Matemáticas y Eficacia: lo complejo, lo tratable y lo probable.*

Luis M. Pardo
Universidad de Cantabria

May 17, 2006

*Matemáticas en Acción '2005/06

Algunas "Ficciones" Publicitarias

Vivimos Tiempos Digitales de la Informática[†].

Ubicuidad del universo digital (está presente en todos los dominios de la vida....)

Creencia en el poder Omnímodo de la Computación...

[†]Digital: del dedo

Hay algo "incompleto" en estos pensamientos.

Son pensamientos "simplistas"

SÓLO ES PUBLICIDAD![‡]

[‡]Uno no debe creer todo lo que se dice en los púlpitos, en las cátedras y en la Tele...

Big Fact:

La informática es un instrumento útil, pero tiene sus LIMITACIONES.

Little Fact:

La informática representa el único caso de la Historia de la Ciencia en el que el Modelo Matemático antecede al objeto físico.

Por eso la Matemática debe cuidar su responsabilidad para con la informática.

Algunas Limitaciones Fundacionales

[Turing, 1936]: La informática es incapaz de manipular números reales computables. (Sobre la existencia y computabilidad de $\mathbb{R}$)
Ergo, los estudios y métodos del análisis matemático (EDO',EDP's, Aproximación, etc...) no son susceptibles de ser manipulados por un ordenador: el análisis es continuo la computación es discreta.[§]

[Gödel, 1933]: Hay preguntas enunciables sobre los números enteros y naturales que tienen respuesta demostrable (son Teoremas), pero no tienen tratamiento computacional.

[§]Aún en [Demmel, 2005] el autor intenta entender qué y cómo hacer análisis numérico bien fundamentado.

Limitaciones menos duras: Eficacia

Balanzas y Monedas

Problemas fáciles con monedas falsas.

[**La Falsa Moneda**]Dadas n monedas de igual aspecto y una balanza, sabiendo que sólo una es falsa (en peso), encontrarla.

Problemas fáciles con monedas falsas.

[La Falsa Moneda]Dadas n monedas de igual aspecto, sabiendo que sólo una es falsa en peso, encontrarla.

Usando una balanza, bastará con hacer

$$\log n + 1,$$

comparaciones.

Problemas fáciles con monedas falsas.

[La Falsa Moneda]Dadas n monedas de igual aspecto, sabiendo que sólo una es falsa en peso, encontrarla.

Usando una balanza, bastará con hacer

$$\log n + 1,$$

comparaciones.

Y no se puede hacer con menos pesadas !!.

Otras variantes.

[**La Falsa Moneda**]Dadas n monedas de igual aspecto, sabiendo que, a lo sumo, hay una falsa, detectarla.

[**La Más Falsa de Todas**] Dadas n monedas de igual aspecto, detectar la más pesada.

[**Muchas monedas iguales**]Dadas n monedas, decidir si k de ellas son iguales.

[Las Monedas Auténticas que no consigo cambiar]

Un viajero ha pasado su vida recorriendo el globo. En su cuarto se amontonan piezas de monedas, de ésas que nunca nos cambian en los aeropuertos, de aspectos y valores muy diversos. Un cambista de Brooklyn, está dispuesto a cambiarle las monedas por dólares con una condición: sólo le cambiará monedas por valor de cinco mil dólares en billetes.

[Las Monedas Auténticas que no consigo cambiar]

Un viajero ha pasado su vida recorriendo el globo. En su cuarto se amontonan piezas de monedas, de ésas que nunca nos cambian en los aeropuertos, de aspectos y valores muy diversos. Un cambista de Brooklyn, está dispuesto a cambiarle las monedas por dólares con una condición: sólo le cambiará monedas por valor de cinco mil dólares en billetes.

Después de varios intentos infructuosos, prolongados durante varios años, el viajero reconoce que no puede seleccionar esas monedas. Pide ayuda a sus amigos, que también fracasan, éstos a sus conocidos y así hasta dar con un matemático. A la sazón el cambista ya no está interesado en las monedas del viajero y a éste sólo le queda la curiosidad de entender el porqué de tantos fracasos para una tarea aparentemente tan sencilla.

[Fabricante de Ventanas]

Medidas de todas las ventanas de un edificio (casi todas distintas): $x_1, \ldots, x_n$.

Comprar barras de Aluminio (cada una de 6 metros de largo).

Ajustar las medidas para no perder más de 10 cm de barra por corte.

[Mochilas]

Diversos productos en un almacén $x_1, \ldots, x_n$.

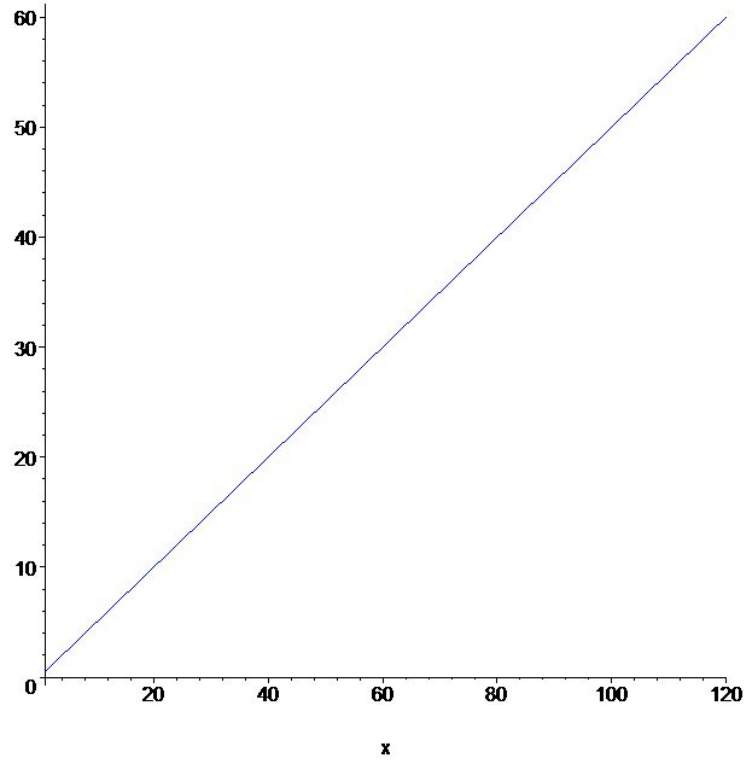
Camión de reparto con una capacidad (3 Tm).

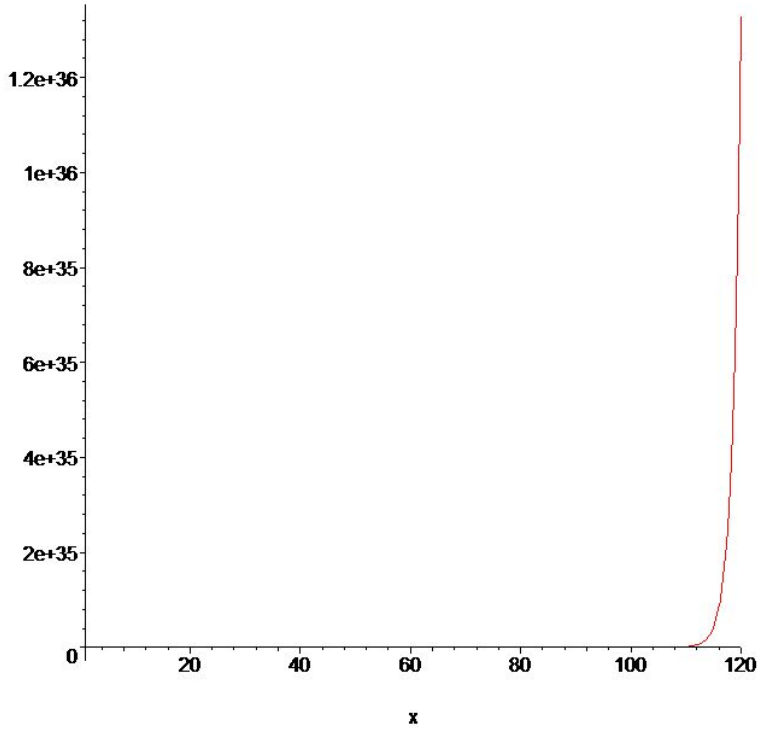
Tratar de cargar el camión en algún viaje sin dejar huecos vacíos.

Teorema [Cook, 1972]
Nadie en el mundo sabe resolver el problema de las monedas del viajero sin hacer 2^n *pruebas, donde* n *es el número de monedas.*

Funciones de Complejidad. Relacionan el tamaño de los datos con el número de pasos de cálculo,

Gráficamente

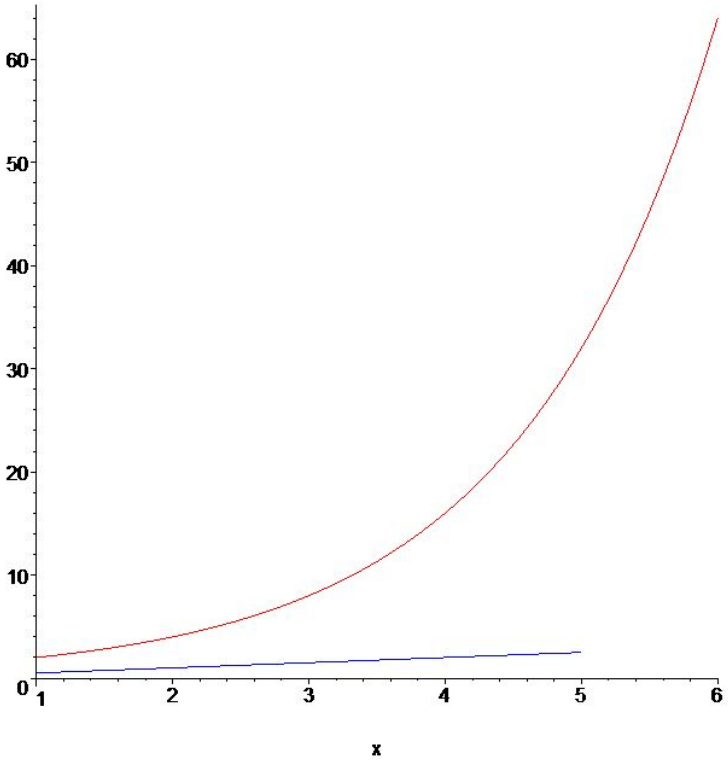


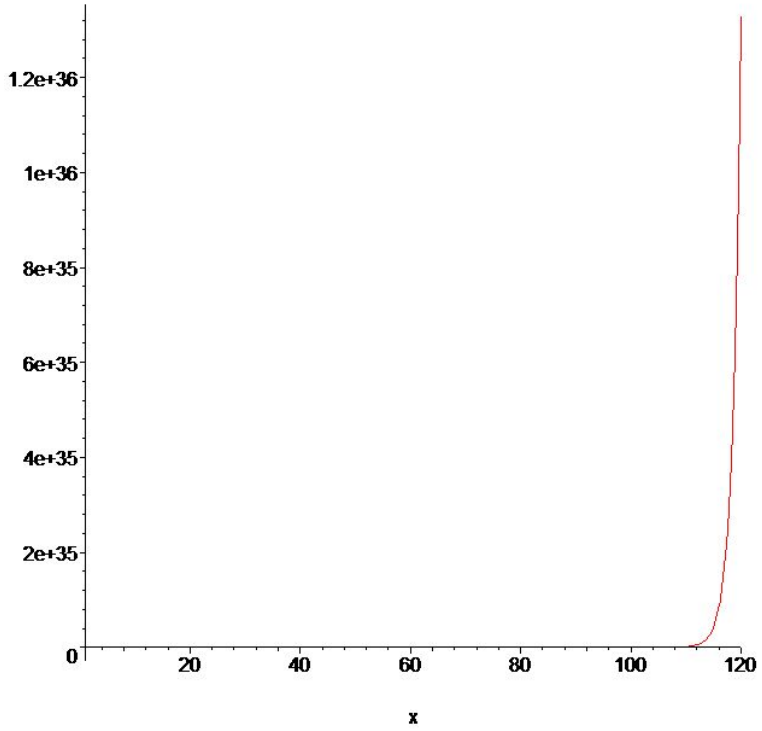


Tiempo Lineal

Tiempo Exponencial

Uno Frente al Otro





Mediante una Tabla

El mejor ordenador existente (Blue Gene/L de IBM)
Según el Top500 de Supercomputing fuciona a una velocidad de entre 28.10^7 Mips (experimentales) y 36.10^7 Mips.

