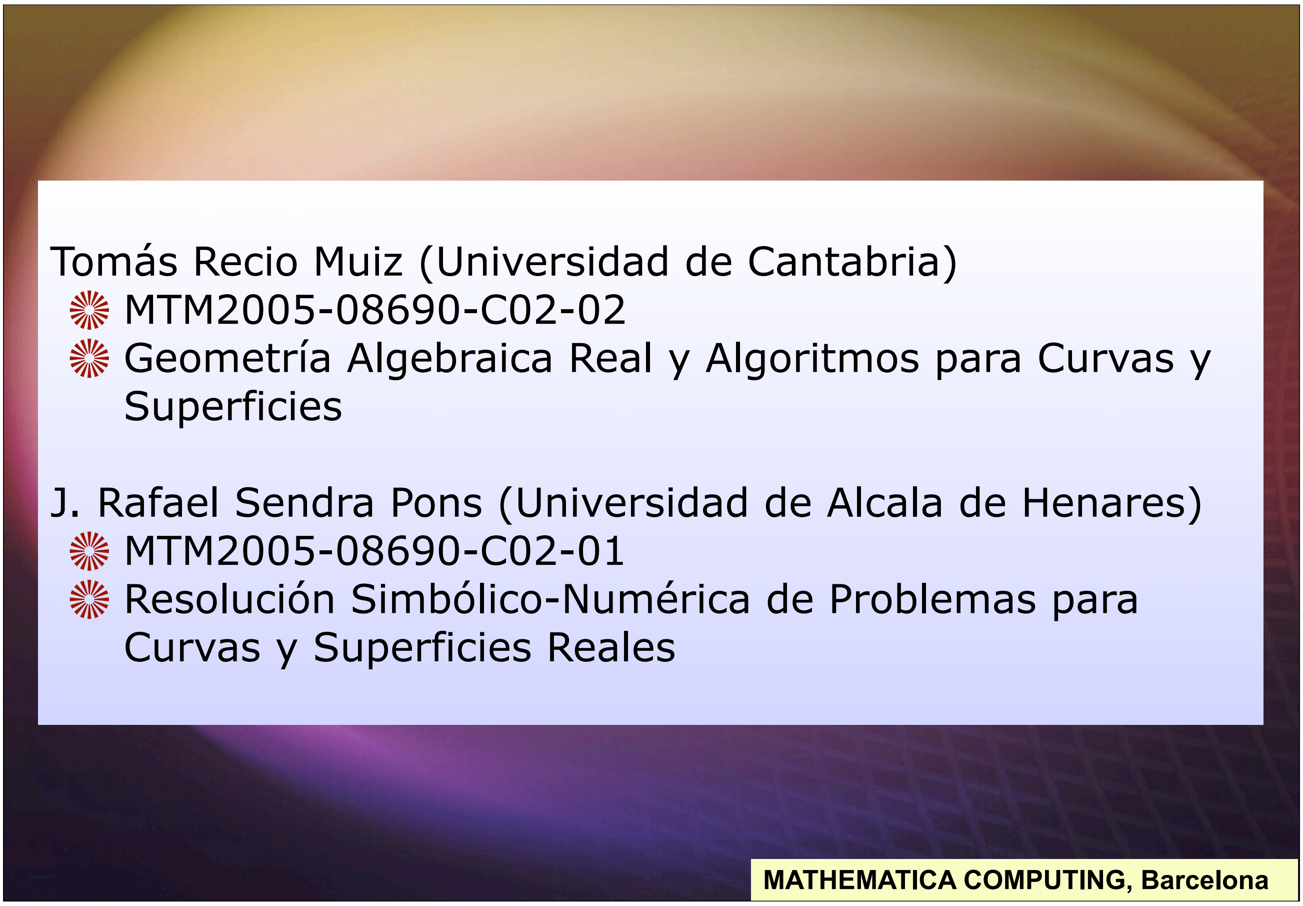
Geometría Industrial: Experimentación en CAD (PSE)

Efectividad, Eficiencia y Eficacia en Algebra Computacional

Laureano Gonzalez-Vega
Departamento de Matematicas, Estadistica y Computacion
Universidad de Cantabria, Spain

MATHEMATICA COMPUTING, Barcelona



Tomás Recio Muiz (Universidad de Cantabria)
- MTM2005-08690-C02-02
- Geometría Algebraica Real y Algoritmos para Curvas y Superficies

J. Rafael Sendra Pons (Universidad de Alcala de Henares)
- MTM2005-08690-C02-01
- Resolución Simbólico-Numérica de Problemas para Curvas y Superficies Reales

MATHEMATICA COMPUTING, Barcelona

Geometría Industrial: Experimentación en CAD (PSE)

Utilización de información algebro-geométrica para poder resolver en la forma más eficiente posible problemas de manipulación de curvas y superficies en CAGD o CAD (intersecciones, offsets, blendings, etc.).

La parte simbólica:

- prepara el problema para que la resolución numérica final sea más robusta y eficaz, o
- proporciona una "closed form solution" que solo tiene ser evaluada.

MATHEMATICA COMPUTING, Barcelona

CLOSED FORM SOLUTIONS

Let $\mathcal{A} : X^T AX = 0$ and $\mathcal{B} : X^T BX = 0$ be two ellipsoids and

$$f(\lambda) = \det(\lambda A + B) = \lambda^4 + a\lambda^3 + b\lambda^2 + c\lambda + d$$

their characteristic polynomial (once turned monic).

The two ellipsoids are separated if and only if:

$P_1>0, P_2>0, P_3=0, P_4<0, P_5=0$

$P_1>0, P_2>0, P_3>0, \quad P_5<0$

$P_1>0, P_2>0, P_3=0, \quad P_5<0, P_6<0$

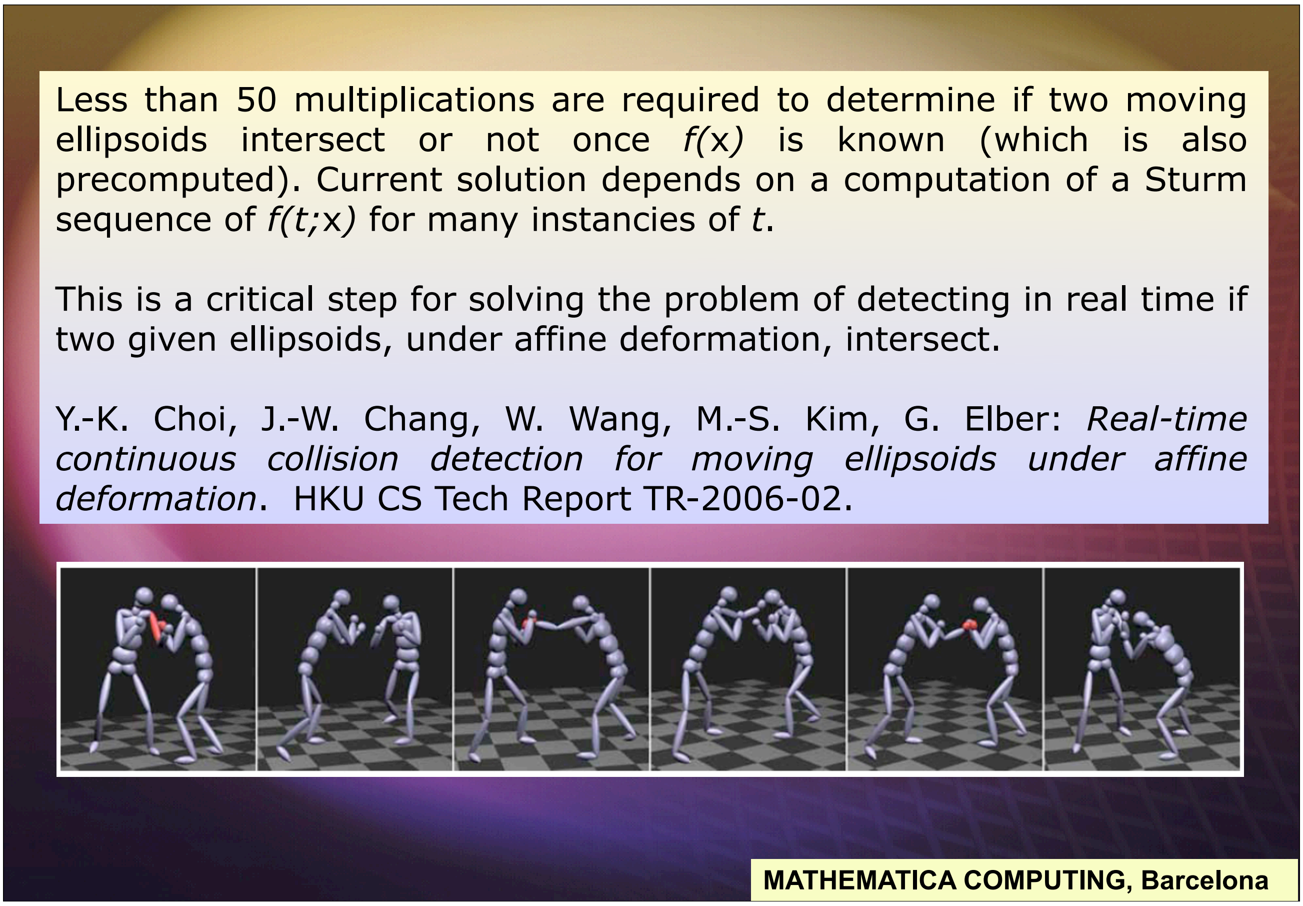
$P_1>0, P_2>0, P_3>0, P_4>0, P_5\geq 0, P_6>0$

$P_1>0, P_2>0, P_3>0, P_4<0, P_5>0, P_6<0$

$P_1>0, P_2>0, P_3=0, P_4<0, P_5>0, P_6<0$

$P_5 := b\, a^2 + 3\, a\, c - 4\, b^2$

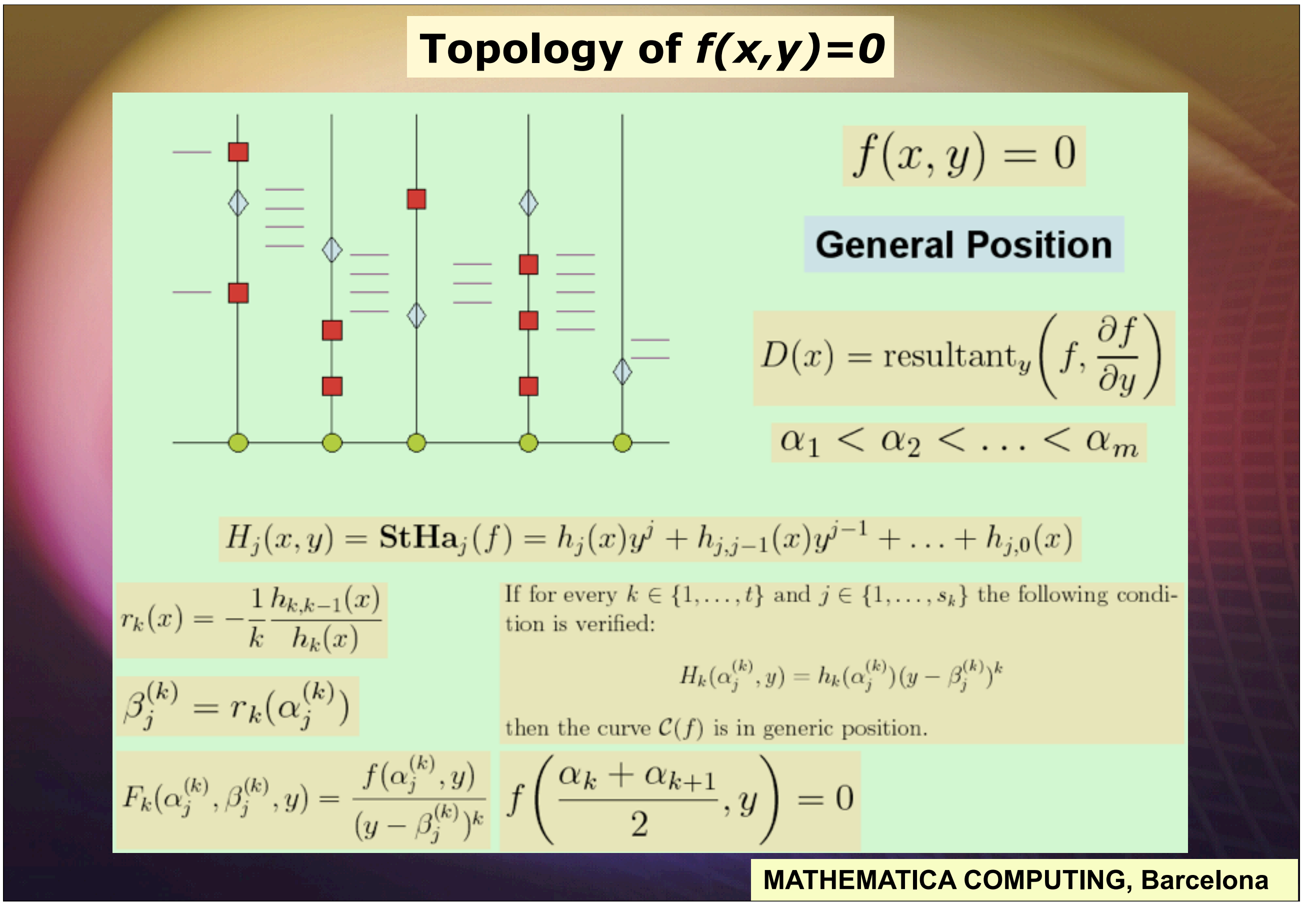
MATHEMATICA COMPUTING, Barcelona



Less than 50 multiplications are required to determine if two moving ellipsoids intersect or not once *f*(x) is known (which is also precomputed). Current solution depends on a computation of a Sturm sequence of *f(t;*x*)* for many instancies of *t*.

