

Hecho del Día:

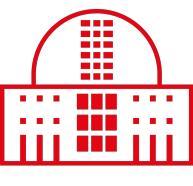


Source: Wikimedia

Hoy,
¡David Hilbert
hubiera cumplido
162 años!

„Wir müssen wissen,
wir werden wissen.“

El Resolvedor
DESCARTES
es
Quasi-Óptimo
en media



Josué TONELLI-CUETO
Johns Hopkins University

s9. Álgebra Computacional
& Aplicaciones

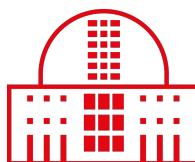
DESCARTES

Elatzailea

batez beste

ia optimoa

da



RSME'24
UPNA PAMPLONA

Josué TONELLI-CUETO
Johns Hopkins University

sq. Álgebra Computacional
& Aplicaciones

Trabajo de:

Elias TSIGARIDAS

Josué TONELLI-CUETO



Alperen A. ERGÜR

• Cómo encontramos
las raíces Reales
de un polinomio univariado?

• Cómo encontramos
las raíces Reales
de un polinomio univariado?

y cómo
lo hacemos rápido?

Aislamiento de Raíces Reales I: EL PROBLEMA

Aislamiento de Raíces Reales I:

EL PROBLEMA

ENTRADA:

Aislamiento de Raíces Reales I:

EL PROBLEMA

ENTRADA:

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

Aislamiento de Raíces Reales I:

EL PROBLEMA

ENTRADA:

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

SALIDA:

Aislamiento de Raíces Reales I:

EL PROBLEMA

ENTRADA:

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

SALIDA:

Intervalos J_1, \dots, J_k t.q.

Aislamiento de Raíces Reales I:

EL PROBLEMA

ENTRADA:

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

SALIDA:

Intervalos J_1, \dots, J_k t.q.

1) $J_i = (a_i, b_i)$ con $a_i, b_i \in \mathbb{Q}$

Aislamiento de Raíces Reales I:

EL PROBLEMA

ENTRADA:

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

SALIDA:

Intervalos J_1, \dots, J_k t.q.

$$1) J_i = (a_i, b_i) \text{ con } a_i, b_i \in \mathbb{Q}$$

$$2) \mathbb{Z}(g) \cap \mathbb{R} \subseteq \bigcup_i J_i$$

Aislamiento de Raíces Reales I:

EL PROBLEMA

ENTRADA:

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

SALIDA:

Intervalos J_1, \dots, J_k t.q.

$$1) J_i = (a_i, b_i) \text{ con } a_i, b_i \in \mathbb{Q}$$

$$2) \mathbb{Z}(g) \cap \mathbb{R} \subseteq \bigcup_i J_i$$

$$3) \forall i, \#\mathbb{Z}(g) \cap J_i = 1$$

Aislamiento de Raíces Reales I:

EL PROBLEMA

ENTRADA:

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

PARÁMETROS

DE TAMAÑO:

SALIDA:

Intervalos J_1, \dots, J_k t.q.

$$1) J_i = (a_i, b_i) \text{ con } a_i, b_i \in \mathbb{Q}$$

$$2) \mathbb{Z}(g) \cap \mathbb{R} \subseteq \bigcup_i J_i$$

$$3) \forall i, \#\mathbb{Z}(g) \cap J_i = 1$$

Aislamiento de Raíces Reales I:

EL PROBLEMA

ENTRADA:

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

PARÁMETROS

DE TAMAÑO:

d : grado de g

SALIDA:

Intervalos J_1, \dots, J_k t.q.

1) $J_i = (a_i, b_i)$ con $a_i, b_i \in \mathbb{Q}$

2) $\mathbb{Z}(g) \cap \mathbb{R} \subseteq \bigcup_i J_i$

3) $\forall i, \#\mathbb{Z}(g) \cap J_i = 1$

Aislamiento de Raíces Reales I:

EL PROBLEMA

ENTRADA:

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

PARÁMETROS

DE TAMAÑO:

d : grado de g

γ : tamaño bit de los coeficientes de g

SALIDA:

Intervalos J_1, \dots, J_k t.q.

1) $J_i = (a_i, b_i)$ con $a_i, b_i \in \mathbb{Q}$

2) $Z(g) \cap \mathbb{R} \subseteq \bigcup_i J_i$

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

Aislamiento de Raíces Reales I:

EL PROBLEMA

ENTRADA:

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

PARÁMETROS

DE TAMAÑO:

d : grado de g

γ : tamaño bit de los coeficientes de g

MEDIDA DEL TIEMPO DE CÓMPUTO.

SALIDA:

Intervalos J_1, \dots, J_k t.q.

1) $J_i = (a_i, b_i)$ con $a_i, b_i \in \mathbb{Q}$

2) $Z(g) \cap \mathbb{R} \subseteq \bigcup_i J_i$

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

Aislamiento de Raíces Reales I:

EL PROBLEMA

ENTRADA:

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

PARÁMETROS

DE TAMAÑO:

d : grado de g

γ : tamaño bit de los coeficientes de g

MEDIDA DEL TIEMPO DE CÓMPUTO:

Complejidad Bit

SALIDA:

Intervalos J_1, \dots, J_k t.q.

1) $J_i = (a_i, b_i)$ con $a_i, b_i \in \mathbb{Q}$

2) $Z(g) \cap \mathbb{R} \subseteq \bigcup_i J_i$

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

Aislamiento de Raíces Reales II: Estado del Arte

Aislamiento de Raíces Reales II: Estado del Arte

resolvedor STURM

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

Aislamiento de Raíces Reales II:

Estado del Arte

resolvedor

STURM

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

resolvedor

DESCARTES

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

Aislamiento de Raíces Reales II: Estado del Arte

resolvedor STURM

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

resolvedor DESCARTES

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

ANewDSC

(Sagraloff & Mehlhorn; 2016)

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

Aislamiento de Raíces Reales II:

Estado del Arte

resolvedor STURM

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

resolvedor DESCARTES

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

ANEWDESC

(Sagraloff & Mehlhorn; 2016)

algoritmo de PAN

(Pan; 2002)

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

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

Aislamiento de Raíces Reales II: Estado del Arte

resolvedor STURM

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

resolvedor DESCARTES

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

ANewDSC

(Sagraloff & Mehlhorn; 2016)

algoritmo de PAN

(Pan; 2002) ↑ Campeón Teórico

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

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

Aislamiento de Raíces Reales II: Estado del Arte

resolvedor STURM

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

resolvedor DESCARTES

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

ANewDSC ← Campeón práctico
(Sagraloff & Mehlhorn; 2016)

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

algoritmo de PAN

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

(Pan; 2002) ↑ Campeón teórico

Aislamiento de Raíces Reales III: ¡Qué deseamos?

Aislamiento de Raíces Reales III: ¡Qué deseamos?

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

Aislamiento de Raíces Reales III: ¡Qué deseamos?

$$\tilde{G}(d\gamma)$$

resolver casi tan rápido
como leemos el polinomio!