Mediante una Tabla

El mejor ordenador existente (Blue Gene/L de IBM)
Según el Top500 de Supercomputing fuciona a una velocidad de entre 28.10^7 Mips (experimentales) y 36.10^7 Mips.

	n=10	**n=50**	**n= 100**	**n=150**
Tiempo n/2	$\leq$ 1 Nanos	$\leq$ 1 Ns	$\leq$ 1 Ns	$\leq$ 1 Ns
Tiempo n^3	$\leq$ 1 Nanos	$\leq$ 1 segs.	$\leq$ 1 segs.	$\leq$ 1 segs.
Tiempo 2^n	$\leq$ 1 Nanos	$\leq$ 1/13 s	$\geq 10^4$ Años	$\geq 10^9$ **Mill. Años**

Hay miles de problemas "sencillos" cuya función de complejidad es mucho peor que 2^n irremediablemente.

Explicar el Fenómeno

Un pequeño resumen de su historia.

A través de un sencillo y clásico problema de Algebra.

Ecuaciones Polinomiales.

Polinomios

Son las funciones más inmediatamente computacionales:

Sólo requieren saber sumar,restar, multiplicar y ... ni siquiera hay que saber dividir.

Y, sin embargo, son capaces de producir grandes "malformaciones" científicas.

Han sido usados como "aproximación" a la verdad.

Y, sin embargo, han sido la fuente de gran parte del pensamiento matemático.

Han sido negados en muchos procesos de modelización.

Y, sin embargo, se acude a ellos cuando se quiere modelizar con la ayuda del ordenador.

El chiste de los polinomios

Un polinomo define una función "evaluable" de muchas maneras:

$$f : \mathbb{C}^n \longrightarrow \mathbb{C}.$$

$$f \in \mathbb{C}[X_1, \ldots, X_n].$$

$$f := \sum_{\mu \in \mathbb{N}^n} a_\mu X_1^{\mu_1} \cdots X_n^{\mu_n},$$

con todos los a_μ nulos salvo un conjuno finito.

O sea, f se puede calcular con un número finito de sumas, restas y multiplicaciones de constantes y valores de las variables $X_1, \ldots, X_n$.

Es fácil ir...

Dado $x \in \mathbb{C}^n$, es posible y fácil hallar $f(x) \in \mathbb{C}$.

Es fácil ir...Difícil volver

Dado $x \in \mathbb{C}^n$, es posible y fácil hallar $f(x) \in \mathbb{C}$.

Dado $b \in \mathbb{C}$, es difícil hallar $f^{-1}(b)$.

Geometría Algebraica.

Conjunto algebraico:

$V \in \mathbb{C}^n$ dado mediante:

$$V = f_1^{-1}(b), \ldots, f_m^{-1}(b).$$

$$F := (f_1, \ldots, f_m) : \mathbb{C}^n \longrightarrow \mathbb{C}^m$$

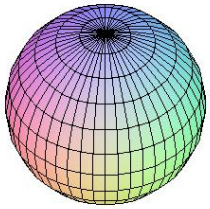
$$V = F^{-1}(b)$$

.

Una pregunta simple:
Cuál es la "pinta" de un conjunto algebraico?

Uno/Tres ejemplos simples:

$$X^2 + Y^2 + Z^2 = \varepsilon.$$

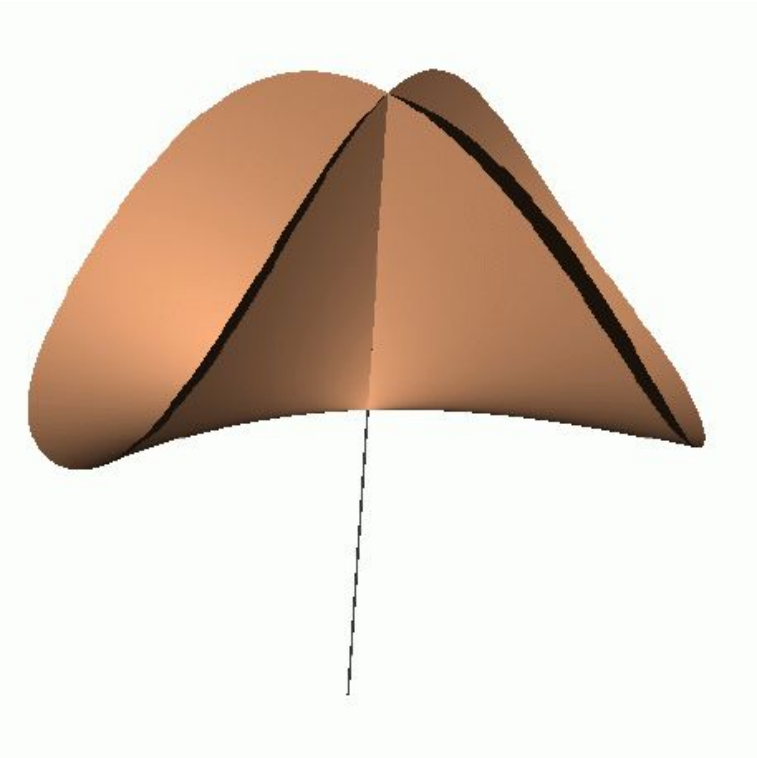


$\varepsilon = 1$

$\varepsilon = 0 \qquad (0,0,0)$

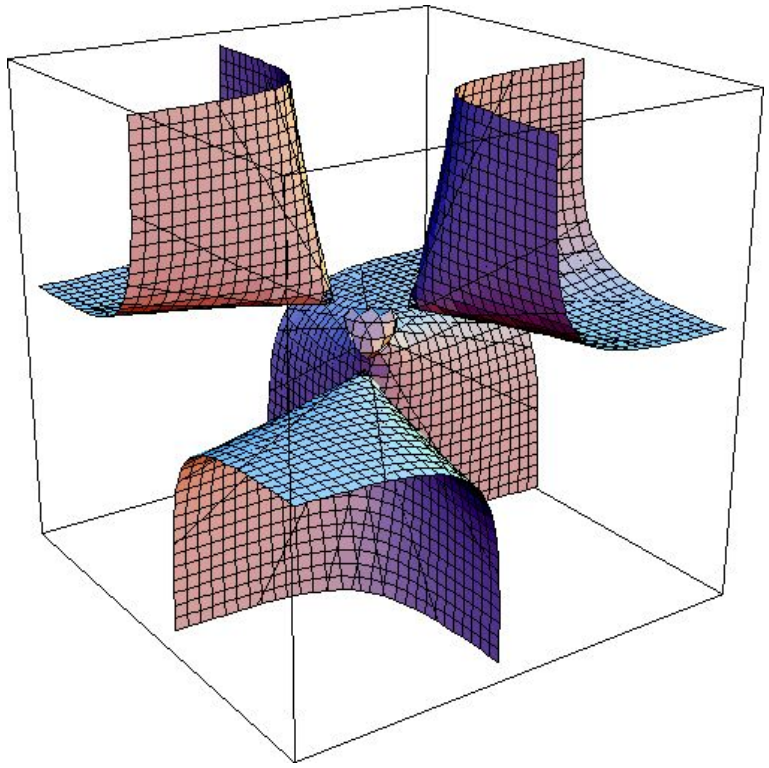
$\varepsilon = -1 \qquad \emptyset$

Ejemplos de singularidades: Paraguas de Withney



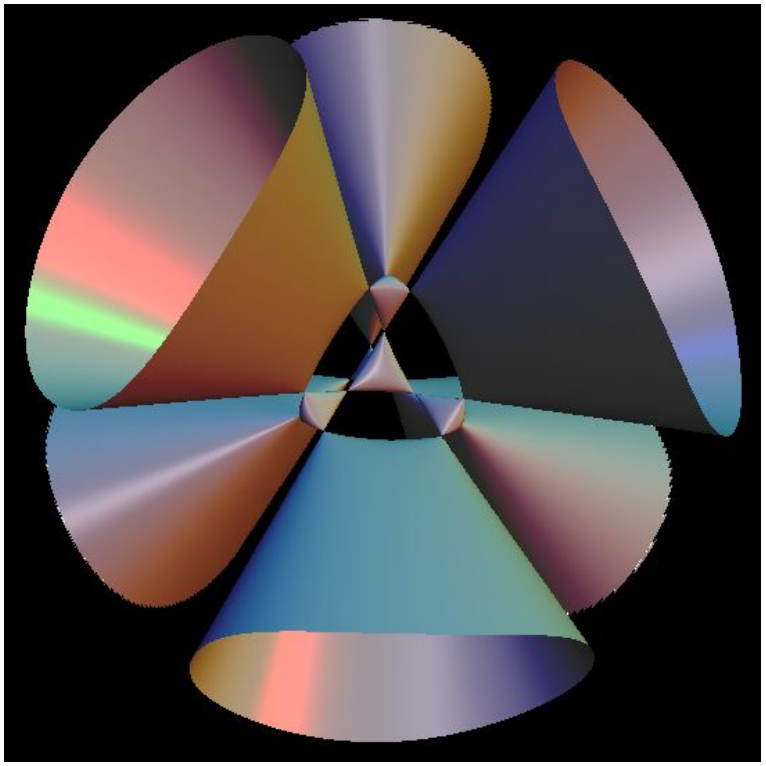
$$x^2 - y^2 z = 0.$$

Ejemplos de singularidades: Cúbica de Cayley



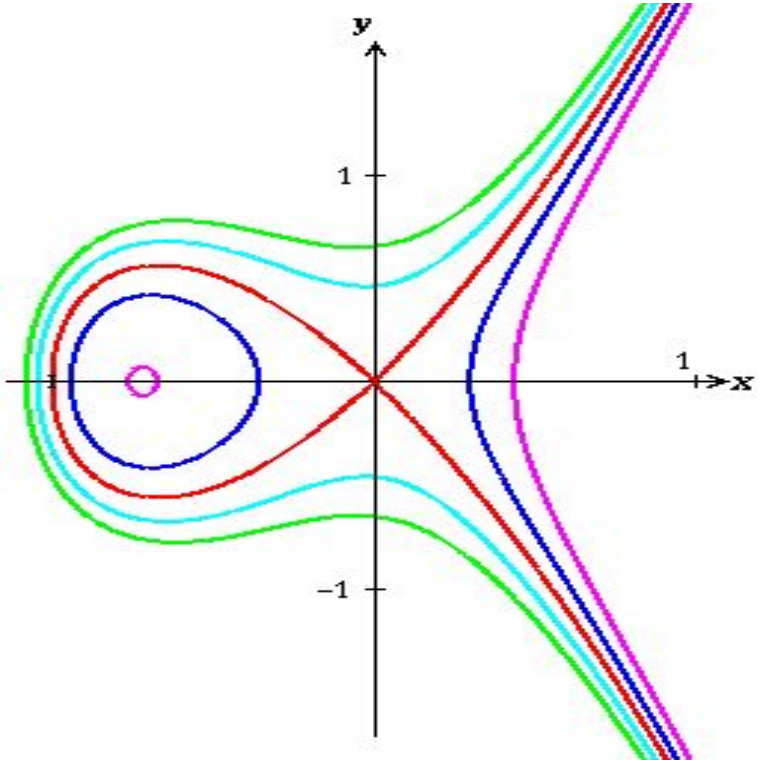
$$4(x^2 + y^2 + z^2) + 16xyz - 1 = 0.$$

Ejemplos de singularidades: Kummer



$$-(1-\sqrt{2}x-z)(1+\sqrt{2}x-z)(1-\sqrt{2}y+z)(1+\sqrt{2}y+z)+$$
$$+(x^2+y^2+z^2-1)^2=0.$$

Qué difícil es saber la pinta cuando uno vuelve de un polinomio!



$$y^2 = x^3 + x^2 + bx + 2b$$

b = 0 b = 0.1 b = -0.05 b = -0.112

Los Casos “Fáciles”: n=1 o deg(F)=1.