This is a critical step for solving the problem of detecting in real time if two given ellipsoids, under affine deformation, intersect.

Y.-K. Choi, J.-W. Chang, W. Wang, M.-S. Kim, G. Elber: *Real-time continuous collision detection for moving ellipsoids under affine deformation*. HKU CS Tech Report TR-2006-02.



Topology of *f(x,y)=0*

$$f(x,y)=0$$

General Position

$$D(x)=\text{resultant}_y\left(f,\frac{\partial f}{\partial y}\right)$$

$$\alpha_1<\alpha_2<\ldots<\alpha_m$$

$$H_j(x,y)=\mathbf{StHa}_j(f)=h_j(x)y^j+h_{j,j-1}(x)y^{j-1}+\ldots+h_{j,0}(x)$$

$$r_k(x)=-\frac{1}{k}\frac{h_{k,k-1}(x)}{h_k(x)}$$

$$\beta_j^{(k)}=r_k(\alpha_j^{(k)})$$

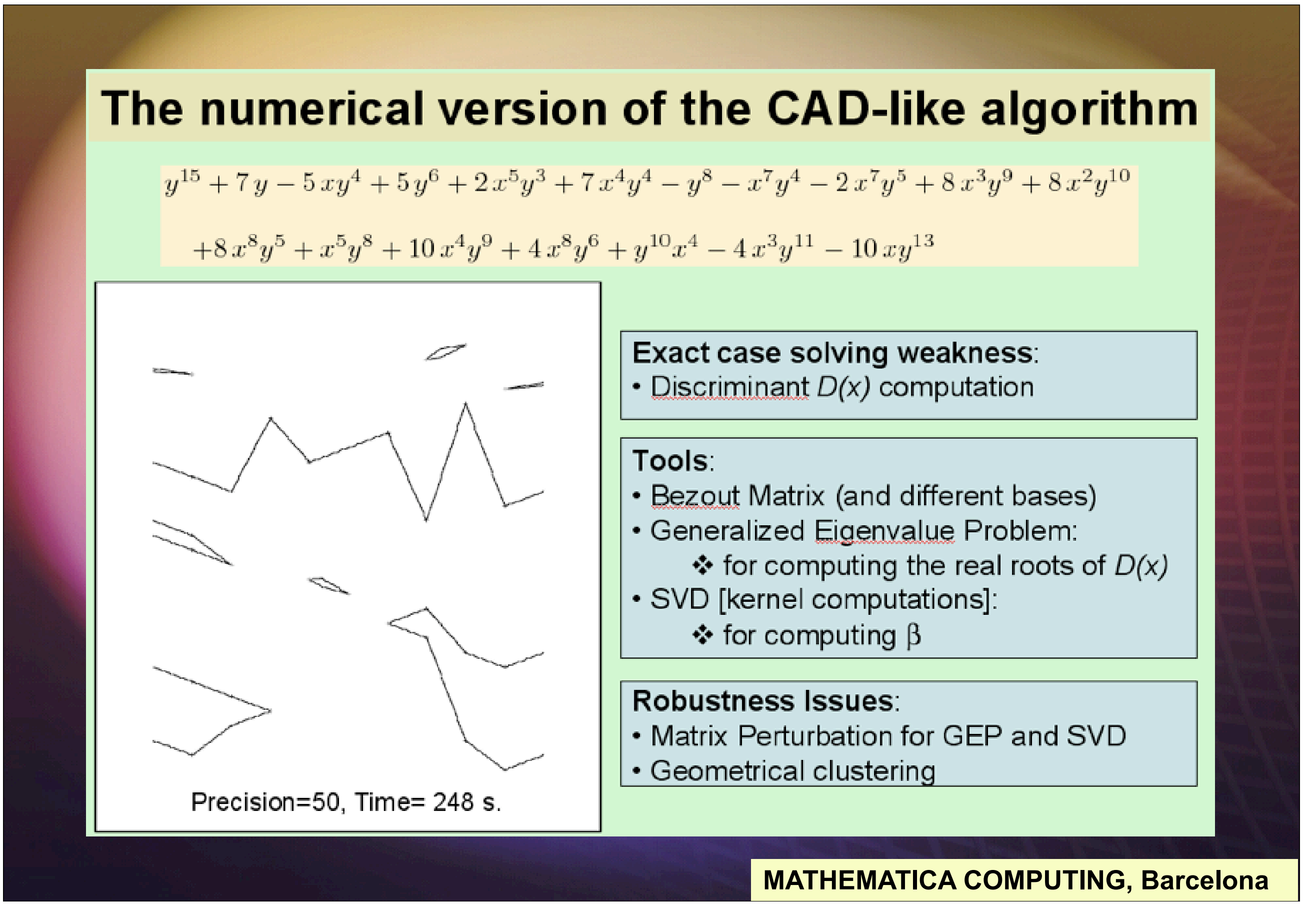
If for every $k\in\{1,\ldots,t\}$ and $j\in\{1,\ldots,s_k\}$ the following condition is verified:

$$H_k(\alpha_j^{(k)},y)=h_k(\alpha_j^{(k)})(y-\beta_j^{(k)})^k$$

then the curve $\mathcal{C}(f)$ is in generic position.

$$F_k(\alpha_j^{(k)},\beta_j^{(k)},y)=\frac{f(\alpha_j^{(k)},y)}{(y-\beta_j^{(k)})^k}$$

