

Hecho del Día:

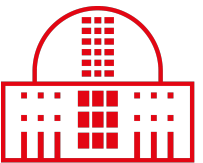


Source: Wikimedia

Hoy,
¡David Hilbert
hubiera cumplido
162 años!

„Wir müssen wissen,
wir werden wissen.“

El Resolvedor DESCARTES es Cuasi-Óptimo en media



RSME'24
UPNA PAMPLONA

Josué TONELLI-CUETO
Johns Hopkins University

59. Álgebra Computacional
& Aplicaciones

DESCARTES

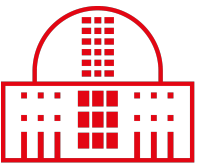
Elatzaila

batez beste

ia optimoa

da

Josué TONELLI-CUETO
Johns Hopkins University



RSME'24
UPNA PAMPLONA

59. Álgebra Computacional
& Aplicaciones

Trabajo de:

Elias Tsigaridas

Josué Tonelli-Cueto



Alperen A. Ergür

¿Cómo encontramos
las raíces Reales
de un polinomio univariado?

¿Y cómo
lo hacemos rápido?

Aislamiento de Raíces Reales I:

EL PROBLEMA

ENTRADA:

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

PARÁMETROS

DE TAMAÑO:

d : grado de f

γ : tamaño bit de los coeficientes de f

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

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

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

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

(Sagraloff & Mehlhorn; 2016)

algoritmo de PAN

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

(Pan; 2002)  Campeón teórico

Aislamiento de Raíces Reales III:

¿Qué deseamos?

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

• resolver casi tan rápido
como leemos el polinomio!

Resolvedor DESCARTES I:

Regla de Signos

$V(\textcolor{blue}{g}) := \# \text{ variaciones de signo}$
de $\textcolor{blue}{g}_0, \textcolor{blue}{g}_1, \textcolor{blue}{g}_2, \dots$ ignorando ceros

TEO (Regla de signos de Descartes)

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

Aún más,

$$\textcolor{blue}{V}(\textcolor{blue}{g}) \leq 1 \Rightarrow \text{I gualdad}$$

COR

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



Retrato por Frans Hal

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



Resolvedor DESCARTES II:

El Oráculo de Descartes

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

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

3) Exactitud II: (Teoremas de Obreshkoff)

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

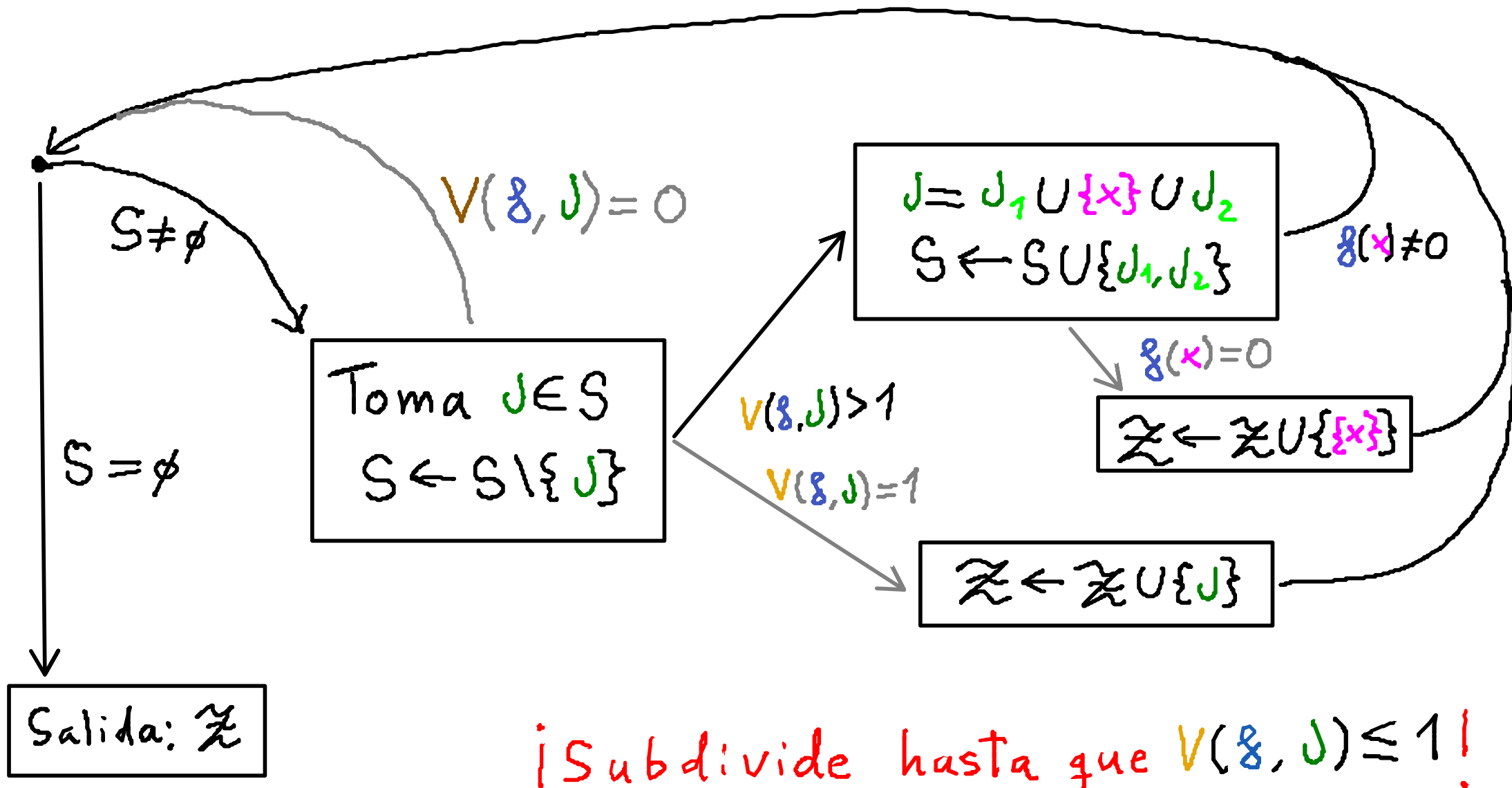
donde $D(x, r) := \{z \in \mathbb{C} \mid |z - x| \leq r\}$,