Resolvedor DESCARTES I: Regla de Signos

5



Retrato por Frans Hal

Resolvedor DESCARTES I: Regla de Signos

$V(g) := \#$ variaciones de signo
de g_0, g_1, g_2, \dots ignorando ceros



Retrato por Frans Hal

Resolvedor DESCARTES I: Regla de Signos

$V(g) := \#$ variaciones de signo
de g_0, g_1, g_2, \dots ignorando ceros

TEO (Regla de signos de Descartes)



Retrato por Frans Hal

Resolvedor DESCARTES I: Regla de Signos

$V(\gamma) := \#$ variaciones de signo
de $\gamma_0, \gamma_1, \gamma_2, \dots$ ignorando ceros

TEO (Regla de signos de Descartes)

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



Retrato por Frans Hal

Resolvedor DESCARTES I: Regla de Signos

$V(\gamma) := \#$ variaciones de signo
de $\gamma_0, \gamma_1, \gamma_2, \dots$ ignorando ceros

TEO (Regla de signos de Descartes)

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

Aún más,

$$V(\gamma) \leq 1 \Rightarrow \text{Igualdad}$$



Retrato por Frans Hal

Resolvedor DESCARTES I: Regla de Signos

$V(\gamma) := \#$ variaciones de signo
de $\gamma_0, \gamma_1, \gamma_2, \dots$ ignorando ceros

TEO (Regla de signos de Descartes)

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

Aún más,

$$V(\gamma) \leq 1 \Rightarrow \text{Igualdad}$$

COR

$$\#\mathcal{Z}(\gamma, (a, b))$$



Retrato por Frans Hal

Resolvedor DESCARTES I: Regla de Signos

$V(g) := \#$ variaciones de signo
de g_0, g_1, g_2, \dots ignorando ceros

TEO (Regla de signos de Descartes)

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

Aún más,

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

COR

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



Retrato por Frans Hal

Resolvedor DESCARTES I: Regla de Signos

$V(g) := \#$ variaciones de signo
de g_0, g_1, g_2, \dots ignorando ceros

TEO (Regla de signos de Descartes)

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

Aún más,

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

COR

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



Retrato por Frans Hal

biyección $(0, \infty) \rightarrow (a, b)$

Resolvedor DESCARTES II: El Oráculo de Descartes

Resolvedor DESCARTES II: El Oráculo de Descartes

1) Sobreconteo:

Resolvedor DESCARTES II: El Oráculo de Descartes

1) Sobreconteo: $\#Z(g, j) \leq V(g, j)$

Resolvedor DESCARTES II: El Oráculo de Descartes

1) Sobreconteo: $\#Z(8, j) \leq V(8, j)$

2) Exactitud I: $V(8, j) \leq 1$

Resolvedor DESCARTES II:

El Oráculo de Descartes

1) Sobreconteo: $\#Z(g, j) \leq V(g, j)$

2) Exactitud I: $V(g, j) \leq 1 \Rightarrow \#Z(g, j) = V(g, j)$

Resolvedor DESCARTES II:

El Oráculo de Descartes

1) Sobreconteo: $\#Z(g, j) \leq V(g, j)$

2) Exactitud I: $V(g, j) \leq 1 \Rightarrow \#Z(g, j) = V(g, j)$

3) Exactitud II:

Resolvedor DESCARTES II:

El Oráculo de Descartes

1) Sobreconteo: $\#Z(g, j) \leq V(g, j)$

2) Exactitud I: $V(g, j) \leq 1 \Rightarrow \#Z(g, j) = V(g, j)$

3) Exactitud II: (Teoremas de Obreshkoff)

Resolvedor DESCARTES II:

El Oráculo de Descartes

- 1) Sobreconteo: $\#\mathcal{Z}(g, J) \leq V(g, J)$
- 2) Exactitud I: $V(g, J) \leq 1 \Rightarrow \#\mathcal{Z}(g, J) = V(g, J)$
- 3) Exactitud II: (Teoremas de Obreshkoff)

$$\#\mathcal{Z}(g, D(m(J)), c w(J)) \leq k$$

donde $D(x, r) := \{z \in \mathbb{C} \mid |z - x| \leq r\}$,

$m(J)$:= punto medio de J & $w(J)$:= ancho de J

Resolvedor DESCARTES II:

El Oráculo de Descartes

- 1) Sobreconteo: $\#Z(g, J) \leq V(g, J)$
- 2) Exactitud I: $V(g, J) \leq 1 \Rightarrow \#Z(g, J) = V(g, J)$
- 3) Exactitud II: (Teoremas de Obreshkoff)

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

donde $D(x, r) := \{z \in \mathbb{C} \mid |z - x| \leq r\}$,

$m(J) :=$ punto medio de J & $w(J) :=$ ancho de J

Resolvedor DESCARTES II:

El Oráculo de Descartes

- 1) Sobreconteo: $\#\mathcal{Z}(g, J) \leq V(g, J)$
- 2) Exactitud I: $V(g, J) \leq 1 \Rightarrow \#\mathcal{Z}(g, J) = V(g, J)$
- 3) Exactitud II: (Teoremas de Obreshkoff)

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

donde $D(x, r) := \{z \in \mathbb{C} \mid |z - x| \leq r\}$,

$m(J) :=$ punto medio de J & $w(J) :=$ ancho de J
- 4) Subaditividad:

Resolvedor DESCARTES II:

El Oráculo de Descartes

- 1) Sobreconteo: $\#Z(g, J) \leq V(g, J)$
- 2) Exactitud I: $V(g, J) \leq 1 \Rightarrow \#Z(g, J) = V(g, J)$
- 3) Exactitud II: (Teoremas de Obreshkoff)

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

donde $D(x, r) := \{z \in \mathbb{C} \mid |z - x| \leq r\}$,

$m(J) :=$ punto medio de J & $w(J) :=$ ancho de J

- 4) Subaditividad:

$$\bigcup_i J_i \subseteq J$$

Resolvedor DESCARTES II:

El Oráculo de Descartes

1) Sobreconteo: $\#\mathcal{Z}(g, J) \leq V(g, J)$

2) Exactitud I: $V(g, J) \leq 1 \Rightarrow \#\mathcal{Z}(g, J) = V(g, J)$

3) Exactitud II: (Teoremas de Obreshkoff)

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

donde $D(x, r) := \{z \in \mathbb{C} \mid |z - x| \leq r\}$,

$m(J) :=$ punto medio de J & $w(J) :=$ ancho de J

4) Subadicitividad:

$\bigcup_i J_i \subseteq J \Rightarrow \sum_i V(g, J_i) \leq V(g, J)$

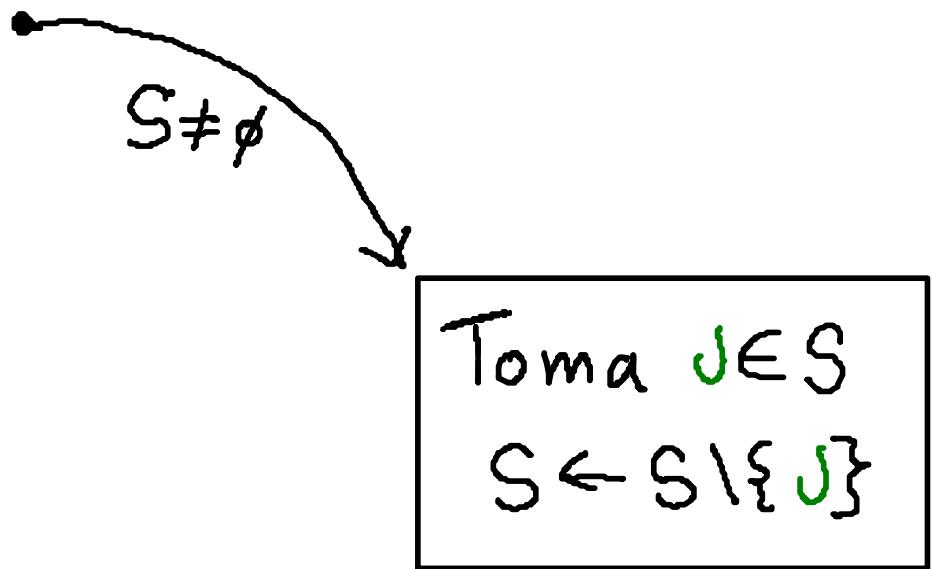
Resolvedor DESCARTES III: El Algoritmo

7

¡Subdivide hasta que $V(8, J) \leq 1$!