$$f\left(\frac{\alpha_k+\alpha_{k+1}}{2},y\right)=0$$



The numerical version of the CAD-like algorithm

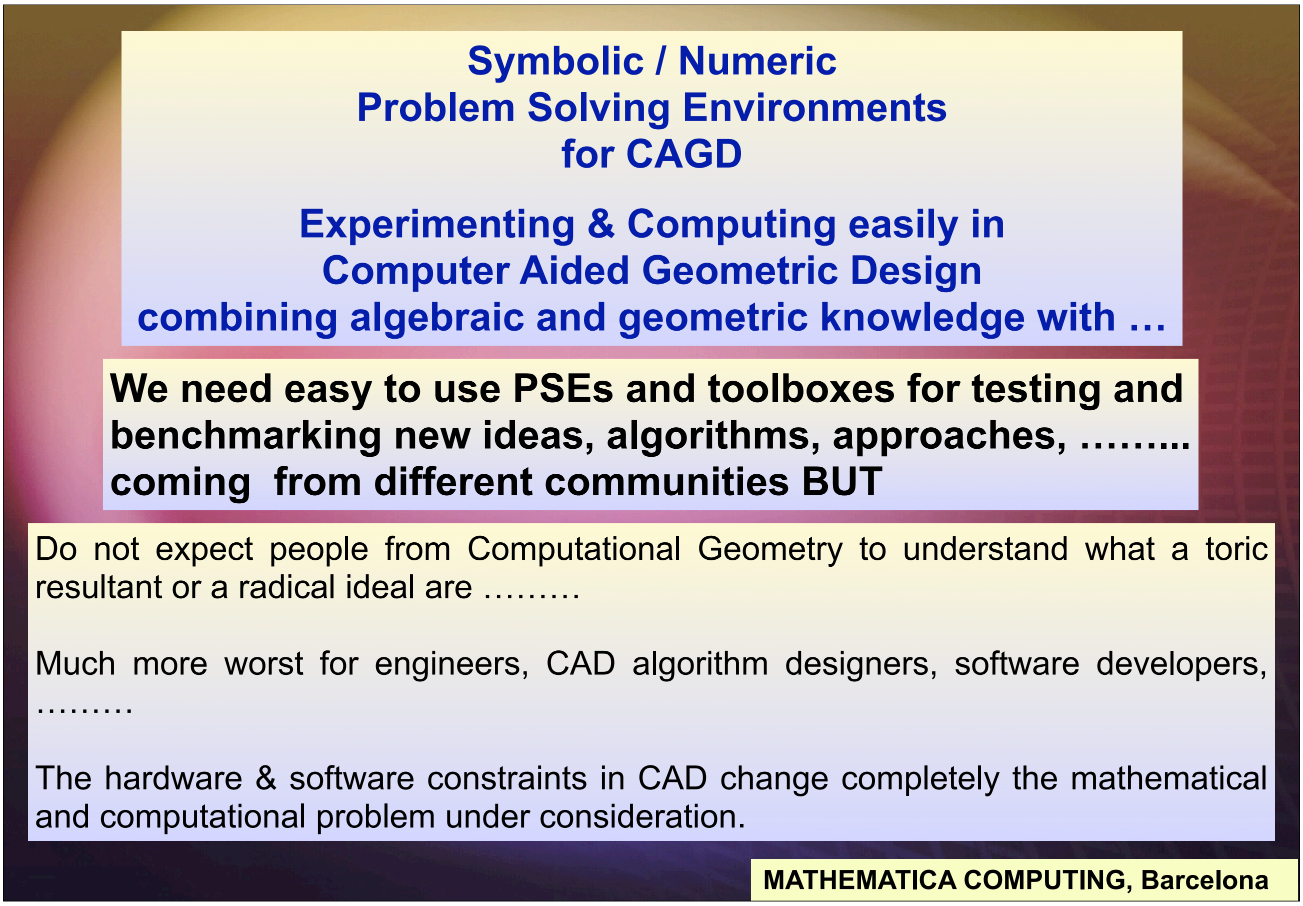
$$y^{15}+7\,y-5\,xy^4+5\,y^6+2\,x^5y^3+7\,x^4y^4-y^8-x^7y^4-2\,x^7y^5+8\,x^3y^9+8\,x^2y^{10}$$
$$+8\,x^8y^5+x^5y^8+10\,x^4y^9+4\,x^8y^6+y^{10}x^4-4\,x^3y^{11}-10\,xy^{13}$$

Precision=50, Time= 248 s.

Exact case solving weakness:
- Discriminant *D(x)* computation

Tools:
- Bezout Matrix (and different bases)
- Generalized Eigenvalue Problem:
  - ❖ for computing the real roots of *D(x)*
- SVD [kernel computations]:
  - ❖ for computing β

Robustness Issues:
- Matrix Perturbation for GEP and SVD
- Geometrical clustering



Symbolic / Numeric
Problem Solving Environments
for CAGD

Experimenting & Computing easily in
Computer Aided Geometric Design
combining algebraic and geometric knowledge with …

We need easy to use PSEs and toolboxes for testing and benchmarking new ideas, algorithms, approaches, ……... coming from different communities BUT

Do not expect people from Computational Geometry to understand what a toric resultant or a radical ideal are ………

Much more worst for engineers, CAD algorithm designers, software developers, ………

The hardware & software constraints in CAD change completely the mathematical and computational problem under consideration.

A SMALL CAGD SYSTEM WITH EXACT/MIXED ARITHMETIC

Experimentations with precision by using symbolic and numerical techniques.

Exact and generic implicititation.

Cubic A-splines manipulation.

Topologically reliable computation of f(x,y)=0 and g(x,y,z)=0.

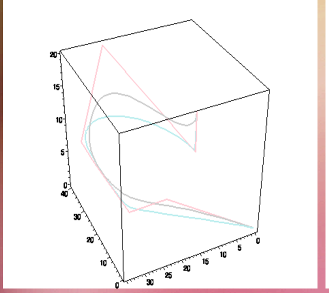
Symbolic/Numerical Polynomial System Solving (connection to external software in some cases).

Curve and surface intersections:
- implicit-implicit, parametric-implicit, parametric-parametric,
- tangential intersections,
- curve tracing through ode numerical solving.

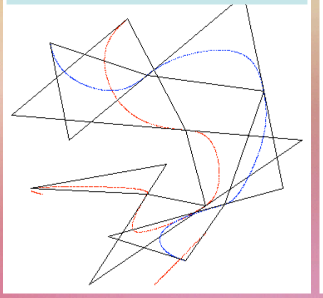
Code generation (C, Visual Basic, ...) when needed.

Maplet based and web availabity in the near future.

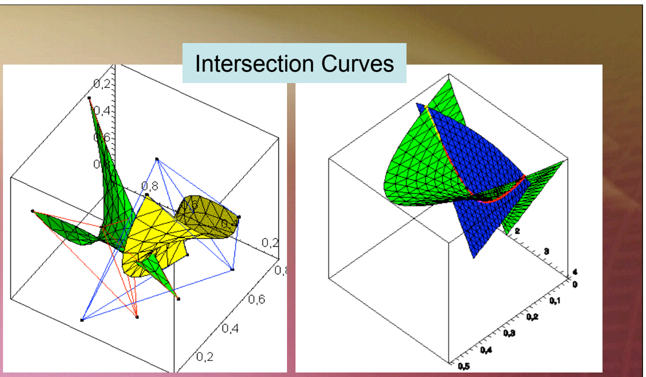
B-spline and NURBS

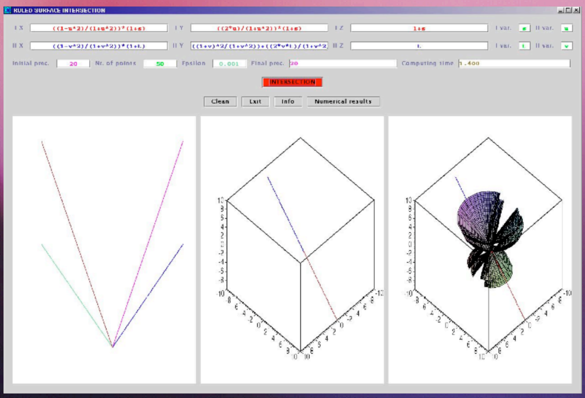


Cubic A-spline Intersection



Intersection Curves

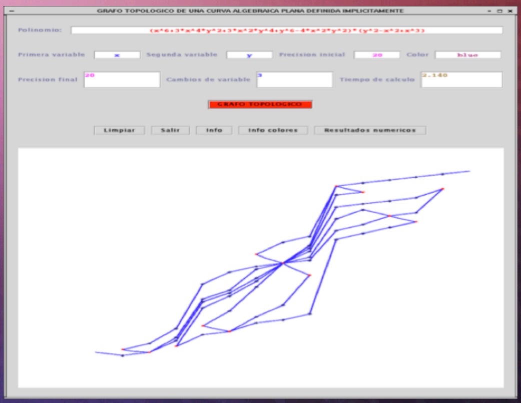



RULED SURFACE INTERSECTION

I X ((1-u^2)/(1+u^2))*(1+s) I Y ((2*u)/(1+u^2))*(1+s) I Z 1+s I var. s II var. u

II X ((1-v^2)/(1+v^2))*(1+t) II Y ((1+v)^2/(1+v^2))+((2*v*t)/(1+v^2 II Z t I var. t II var. v

