# Approximate Algebraic Geometry 

## for curves and surfaces

B. Mourrain

Grilato
INRIA, BP 93, 06902 Sophia Antipolis
1st October 2003

# Symbolic-numeric methods 

## for curves and surfaces

B. Mourrain

Grilato
INRIA, BP 93, 06902 Sophia Antipolis
1st October 2003

# Certified/controlled algorithms 

## for curves and surfaces

B. Mourrain

Grilato
INRIA, BP 93, 06902 Sophia Antipolis
1st October 2003

Long time ago

## Long time ago

$\mathbb{Z}$ : Addition, substraction as geometric operations.

## Long time ago

$\mathbb{Z}$ : Addition, substraction as geometric operations.
$\mathbb{Q}$ : Ratio of numbers. Thalès and the pyramids (-620-546).
The multiplication is commutative (Pappus theorem).

## Long time ago

$\mathbb{Z}$ : Addition, substraction as geometric operations.
$\mathbb{Q}:$ Ratio of numbers. Thalès and the pyramids (-620-546).
The multiplication is commutative (Pappus theorem).
!! all is number (commensurable) for the Pythagore's school (-585-400).

## Long time ago

$\mathbb{Z}$ : Addition, substraction as geometric operations.
$\mathbb{Q}:$ Ratio of numbers. Thalès and the pyramids (-620-546).
The multiplication is commutative (Pappus theorem).
!! all is number (commensurable) for the Pythagore's school (-585-400).
?? No, dare to say Hippase de Métaponte, not $\sqrt{2}$.

## Long time ago

$\mathbb{Z}$ : Addition, substraction as geometric operations.
$\mathbb{Q}:$ Ratio of numbers. Thalès and the pyramids (-620-546).
The multiplication is commutative (Pappus theorem).
!! all is number (commensurable) for the Pythagore's school (-585-400).
?? No, dare to say Hippase de Métaponte, not $\sqrt{2}$.
$\mathbb{R}$ : It's not a problem, says Dedekind, the missing numbers are those which are inbetween.

## Long time ago

$\mathbb{Z}$ : Addition, substraction as geometric operations.
$\mathbb{Q}:$ Ratio of numbers. Thalès and the pyramids (-620-546).
The multiplication is commutative (Pappus theorem).
!! all is number (commensurable) for the Pythagore's school (-585-400).
?? No, dare to say Hippase de Métaponte, not $\sqrt{2}$.
$\mathbb{R}$ : It's not a problem, says Dedekind, the missing numbers are those which are inbetween.
$\overline{\mathbb{Q}}:$ Yes, but $\sqrt{2}$ is special, says Galois.

## Effective Geometric Objects

$\square$ Effective real numbers are such that we can ask:

- algebraic::approximate(int n) a numerical approximation to an arbitrary precision $2^{n}$,
- compare(algebraic a, algebraic b) with a certified answer.


## Effective Geometric Objects

$\square$ Effective real numbers are such that we can ask:

- algebraic::approximate(int n) a numerical approximation to an arbitrary precision $2^{n}$,
- compare(algebraic a, algebraic b) with a certified answer.
$\square$ Effective points, segments, ...
- defined with effective coordinates,
- or provide directly approximation and queries at the geometric level.


## Effective Geometric Objects

$\square$ Effective real numbers are such that we can ask:

- algebraic::approximate(int n) a numerical approximation to an arbitrary precision $2^{n}$,
- compare(algebraic a, algebraic b) with a certified answer.
$\square$ Effective points, segments, ...
- defined with effective coordinates,
- or provide directly approximation and queries at the geometric level.
$\square$ Effective curved objects
- defined implicitly with algorithms to operate on them,
- combine it with numerical, geometric approximation.


## Effective Geometric Objects

$\square$ Effective real numbers are such that we can ask:

- algebraic::approximate(int n) a numerical approximation to an arbitrary precision $2^{n}$,
- compare(algebraic a, algebraic b) with a certified answer.
$\square$ Effective points, segments, ...
- defined with effective coordinates,
- or provide directly approximation and queries at the geometric level.
$\square$ Effective curved objects
- defined implicitly with algorithms to operate on them,
- combine it with numerical, geometric approximation.


## Numbers

## Algebraic numbers

## Represented as

$\square$ an arithmetic tree $(\sqrt{x+y+2 \sqrt{x y}}-\sqrt{x}-\sqrt{y})$, and/or
$\square$ a (irreducible) polynomial $p(x)=0$ and an isolating interval.

## Algebraic numbers

## Represented as

$\square$ an arithmetic tree $(\sqrt{x+y+2 \sqrt{x y}}-\sqrt{x}-\sqrt{y})$, and/or
$\square$ a (irreducible) polynomial $p(x)=0$ and an isolating interval.

- Isolation via Descartes, Uspenksy, de Casteljau, Sturm algorithm.


## Algebraic numbers

## Represented as

$\square$ an arithmetic tree $(\sqrt{x+y+2 \sqrt{x y}}-\sqrt{x}-\sqrt{y})$, and/or
$\square$ a (irreducible) polynomial $p(x)=0$ and an isolating interval.

- Isolation via Descartes, Uspenksy, de Casteljau, Sturm algorithm.
- Queries via Sturm(-Habicht) method, interval arithmetic, numerical approximation and separating bounds.


## Algebraic numbers

## Represented as

$\square$ an arithmetic tree $(\sqrt{x+y+2 \sqrt{x y}}-\sqrt{x}-\sqrt{y})$, and/or
$\square$ a (irreducible) polynomial $p(x)=0$ and an isolating interval.