El Caso deg(F)=1:

Sitemas de Ecuaciones Lineales:

$$AX = B?,$$

Gauss y Wilhelm Jordan ya....

o puede que no.... Algebra Lineal Numérica o Simbólica.

El caso $n = 1$

Input: Un polinomio Univariado

$$f := X^n + a_{n-1}X^{n-1} + \cdots + a_0.$$

Output: Una (o todas) raíz.

$$\zeta, \quad f(\zeta) = 0.$$

Resolver por "radicales" **?????**

Scipione del Ferro (1465–1526)

Tartaglia (1500–1557)

Cardano (1501-1576)

F. Viète (1540–1603) El Abogado.

Aunque no se sabe bien qué ventajas aporta la resolución por radicales, llegan hasta ecuaciones de grado 4.

N. Abel (1802-1829)

Démonstration

de l'impossibilité de la résolution générale des équations du cinquième degré.

Les géomètres se sont beaucoup occupés de la résolution générale des équations algébriques, et plusieurs d'entre eux ont cherché à en prouver l'impossibilité; mais si je ne me trompe pas, on n'a pas y reussi jusqu'à présent. J'ose donc esperer que les géomètres veulent recevoir avec bienveillance ce mémoire qui a pour but de remplir cette lacune dans la théorie des équations algébriques.

Soit

$$y^5 - ay^4 + by^3 - cy^2 + dy - e = 0$$

l'équation générale du cinquième dégré et supposons qu'elle est résoluble algébriquement c'est-à-dire qu'on peut exprimer y par une fonction des quantités a b c d et e, formée par des radicaux. Il est clair qu'on peut dans ce cas mettre y sous cette forme:

$$y = p + p_1 R^{\frac{1}{m}} + p_2 R^{\frac{2}{m}} + \ldots\ldots + p_{m-1} R^{\frac{m-1}{m}}$$

m étant un nombre premier et R p p_1 p_2 etc. des fonctions de la même forme que y, et ainsi de suite jusqu'à ce qu'on parviendra à des fonctions rationnelles des quantités a b c d et e. On peut aussi supposer qu'il est impossible d'exprimer $R^{\frac{1}{m}}$ par une fonction rationnelle des quantités a b etc. p p_1 p_2 etc., et en mettant $\frac{R}{p_1^m}$ au lieu de R il est clair qu'on peut faire $p_1 = 1$. On aura donc:

$$y = p + R^{\frac{1}{m}} + p_2 R^{\frac{2}{m}} + \ldots p_{m-1} R^{\frac{m-1}{m}}$$

Hay ecuaciones de grado mayor que cinco que no son resolubles por radicales!!!!.

Galois (1811-1832)

Evariste Galois (1811–1832)

Dos dibujos de E. Galois, el segundo de 1848 por su hermano

cela s'appelle la ...

En d'autres termes, quand un groupe G en contient un autre H, le groupe G peut se partager en groupes ~~[illegible]~~ que l'on obtient chacun en opérant sur les permutations de H une même substitution, en sorte $G = H + HS + HS' + \ldots$ et aussi il peut se décomposer en groupes qui ont tous les mêmes substitutions en sorte que $G = H + TH + T'H + \ldots$ Ces deux genres de décompositions ne coïncident pas ordinairement. Quand elles coïncident, la décomposition est dite propre.

Si ces groupes ont chacun un nombre premier de permutations, l'équation ~~avec~~ sera soluble par radicaux; sinon, non.

E. Galois, “ *Mémoires...*”

Si maintenant vous me donnez une équation que vous aurez choisie à votre gré et que vous désiriez connaître si elle est ou non soluble par radicaux, je n'aurai rien à y faire que de vous indiquer le moyen de répondre à votre question,...

sans vouloir charger ni moi ni personne de le faire. En un mot, les calculs sont impraticables.

Galois ha descubierto la eficacia o complejidad de algoritmos.

Galois ha descubierto la eficacia o complejidad de algoritmos.

Ejemplo:Para un polinomio de grado 15, se necesita (con probabilidad 1, un espacio vectorial de dimensión

$$10^{12}.$$

Hay problemas Tratables y problemas Intratables por la dificultad de sus cálculos.

Galois ha descubierto la eficacia o complejidad de algoritmos.

Hay problemas Tratables y problemas Intratables por la dificultad de sus cálculos.

Ejemplo:Para un polinomio de grado 15, se necesita (con probabilidad 1, un espacio vectorial de dimensión

$$10^{12}.$$

Pero... Qué es "cálculos"?

Hasta 1933, los matemáticos (ni siquiera habían imaginado) que no sabían lo que es un algoritmo, método, procedimiento o programa!!!!!!!!!!

Problema X de Hilbert

Dar un algoritmo que decida si una ecuación polinomial tiene soluciones racionales.

Una ecuación polinomial y muchas variables.

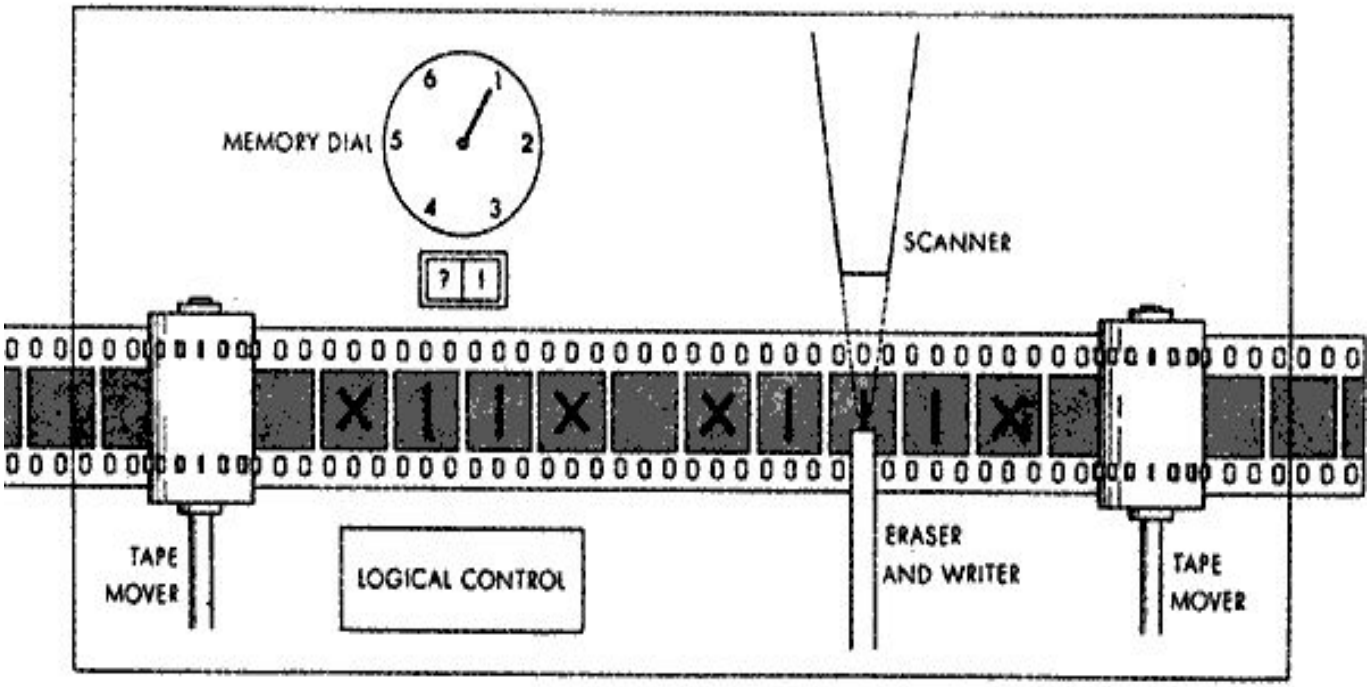
Dos visionarios y uno que les comprendió

