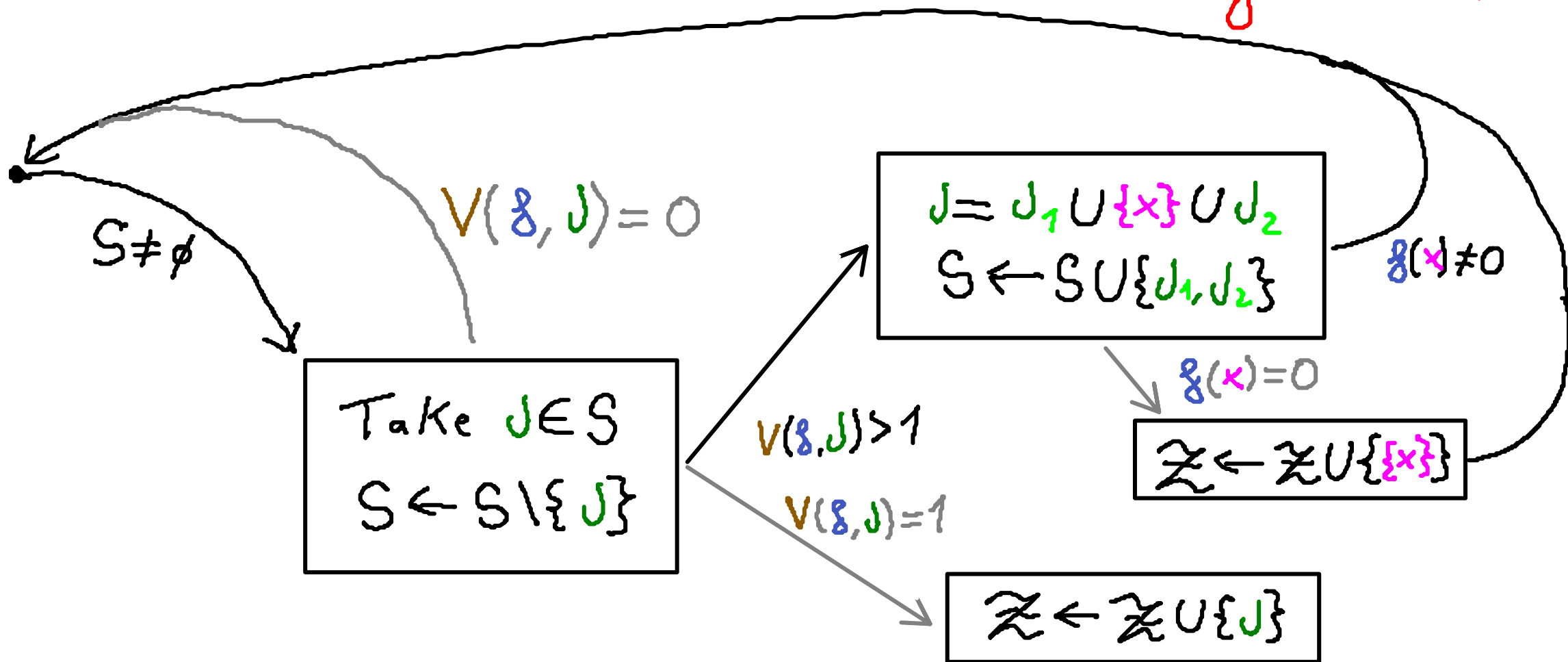
DESCARTES SOLVER III:

The Algorithm



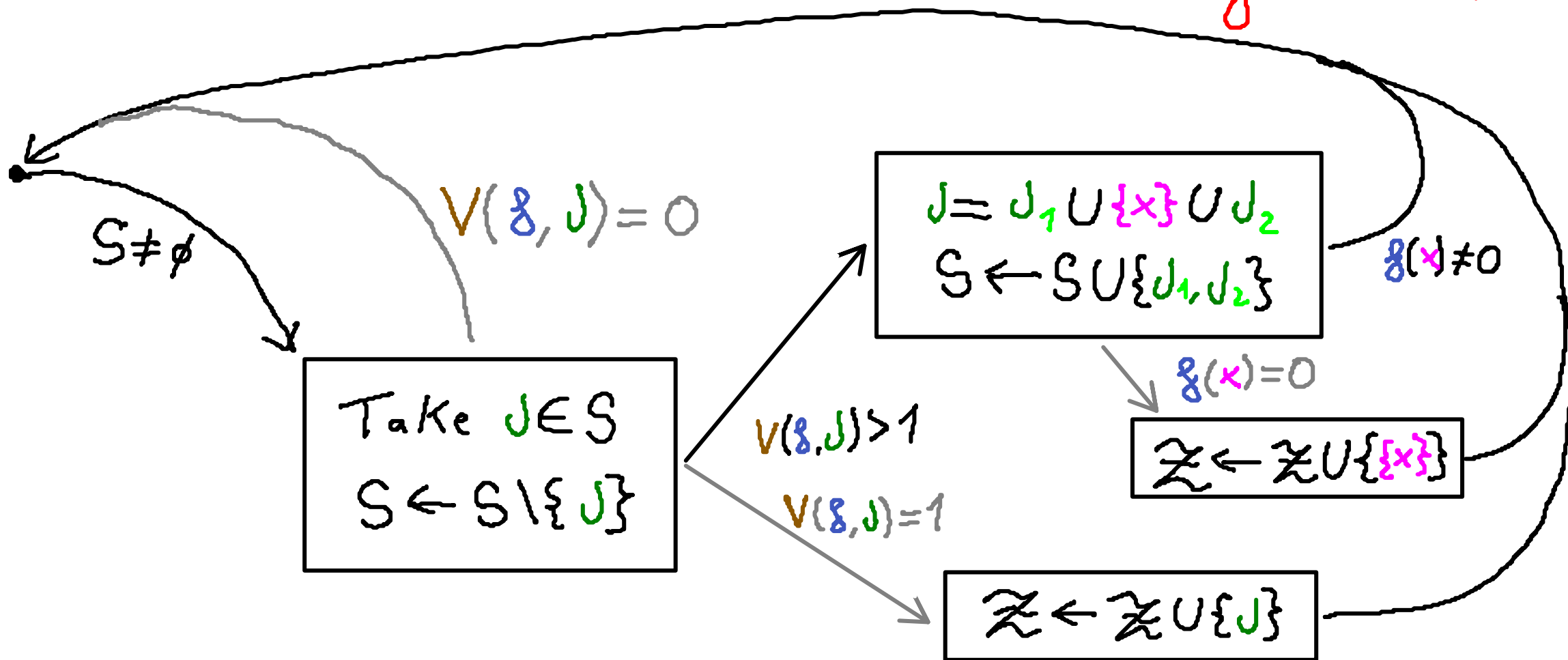
DESCARTES SOLVER III:

The Algorithm



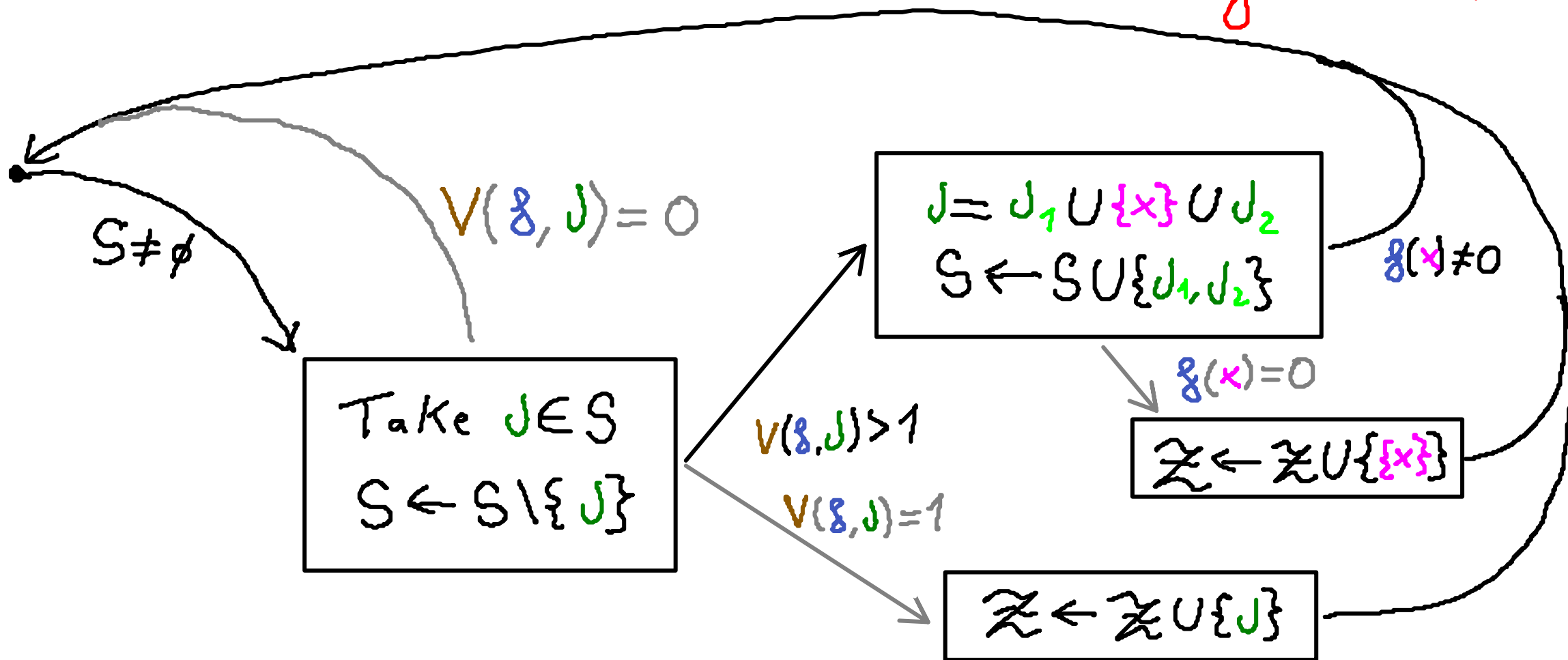
DESCARTES SOLVER III:

The Algorithm



DESCARTES SOLVER III:

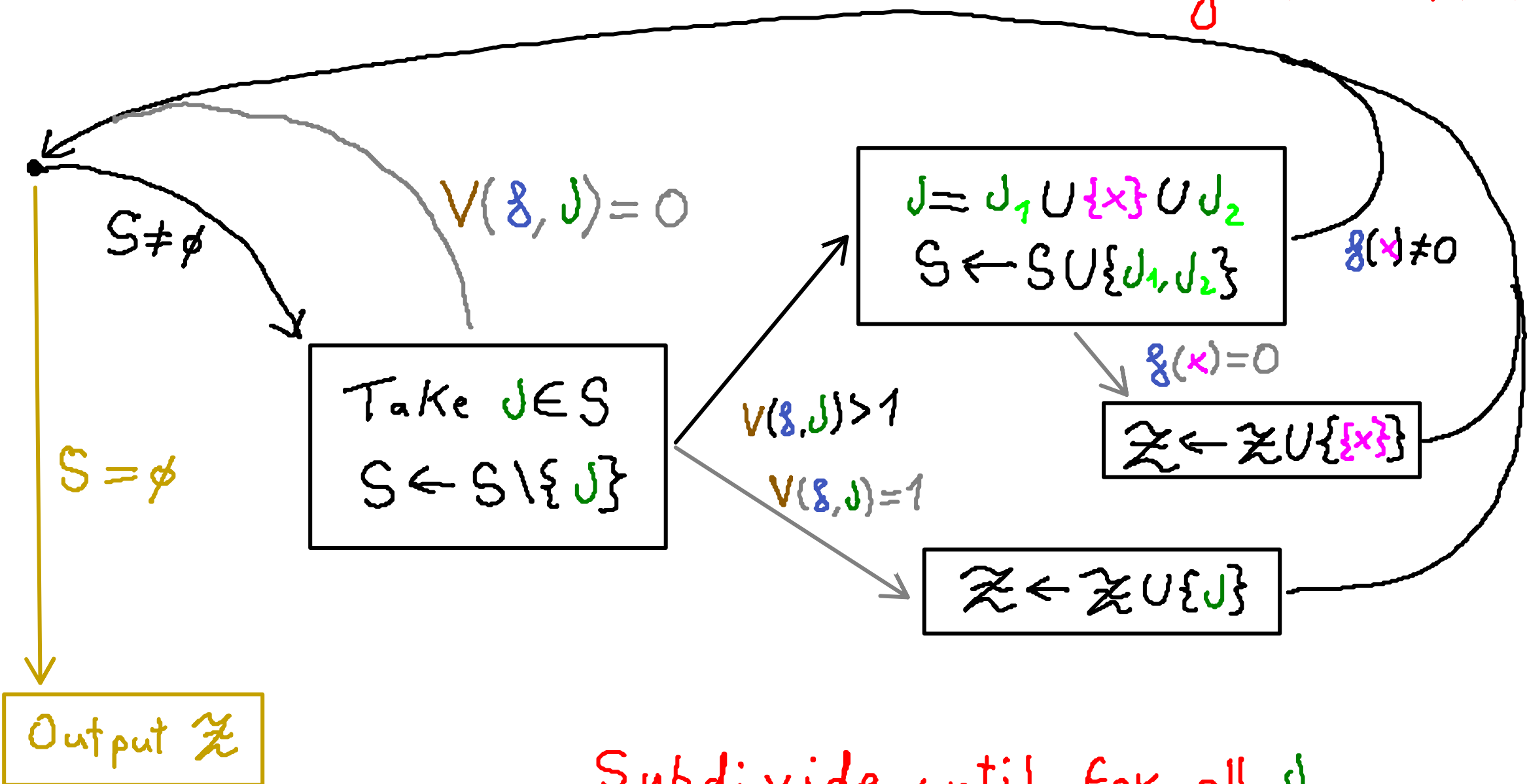
The Algorithm



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

DESCARTES SOLVER III:

The Algorithm



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

Real Root Isolation IV:

Are we being pessimistic?

Worst-case complexity:

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



Pessimistic in practice

DESCARTES SOLVER

seems to behave faster in practice!

! Can we explain this?

Real Root Isolation V:

Beyond pessimism

Worst-case complexity:

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

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

(Roughgarden, 2021)



Probabilistic complexity

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

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

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

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

On average, DESCARTES is almost optimal!

Beyond pessimism II:

Random Bit Polynomials

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

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

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

weight of F :

$$w(F) := \max\{\mathbb{P}(F_k = c) \mid c \in \mathbb{R}, k \in \{0, 1, \overset{\text{No middle indexes!}}{\downarrow} d-1, d\}\}$$

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

Beyond pessimism III:

MAIN THEOREM

MAIN THM (Ergür, T-C, Tsigaridas)

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

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

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

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

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

$$F = \sum_{k=0}^d f_k X^k \quad \text{with } f_k \sim \mathcal{U}(\sigma_k([1, 2^\tau] \cap \mathbb{N}))$$

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

Beyond pessimism V:

Examples of Random Bit Polynomials II

• Exact bitsize

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

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

+ their combinations

Our random model is flexible!

SUMMING UP:

DESCARTES' SOLVER

IS ALMOST OPTIMAL ON AVERAGE!

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

Eskerrik Asko
bere arretagatik!

¡ Muchas Gracias
por su Atención!