- Isolation via Descartes, Uspenksy, de Casteljau, Sturm algorithm.
- Queries via Sturm(-Habicht) method, interval arithmetic, numerical approximation and separating bounds.
- Comparison of two numbers by refinement until a separating bound:

$$
\alpha \neq 0 \Rightarrow|\alpha|>B(\text { Symbolic Expression of } \alpha) .
$$

## Subdvision solver

$\square$ Bernstein basis: $f(x)=\sum_{i=0}^{d} b_{i} B_{d}^{i}(x)$, where $B_{d}^{i}(x)=\binom{d}{i} x^{i}(1-$ $x)^{d-i}$.

$$
\mathbf{b}=\left[b_{i}\right]_{i=0, \ldots, d} \text { are called the control coefficients. }
$$

## Subdvision solver

$\square$ Bernstein basis: $f(x)=\sum_{i=0}^{d} b_{i} B_{d}^{i}(x)$, where $B_{d}^{i}(x)=\binom{d}{i} x^{i}(1-$ $x)^{d-i}$.
$\mathbf{b}=\left[b_{i}\right]_{i=0, \ldots, d}$ are called the control coefficients.

- $f(0)=b_{0}, f(1)=b_{d}$,


## Subdvision solver

$\square$ Bernstein basis: $f(x)=\sum_{i=0}^{d} b_{i} B_{d}^{i}(x)$, where $B_{d}^{i}(x)=\binom{d}{i} x^{i}(1-$ $x)^{d-i}$.

$$
\mathbf{b}=\left[b_{i}\right]_{i=0, \ldots, d} \text { are called the control coefficients. }
$$

- $f(0)=b_{0}, f(1)=b_{d}$,
- $f^{\prime}(x)=\sum_{i=0}^{d-1} \Delta(\mathbf{b})_{i} B_{d-1}^{i}(x)$ where $\Delta(\mathbf{b})_{i}=b_{i+1}-b_{i}$.


## Subdvision solver

$\square$ Bernstein basis: $f(x)=\sum_{i=0}^{d} b_{i} B_{d}^{i}(x)$, where $B_{d}^{i}(x)=\binom{d}{i} x^{i}(1-$ $x)^{d-i}$.

$$
\mathbf{b}=\left[b_{i}\right]_{i=0, \ldots, d} \text { are called the control coefficients. }
$$

- $f(0)=b_{0}, f(1)=b_{d}$,
- $f^{\prime}(x)=\sum_{i=0}^{d-1} \Delta(\mathbf{b})_{i} B_{d-1}^{i}(x)$ where $\Delta(\mathbf{b})_{i}=b_{i+1}-b_{i}$.
$\square$ Subdivision by de Casteljau algorithm:

$$
\begin{aligned}
& b_{i}^{0}=b_{i}, i=0, \ldots, d, \\
& b_{i}^{r}(t)=(1-t) b_{i}^{r-1}(t)+t b_{i+1}^{r-1}(t), \quad i=0, \ldots, d-r .
\end{aligned}
$$

## Subdvision solver

$\square$ Bernstein basis: $f(x)=\sum_{i=0}^{d} b_{i} B_{d}^{i}(x)$, where $B_{d}^{i}(x)=\binom{d}{i} x^{i}(1-$ $x)^{d-i}$.

$$
\mathbf{b}=\left[b_{i}\right]_{i=0, \ldots, d} \text { are called the control coefficients. }
$$

- $f(0)=b_{0}, f(1)=b_{d}$,
- $f^{\prime}(x)=\sum_{i=0}^{d-1} \Delta(\mathbf{b})_{i} B_{d-1}^{i}(x)$ where $\Delta(\mathbf{b})_{i}=b_{i+1}-b_{i}$.
$\square$ Subdivision by de Casteljau algorithm:

$$
\begin{aligned}
& b_{i}^{0}=b_{i}, i=0, \ldots, d, \\
& b_{i}^{r}(t)=(1-t) b_{i}^{r-1}(t)+t b_{i+1}^{r-1}(t), \quad i=0, \ldots, d-r .
\end{aligned}
$$

- The control coefficients $\mathbf{b}^{-}(t)=\left(b_{0}^{0}(t), b_{0}^{1}(t), \ldots, b_{0}^{d}(t)\right)$ and $\mathbf{b}^{+}(t)=$ ( $\left.b_{0}^{d}(t), b_{1}^{d-1}(t), \ldots, b_{d}^{0}(t)\right)$ describe $f$ on $[0, t]$ and $[t, 1]$.


## Subdvision solver

$\square$ Bernstein basis: $f(x)=\sum_{i=0}^{d} b_{i} B_{d}^{i}(x)$, where $B_{d}^{i}(x)=\binom{d}{i} x^{i}(1-$ $x)^{d-i}$.

$$
\mathbf{b}=\left[b_{i}\right]_{i=0, \ldots, d} \text { are called the control coefficients. }
$$

- $f(0)=b_{0}, f(1)=b_{d}$,
- $f^{\prime}(x)=\sum_{i=0}^{d-1} \Delta(\mathbf{b})_{i} B_{d-1}^{i}(x)$ where $\Delta(\mathbf{b})_{i}=b_{i+1}-b_{i}$.
$\square$ Subdivision by de Casteljau algorithm:

$$
\begin{aligned}
& b_{i}^{0}=b_{i}, i=0, \ldots, d, \\
& b_{i}^{r}(t)=(1-t) b_{i}^{r-1}(t)+t b_{i+1}^{r-1}(t), \quad i=0, \ldots, d-r .
\end{aligned}
$$

- The control coefficients $\mathbf{b}^{-}(t)=\left(b_{0}^{0}(t), b_{0}^{1}(t), \ldots, b_{0}^{d}(t)\right)$ and $\mathbf{b}^{+}(t)=$ ( $\left.b_{0}^{d}(t), b_{1}^{d-1}(t), \ldots, b_{d}^{0}(t)\right)$ describe $f$ on $[0, t]$ and $[t, 1]$.
- For $t=\frac{1}{2}, b_{i}^{r}=\frac{1}{2}\left(b_{i}^{r-1}+b_{i+1}^{r-1}\right)$.; use of adapted arithmetic.
- Number of arithmetic operations bounded by $\mathcal{O}\left(d^{2}\right)$, memory space $\mathcal{O}(d)$. Indeed, asymptotic complexity $\mathcal{O}(d \log (d))$.
$\square$ Isolation of real roots
Proposition: (Descartes rule) $\#\{f(x)=0 ; x \in[0,1]\}=V(\mathbf{b})-2 p, p \in \mathbb{N}$.