Resolvedor DESCARTES III: El Algoritmo

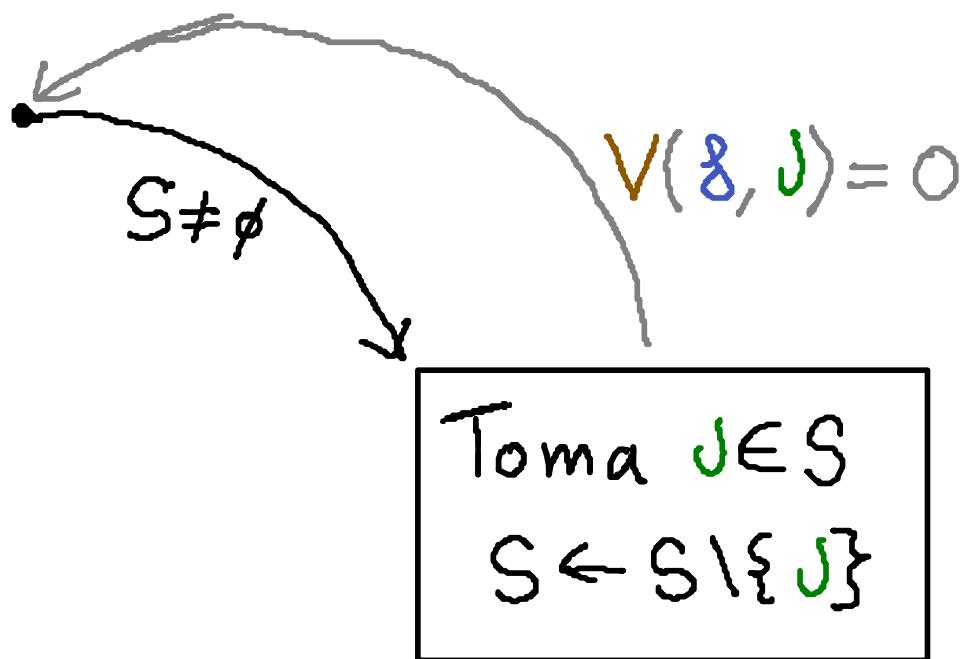
7



i Subdivide hasta que $V(S, j) \leq 1$!

Resolvedor DESCARTES III: El Algoritmo

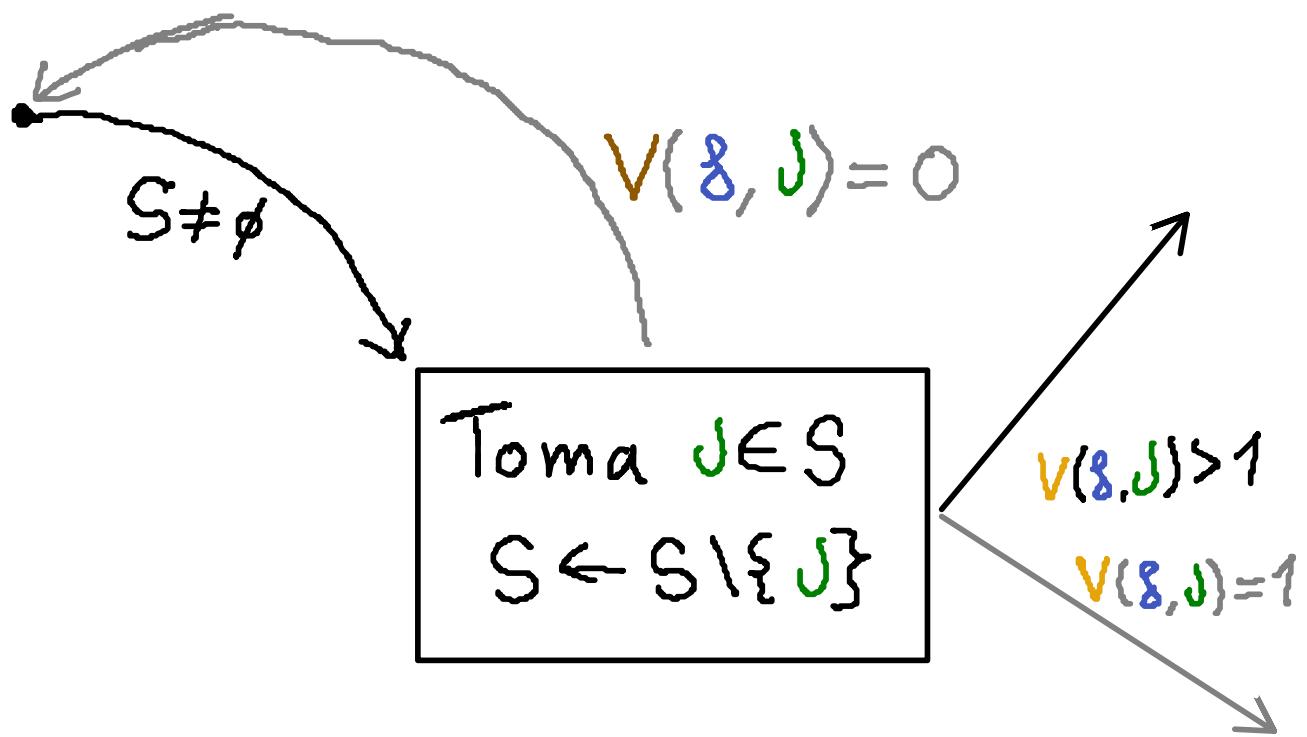
7



¡Subdivide hasta que $V(g, j) \leq 1$!