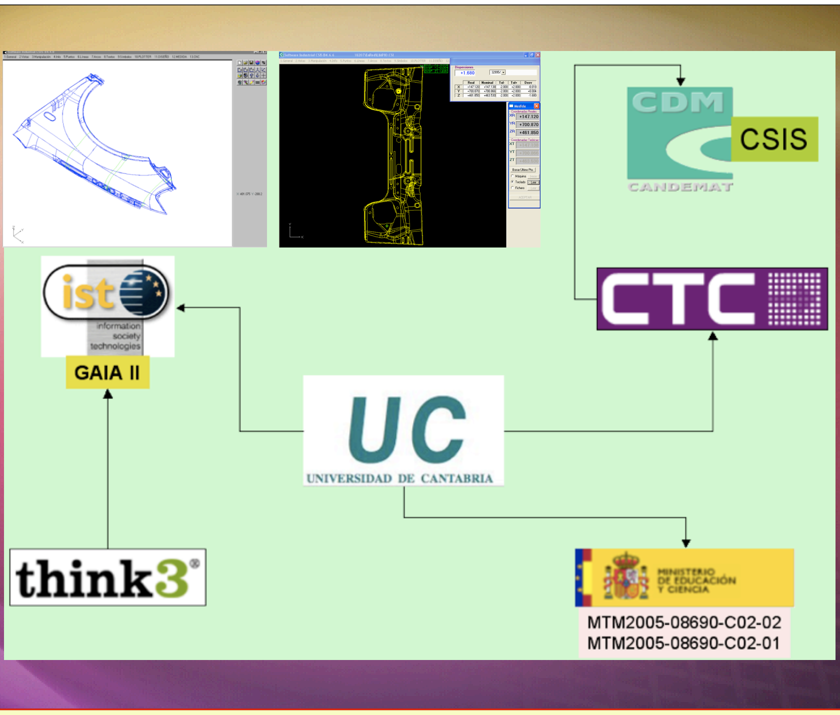
Initial prec. 20 Nr. of points 50 Epsilon 0.001 Final prec. 20 Computing time 1.400


GRAFO TOPOLOGICO DE UNA CURVA ALGEBRAICA PLANA DEFINIDA IMPLICITAMENTE

Polinomio: (x^6+3*x^4*y^2+3*x^2*y^4+y^6-4*x^2*y^2)*(y^2-x^2+x^3)

Primera variable x Segunda variable y Precision inicial 20 Color blue

Precision final 20 Cambios de variable 3 Tiempo de calculo 2.140



Software used: Maple, CSIS, SYNAPS, Think3, ...

Efectividad, Eficiencia y Eficacia en Algebra Computacional

CONJECTURES: ONE EXAMPLE

Let $\mathbb{K}$ be a field of characteristic zero and $P(x) \in \mathbb{K}[x]$ with $\deg(P) = n$.

$$\text{for } 1 \leq i \leq n-1: \ \deg(\gcd(P, P^{(i)})) \geq 1$$

$$\Updownarrow$$

$$\exists\, \alpha \in \mathbb{K}, P(x) = (x - \alpha)^n$$

P(x) has a root with any of its derivatives if and only if *P(x)* is a power of a linear factor.

$$P(x) = (x-\beta_1)(x-\beta_2)(x-\beta_3)(x-\beta_4)(x-\beta_5)(x-\beta_6)(x-\beta_7)$$

$$\begin{aligned}
0 = \;& (-2\beta_1\beta_2\beta_5\beta_6 + \cdots - 2\beta_1\beta_2\beta_3\beta_6)(-\beta_1\beta_2\beta_5\beta_6 + \cdots - \beta_1\beta_2\beta_3\beta_6)\\
& (6{\beta_3}^4 + \cdots - 2\beta_1\beta_2\beta_3\beta_6)(-2\beta_1\beta_2\beta_5\beta_6 + \cdots + \beta_1\beta_2\beta_3\beta_6)\\
& (2\beta_1\beta_2\beta_5\beta_6 + \cdots + 2\beta_1\beta_2\beta_3\beta_6) = H_{11}H_{12}H_{13}H_{14}H_{15}
\end{aligned}$$

$$\begin{aligned}
0 = \;& (3{\beta_1}^2\beta_2\beta_3 + \cdots - 2\beta_1\beta_2\beta_3\beta_6)({\beta_1}^2\beta_2\beta_3 + \cdots + 2\beta_1\beta_2\beta_3\beta_6)\\
& (-3{\beta_1}^2\beta_2\beta_3 + \cdots - 6\beta_1\beta_2\beta_3\beta_6)(3{\beta_1}^2\beta_2\beta_3 + \cdots - 6\beta_1\beta_2\beta_3\beta_6)\\
& = H_{21}H_{22}H_{23}H_{24}H_{25}H_{26}\\
0 = \;& (-8\beta_1\beta_2\beta_3 + \cdots 2\beta_1\beta_2\beta_4)(2\beta_1\beta_2\beta_3 + \cdots + 2\beta_1\beta_2\beta_4)\\
& (3\beta_1\beta_2\beta_3 + \cdots + 3\beta_1\beta_2\beta_4)(2\beta_1\beta_2\beta_3 + \cdots - 8\beta_1\beta_2\beta_4)\\
& (8\beta_1\beta_2\beta_3 + \cdots + 8\beta_1\beta_2\beta_4)(2\beta_1\beta_2\beta_3 + \cdots + 2\beta_1\beta_2\beta_4)\\
& = H_{31}H_{32}H_{33}H_{34}H_{35}H_{36}\\
0 = \;& (\beta_2\beta_5 + \cdots + 15{\beta_6}^2)(-5\beta_2\beta_5 + \cdots + 15{\beta_5}^2)\\
& (\beta_2\beta_5 + \cdots - 4\beta_1\beta_2)(\beta_2\beta_5 + \cdots + 15{\beta_3}^2)\\
& (\beta_2\beta_5 + \cdots + 15{\beta_4}^2)(-5\beta_2\beta_5 + \cdots + 15{\beta_2}^2)\\
& = H_{41}H_{42}H_{43}H_{44}H_{45}H_{46}\\
0 = \;& (-6\beta_5 + \cdots + \beta_6)(5\beta_1 + \cdots - \beta_6)(-6\beta_2 + \cdots + \beta_6)\\
& (-6\beta_3 + \cdots + \beta_6)(-6\beta_4 + \cdots + \beta_6)\\
& (-6\beta_6 + \cdots + \beta_5) = H_{51}H_{52}H_{53}H_{54}H_{55}H_{56}
\end{aligned}$$

Experimentation

The conjecture has been verified until degree nine with the help of Maple.