K. Gödel

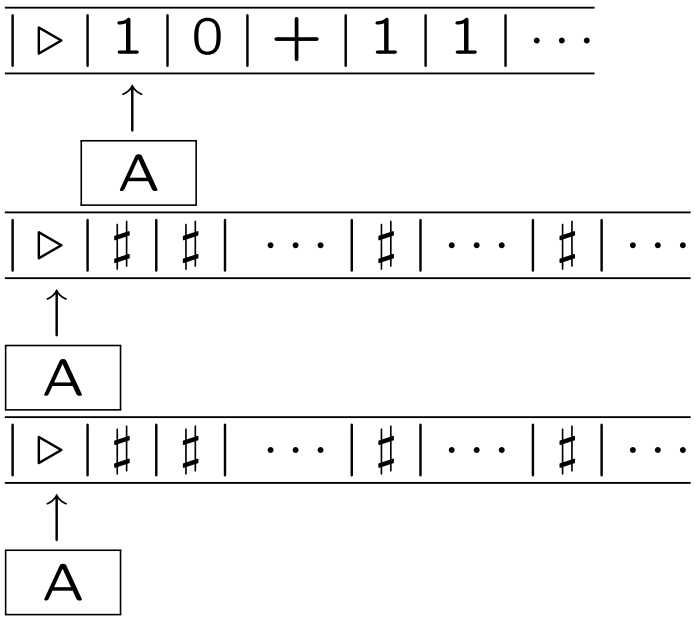
A. Turing

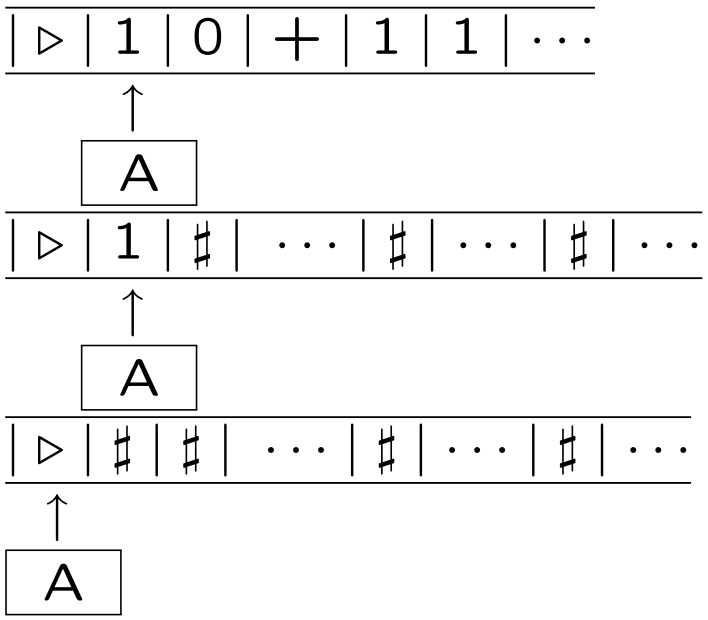
A. Church

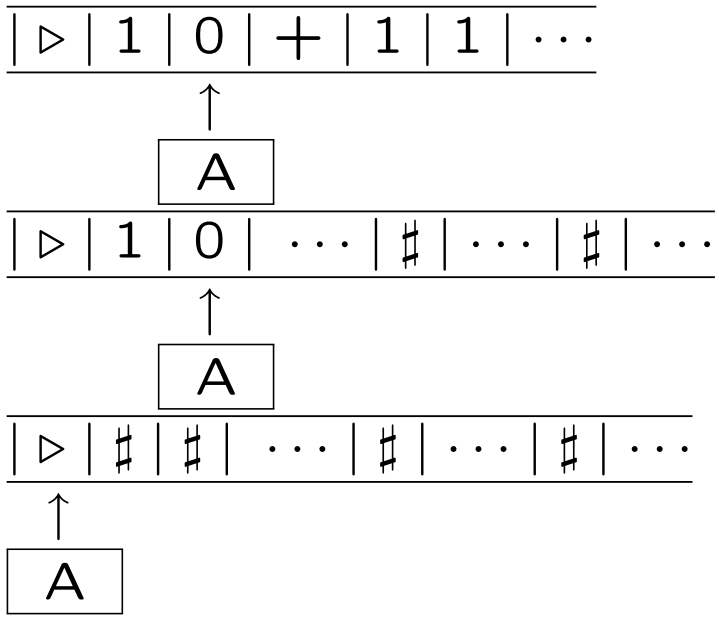
Un “algoritmo” es una máquina de Turing.

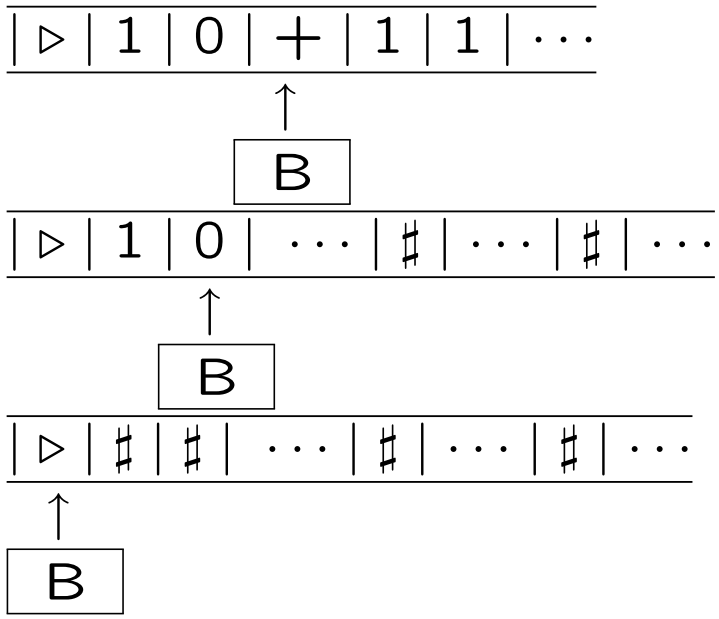


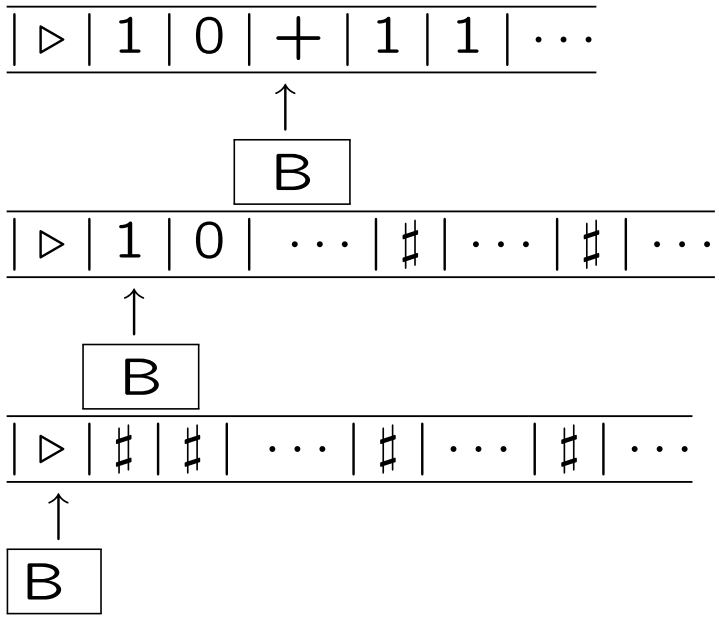
Dibujo de Lee Manovich

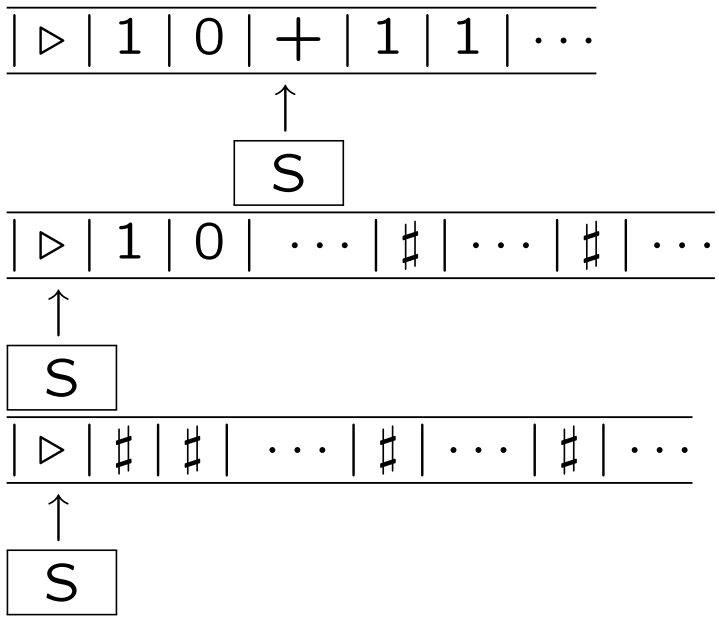

| ▷ | 1 | 0 | + | 1 | 1 | ···
A
| ▷ | ♯ | ♯ | ··· | ♯ | ··· | ♯ | ···
A
| ▷ | ♯ | ♯ | ··· | ♯ | ··· | ♯ | ···
A

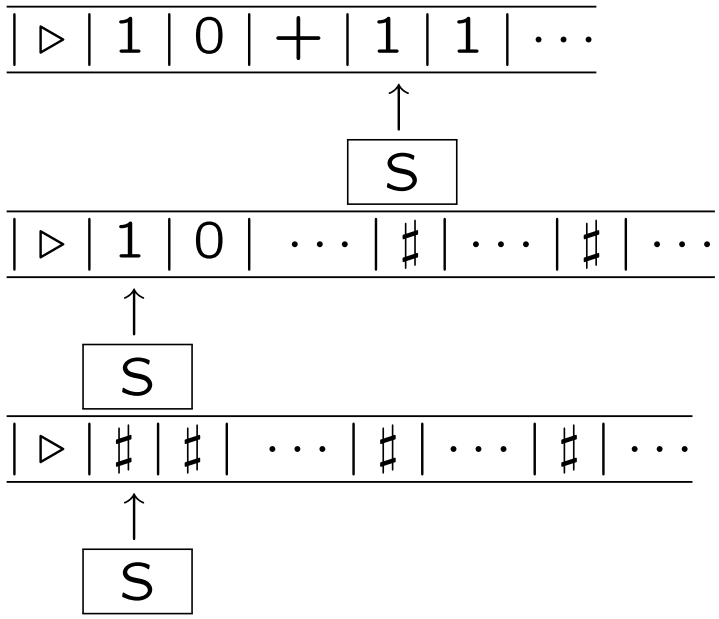

| ▷ | 1 | 0 | + | 1 | 1 | · · ·
A
| ▷ | 1 | ♯ | · · · | ♯ | · · · | ♯ | · · ·
A
| ▷ | ♯ | ♯ | · · · | ♯ | · · · | ♯ | · · ·
A