Resolvedor DESCARTES III: El Algoritmo

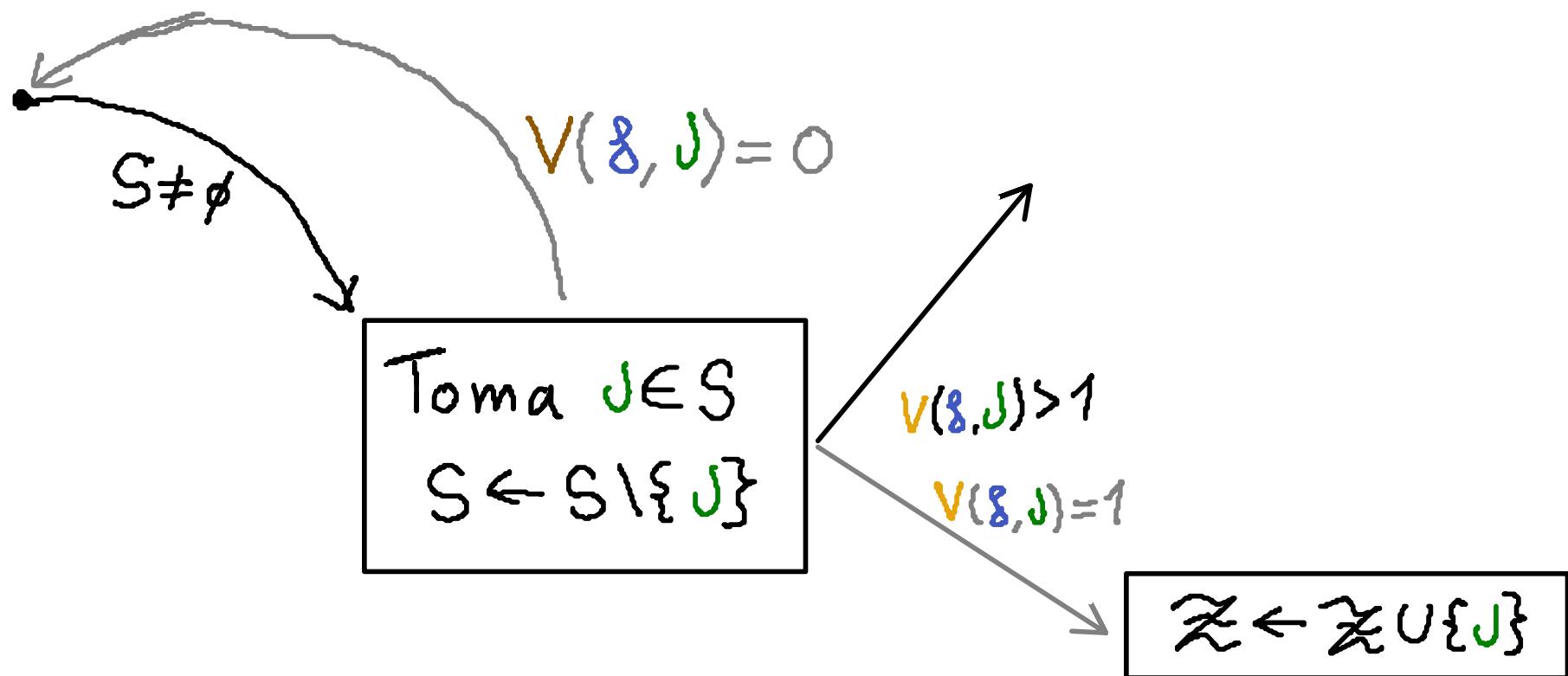
7



¡Subdivide hasta que $V(S, J) \leq 1$!

Resolvedor DESCARTES III: El Algoritmo

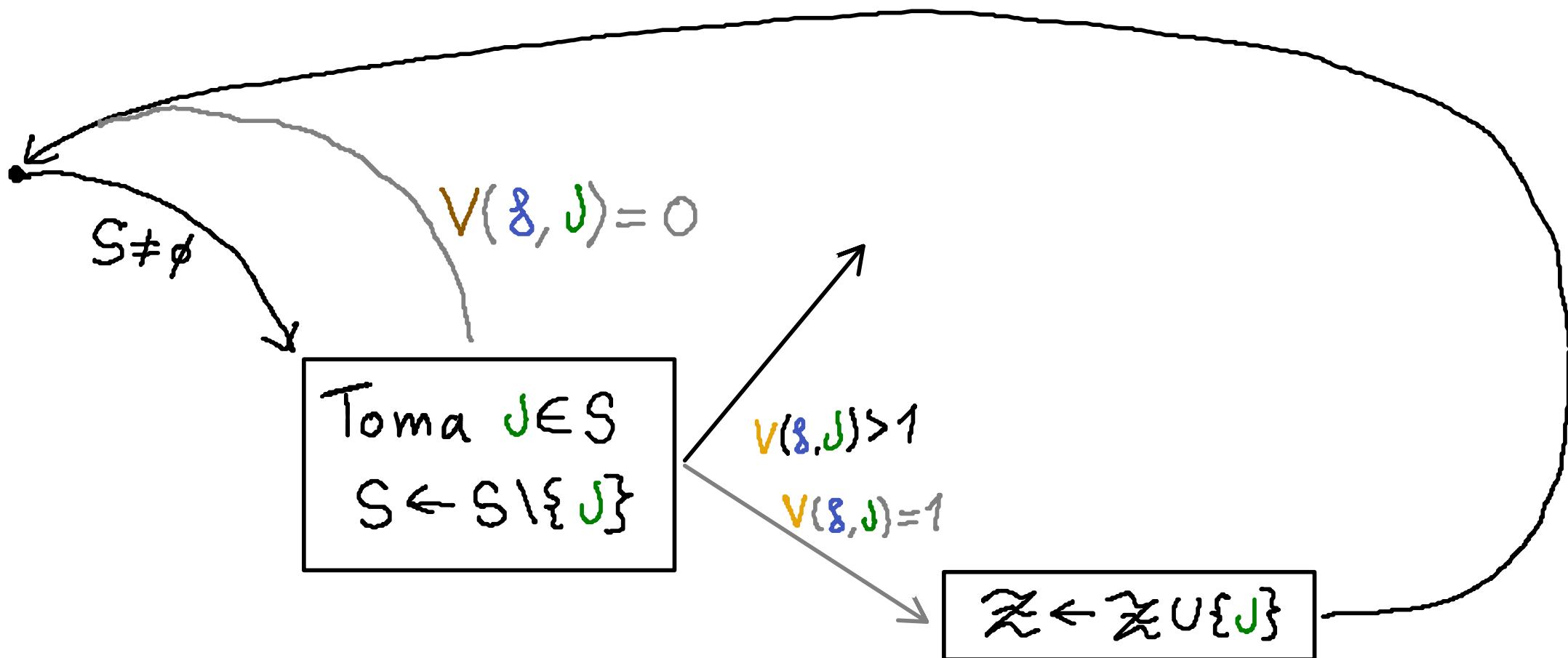
7



¡Subdivide hasta que $V(S, J) \leq 1$!