Maple tools used:

-. Polynomial manipulation.
-. Factorization of polynomials.
-. Groebner Basis.

$$P(x) = (x-\beta_1)^a(x-\beta_2)^b(x-\beta_3)^c, \quad n = a+b+c > 2$$

ESTADO DEL ARTE

The conjecture is not true in characteristic *p*:

x^{p+1}-x^p has a common root with any of its derivatives in characteristic *p.*

J. Schicho et al (2006):

The conjecture has been proven for degrees *p^r* and *2p^r,* with *p* any prime.

R. M. de Frutos (2006):

The conjecture has been proven for trinomials.

The first remaining open case for the conjecture is degree *12* whose treatment is underway. But also 20, 24 and 28 !

EFFICIENCY ANALYSIS

Mark Van Hoeij:

Factoring polynomials and the knapsack problem

Journal of Number Theory, 2001

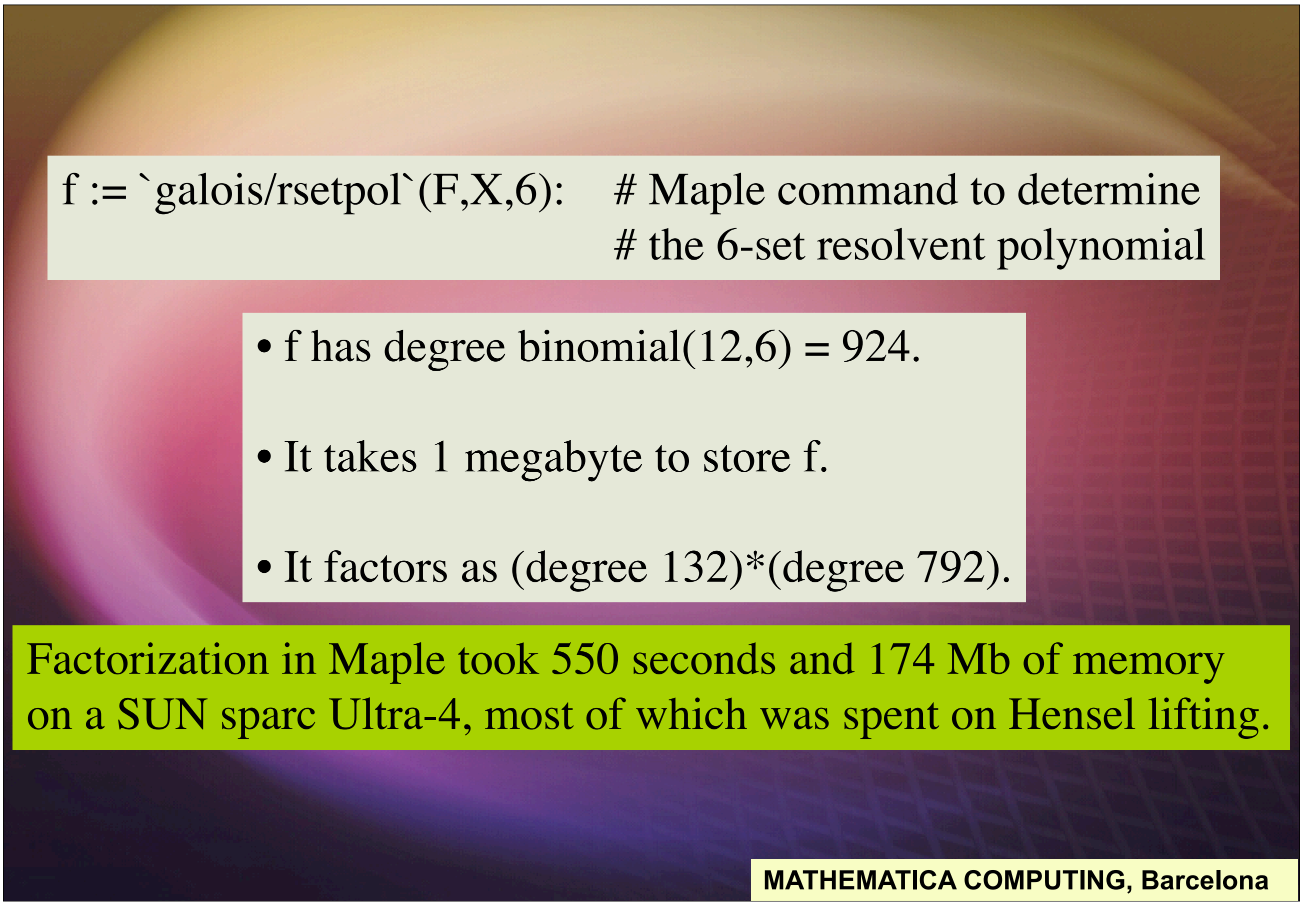
Se puede usar LLL para factorizar polinomios de forma eficiente.

$$F := X^{12} + \frac{100}{3} X^{11} + 450\, X^{10} + 3100\, X^{9} + 10975\, X^{8} + 15000\, X^{7} - 14500\, X^{6} - 49000\, X^{5} + 15375\, X^{4} + 57500\, X^{3} + 7500\, X + 625$$

The Galois group of F over Q is the Mathieu group M12.
(http://for.mat.bham.ac.uk/atlas/html/M12.html for details on M12)

F is obtained from the polynomial given in:

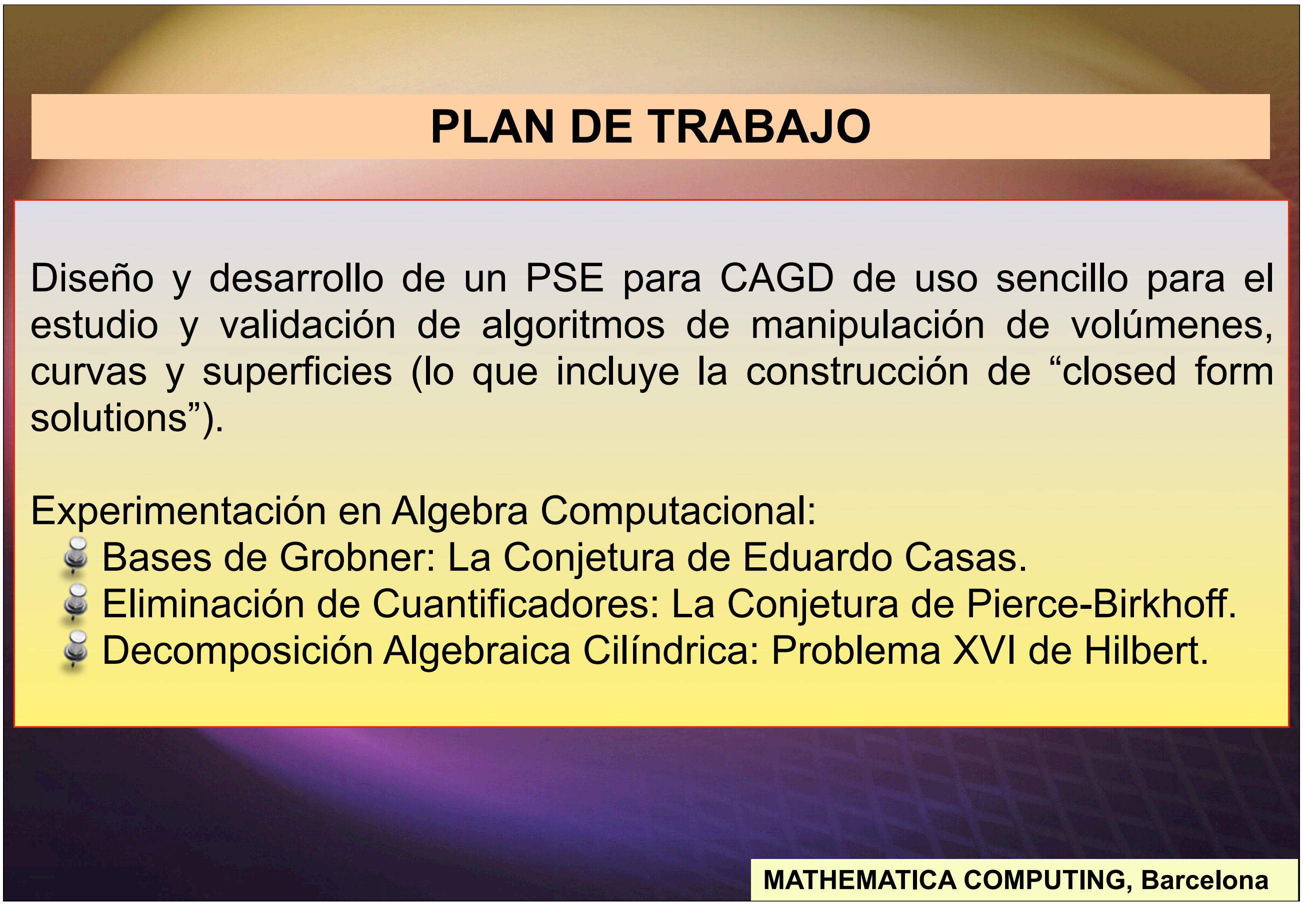
Matzat, B. H., Zeh-Marschke, A. (1986).
"*Realisierung der Mathieugruppen M11 und M12 als Galoisgruppen ueber Q*",
J. Number Theory, 23, 195-202.



```
f := `galois/rsetpol`(F,X,6):    # Maple command to determine
                                 # the 6-set resolvent polynomial
```

- f has degree binomial(12,6) = 924.
- It takes 1 megabyte to store f.
- It factors as (degree 132)*(degree 792).

Factorization in Maple took 550 seconds and 174 Mb of memory on a SUN sparc Ultra-4, most of which was spent on Hensel lifting.

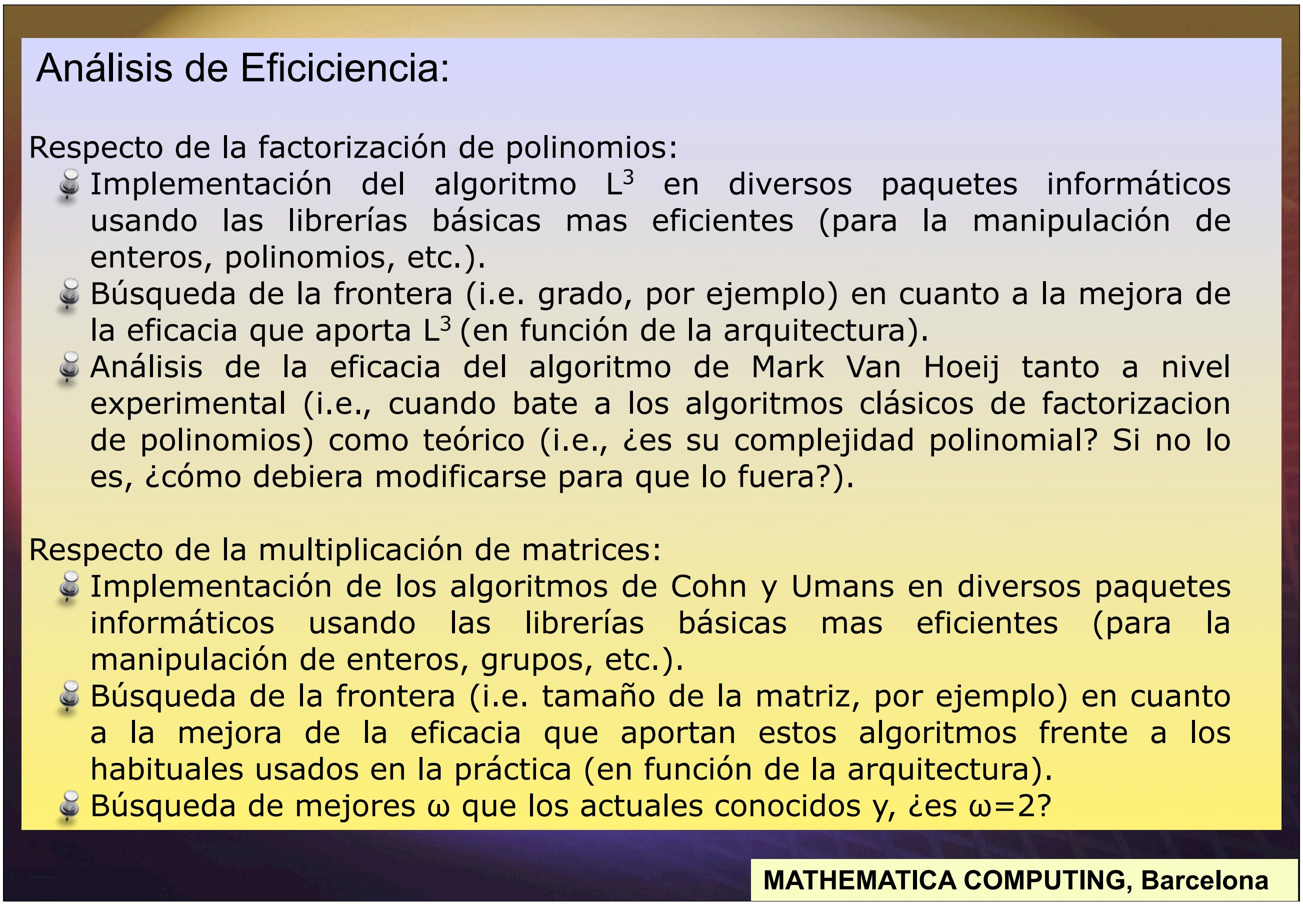


PLAN DE TRABAJO

Diseño y desarrollo de un PSE para CAGD de uso sencillo para el estudio y validación de algoritmos de manipulación de volúmenes, curvas y superficies (lo que incluye la construcción de "closed form solutions").