## $\square$ Isolation of real roots

Proposition: (Descartes rule) $\#\{f(x)=0 ; x \in[0,1]\}=V(\mathbf{b})-2 p, p \in \mathbb{N}$.

Algorithm: isolation of the roots of $f$ on the interval $[a, b]$
INPUT: A representation $(\mathbf{b},[a, b])$ associate with $f$ and $\epsilon$.

- If $V(\mathbf{b})>1$ and $|b-a|>\epsilon$, subdivide;
- If $V(\mathbf{b})=0$, remove the interval.
- If $V(\mathbf{b})=1$, output interval containing one and only one root.
- If $|b-a| \leq \epsilon$ and $V(\mathbf{b})>0$ output the interval and the multiplicity.

OUTPUT: list of isolating intervals in $[a, b]$ for the real roots of $f$ or the $\epsilon$-multiple root.

## $\square$ Isolation of real roots

Proposition: (Descartes rule) $\#\{f(x)=0 ; x \in[0,1]\}=V(\mathbf{b})-2 p, p \in \mathbb{N}$.

Algorithm: isolation of the roots of $f$ on the interval $[a, b]$
INPUT: A representation $(\mathbf{b},[a, b])$ associate with $f$ and $\epsilon$.

- If $V(\mathbf{b})>1$ and $|b-a|>\epsilon$, subdivide;
- If $V(\mathbf{b})=0$, remove the interval.
- If $V(\mathbf{b})=1$, output interval containing one and only one root.
- If $|b-a| \leq \epsilon$ and $V(\mathbf{b})>0$ output the interval and the multiplicity.

OUTPUT: list of isolating intervals in $[a, b]$ for the real roots of $f$ or the $\epsilon$-multiple root.

- Multiple roots (and their multiplicity) computed within a precision $\epsilon$.
- $x:=t /(1-t):$ Uspensky method.
- Complexity: $\mathcal{O}\left(\frac{1}{2} d(d+1) r\left(\left\lceil\log _{2}\left(\frac{1+\sqrt{3}}{2 s}\right)\right\rceil-\log _{2}(r)+4\right)\right)[\mathrm{MVY} 02+]$
- Natural extension to B-splines.


## Benchmarks

## Pentium III 933Mhz.

The number of equations per s. ( $\mathrm{C}++$ with 64 -bit floats; $\epsilon=0.000001$ ):

| d | 8 | 9 | 12 | 16 | 18 | 20 |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: |
|  | 25000 | $20-22000$ | $12-13000$ | $7.5-8000$ | $5.9-6.2000$ | 5.4000 |

Equations per s. (precision bits vs. degree; $\epsilon=0.000001$ ) using GMP library:

| d | 16 | 20 | 30 | 40 | 60 | 80 | 100 |
| ---: | ---: | ---: | ---: | ---: | ---: | ---: | ---: |
| 128-bit | 96 | 62.5 | 25.4 | 12.5 | - | - | - |
| 192-bit | 83.3 | 53.2 | 21.5 | 10.8 | 4.0 | - | - |
| 256-bit | 73.5 | 47.2 | 18.9 | 9.5 | 3.6 | 1.8 | - |
| 384-bit | 60.2 | 37.7 | 15.2 | 7.6 | 2.9 | 1.4 | 0.8 |
| 512-bit | 51 | 31.2 | 12.2 | 6.1 | 2.3 | 1.2 | 0.7 |

Compare favorably with other efficient solvers (Aberth method, mpsolve).
[Demo]

## Sweeping a set of (conic) circular arcs



## Sweeping a set of (conic) circular arcs



- Arcs represented by the equations of a circle and two lines.
- By resultant computation, it reduces to sign evaluations of algebraic polynomials $P_{i}$ (degree $\leq 12$ ):

$$
P_{4} t^{4}+P_{3} t^{3}+P_{2} t^{2}+P_{1} t+P_{0}=0
$$

- Inputs parameters in a bounded grid; static error bounds.
- Filtering technics can be used easily.
- Efficiency:



## Preliminary benchmarks



| A: 100, S:23123, V: 1916, E: 6878 | Sweep (s) | Incr. (s) |
| :--- | ---: | ---: |
| SplCart, ExDFMT, double | 0.6 | 0.7 |
| RefCart, ExDFMT, double | 0.8 | 0.2 |
| SpICart, ExDFMT, ZZraw | 9.3 | 11.0 |
| SCN, ExDFMT, ZZraw | 6.0 | 7.0 |
| SCN, ExDFMT, Gmpz | 9.0 | 6.0 |
| RefCart, ExDFMT, ZZraw | 8.2 | 9.3 |
| SpICart, Naive, Core | 23.2 | 34.7 |
| RefCart, Naive, Core | 24.9 | 36.3 |
| SplCart, Naive, Leda | 30.7 | 21.6 |
| RefCart, Naive, Leda | 30.8 | 21.9 |
| SplCart, ExDFMT, Gmpq | 51.7 | 60.5 |
| RefCart, ExDFMT, Gmpq | 57.5 | 61.2 |

A:Arcs, S:Seed, V:Vertices, E:Edges. Random data.

| A: 400, S: 43123, V: 33653, E: 131402 | Sweep (sec) | Incr. (sec) |
| :--- | ---: | ---: |
| SplCart, ExDFMT, double | 3.5 | 0.6 |
| RefCart, ExDFMT, double | 5.0 | 1.3 |
| SpICart, ExDFMT, ZZraw | 179.5 | 174.9 |
| RefCart, ExDFMT, ZZraw | 156.9 | 147.2 |
| SCN, ExDFMT, ZZraw | 100.0 | 95.0 |
| SCN, ExDFMT, Gmpz | 140.0 | 25.0 |
| SpICart, Naive, Core | Abort | Abort |
| RefCart, Naive, Core | Abort | Abort |
| SpICart, Naive, Leda | 520.6 | 337.7 |
| RefCart, Naive, Leda | 523.6 | 345.6 |
| SpICart, ExDFMT, Gmpq, | 989.9 | 960.3 |
| RefCart, ExDFMT, Gmpq, | 1104.0 | 1009.3 |