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

4) Subaditividad:

$$\bigcup_i J_i \subseteq J \Rightarrow \sum_i V(\mathcal{S}, J_i) \leq V(\mathcal{S}, J)$$

Resolvedor DESCARTES III: El Algoritmo ⁷



¿Por qué

es DESCARTES

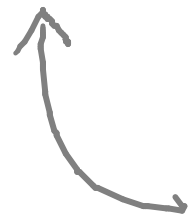
tan rápido en la práctica?

Paradigmas de Complejidad I:

¿Somos demasiado pesimistas?

Complejidad del Peor Caso:

$$\max \{ \text{cost}(\text{RESOLVEDOR}, \mathcal{E}) \mid \text{bit-size}(\mathcal{E}) \leq \gamma, \deg(\mathcal{E}) \leq d \}$$



¡pesimista en la práctica!

Paradigmas de Complejidad II:

Más allá del pesimismo

Complejidad del Peor Caso:

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

(Goldstein & von Neumann, 1951) } (Rough garden, 2021)
 (Demmel, 1988) (Smale; 1985, 1997) ↓

Complejidad Probabilística

$$\mathbb{E}_f \{ \text{cost}(\text{RESOLVEDOR}, f) \mid \text{bit-size}(f) \leq r, \deg(f) \leq d \}$$

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

Más allá del Pesimismo I:

Forma Simple

$$F = \sum_{k=1}^d f_k X^k \quad \text{polinomio aleatorio bit uniforme}$$

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

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

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

↑
¡cuasi-óptimo
en media!

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 :

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

peso de f :

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

↖ No hay errata!

uniformidad de f :

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

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

Flexibilidad del Modelo Aleatorio I:

Control de Soporte

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

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

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

Entonces...

$$u(F) = 0$$

Flexibilidad del Modelo Aleatorio II:

Control de Signos

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

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

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

Entonces...

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

Flexibilidad del Modelo Aleatorio III:

Control de tamaño bit

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

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

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

Entonces...

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

Flexibilidad del Modelo Aleatorio IV

+ todas las combinaciones

Más allá del Pesimismo III:

TEOREMA PRINCIPAL

TEO. PRIN. (Ergür, T-C, Tsigaridas)

$$\mathbb{E}_{\mathbf{f}} \text{cost}(\text{DESCARTES}, \mathbf{f}) = \hat{\mathcal{O}}_{\mathbf{B}}(d^2 + d\gamma)(1 + u(\mathbf{f})^4)$$

Obs 1. En muchos casos,

$$u(\mathbf{f}) = \mathcal{O}(1)$$

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?

Pococonomios I: ¿Qué son?

Def. (Kushnirenko)

Un pococonomio es un polinomio
con pocos términos

Ex. $f = 53 - 48x^2 + 500x^{3400}$

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

Origen del Nombre:

polinomio $\rightarrow$ polynomial $\rightarrow$ многочлены

$\rightarrow$ малочлены $\rightarrow$ Fewnomial $\rightarrow$ pococonomio

Poconomios II: ¿Qué queremos?

tamaño bit del mayor exponente

↓

$$\hat{O}_B \left(\text{poly}(t, \log d, \gamma) \right)$$

↑

monomios

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

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.

COR. No hay un resolutor eficiente
de poconomios

Poconomios IV:

Posibilidad en el Caso Medio

TEO (Ergür, TC, Tsigaridas)

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

(Jindal & Sagraloff, 2017)

PREGUNTA ABIERTA:

¿Podemos mejorar la cota?

Eskerriak Asko

zuen arretagatik!

¡Muchas Gracias

por vuestra atención!

galderak? ¿preguntas?