Experimentación en Algebra Computacional:

- Bases de Grobner: La Conjetura de Eduardo Casas.
- Eliminación de Cuantificadores: La Conjetura de Pierce-Birkhoff.
- Decomposición Algebraica Cilíndrica: Problema XVI de Hilbert.



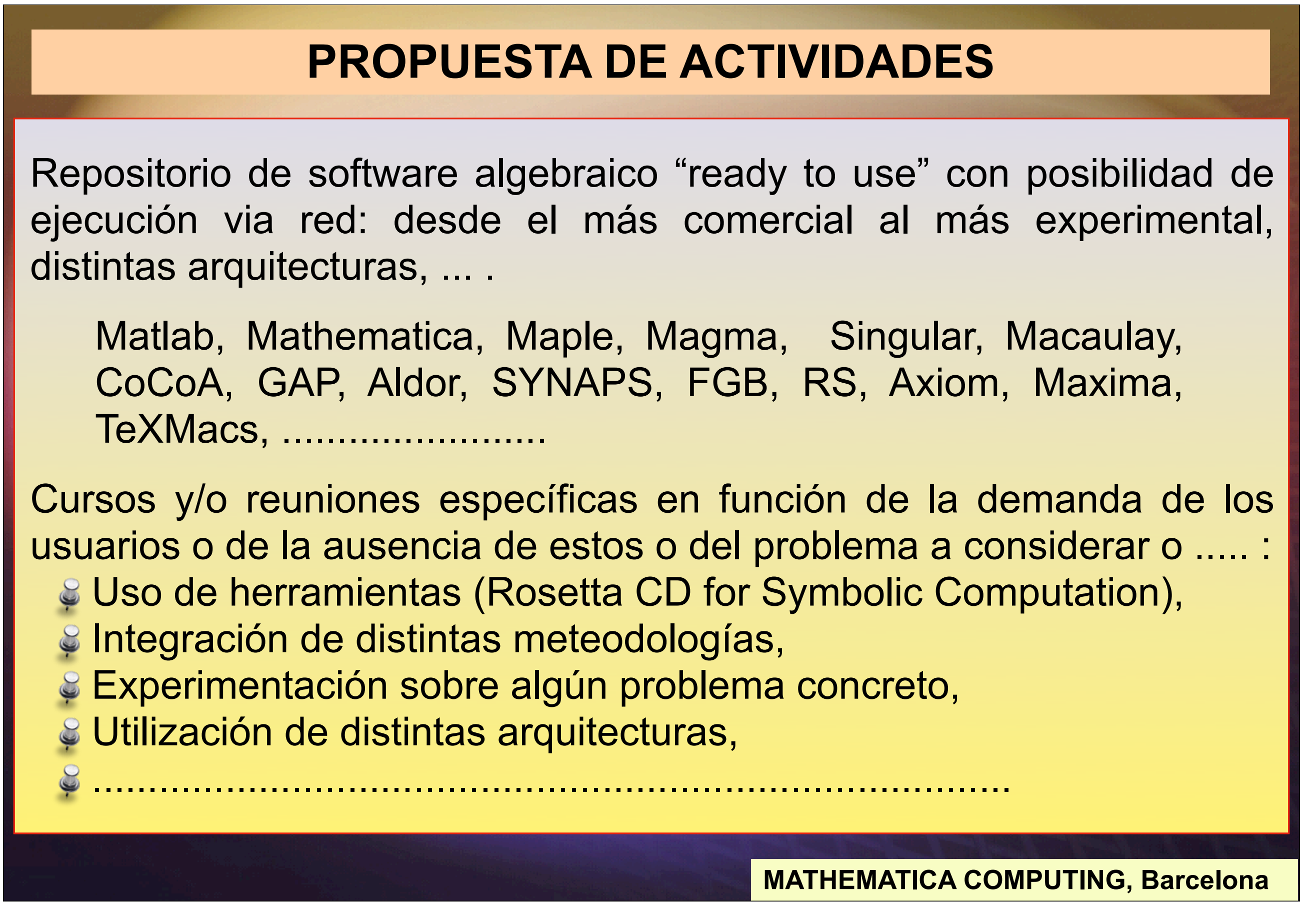
Análisis de Eficiciencia:

Respecto de la factorización de polinomios:

- Implementación del algoritmo L^3 en diversos paquetes informáticos usando las librerías básicas mas eficientes (para la manipulación de enteros, polinomios, etc.).
- Búsqueda de la frontera (i.e. grado, por ejemplo) en cuanto a la mejora de la eficacia que aporta L^3 (en función de la arquitectura).
- Análisis de la eficacia del algoritmo de Mark Van Hoeij tanto a nivel experimental (i.e., cuando bate a los algoritmos clásicos de factorizacion de polinomios) como teórico (i.e., ¿es su complejidad polinomial? Si no lo es, ¿cómo debiera modificarse para que lo fuera?).

Respecto de la multiplicación de matrices:

- Implementación de los algoritmos de Cohn y Umans en diversos paquetes informáticos usando las librerías básicas mas eficientes (para la manipulación de enteros, grupos, etc.).
- Búsqueda de la frontera (i.e. tamaño de la matriz, por ejemplo) en cuanto a la mejora de la eficacia que aportan estos algoritmos frente a los habituales usados en la práctica (en función de la arquitectura).
- Búsqueda de mejores ω que los actuales conocidos y, ¿es $\omega=2$?



PROPUESTA DE ACTIVIDADES

Repositorio de software algebraico “ready to use” con posibilidad de ejecución via red: desde el más comercial al más experimental, distintas arquitecturas, ...

Matlab, Mathematica, Maple, Magma, Singular, Macaulay, CoCoA, GAP, Aldor, SYNAPS, FGB, RS, Axiom, Maxima, TeXMacs, ...

Cursos y/o reuniones específicas en función de la demanda de los usuarios o de la ausencia de estos o del problema a considerar o ..... :

- Uso de herramientas (Rosetta CD for Symbolic Computation),
- Integración de distintas meteodologías,
- Experimentación sobre algún problema concreto,
- Utilización de distintas arquitecturas,
- ....

F. Carreras
M. Romano
L. F. Tabera
C. Tanasescu

F. Sansegundo
C. Villarino

S. Corvez
J. Espinola
I. Necula

F. Etayo
M. Fioravanti
L. Gonzalez-Vega
J. Puig-Pey
T. Recio
R. Sendra

G. Diaz-Toca
S. Perez
S. Rueda
J. Sendra

J. Caravantes
E. Briand
E. Mainar
I. Rua

MATHEMATICA COMPUTING, Barcelona