## Benchmarks

| Times |  |  |  |  |  |  | Exactness |  |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| Data |  | Naive |  | Polynomial |  |  | Naive | Pol. |
|  |  | double | Interval + real | double | GMP | $\begin{gathered} \text { static } \\ + \text { semi-static } \\ + \text { Naive Int. } \\ + \text { GMP } \end{gathered}$ | double | double |
|  |  | $\mu \mathrm{s}$ | $\mu \mathrm{s}$ | $\mu \mathrm{s}$ | $\mu \mathrm{s}$ | $\mu \mathrm{s}$ | \% | \% |
| $l_{1} \leq r_{2} ?$ | rnd22 | 0.60 | 2.48 | 0.25 | 82 | 0.36 | 100 | 100 |
|  | rnd16 | 0.60 | 2.48 | 0.25 | 78 | 0.41 | 100 | 100 |
|  | almost | 0.60 | 67. | 0.25 | 115 | 6.80 | 99 | 78 |
|  | degenerate | 0.60 | 2170. | 0.25 | 115 | 128. | 8 | 17 |
| $l_{1} \leq l_{2} ?$ | rnd22 | 0.60 | 2.45 | 0.28 | 107 | 0.44 | 100 | 100 |
|  | rnd16 | 0.60 | 2.45 | 0.28 | 102 | 0.56 | 100 | 100 |
|  | almost | 0.60 | 38.1 | 0.28 | 130 | 5.64 | 99 | 99 |
|  | degenerate | 0.60 | 2180. | 0.28 | 130 | 144. | 7 | 5 |

- PC-Linux Pentium-III 500MHz, g++ 2.95.1-02 -mcpu=pentiumpro -march=pentiumpro
- rnda: pick at random in $[-M, M]^{2}, M=2^{a}$, the centers of two cercles and a common point. Arc defined by radical axis and first cercle.
- degenerate: same construction with ending points of same abcissae.
- almost: same construction with one square radius slightly incremented.


## Points

## Solvers



## Solvers

- Analytic solvers: exploit the value of $f$ and its derivatives.

Newton like methods, Minimisation methods, Weierstrass method.
$\square$
$\square$

## Solvers

- Analytic solvers: exploit the value of $f$ and its derivatives.

Newton like methods, Minimisation methods, Weierstrass method.

- Homotopic solvers: deform a system with known roots into the system to solve.

Projective, toric, flat, deformation.
$\square$
$\square$
$\square$

## Solvers

- Analytic solvers: exploit the value of $f$ and its derivatives.

Newton like methods, Minimisation methods, Weierstrass method.

- Homotopic solvers: deform a system with known roots into the system to solve.

Projective, toric, flat, deformation.

- Subdivision solvers: use an exclusion criterion to isolate the roots.

Taylor exclusion function, interval arithmetic, Descartes rule.
$\square$
$\square$

## Solvers

- Analytic solvers: exploit the value of $f$ and its derivatives.

Newton like methods, Minimisation methods, Weierstrass method.

- Homotopic solvers: deform a system with known roots into the system to solve.

Projective, toric, flat, deformation.

- Subdivision solvers: use an exclusion criterion to isolate the roots.

Taylor exclusion function, interval arithmetic, Descartes rule.

- Algebraic solvers: exploit the known relation between the unkowns.

Gröbner basis, normal form computations. Reduction to univariate or eigenvalue problems.
$\square$

## Solvers

- Analytic solvers: exploit the value of $f$ and its derivatives.

Newton like methods, Minimisation methods, Weierstrass method.

- Homotopic solvers: deform a system with known roots into the system to solve.

Projective, toric, flat, deformation.

- Subdivision solvers: use an exclusion criterion to isolate the roots.

Taylor exclusion function, interval arithmetic, Descartes rule.

- Algebraic solvers: exploit the known relation between the unkowns.

Gröbner basis, normal form computations. Reduction to univariate or eigenvalue problems.

- Geometric solvers: project the problem onto a smaller subspace.

Resultant-based methods. Reduction to univariate or eigenvalue problems.

## Solvers

- Analytic solvers: exploit the value of $f$ and its derivatives.

Newton like methods, Minimisation methods, Weierstrass method.

- Homotopic solvers: deform a system with known roots into the system to solve.

Projective, toric, flat, deformation.

- Subdivision solvers: use an exclusion criterion to isolate the roots.

Taylor exclusion function, interval arithmetic, Descartes rule.

- Algebraic solvers: exploit the known relation between the unkowns.

Gröbner basis, normal form computations. Reduction to univariate or eigenvalue problems.

- Geometric solvers: project the problem onto a smaller subspace.

Resultant-based methods. Reduction to univariate or eigenvalue problems.

## Multiplication operators

We assume that $\mathcal{Z}(I)=\left\{\zeta_{1}, \ldots, \zeta_{d}\right\} \Leftrightarrow \mathcal{A}=\mathbb{K}[\mathbf{x}] / I$ of finite dimension $D$ over $\mathbb{K}$.

$$
\left.\begin{array}{rlrl}
M_{a}: \mathcal{A} & \rightarrow \mathcal{A} & M_{a}^{t}: \widehat{\mathcal{A}} & \rightarrow \hat{\mathcal{A}} \\
u & \mapsto a u & & \mapsto
\end{array}\right)
$$

## Multiplication operators

We assume that $\mathcal{Z}(I)=\left\{\zeta_{1}, \ldots, \zeta_{d}\right\} \Leftrightarrow \mathcal{A}=\mathbb{K}[\mathbf{x}] / I$ of finite dimension $D$ over $\mathbb{K}$.

$$
\begin{aligned}
M_{a}: \mathcal{A} & \rightarrow \mathcal{A} & M_{a}^{\mathrm{t}}: \widehat{\mathcal{A}} & \rightarrow \widehat{\mathcal{A}} \\
u & \mapsto a u & \Lambda & \mapsto a \cdot \Lambda=\Lambda \circ M_{a}
\end{aligned}
$$

## Theorem:

$\square$ The eigenvalues of $M_{a}$ are $\left\{a\left(\zeta_{1}\right), \ldots, a\left(\zeta_{d}\right)\right\}$.
$\square$ The eigenvectors of all $\left(M_{a}^{\mathrm{t}}\right)_{a \in \mathcal{A}}$ are (up to a scalar) $\mathbf{1}_{\zeta_{i}}: p \mapsto p\left(\zeta_{i}\right)$.