Resolvedor DESCARTES III: El Algoritmo

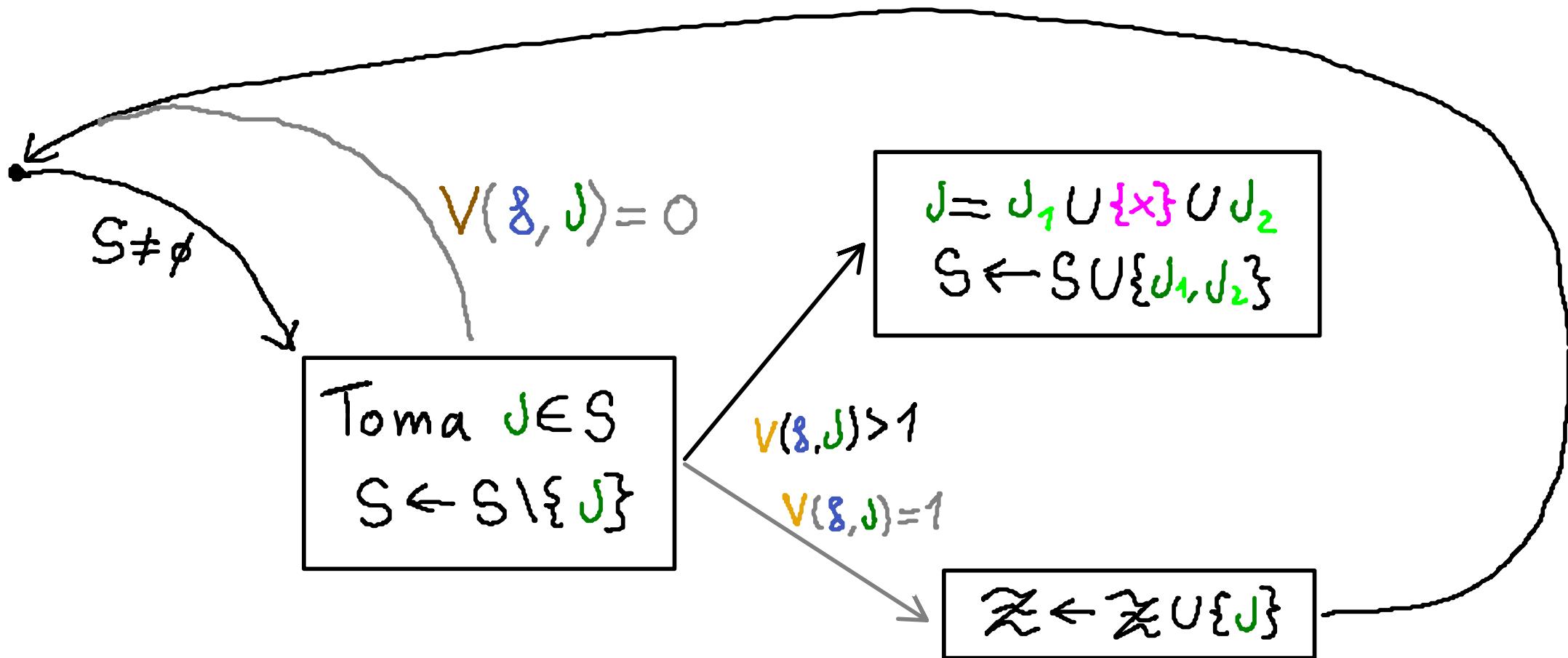
7



¡Subdivide hasta que $V(8, J) \leq 1$!

Resolvedor DESCARTES III: El Algoritmo

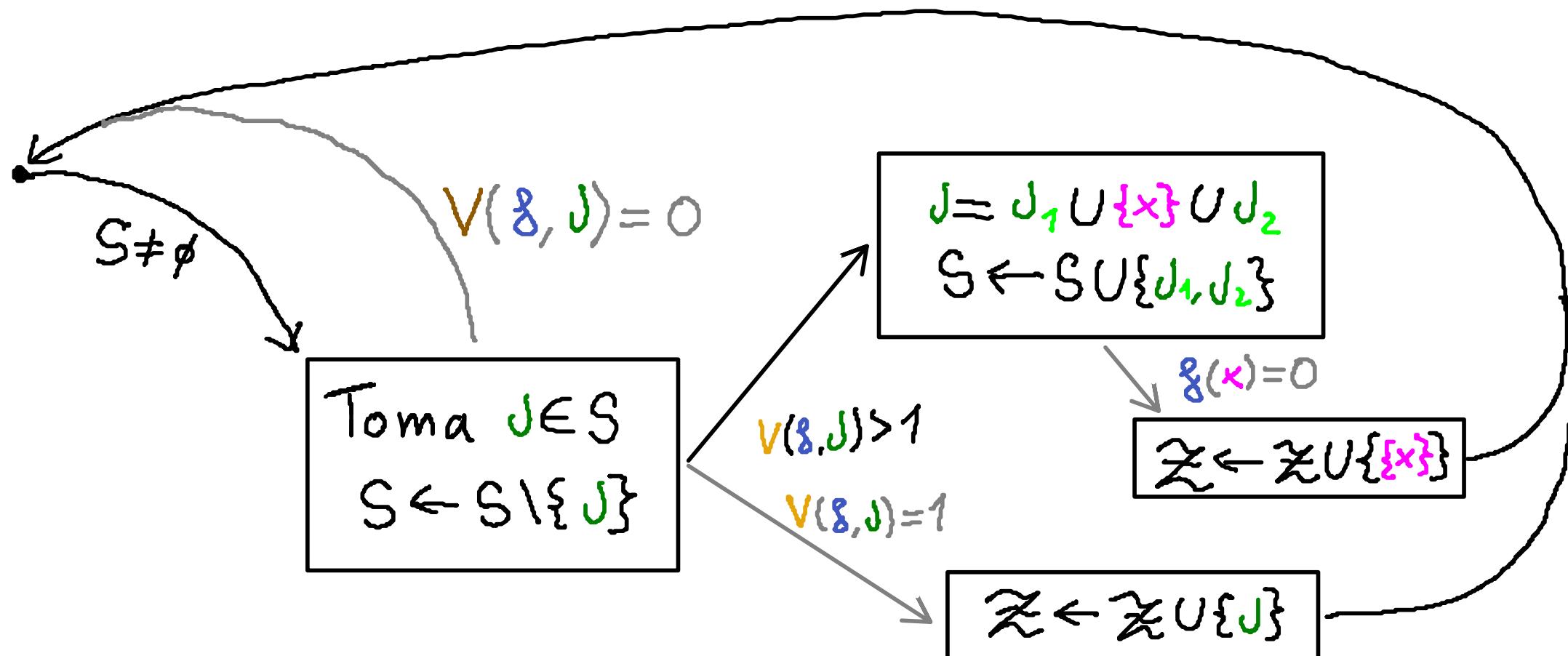
7



¡Subdivide hasta que $V(8, J) \leq 1$!