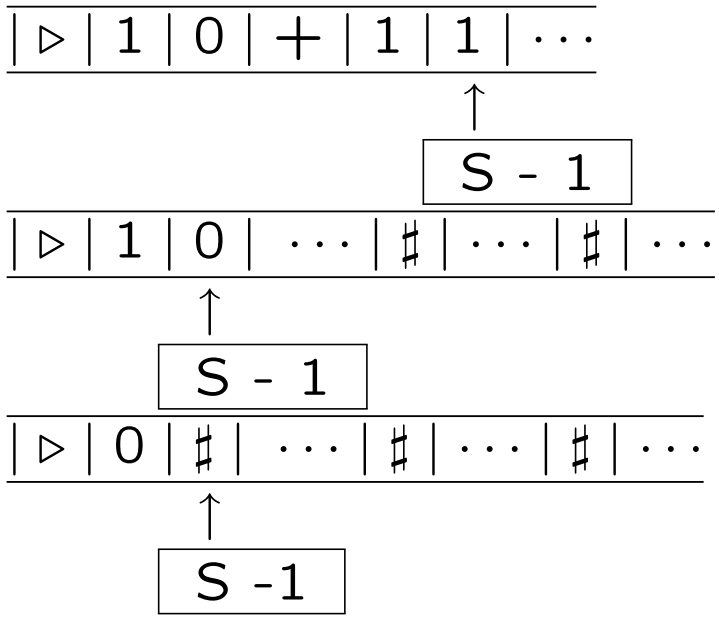

| ▷ | 1 | 0 | + | 1 | 1 | ···
A
| ▷ | 1 | 0 | ··· | ♯ | ··· | ♯ | ···
A
| ▷ | ♯ | ♯ | ··· | ♯ | ··· | ♯ | ···
A

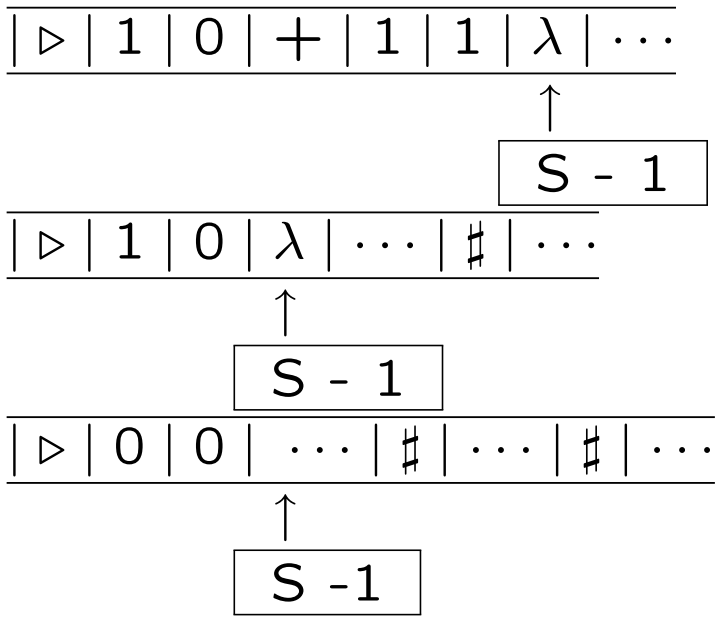

| ▷ | 1 | 0 | + | 1 | 1 | ···
B
| ▷ | 1 | 0 | ··· | ♯ | ··· | ♯ | ···
B
| ▷ | ♯ | ♯ | ··· | ♯ | ··· | ♯ | ···
B

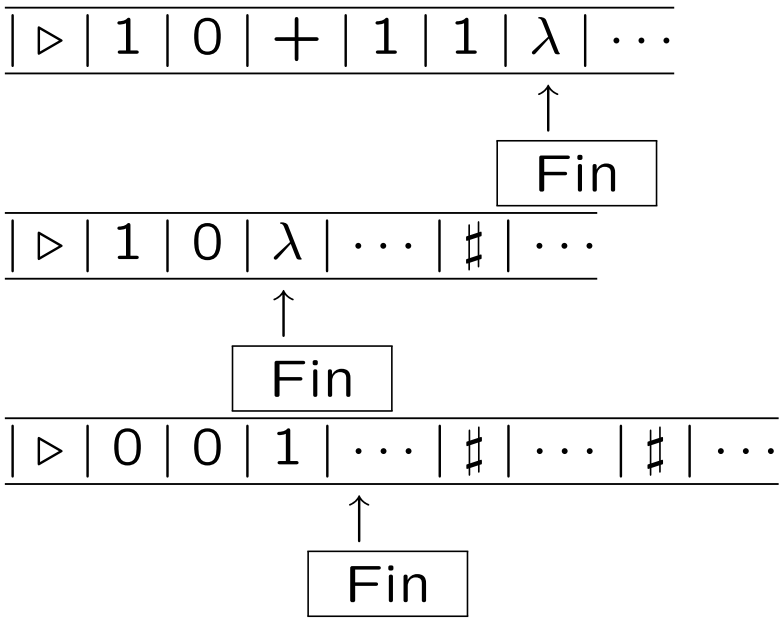

▷ 1 0 + 1 1 ···
B
▷ 1 0 ··· ♯ ··· ♯ ···
B
▷ ♯ ♯ ··· ♯ ··· ♯ ···
B


| ▷ | 1 | 0 | + | 1 | 1 | ···
S
| ▷ | 1 | 0 | ··· | ♯ | ··· | ♯ | ···
S
| ▷ | ♯ | ♯ | ··· | ♯ | ··· | ♯ | ···
S


| ▷ | 1 | 0 | + | 1 | 1 | ···
S
| ▷ | 1 | 0 | ··· | ♯ | ··· | ♯ | ···
S
| ▷ | ♯ | ♯ | ··· | ♯ | ··· | ♯ | ···
S


| ▷ | 1 | 0 | + | 1 | 1 | ···
S - 1
| ▷ | 1 | 0 | ··· | ♯ | ··· | ♯ | ···
S - 1
| ▷ | 0 | ♯ | ··· | ♯ | ··· | ♯ | ···
S -1


| ▷ | 1 | 0 | + | 1 | 1 | λ | ···
S - 1
| ▷ | 1 | 0 | λ | ··· | ♯ | ···
S - 1
| ▷ | 0 | 0 | ··· | ♯ | ··· | ♯ | ···
S -1


| ▷ | 1 | 0 | + | 1 | 1 | λ | ···
Fin
| ▷ | 1 | 0 | λ | ··· | ♯ | ···
Fin
| ▷ | 0 | 0 | 1 | ··· | ♯ | ··· | ♯ | ···
Fin

Lo importante no es la máquina (hardware), sino el "programa" (software)

Una hojita de papel donde se encuentran las descripciones de las operaciones a realizar según las "configuraciones" que se nos presentan.

La Importancia del Invento.

Escenario:

Segunda Guerra Mundial.

Batalla de Inglaterra: Sitiada por mar y por aire...

Hay que predecir los ataques alemanes, interceptando sus medios de Comunicación.

El Proyecto Ultra de Churchill.

Enigma

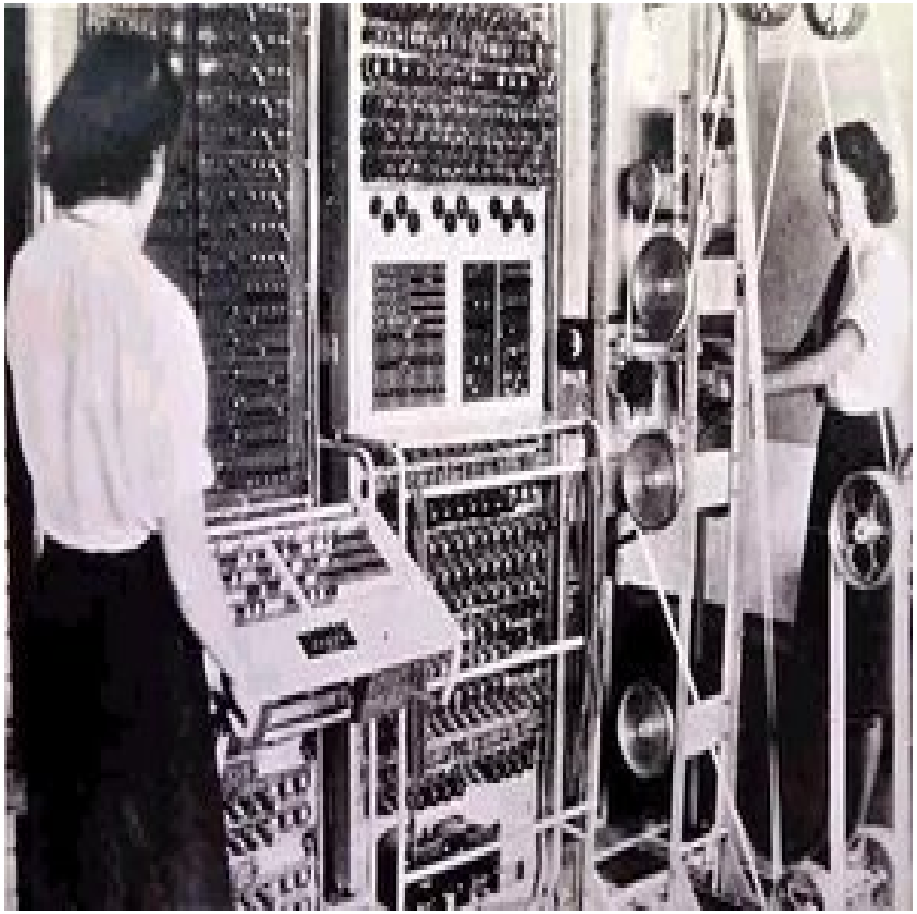
Lorentz de 12 rotores

Blecthley Park

Un barracón restaurado para turistas

Un “verdadero” barracón de trabajo

La casa de Turing



Una foto de la época de Colossus

Un intento de reconstruir Colossus

Y después de Colossus

ENIAC, Mark I y II,....IBM...MacIntosh....Linux....

La Era de los circuitos de silicio (Ingeniería).

En Matemáticas: la Computación Numérica, la Computación Simbólica....

Pero seguimos sin saber por qué no se pueden resolver problemas como las monedas del viajero o las ventanas de aluminio en los super-ordenadores de hoy en día...!!!!!!!!

Stearns y Hartmanis (60's): La máquina de Turing como patrón de medida.

Cook y Karp (70's) : Descubrimiento de la Frontera de la Intratable.

Rivest, Adleman, Sharir (70's): De cuando la Complejidad se vuelve útil.

Solovay–Strassen, Miller–Rabin (70's): Probabilismo como alternativa utilizable.

El mundo al revés: RSA

Hecho 1.- **Nadie en el mundo sabe factorizar números enteros de manera tratable!**

Hecho 2.- **Se pueden encontrar primos grandes de manera probabilista (o determinítica–desde 2002) tratable!**

La Fortuna de algunos:
Usemos el Teorema Pequeño de Fermat para la Criptografía....

R.S.A.

N.B.- No enseñemos a los chicos a hallar el máximo común divisor mediante factorización. Es un crimen de lesa complejidad!!

Garey–Johnson...o cómo conservar el empleo.

Cook.... o cómo encontrar a alguien en una fiesta.

Wiles...o cómo dar un millón de dólares por resolver un problema.

Problemas NP-duros.

(La Frontera de la Intratable)

PROBLEMAS INTRATABLES PARA LA COMPUTACIÓN
(Tiempo mayor que exponencial)

LA FRONTERA DE LO INTRATABLE
(NP-completos y NP-duros)

PROBLEMAS TRATABLES
(Tiempo polinomial)

Demasiados Problemas en la Frontera

Desde los primeros resultados de Cook y Karp, han aparecido montones de problemas en esa frontera.

Problemas de Grafos: CLIQUE, Hamiltonian Circuit,...

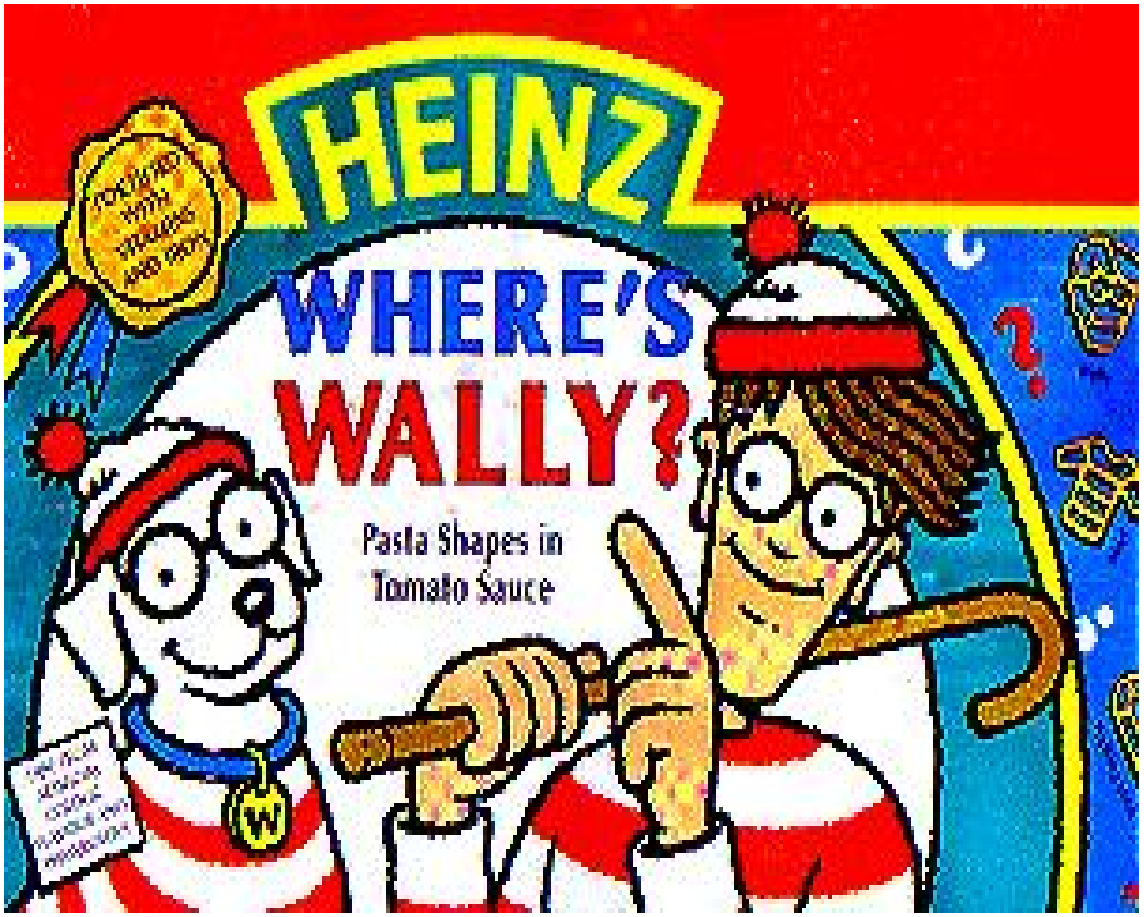
Problemas de Optimización: Integer Programming, Knapsack, Travelling Salesman,...