## Multiplication operators

We assume that $\mathcal{Z}(I)=\left\{\zeta_{1}, \ldots, \zeta_{d}\right\} \Leftrightarrow \mathcal{A}=\mathbb{K}[\mathbf{x}] / I$ of finite dimension $D$ over $\mathbb{K}$.

$$
\left.\begin{array}{rlrl}
M_{a}: \mathcal{A} & \rightarrow \mathcal{A} & M_{a}^{\mathrm{t}}: \widehat{\mathcal{A}} & \rightarrow \hat{\mathcal{A}} \\
u & \mapsto a u & & \mapsto
\end{array}\right)
$$

Theorem:
$\square$ The eigenvalues of $M_{a}$ are $\left\{a\left(\zeta_{1}\right), \ldots, a\left(\zeta_{d}\right)\right\}$.
$\square$ The eigenvectors of all $\left(M_{a}^{\mathrm{t}}\right)_{a \in \mathcal{A}}$ are (up to a scalar) $\mathbf{1}_{\zeta_{i}}: p \mapsto p\left(\zeta_{i}\right)$.

Theorem: In a basis of $\mathcal{A}$, all the matrices $M_{a}(a \in \mathcal{A})$ are of the form

$$
\mathrm{M}_{a}=\left[\begin{array}{ccc}
\mathrm{N}_{a}^{1} & & \mathbf{0} \\
& \ddots & \\
\mathbf{0} & & \mathrm{~N}_{a}^{d}
\end{array}\right] \text { with } \mathrm{N}_{a}^{i}=\left[\begin{array}{ccc}
a\left(\zeta_{i}\right) & & \star \\
\mathbf{0} & \ddots & a\left(\zeta_{i}\right)
\end{array}\right]
$$

## Multiplication operators

We assume that $\mathcal{Z}(I)=\left\{\zeta_{1}, \ldots, \zeta_{d}\right\} \Leftrightarrow \mathcal{A}=\mathbb{K}[\mathbf{x}] / I$ of finite dimension $D$ over $\mathbb{K}$.

$$
\left.\begin{array}{rlrl}
M_{a}: \mathcal{A} & \rightarrow \mathcal{A} & M_{a}^{\mathrm{t}}: \widehat{\mathcal{A}} & \rightarrow \hat{\mathcal{A}} \\
u & \mapsto a u & & \Lambda
\end{array}\right)
$$

## Theorem:

$\square$ The eigenvalues of $M_{a}$ are $\left\{a\left(\zeta_{1}\right), \ldots, a\left(\zeta_{d}\right)\right\}$.
$\square$ The eigenvectors of all $\left(M_{a}^{\mathrm{t}}\right)_{a \in \mathcal{A}}$ are (up to a scalar) $\mathbf{1}_{\zeta_{i}}: p \mapsto p\left(\zeta_{i}\right)$.

Theorem: In a basis of $\mathcal{A}$, all the matrices $M_{a}(a \in \mathcal{A})$ are of the form

$$
\mathrm{M}_{a}=\left[\begin{array}{ccc}
\mathbb{N}_{a}^{1} & & 0 \\
& \ddots & \\
0 & & \mathrm{~N}_{a}^{d}
\end{array}\right] \text { with } \mathrm{N}_{a}^{i}=\left[\begin{array}{ccc}
a\left(\zeta_{i}\right) & & \star \\
0 & \ddots & a\left(\zeta_{i}\right)
\end{array}\right]
$$

Corollary: (Chow form)
$\Delta(\mathbf{u})=\operatorname{det}\left(u_{0}+u_{1} \mathbb{M}_{x_{1}}+\cdots+u_{n} \mathbb{M}_{x_{n}}\right)=\prod_{\zeta \in \mathcal{Z}(I)}\left(u_{0}+u_{1} \zeta_{1}+\cdots+u_{n} \zeta_{n}\right)^{\mu_{\zeta}}$.

## Resultant in one variable

$$
\text { Let } f_{0}=c_{0,0}+\cdots+c_{0, d_{0}} x^{d_{0}}, \quad f_{1}=c_{1,0}+\ldots+c_{1, d_{1}} x^{d_{1}}\left(\text { with } d_{0} \leq d_{1}\right)
$$

## Resultant in one variable

Let $f_{0}=c_{0,0}+\cdots+c_{0, d_{0}} x^{d_{0}}, \quad f_{1}=c_{1,0}+\ldots+c_{1, d_{1}} x^{d_{1}}\left(\right.$ with $\left.d_{0} \leq d_{1}\right)$. Sylvester (1840)

## Resultant in one variable

Let $f_{0}=c_{0,0}+\cdots+c_{0, d_{0}} x^{d_{0}}, \quad f_{1}=c_{1,0}+\ldots+c_{1, d_{1}} x^{d_{1}}\left(\right.$ with $\left.d_{0} \leq d_{1}\right)$. Sylvester (1840)

$$
\left.\begin{array}{c}
\overbrace{f_{0} \cdots x^{d_{1}-1_{f}}}^{d_{0}+d_{1}} \\
{\left[\begin{array}{ccc|ccc}
f_{1} \cdots & \cdots x_{0}-1_{f_{1}} \\
c_{0,0} & & 0 & c_{1,0} & & 0 \\
\vdots & \ddots & & \vdots & \ddots & \\
\vdots & & c_{0,0} & \vdots & & c_{1,0} \\
c_{0, d_{0}} & & \vdots & c_{1, d_{1}} & & \vdots \\
& \ddots & \vdots & & \ddots & \vdots \\
0 & & c_{0, d_{0}} & 0 & & c_{1, d_{1}}
\end{array}\right]}
\end{array} \begin{array}{l}
1 \\
x \\
x^{d_{1}-1} \\
\\
x^{d_{0}+d_{1}-1}
\end{array}\right\} d_{0}+d_{1}
$$