Resolvedor DESCARTES III: El Algoritmo

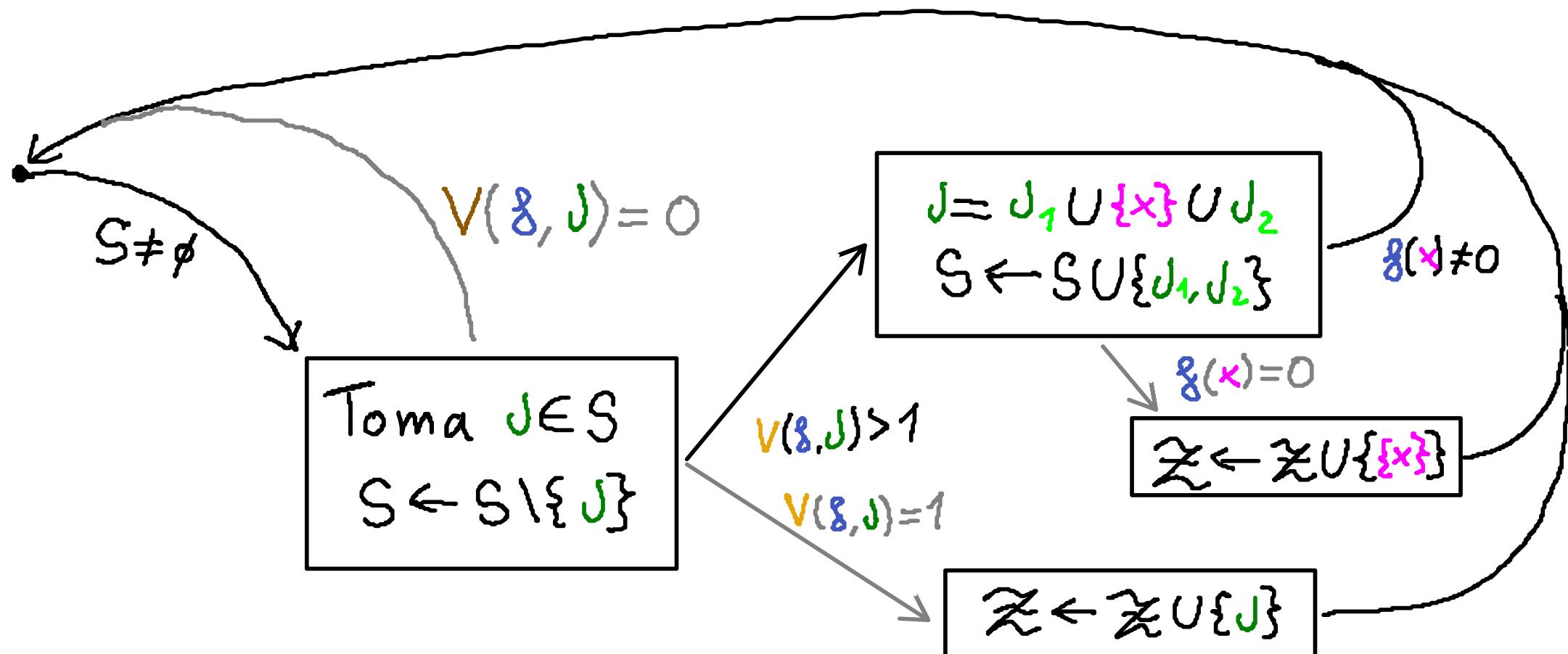
7



¡Subdivide hasta que $V(\emptyset, J) \leq 1$!

Resolvedor DESCARTES III: El Algoritmo

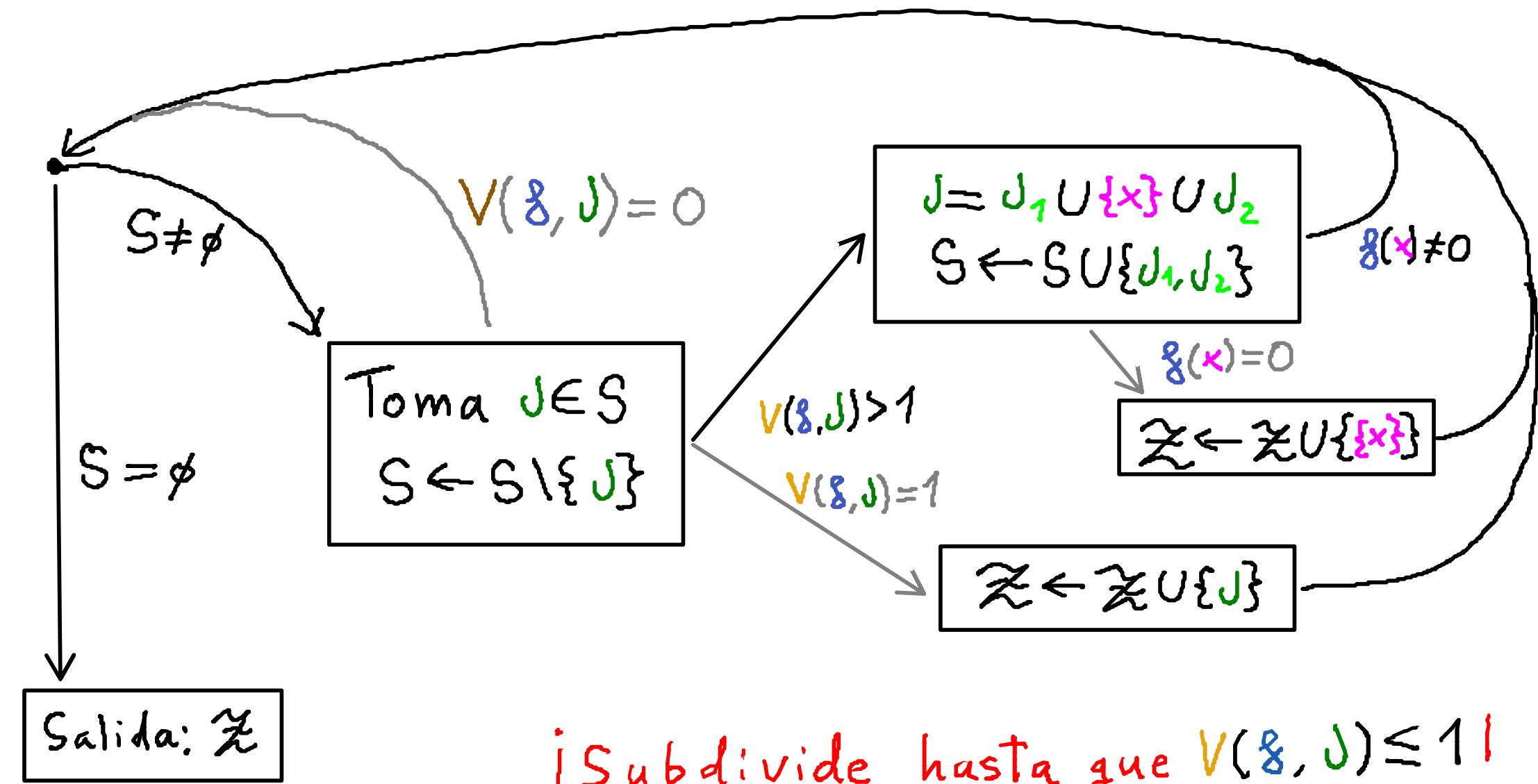
7



¡Subdivide hasta que $V(\delta, J) \leq 1$!

Resolvedor DESCARTES III: El Algoritmo

7



¿Por qué
es DESCARTES
tan rápido en la práctica?

Paradigmas de Complejidad I: ¿Somos demasiado pesimistas?

Paradigmas de Complejidad I: ¡Somos demasiado pesimistas?

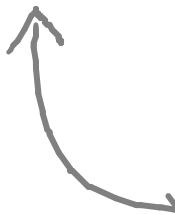
Complejidad del Peor Caso:

$$\max \left\{ \text{cost}(\text{RESOLVEDOR}, g) \mid \text{bit-size}(g) \leq r, \deg(g) \leq d \right\}$$

Paradigmas de Complejidad I: ¿Somos demasiado pesimistas?

Complejidad del Peor Caso:

$$\max \left\{ \text{cost}(\text{RESOLVEDOR}, g) \mid \text{bit-size}(g) \leq r, \deg(g) \leq d \right\}$$



¡pesimista en la práctica!