Problemas de Lógica: SAT, 3SAT...

Problemas de Códigos: Separation,...

Problemas en cualquier ámbito de la Computación....

Un Ejemplo Visual



Fácil de Verificar

Y si Wally no está?

Entonces el Problema es NP-duro.

Un Problema que los contiene a todos

Nullstellensatz de Hilbert–Kronecker

Dados polinomios multivariados $f_1, \ldots, f_s \in \mathbb{C}[X_1, \ldots, X_n]$,

Decidir si poseen alguna solución en común

$$\exists z \in \mathbb{C}^n, \quad f_i(z) = 0, \quad 1 \leq i \leq n?$$

Es un Problema NP-duro y toda la frontera está constituida por instancias particulares!!!!!!.

N.B.- No suspendamos a nadie que no discuta bien sistemas de ecuaciones lineales con dos o más parámetros si...No se la ha enseñado como tratarlos!!!!!!!!!

Un Ejemplo : Knapsack (Mochila)

Tenemos n monedas de valores $m_1, \ldots, m_n$

Un cambista quiere cambiarnos exactamente el valor k.

$$\exists S \subseteq \{1, \ldots, n\}, \quad \sum_{i \in S} m_i = k \ ?$$

En forma de Nullstellensatz:

Existe solución en $\mathbb{C}^n$ del siguiente sistema?

$$X_1^2 - X_1 = 0, \ldots, X_n^2 - X_n = 0, \sum_{i=1}^{n} m_i X_i = k \ ?$$

Problema 3. Es **P** igual a **NP** ?

Problema 4. Soluciones Entera de Polinomios y Complejidad. Relaciones?

Problema 5. Estimaciones de altura de Curvas diofánticas.

Problema 17. Complejidad de la Resolución Numérica de Ecuaciones Polinomiales.

Smale in Pictures

Smale in Pictures

Smale in Pictures

Un Paso hacia adelante Reciente

Solving Smale's 17th Problem (Bezout $5\frac{1}{2}$)

Trabajo con C. Beltrán (2005).

Presentado en

Foundations of Computational Mathematics '05

30 June – 9 July 2005, Santander

PLENARY SPEAKERS

- ★ Douglas ARNOLD (Minneapolis)
- ★ James DEMMEL (Berkeley)
- ★ Jan DENEF (Leuven)
- ★ Michael GRIEBEL (Bonn)
- ★ Ernst HAIRER (Genève)
- ★ Adrian LEWIS (Vancouver)
- ★ Stephane MALLAT (Paris)
- ★ Elizabeth MANSFIELD (Canterbury)
- ★ Robert MEYERHOFF (Boston)
- ★ Konstantin MISCHAIKOW (Atlanta)
- ★ Luis Miguel PARDO (Santander)
- ★ Ian SLOAN (Sydney)
- ★ Bernd STURMFELS (Berkeley)
- ★ Endre SÜLI (Oxford)
- ★ Eva TARDOS (Ithaca)
- ★ Vladimir TEMLYAKOV (Columbia)
- ★ Shang-Hua TENG (Boston)
- ★ Enrique ZUAZUA (Madrid)

WORKSHOPS

Nonplenary lectures will be held in 21 workshops, spanning a broad range of mathematical topics:

Foundations of numerical PDEs
Christoph Schwab & Eitan Tadmor

Geometric integration and computational mechanics
Begoña Cano, Debra Lewis & Brynjulf Owren

Information-based complexity
Leszek Plaskota & Ian Sloan

Learning theory
Steve Smale, David McAllester, Tomaso Poggio & Gabor Lugasi

Optimization
Raphael Hauser, Jim Renegar & Philippe Toint

Special functions and orthogonal polynomials
Mourad Ismail, Guillermo Lopez & Ed Saff

Approximation theory
Martin Buhmann & Juan Manuel Peña

Computational algebraic geometry
Teresa Krick & Andrei Gabrielov

Computational number theory
Alan Lauder & Jonathan Pila

Multiresolution and adaptivity in numerical PDEs
Wolfgang Dahmen, Bob Russell & Endre Süli

Numerical linear algebra
Lothar Reichel & Steve Vavasis

Relations to computer science: Algorithmic game theory and metric embeddings
Avrim Blum & Allan Borodin

Real-number complexity
Peter Bürgisser & Gregorio Malajovich

Computational dynamics
Jean-Pierre Ramis, Carles Simo & Warwick Tucker

Geometric modelling and animation
Tom Lyche & Larry Schumaker

Image and signal processing
Albert Cohen & Guillermo Sapiro

Stochastic computation
Brad Baxter & Thomas Müller-Gronbach

Symbolic analysis
Elizabeth Mansfield, Peter Olver & Mike Singer

Computational geometry and topology
Rich Schwartz & Abigail Thompson

Mathematical control theory and applications
Eduardo Casas, Uwe Helmke, Jean-Pierre Raymond & Enrique Zuazua

Random matrices
Ioana Dumitriu, Alan Edelman & Raj Rao

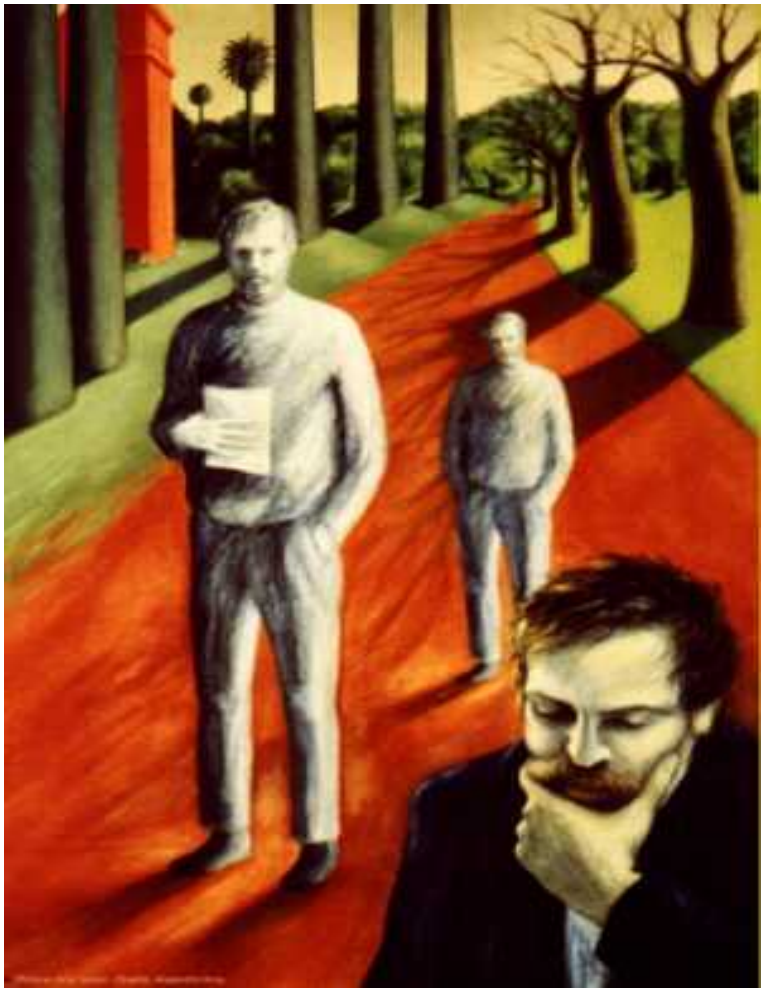
Main local organiser:
Luis Miguel PARDO

FoCM Executive Committee:
Endre SÜLI (Chair)
Raphael HAUSER (Secretary)
Jim RENEGAR (Treasurer)
Sue BRENNER
Felipe CUCKER
Wolfgang DAHMEN
Jean-Pierre DEDIEU
Ron DeVORE
Alan EDELMAN
Arieh ISERLES
Liz MANSFIELD
Peter OLVER
Allan PINKUS
Mike SHUB
Ian SLOAN
Eitan TADMOR
Mike TODD
Henryk WOŹNIAKOWSKI
Antonella ZANNA

FoCM

http://www.focm.net/FoCM05/

Y en TERA'05:Una conferencia en honor de Joos Heintz



Las Ideas de Shub & Smale

Empieza S. Smale en 1981

Caso univariado: Shub & Smale 1985–89

Caso Multivariado: Shub & Smale 1990–96

Caso Multivariado: 1996–2005–EL PARÓN!!!!. Problema 17 y Conjeturas varias.

Ceros Aproximados: Puntos donde el operador de Newton converge a una velocidad doblemente exponencial.

Un Sistema de Ecuaciones Polinomiales

$$F := [f_1, \ldots, f_n] \in \mathcal{H}_{(d)},$$

$deg(f_i) = d_i$, $(d) := (d_1, \ldots, d_n)$.

$$N_F(z) := z - DF(z)^{-1}(F(z)).$$

1990-91: Shub & Smale: comprensión de los principales fenómenos locales: $\gamma-$, $\alpha-$, $\mu-$ Teoremas.