## Bézout (1779)

$\Theta_{f_{0}, f_{1}}(x, y):=\frac{f_{1}(x) f_{0}(y)-f_{1}(y) f_{0}(x)}{y-x}=\sum_{i=0}^{d_{1}-1} \theta_{f_{0}, f_{1}, i}(x) y^{i}=\sum_{i=0}^{d_{1}-1} \sum_{j=0}^{d_{1}-1} \theta_{i, j} x^{i} y^{j}$.
The Bézout matrix is $\mathrm{B}_{f_{0}, f_{1}}=\left(\theta_{i, j}\right)_{0 \leq i, i \leq d_{1}}$.

## Resultant in one variable

Let $f_{0}=c_{0,0}+\cdots+c_{0, d_{0}} x^{d_{0}}, \quad f_{1}=c_{1,0}+\ldots+c_{1, d_{1}} x^{d_{1}}\left(\right.$ with $\left.d_{0} \leq d_{1}\right)$. Sylvester (1840)

## Bézout (1779)

$\Theta_{f_{0}, f_{1}}(x, y):=\frac{f_{1}(x) f_{0}(y)-f_{1}(y) f_{0}(x)}{y-x}=\sum_{i=0}^{d_{1}-1} \theta_{f_{0}, f_{1}, i}(x) y^{i}=\sum_{i=0}^{d_{1}-1} \sum_{j=0}^{d_{1}-1} \theta_{i, j} x^{i} y^{j}$.
The Bézout matrix is $\mathrm{B}_{f_{0}, f_{1}}=\left(\theta_{i, j}\right)_{0 \leq i, i \leq d_{1}}$.
Theorem : $R\left(c_{i, j}\right):=\operatorname{det}(S)$ vanishes iff $f_{0}=0, f_{1}=0$ has a common root.

## Solving $f_{1}=\cdots=f_{n}=0$ by hiding a variable

1. Construct the resultant matrix $\mathrm{S}\left(x_{n}\right)$ of $f_{1}, \ldots, f_{n}$ as polynomials in $x_{1}, \ldots, x_{n-1}$ with coefficients in $\mathbb{K}\left[x_{n}\right]$.
2. Solve $\mathrm{S}\left(x_{n}\right)^{t} \mathbf{w}=0$.

- Either by solving $\operatorname{det}\left(\mathrm{S}\left(x_{n}\right)\right)=0$ and by deducing the corresponding w.
- or by reducing it to an eigenproblem:

$$
\left(\mathrm{S}_{d}^{t} x_{n}^{d}+\mathrm{S}_{d-1}^{t} x_{n}^{d-1}+\cdots+\mathrm{S}_{0}^{t}\right) \mathbf{w}=0
$$

$$
\left(\left[\begin{array}{cccc}
0 & \mathbb{I} & \cdots & 0 \\
\vdots & \ddots & \ddots & \vdots \\
0 & \cdots & 0 & \mathbb{I} \\
\mathrm{~S}_{0}^{t} & \cdots & \mathrm{~S}_{d-2}^{t} & \mathrm{~S}_{d-1}^{t}
\end{array}\right]-x_{n}\left[\begin{array}{cccc}
\mathrm{S}_{d}^{t} & 0 & \cdots & 0 \\
0 & \ddots & \ddots & \vdots \\
\vdots & \ddots & \mathrm{~S}_{d}^{t} & 0 \\
0 & \cdots & 0 & \mathrm{~S}_{d}^{t}
\end{array}\right]\right) \underline{\mathrm{w}}=0
$$

3. Deduce the other coordinates of the roots from $\mathbf{w}$.

## Comparison



| Alg. mth. | \# r-roots | deg. | \# x-roots | Time | Sylv. SVD | \# r-roots | deg. | \# x-roots | Time |
| :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: | :---: |
| 1 | 2 | 4 | 2 | 0.02 s | 1 | 2 | 4 | 2 | 0.00 s |
| 2 | 6 | 3 | 6 | 0.02 s | 2 | 6 | 3 | 4 | 0.00 s |
| 3 | 6 | 3 | 6 | 0.02 s | 3 | 6 | 3 | 1 | 0.00 s |
| 4 | 4 | 2 | 4 | 0.02 s | 4 | 4 | 2 | 2 | 0.00 s |
| 5 | 16 | 4 | 8 | 0.02 s | 5 | 16 | 4 | 0 | - |
| 6 | 4 | 2 | 4 | 0.02 s | 6 | 4 | 2 | 4 | 0.00 s |
| 7 | 8 | 4 | 8 | 0.02 s | 7 | 8 | 4 | 3 | 0.00 s |
| 8 | 6 | 3 | 0 | - | 8 | 6 | 3 | 2 | 0.00 s |
| 9 | 8 | 4 | 8 | 0.03 s | 9 | 8 | 4 | Np | - |
| 10 | 12 | 6 | 12 | 0.03 s | 10 | 12 | 6 | Np | - |
| 11 | 10 | 10 | 10 | 0.12 s | 11 | 10 | 10 | Np | - |
| 12 | 16 | 6 | 0 | - | 12 | 16 | 6 | 10 | 0.07 s |
| 13 | 6 | 5 | 6 | 0.02 s | 13 | 6 | 5 | 2 | 0.00 s |
| 14 | 42 | 6 | 42 | 0.12 s | 14 | 42 | 6 |  |  |
| Sylv. Eig. | \# r-roots | deg. | \# x-roots | Time | Bez. Eig. | \# r-roots | deg. | \# x-roots | Time |
| 1 | 2 | 4 | Np | - | 1 | 2 | 4 | Np | - |
| 2 | 6 | 3 | 6 | 0.00 s | 2 | 6 | 3 | Uc | - |
| 3 | 6 | 3 | 4 | 0.00 s | 3 | 6 | 3 | 3 | 0.00 s |
| 4 | 4 | 2 | 4 | 0.00 s | 4 | 4 | 2 | Np | - |
| 5 | 16 | 4 | 16 | 0.01 s | 5 | 16 | 4 | Np | - |
| 6 | 4 | 2 | Np | - | 6 | 4 | 2 | Np | - |
| 7 | 8 | 4 | 2 | 0.00 s | 7 | 8 | 4 | 1 | 0.01 s |
| 8 | 6 | 3 | 0 | 0.00 s | 8 | 6 | 3 | 2 | 0.01 s |
| 9 | 8 | 4 | Np | - | 9 | 8 | 4 | 6 | 0.00 s |
| 10 | 12 | 6 | Np | - | 10 | 12 | 6 | 11 | 0.00 s |
| 11 | 10 | 10 | 3 | 0.82 s | 11 | 10 | 10 | 6 | 0.19 s |
| 12 | 16 | 6 | Np | - | 12 | 16 | 6 | Np | - |
| 13 | 6 | 5 | 1 | 0.00 s | 13 | 6 | 5 | 2 | 0.00 s |
| 14 | 42 | 6 | Np | - | 14 | 42 | 6 | Np | - |