Paradigmas de Complejidad II:

Más allá del pesimismo

Complejidad del Peor Caso:

$$\max \left\{ \text{cost}(\text{RESOLVEDOR}, g) \mid \text{bit-size}(g) \leq r, \deg(g) \leq d \right\}$$

Paradigmas de Complejidad II:

Más allá del pesimismo

Complejidad del Peor Caso:

$$\max \left\{ \text{cost}(\text{RESOLVEDOR}, g) \mid \text{bit-size}(g) \leq \gamma, \deg(g) \leq d \right\}$$

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

{ (Roughgarden, 2021)

Paradigmas de Complejidad II:

Más allá del pesimismo

Complejidad del Peor Caso:

$$\max \left\{ \text{cost}(\text{RESOLVEDOR}, g) \mid \text{bit-size}(g) \leq \gamma, \deg(g) \leq d \right\}$$

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

{ (Roughgarden, 2021)

Complejidad Probabilística

$$\mathbb{E}_F \left\{ \text{cost}(\text{RESOLVEDOR}, F)^e \mid \text{bit-size}(F) \leq \gamma, \deg(F) \leq d \right\}$$

Paradigmas de Complejidad II:

Más allá del pesimismo

Complejidad del Peor Caso:

$$\max \left\{ \text{cost}(\text{RESOLVEDOR}, g) \mid \text{bit-size}(g) \leq r, \deg(g) \leq d \right\}$$

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

{ (Roughgarden, 2021)

Complejidad Probabilística

$$\mathbb{E}_F \left\{ \text{cost}(\text{RESOLVEDOR}, F)^e \mid \text{bit-size}(F) \leq r, \deg(F) \leq d \right\}$$

¿Cuál es una 'buena elección'
 del modelo aleatorio F ?

Más allá del Pessimismo I:

Forma Simple

Más allá del Pesimismo I:

Forma Simple

$$f = \sum_{k=1}^d f_k X^k$$

polinomio aleatorio bit uniforme

Más allá del Pesimismo I:

Forma Simple

$$f = \sum_{k=1}^d f_k x^k$$

polinomio aleatorio bit uniforme

si $f_k \sim \mathcal{U}([-2^\gamma, 2^\gamma] \cap \mathbb{Z})$ independientes

Más allá del Pesimismo I:

Forma Simple

$F = \sum_{k=1}^d f_k X^k$ polinomio aleatorio bit uniforme
 si $f_k \sim \mathcal{U}([-2^\gamma, 2^\gamma] \cap \mathbb{Z})$ independientes

TEO. PRINCIPAL SIMPLE (Ergür, T-C & Tsigaridas)

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

Más allá del Pesimismo I:

Forma Simple

$F = \sum_{k=1}^d f_k X^k$ polinomio aleatorio bit uniforme
 si $f_k \sim \mathcal{U}([-2^\gamma, 2^\gamma] \cap \mathbb{Z})$ independientes

TEO. PRINCIPAL SIMPLE (Ergür, T-C & Tsigaridas)

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

icuasi-óptimo
en media!

Más allá del Pesimismo II: Polinomios Aleatorios Bit

Más allá del Pesimismo II:

Polinomios Aleatorios Bit

$$f = \sum_{k=1}^d f_k X^k \in \mathbb{Z}[X] \text{ con } f_k \text{ independientes}$$

Más allá del Pesimismo II:

Polinomios Aleatorios Bit

$$f = \sum_{k=1}^d f_k X^k \in \mathbb{Z}[X] \text{ con } f_k \text{ independientes}$$

Tamaño bit de f :

Más allá del Pesimismo II:

Polinomios Aleatorios Bit

$$f = \sum_{k=1}^d f_k x^k \in \mathbb{Z}[x] \text{ con } f_k \text{ independientes}$$

Tamaño bit de f :

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

Más allá del Pesimismo II:

Polinomios Aleatorios Bit

$$f = \sum_{k=1}^d f_k x^k \in \mathbb{Z}[x] \text{ con } f_k \text{ independientes}$$

Tamaño bit de f :

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

Más allá del Pesimismo II:

Polinomios Aleatorios Bit

$$f = \sum_{k=1}^d f_k x^k \in \mathbb{Z}[x] \text{ con } f_k \text{ independientes}$$

Tamaño bit de f :

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

Peso de f :

Más allá del Pesimismo II:

Polinomios Aleatorios Bit

$$f = \sum_{k=1}^d f_k x^k \in \mathbb{Z}[x] \text{ con } f_k \text{ independientes}$$

Tamaño bit de f :

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

Peso de f :

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

Más allá del Pesimismo II:

Polinomios Aleatorios Bit

$$f = \sum_{k=1}^d f_k x^k \in \mathbb{Z}[x] \text{ con } f_k \text{ independientes}$$

Tamaño bit de f :

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

Peso de f :

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

↓
No hay errata!

Más allá del Pesimismo II:

Polinomios Aleatorios Bit

$$F = \sum_{k=1}^d f_k X^k \in \mathbb{Z}[X] \text{ con } f_k \text{ independientes}$$

Tamaño bit de F :

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

Peso de F :

$$w(F) := \max \{P(f_k=c) \mid k \in \{0, d\}, c \in \mathbb{Z}\}$$

↓
No hay errata!

Uniformidad de F :

Más allá del Pesimismo II:

Polinomios Aleatorios Bit

$$F = \sum_{k=1}^d f_k X^k \in \mathbb{Z}[X] \text{ con } f_k \text{ independientes}$$

Tamaño bit de F :

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

Peso de F :

$$w(F) := \max \{P(f_k=c) \mid k \in \{0, d\}, c \in \mathbb{Z}\}$$

↓
No hay errata!

Uniformidad de F :

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

Más allá del Pesimismo II:

Polinomios Aleatorios Bit

$$F = \sum_{k=1}^d F_k X^k \in \mathbb{Z}[X] \text{ con } F_k \text{ independientes}$$

Tamaño bit de F :

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

Peso de F :

$$w(F) := \max \{P(F_k=c) \mid k \in \{0, d\}, c \in \mathbb{Z}\}$$

↓
No hay errata!

Uniformidad de F :

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

$\triangleleft F \text{ uniform} \Rightarrow u(F) = 0$

Flexibilidad del Modelo Aleatorio I: Control de Soporte

Flexibilidad del Modelo Aleatorio I: Control de Soporte

$$o, d \in A \subseteq \{0, \dots, d\}$$

Flexibilidad del Modelo Aleatorio I: Control de Soporte

$$0, d \in A \subseteq \{0, \dots, d\}$$

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

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

Flexibilidad del Modelo Aleatorio I: Control de Soporte

$$0, d \in A \subseteq \{0, \dots, d\}$$

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

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

Entonces...

$$u(F) = 0$$

Flexibilidad del Modelo Aleatorio II: Control de Signos

Flexibilidad del Modelo Aleatorio II: Control de Signos

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

Flexibilidad del Modelo Aleatorio II: Control de Signos

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

$$f = \sum_{k=1}^d f_k x^k \in \mathbb{Z}[x]$$

con $f_k \sim \mathcal{U}(\sigma_k([0, 2^\tau] \cap \mathbb{N}))$ ind

Flexibilidad del Modelo Aleatorio II:

Control de Signos

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

$$F = \sum_{k=1}^d f_k X^k \in \mathbb{Z}[X]$$

con $f_k \sim \mathcal{U}(\sigma_k([0, 2^\tau] \cap \mathbb{N}))$ ind

Entonces...