Un Esquema Algorítmico

Input $F \in \mathcal{H}_{(d)}$

Esquema de Deformación Homotópica de Newton *Con Par Inicial*

$$(G, zeta) \in \mathcal{H}_{(d)} \times \mathbb{P}_n(\mathbb{C}), \;\; G(zeta) = 0.$$

Siguiendo un segmento de Ecuaciones:

$$F_t := (1-t)F + tG, \quad t \in [0,1].$$

(Una Curva de Ecuaciones Soluciones $\{(F_t, \zeta_t) \; : \; \zeta_t \in V(F_t), t \in [0,1]\}$)

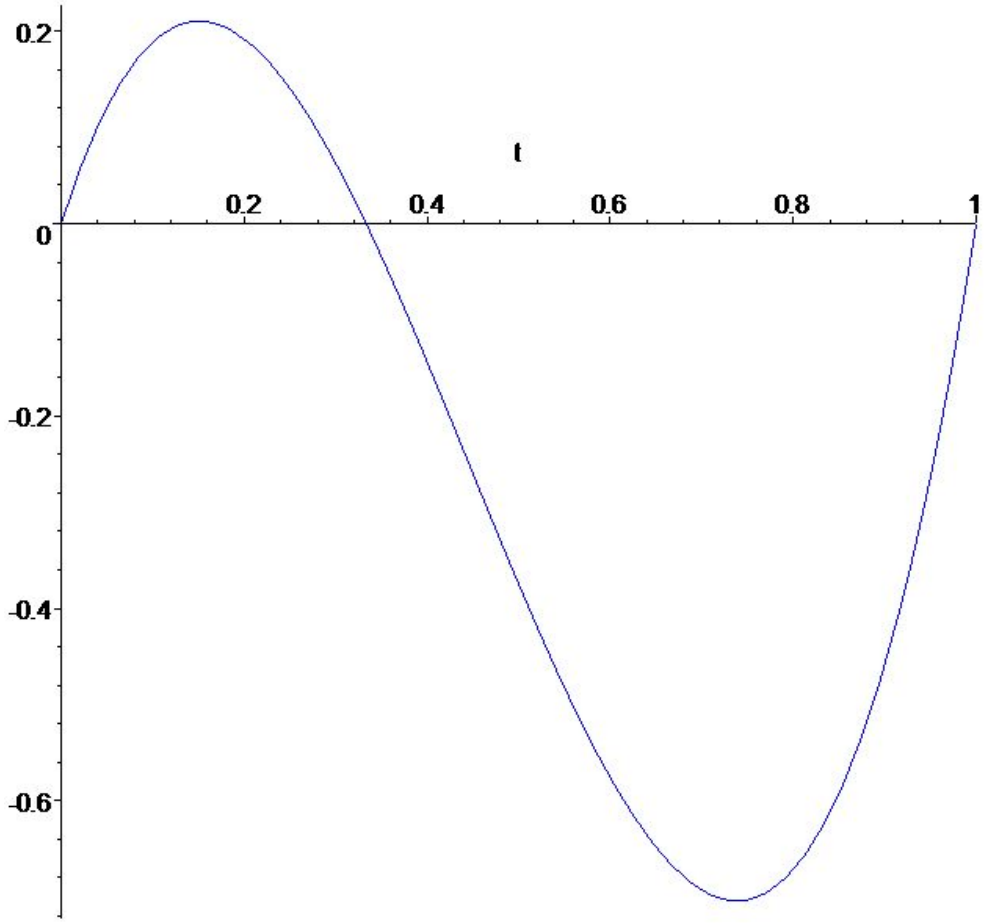
Desde un cero aproximado de (G, z) $(t = 1)$, hallar algún cero aproximado de F $(t = 0)$

Output:

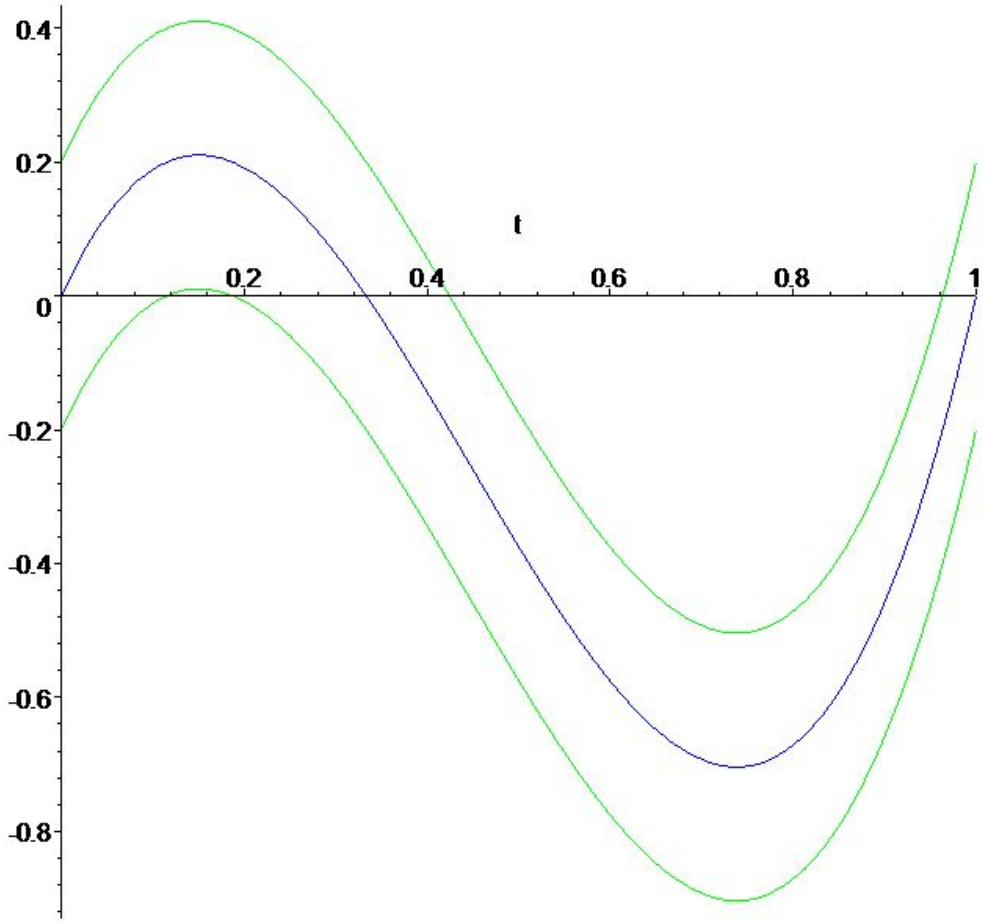
– O bien Fallo

– O un cero Aproximado de F.

