Matrix-Based Implicit Representations of Rational Algebraic Curves and Applications

Thang Luu Ba
(Joint work with Laurent Busé)

Université de Nice and INRIA Sophia Antipolis

SAGA Workshop, March 15-19/2010, Auron-France

1. Matrix representation of parameterized space curves
   - The implicitation of parameterized space curves
   - μ-basis of a rational curve $\mathcal{C}$
   - The initial Fitting ideal
2. Computing singular points of $\mathcal{C}$ by means of its matrix representation
   - The singular points of $\mathcal{C}$
   - Rank of a representation matrix at a singular point
   - Singular factors
3. Curve/Curve intersection problem
   - Curve/Curve intersection problem
   - Linearization of a univariate polynomial matrix
   - The Algorithm for extracting the regular part
   - Matrix intersection algorithm
4. Conclusion

The parameterized map

Suppose given a parametrization

$$\begin{array}{ccc} \mathbb{P}^1_{\mathbb{K}} & \xrightarrow{\phi} & \mathbb{P}^n_{\mathbb{K}} \\ (s:t) & \mapsto & (f_0 : f_1 : \ldots : f_n)(s,t) \end{array}$$

of a space curve **C** such that

i) f_i are the homogeneous polynomial with the same degree d.

ii) $\gcd(f_0, \ldots, f_n) \in \mathbb{K} \setminus \{0\}$.

$\mathcal{C} :=$ image of ϕ (called a rational curve).

The defining ideal of a parametrized space curve

Let h be ring morphism :

$$\begin{array}{rcl} h : \mathbb{K}[x_0, \ldots, x_n] & \rightarrow & \mathbb{K}[s,t] \\ x_i & \mapsto & f_i(s,t) \quad i = 0, \ldots, n. \end{array}$$

We have

$$I_{\mathcal{C}} = \ker h.$$

Remark.

- $I_{\mathcal{C}}$ is a homogeneous prime ideal of $\mathbb{K}[x_0, \ldots, x_n]$.
- $V_{\mathbb{K}}(I_{\mathcal{C}}) = \mathcal{C}$.
- It is quite difficult to compute $I_{\mathcal{C}}$.

Syzygies of a set polynomial $f_0(s,t),\ldots,f_n(s,t)$

Denote $\mathbf{f} := (f_0,\ldots,f_n)$,

$$\mathrm{Syz}(\mathbf{f}) = \left\{ (g_0(s,t),\ldots,g_n(s,t)) \ : \ \sum_{i=0}^{n} g_i(s,t) f_i(s,t) = 0 \right\}$$

$\subset \oplus_{i=0}^{n} \mathbb{K}[s,t]$.

- By Hilbert-Burch Theorem : $\mathrm{Syz}(\mathbf{f})$ is *free* and *graded* $\mathbb{K}[s,t]$-module of rank n
- Chosing a basis $u_1(s,t), u_2(s,t), \ldots, u_n(s,t)$ of $\mathrm{Syz}(\mathbf{f})$.

μ-basis of a rational curve $\mathcal{C}$

Definition

$u_1(s,t), u_2(s,t), \ldots, u_n(s,t)$ is called a μ-basis of a rational space curve $\mathcal{C}$

Denote $\mu_i := \deg u_i(s,t)$, then

- $\sum_{i=1}^{n} \mu_i = d$.
- The collection of integers $(\mu_1, \mu_2, \ldots, \mu_n)$ is unique if we order $0 \leq \mu_1 \leq \mu_2 \leq \cdots \leq \mu_n$.
- It exist an effective algorithm for computing μ-basis (without base Grobner).

Denote $A := \mathbb{K}[x_0, \ldots, x_n]$; $C := A[s,t]$, we consider the grading of C given by $\deg(s) = \deg(t) = 1$ and $\deg(a) = 0$ for all $a \in A$. Set

$$u_i(s,t,x_0,x_1,\ldots,x_n) = \sum_{j=0}^{n} u_{i,j}(s,t)x_j \in C$$

and B be the cokernel of the following graded map :

$$\phi : \oplus_{i=1}^{n} C(-\mu_i) \xrightarrow{u_1,\ldots,u_n} C : (g_1,\ldots,g_n) \mapsto \sum_{i=1}^{n} u_i g_i \qquad (1)$$

$$\phi_\nu : [\oplus_{i=1}^{n} C(-\mu_i) \xrightarrow{u_1,\ldots,u_n} C]_\nu : (g_1,\ldots,g_n) \mapsto \sum_{i=1}^{n} u_i g_i \qquad (2)$$

- Denote $\mathfrak{F}(B_\nu)$, the *initial Fitting ideal* of B_ν, which is the ideal of A generated by the $(\nu+1)$-minors of a matrix of (2).

Theorem

For all integer $\nu \geq \mu_n + \mu_{n-1} - 1$,

$$\mathfrak{F}(B_\nu) = I_{\mathcal{C}}{}^{\deg(\phi)}$$

at all points on $\mathcal{C}$ except a finite number (possibly zero) support on $\mathcal{C}$.