- Subdvision

| Example | $\varepsilon$ | Evaluation | Number <br> of intervals | Time | Number <br> of real roots |
| :--- | :---: | :---: | :---: | :---: | :---: |
| 10 | $10^{-5}$ | $10^{-5}$ | 5 | 0.030 | 5 |
| 11 | $10^{-5}$ | $10^{-4}$ | 770 | 79.188 | 2 |
| 15 | $10^{-5}$ | $10^{-4}$ | 4 | 0.016 | 4 |

## Curves

Curves


## Curves



## Algorithm: Topology of an implicit curve

- Compute the critical value for the projection along the $y$-abcisses.
- Above each point, compute the $y$-value, with their multiplicity.
- Between two critical points, compute the number of branches.
- Connect the points between two consecutive levels by y-order, the multi-branches beeing at the multiple point.


## Curves



## Algorithm: Topology of an implicit curve

- Compute the critical value for the projection along the $y$-abcisses.
- Above each point, compute the $y$-value, with their multiplicity.
- Between two critical points, compute the number of branches.
- Connect the points between two consecutive levels by y-order, the multi-branches beeing at the multiple point.
$\Rightarrow$ Rationnal representation of the singular $y$ in terms of the $x$.
$\Rightarrow$ Descartes rule to detect the multiple point among the regular ones.


## Examples



| topology | time execution running |
| :--- | :--- |
| 1 | 0.03 s |
| 2 | 0.04 s |
| 3 | 0.04 s |
| 4 | 0.10 s |
| 5 | 0.05 s |
| 6 | 0.05 s |
| 7 | 0.62 s |
| 8 | 0.17 s |
| 9 | 0.02 s |
| 10 | 0.09 s |

## Solving by subdivision methods

Rectangular patches: $f(x, y)=\sum_{i=0}^{d_{1}} \sum_{j=0}^{d_{2}} b_{j, i} B_{d_{1}}^{i}(x) B_{d_{2}}^{j}(y)$ associated with the box $[0,1] \times[0,1]$.

## Solving by subdivision methods

Rectangular patches: $f(x, y)=\sum_{i=0}^{d_{1}} \sum_{j=0}^{d_{2}} b_{j, i} B_{d_{1}}^{i}(x) B_{d_{2}}^{j}(y)$ associated with the box $[0,1] \times[0,1]$.

- Subdivision by row or by column, similar to the univariate case.
- Arithmetic complexity of a subdivision bounded by $\mathcal{O}\left(d^{3}\right) \quad(d=$ $\left.\max \left(d_{1}, d_{2}\right)\right)$, memory space $\mathcal{O}\left(d^{2}\right)$.


## Solving by subdivision methods

Rectangular patches: $f(x, y)=\sum_{i=0}^{d_{1}} \sum_{j=0}^{d_{2}} b_{j, i} B_{d_{1}}^{i}(x) B_{d_{2}}^{j}(y)$ associated with the box $[0,1] \times[0,1]$.

- Subdivision by row or by column, similar to the univariate case.
- Arithmetic complexity of a subdivision bounded by $\mathcal{O}\left(d^{3}\right)(d=$ $\left.\max \left(d_{1}, d_{2}\right)\right)$, memory space $\mathcal{O}\left(d^{2}\right)$.

Triangular patches: $\quad f(x, y)=\sum_{i+j+k=d} b_{i, j, k} \frac{d!}{i!j!k!} x^{i} y^{j}(1-x-y)^{k}$ associated with the representation on the 2 d simplex.

## Solving by subdivision methods

Rectangular patches: $f(x, y)=\sum_{i=0}^{d_{1}} \sum_{j=0}^{d_{2}} b_{j, i} B_{d_{1}}^{i}(x) B_{d_{2}}^{j}(y)$ associated with the box $[0,1] \times[0,1]$.

- Subdivision by row or by column, similar to the univariate case.
- Arithmetic complexity of a subdivision bounded by $\mathcal{O}\left(d^{3}\right)(d=$ $\left.\max \left(d_{1}, d_{2}\right)\right)$, memory space $\mathcal{O}\left(d^{2}\right)$.

Triangular patches: $\quad f(x, y)=\sum_{i+j+k=d} b_{i, j, k} \frac{d!}{i!j!k!} x^{i} y^{j}(1-x-y)^{k}$ associated with the representation on the 2 d simplex.

- Subdivision at a new point. Arithmetic complexity $\mathcal{O}\left(d^{3}\right)$, memory space $\mathcal{O}\left(d^{2}\right)$.
- Combined with Delaunay triangulations.
- Extension to A-patches.