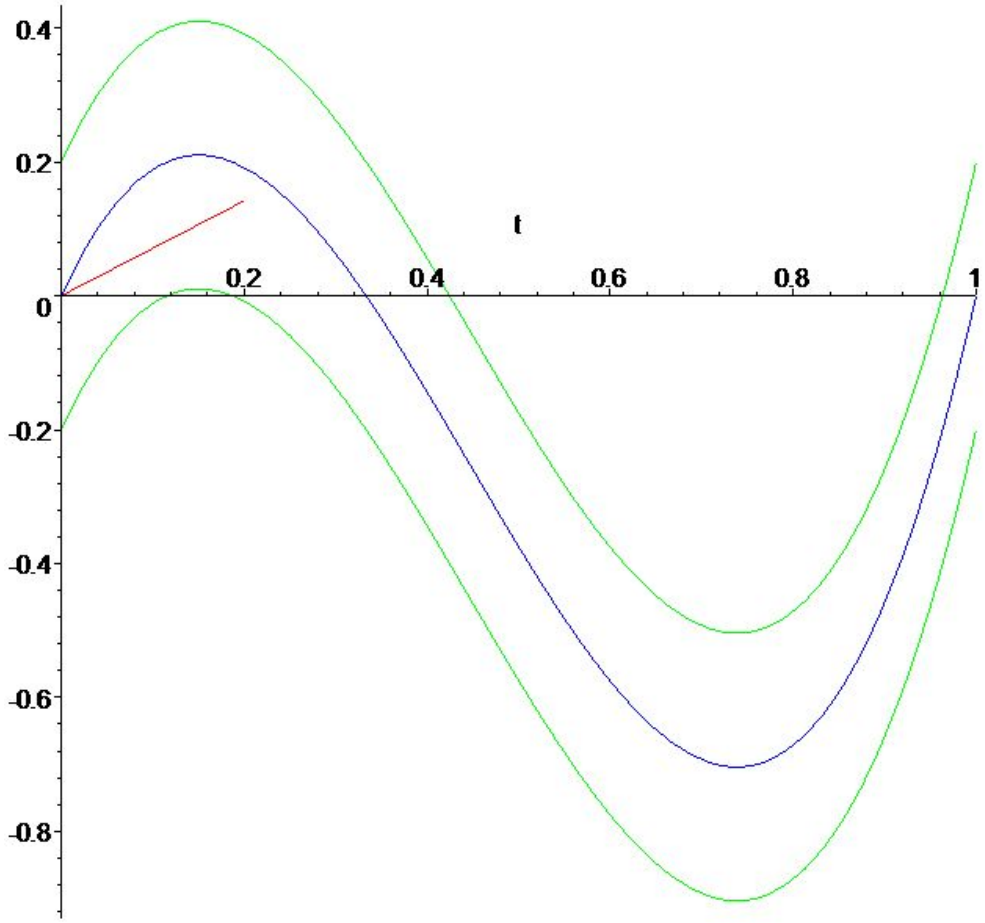
Una "curva" solución



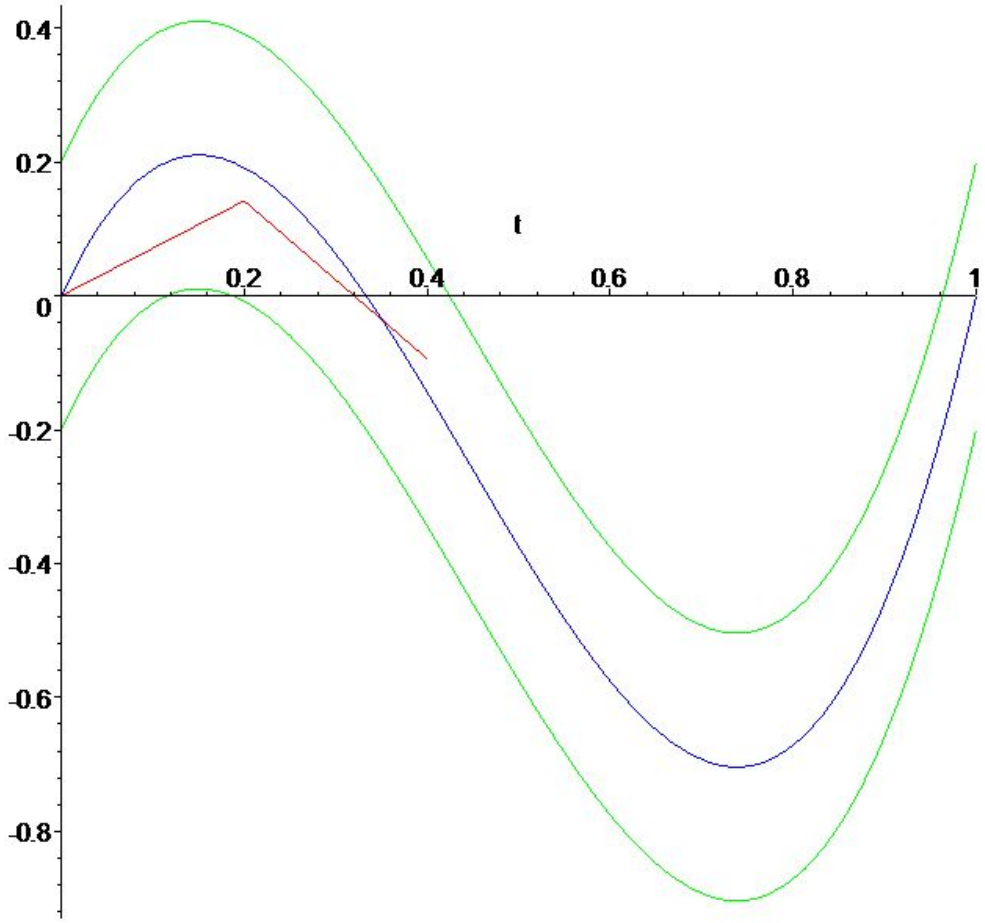
Un "tubo" solución



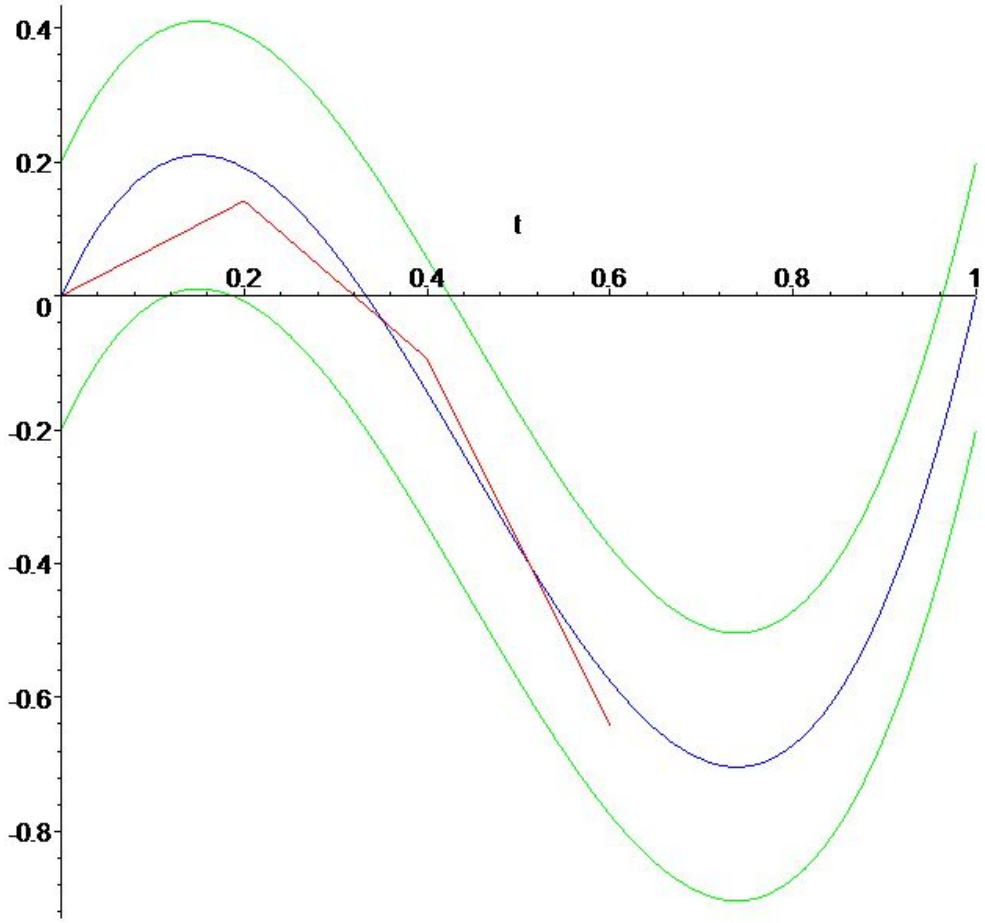
Un pimer "paso" de homotopía



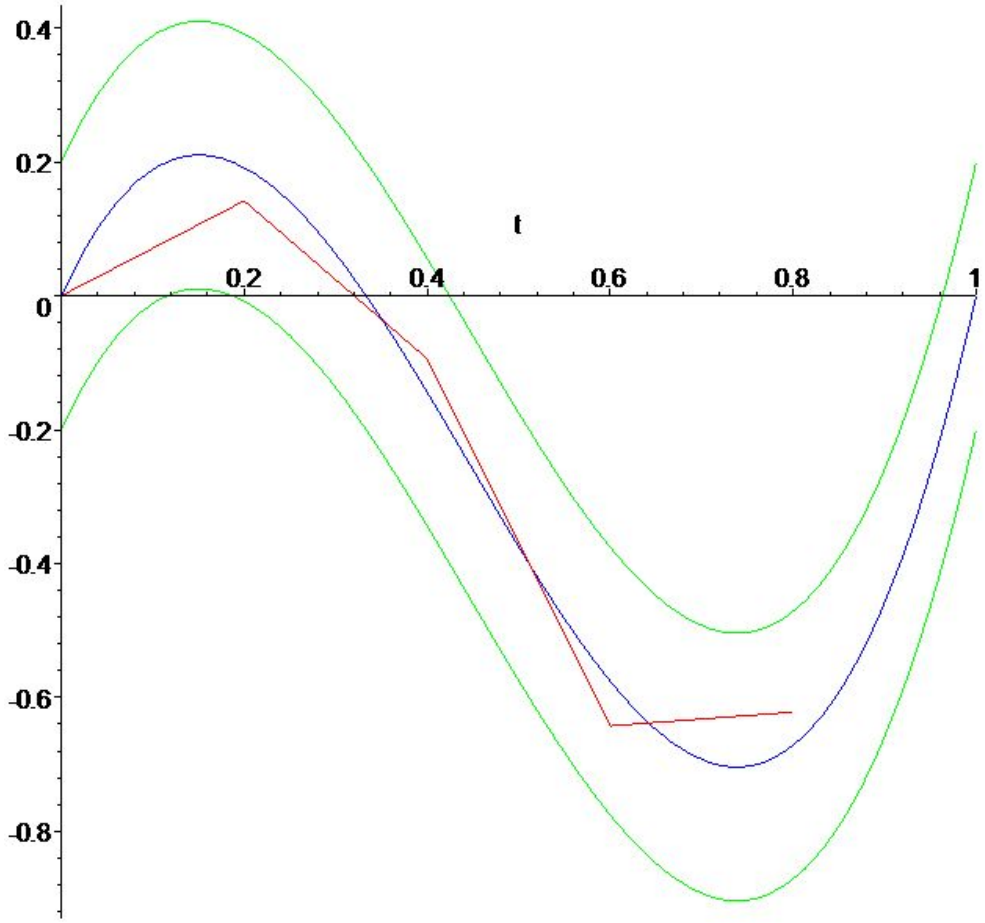
Más "pasos" de homotopía



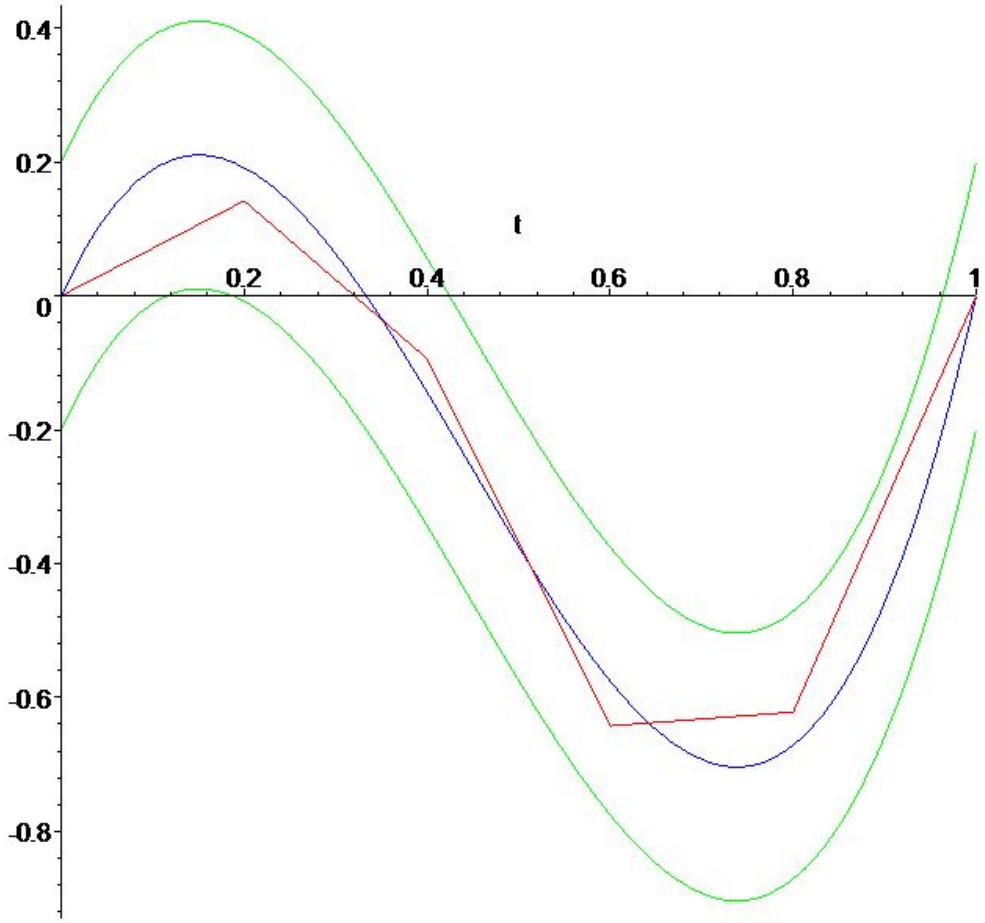
Más "pasos" de homotopía



Más "pasos" aún



Más "pasos" aún



Dónde Empezar la Homotopía?

O mejor, dónde comenzar la homotopía de tal modo que el número de pasos de homotopía sea polinomial y, por tanto, el algoritmo es TRATABLE

$\varepsilon > 0$ un real positivo.

Un dato $(G, zeta) \in \mathcal{H}_{(d)} \times \mathbb{P}_n(\mathbb{C})$ es $\varepsilon-$efficiente si

– *El tiempo es polinomial en* $\varepsilon^{-1}, n, N, d$.

– *NHD con dato inicial* $(G, zeta)$ *resuelve la mayor parte de los sistemas* $F \in \mathcal{H}_{(d)}$*:*

$$Probabilidad[\ F \in \mathcal{H}_{(d)}\ :\ NHD\ \text{resuelve}\ F\ \text{desde}\ (G, \zeta)] \geq 1 - \varepsilon.$$

La probabilidad de que falle el esquema es menor que ε.

Problema: C'omo hallar esos sistemas.

Correct Test Classes (Conjunto Questor) para NHD

[Beltrán- P., 2005]

Una clase $\mathcal{G} \subseteq \mathcal{H}_{(d)} \times \mathbb{P}_n(\mathbb{C})$ es un questor para NHD si:

Para cada $\varepsilon > 0$ la probbilidad de que un dato (aleatoriamente elefido) $(G, zeta) \in \mathcal{G}$ sea $\varepsilon-$efficiente para NHD es mayor que

$$1 - (nNd)^{O(1)}\varepsilon.$$

Bézout $5\frac{1}{2}$

Theorem[Beltrán, P. 2005] *Hemos descrito un conjunto cuestor constructible y fácil de computar para resolver sistemas de ecuaciones polinomiales.*

Significado (I)

Corollary 1 *Existe un algoritmo de probabilidad de error acotada (Monte–Carlo) y de tipo numérico verificando :*

- *El tiempo de ejecución es polinomial en* $O(\varepsilon^{-2}d^2)$.

- *La probabilidad de que un par inicial* $(G, e) \in \mathcal{G}$ *sea* $\varepsilon-$*efficiente es al menos*

$$1 - (ndN)^5\varepsilon.$$

- *La probabilidad de resolver un sistema es al menos:*

$$1 - \varepsilon.$$

Ecuaciones Cúbicas

Corollary 2 *Para grados* $(d) := (3, 3, \ldots, 3)$. *Hay un algoritmo de probabilidad de error acotada tal que :*

- *El tiempo es a lo sumo* $O(n^{21})$.

- *The probability that an input system is solved is at least:*

$$1 - \frac{1}{n^4}.$$

Complejidad a la Turing

Corollary 3 (Beltrán–P., 2005) *Hay una máquina de Turing probabilista que resuleve "la mayor parte" de los sistemas de ecuaciones polinomiales multivariados en tiempo polinomial en la codificación dense de la entrada.*

El Cálculo del Cuerpo que buscaba Galois

Teor. [Castro- Pardo et al., 2001]¶Se puede calcular el cuerpo de escisión de una ecuación polinomial univariada en tiempo polinomial en el orden del grupo de Galois de la ecuacion.

¶Se diseña un algoritmo que combina los métodos Numéricos, con los métodos diofánticos.