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

Flexibilidad del Modelo Aleatorio III:

Control de tamaño bit

Flexibilidad del Modelo Aleatorio III:

Control de tamaño bit

$$\gamma \in \mathbb{N}$$

Flexibilidad del Modelo Aleatorio III:

Control de tamaño bit

$$\gamma \in \mathbb{N}$$

$$f = \sum_{k=1}^d f_k x^k \in \mathbb{Z}[x]$$

con $f_k \sim \mathcal{U}(\{n \in \mathbb{Z} \mid \lfloor \log |n| \rfloor = \gamma\})$ ind

Flexibilidad del Modelo Aleatorio III:

Control de tamaño bit

$$\gamma \in \mathbb{N}$$

$$f = \sum_{k=1}^d f_k x^k \in \mathbb{Z}[x]$$

con $f_k \sim \mathcal{U}(\{n \in \mathbb{Z} \mid \lfloor \log |n| \rfloor = \gamma\})$ ind

Entonces...

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

Flexibilidad del Modelo Aleatorio IV

Flexibilidad del Modelo Aleatorio IV

+ Todas las combinaciones

Más allá del Pesimismo III:

TEOREMA PRINCIPAL

Más allá del Pesimismo III:

TEOREMA PRINCIPAL

TEO. PRIN. (Ergür, T-G, Tsigaridas)

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

Más allá del Pesimismo III:

TEOREMA PRINCIPAL

TEO. PRIN. (Ergür, T-G, Tsigaridas)

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

Obs 1. En muchos casos,

$$u(F) = O(1)$$

Más allá del Pesimismo III:

TEOREMA PRINCIPAL

TEO. PRIN. (Ergür, T-G, Tsigaridas)

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

Obs 1. En muchos casos,

$$u(F) = O(1)$$

Obs 2. Cuasi-optimalidad en media:

$$\gamma \geq d \Rightarrow \text{optimalidad en media}$$

DESCARTES

es cuasi-óptimo en media

¿Y si mi polinomio
es un poco nomio?

Pocohomios I: ¿Qué son?

Poconomios I: ¿Qué son?

Def. (Kushnirenko)

Un poconomio es un polinomio

Poconomios I: ¿Qué son?

Def. (Kushnirenko)

Un poconomio es un polinomio
con pocos términos

Poconomios I: ¿Qué son?

Def. (Kushnirenko)

Un poconomio es un polinomio
con pocos términos

Ex. $y = 53 - 48x^2 + 500x^{300}$

Poconomios I: ¿Qué son?

Def. (Kushnirenko)

Un poconomio es un polinomio
con pocos términos

Ex. $g = 53 - 48x^2 + 500x^{300}$

$$\#\mathcal{Z}(g, \mathbb{R}_+) \leq 2$$

Poconomios I: ¿Qué son?

Def. (Kushnirenko)

Un poconomio es un polinomio
con pocos términos

Ex. $g = 53 - 48x^2 + 500x^{300}$

$$\#\mathcal{Z}(g, \mathbb{R}_+) \leq 2$$

Origen del Nombre:

Poconomios I: ¿Qué son?

Def. (Kushnirenko)

Un poconomio es un polinomio
con pocos términos

Ex. $y = 53 - 48x^2 + 500x^{300}$

$$\#\mathcal{Z}(y, \mathbb{R}) \leq 2$$

Origen del Nombre:
polinomio → polynomial

Poconomios I: ¿Qué son?

Def. (Kushnirenko)

Un poconomio es un polinomio
con pocos términos

$$\text{Ex. } g = 53 - 48x^2 + 500x^{300}$$

$$\#\mathcal{Z}(g, \mathbb{R}_>) \leq 2$$

Origen del Nombre:
polinomio \rightarrow polynomial \rightarrow многочлены

Poconomios I: ¿Qué son?

Def. (Kushnirenko)

Un poconomio es un polinomio
con pocos términos

$$\text{Ex. } g = 53 - 48x^2 + 500x^{300}$$

$$\#\mathcal{Z}(g, \mathbb{R}_>) \leq 2$$

Origen del Nombre:

polinomio \rightarrow polynomial \rightarrow многочлены
 \rightarrow МАЛОЧЛЕНЫ

Poconomios I: ¿Qué son?

Def. (Kushnirenko)

Un poconomio es un polinomio
con pocos términos

Ex. $g = 53 - 48x^2 + 500x^{300}$

$$\#\mathcal{Z}(g, \mathbb{R}) \leq 2$$

Origen del Nombre:

polinomio \rightarrow polynomial \rightarrow многочлены

\rightarrow малочлены \rightarrow Fewnomial \rightarrow poconomio

Poconomios II: ¡Qué queremos!

Poconomios II: ¿Qué queremos?

$$\tilde{\mathcal{O}}_B(\text{poly}(t, \log d, \gamma))$$

Poconomios II: ¿Qué queremos?

tamaño bit del mayor exponente

↓

$$\tilde{\mathcal{O}}_B(\text{poly}(t, \log d, \gamma))$$

Poconomios II: ¿Qué queremos?

tamaño bit del mayor exponente

$$\tilde{\mathcal{O}}_B(\text{poly}(t, \log d, \gamma))$$

monomios

Poconomios II: ¿Qué queremos?

tamaño bit del mayor exponente

$$\tilde{\mathcal{O}}_B(\text{poly}(t, \log d, \gamma))$$

↑
monomios

Esto es,
 resolver en tiempo polinomial
 en el tamaño del poconomio

Poconomios III:

Imposibilidad en el Peor Caso

Poconomios III:

Imposibilidad en el Peor Caso

TEO (Mignotte, 1982)

$$x^d - 2(aX - 1)^2$$

necesita una cantidad de bits
proporcional a $d = 2^{\log d}$ para separar
sus raíces reales.

Poconomios III:

Imposibilidad en el Peor Caso

TEO (Mignotte, 1982)

$$x^d - 2(\alpha x - 1)^2$$

necesita una cantidad de bits
proporcional a $d = 2^{\log d}$ para separar
sus raíces reales.

COR. No hay un resolvente eficiente
de poconomios

Poconomios IV: Posibilidad en el Caso Medio

Poconomios IV: Posibilidad en el Caso Medio

TEO (Ergür, T C, Tsigaridas)

$$\mathbb{E}_F^{\text{cost}}(\text{JINDAL SAGRALOFF}) =$$

(Jindal & Sagraloff, 2017)

Poconomios IV: Posibilidad en el Caso Medio

TEO (Ergür, T C, Tsigaridas)

$$\mathbb{E}_F^{\text{cost}}(\text{JINDAL SAGRALOFF}) = \tilde{O}_B(t^{12} \cdot \log^6 d \cdot \gamma^2) (1 + u(F))^6$$

(Jindal & Sagraloff, 2017)

Poconomios IV: Posibilidad en el Caso Medio

TEO (Ergür, TC, Tsigaridas)

$$\mathbb{E}_F^{\text{cost}}(\text{JINDAL SAGRALOFF}) = \tilde{O}_B(t^{12} \cdot \log^6 d \cdot \gamma^2) (1 + u(F))^6$$

(Jindal & Sagraloff, 2017)

PREGUNTA ABIERTA:

¿Podemos mejorar la cota?

Eskerrik Askor
zuen arretagatik!

Muchas Gracias
por vuestra atención!

galderak? ¿preguntas?