## Approximating an implicit curve

## Algorithm: Representation of the implicit curve $f(x, y)=0$

INPUT: A triangular representation of $f L:=((A, B, C), \mathbf{b})$ and a precision $\epsilon$.

- If at least one of the triangle edges is bigger that $\epsilon$, split the triangle and insert the new triangles in $L$ :
- when the number of sign changes of some row (column or diagonal) is $\geq 2$,
- or when the coefficients of $f_{x}^{\prime}$ (or $f_{y}^{\prime}, f_{z}^{\prime}$ ) have not the same sign.
- Remove the triangle from $L$ if the coefficients of $f$ have the same sign.
- Save it
- when all the edges of the triangle are smaller than $\epsilon$,
- or when the total number of sign changes on the border sides is 2 and $f_{x}^{\prime}$ or $f_{y}^{\prime}, f_{z}^{\prime}$, has a constant sign. Isolate the roots.
OUTPUT: A list of segments approximating the curve $f(x, y)=0$.
- Insertion of the circumcenter (barycenter), in order to break the bad triangle.
- No specific directions/axes used.
- New edges are constructed, no tangency problem.
- Number of triangles related to the complexe local feature size.
- Application to the intersection of curves, surfaces.


## Examples



## Surfaces

## Examples




|  | nb triangles | nb cellules | temps d'execution |
| :---: | :---: | :---: | :---: |
| $\mathrm{A} 1--$ | 8093 | $3962+6 \mathrm{nt}$ | 3.37818 s |
| $\mathrm{~A} 2+-$ | 6395 | $3134+6 \mathrm{nt}$ | 2.90356 s |
| $\mathrm{~A} 2--$ | 3598 | $1768+7 \mathrm{nt}$ | 1.9934 s |
| $\mathrm{~A} 3+-$ | 6179 | $3009+10 \mathrm{nt}$ | 3.01165 s |
| $\mathrm{~A} 3--$ | 6290 | $6290+6 \mathrm{nt}$ | 3.14654 s |
| $\mathrm{~A} 4+-$ | 5859 | $2825+13 \mathrm{nt}$ | 3.14721 s |
| $\mathrm{D} 4+-$ | 4035 | $1975+6 \mathrm{nt}$ | 1.84261 s |
| $\mathrm{D} 4--$ | 8937 | $4340+12 \mathrm{nt}$ | 4.29918 s |
| $\mathrm{D} 4-$ - unfold 1 | 7291 | $3577+10 \mathrm{nt}$ | 3.53391 s |
| $\mathrm{D} 4-$ - unfold 2 | 8269 | $4019+31 \mathrm{nt}$ | 3.86696 s |
| D4 - unfold 3 | 9633 | $4615+14 \mathrm{nt}$ | 4.35244 s |


|  | nb triangles | nb cellules | temps d'execution |
| :---: | :---: | :---: | :---: |
| D5 + - | 7407 | $3596+6 \mathrm{nt}$ | 3.61756 s |
| D5 - - | 4254 | $2014+9 \mathrm{nt}$ | 2.23405 s |
| D6 + - | 3925 | $1882+12 \mathrm{nt}$ | 2.1853 s |
| D6 -- | 6983 | $3364+12 \mathrm{nt}$ | 3.83701 s |
| E6 +- | 6017 | $2920+18 \mathrm{nt}$ | 3.53177 s |
| E6 - - | 3638 | $1751+10 \mathrm{nt}$ | 2.11355 s |
| E7 | 6019 | $2927+24 \mathrm{nt}$ | 3.20513 s |
| E8 | 4524 | $2182+14 \mathrm{nt}$ | 2.78838 s |
| Q1 | 11634 | $4760+185 \mathrm{nt}$ | 9.04296 s |
| Q2 | 8833 | $3821+84 \mathrm{nt}$ | 7.30251 s |
| Q3 | 6661 | $3074+24 \mathrm{nt}$ | 6.55459 s |
| S20 | 8016 | $3498+258 \mathrm{nt}$ | 2.9955 s |
| S21 | 13542 | $4848+1962 \mathrm{nt}$ | 4.16841 s |
| S22 | 16722 | $6234+792 \mathrm{nt}$ | 5.3028 s |
| S23 | 17757 | $6551+1263 \mathrm{nt}$ | 5.28855 s |
| S26 | 8699 | $3310+1178 \mathrm{nt}$ | 4.02468 s |


|  | nb triangles | nb cellules | temps d'execution |
| :---: | :---: | :---: | :---: |
| D5 + - | 7407 | $3596+6 \mathrm{nt}$ | 3.61756 s |
| D5 - - | 4254 | $2014+9 \mathrm{nt}$ | 2.23405 s |
| D6 + - | 3925 | $1882+12 \mathrm{nt}$ | 2.1853 s |
| D6 -- | 6983 | $3364+12 \mathrm{nt}$ | 3.83701 s |
| E6 +- | 6017 | $2920+18 \mathrm{nt}$ | 3.53177 s |
| E6 - - | 3638 | $1751+10 \mathrm{nt}$ | 2.11355 s |
| E7 | 6019 | $2927+24 \mathrm{nt}$ | 3.20513 s |
| E8 | 4524 | $2182+14 \mathrm{nt}$ | 2.78838 s |
| Q1 | 11634 | $4760+185 \mathrm{nt}$ | 9.04296 s |
| Q2 | 8833 | $3821+84 \mathrm{nt}$ | 7.30251 s |
| Q3 | 6661 | $3074+24 \mathrm{nt}$ | 6.55459 s |
| S20 | 8016 | $3498+258 \mathrm{nt}$ | 2.9955 s |
| S21 | 13542 | $4848+1962 \mathrm{nt}$ | 4.16841 s |
| S22 | 16722 | $6234+792 \mathrm{nt}$ | 5.3028 s |
| S23 | 17757 | $6551+1263 \mathrm{nt}$ | 5.28855 s |
| S26 | 8699 | $3310+1178 \mathrm{nt}$ | 4.02468 s |

Thanks for your attention.