Remark.

- $\mathfrak{F}(B_\nu) = I_{\mathcal{C}}$ if ϕ is birational map (i.e.deg(ϕ) = 1).
- $\sqrt{\mathfrak{F}(B_\nu)} = I_{\mathcal{C}}$.

The matrix representation of a space curve $\mathcal{C}$

Suppose that $\nu \geq \mu_n + \mu_{n-1} - 1$, we have

- Matrix $\mathtt{M}(\phi)_\nu$ of linear map ϕ_ν is called a matrix representations of a space curve $\mathcal{C}$. Its entries are linear forms in $\mathbb{K}[x_0 \ldots, x_n]$
- Size of $\mathtt{M}(\phi)_\nu$ is $(\nu+1) \times (n(\nu+1) - d)$.

Remark.

- It is easy to compute $\mathtt{M}(\phi)_\nu$.
- $\mathtt{M}(\phi)_\nu$ can be seen as a bridge between the parametric representation ϕ of $\mathcal{C}$ and its implicit representation $I_{\mathcal{C}}$.

Example

Let $\mathcal{C}$ be the rational space curve given by parameterized

$$
\begin{aligned}
f_0(s,t) &= 3s^4t^2 - 9s^3t^3 - 3s^2t^4 + 12st^5 + 6t^6, \\
f_1(s,t) &= -3s^6 + 18s^5t - 27s^4t^2 - 12s^3t^3 + 33s^2t^4 + 6st^5 - 6t^6, \\
f_2(s,t) &= s^6 - 6s^5t + 13s^4t^2 - 16s^3t^3 + 9s^2t^4 + 14st^5 - 6t^6, \\
f_3(s,t) &= -2s^4t^2 + 8s^3t^3 - 14s^2t^4 + 20st^5 - 6t^6.
\end{aligned}
$$

A μ-basis for $\mathcal{C}$ is :

$$\begin{aligned} u_1 &= (s^2-3st+t^2)x+t^2y \\ u_2 &= (s^2-st+3t^2)y+(3s^2-3st-3t^2)z, \\ u_3 &= 2t^2z+(s^2-2st-2t^2)w. \end{aligned}$$

From $\deg_{s,t}(u_1)=\deg_{s,t}(u_2)=\deg_{s,t}(u_3)=2$, we can chose $\nu=3$, then matrix representation of $\mathcal{C}$ is

$$\begin{pmatrix} x+y & 0 & 3y-3z & 0 & 2z-2w & 0 \\ -3x & x+y & -y-3z & 3y-3z & -2w & 2z-2w \\ x & -3x & y+3z & -y-3z & w & -2w \\ 0 & x & 0 & y+3z & 0 & w \end{pmatrix}.$$

The singular points of $\mathcal{C}$

Let $\mathcal{C}$ be a rational space curve of parameterized by the birational map

$$\begin{array}{ccc} \mathbb{P}^1_{\mathbb{K}} & \xrightarrow{\phi} & \mathbb{P}^3_{\mathbb{K}} \\ (s:t) & \mapsto & (f_0 : f_1 : f_2 : f_3)(s,t). \end{array}$$

Remark.

- The condition birational map is not restrictive.
- Matrix representation of $\mathcal{C}$ is $\mathtt{M}(\phi)_\nu$ with $\nu \geq \mu_3 + \mu_2 - 1$.

Inversion formula of a point on $\mathcal{C}$

Definition

An inversion formula of $P \in \mathcal{C}$ is a homogeneous polynomial $h_P(s,t)$ whose roots (including multiplicities) are the parameter values $(s_i : t_i)$ corresponding to P, i.e.

$$h_P(s,t) = \prod_{i=0}^{\alpha}(t_i s - s_i t)^{r_i}, \sum_{i=0}^{\alpha} r_i = r$$

where $P = \mathbf{f}(s_0,t_0) = \cdots = \mathbf{f}(s_\alpha, t_\alpha)$.

Definition

deg $h_P(s,t)$ is called a multiplicity of P. Denote $m_P(\mathcal{C})$

Remark. This definition corresponds to the classical definition of multiplicity.

Computation of the inversion formula

Lemma

Let $P \in \mathcal{C}$. Then,

$$h_P(s,t) = \gcd(u_1(s,t;P), u_2(s,t;P), u_3(s,t;P)).$$

Rank of a representation matrix at a singular point

Theorem

Given a point $P \in \mathbb{P}^3$, we have

$$\operatorname{rank} \mathtt{M}(\phi)_\nu(P) = \nu + 1 - m_P(\mathcal{C}),$$

or equivalently $\operatorname{corank} \mathtt{M}(\phi)_\nu(P) = m_P(\mathcal{C})$.

Remark. This theorem allows to characterize the singular points with multiplicity by rank of matrix representation.

Denote : $\mathtt{M}(\phi)_\nu(s,t) := \mathtt{M}(\phi)_\nu(f_0, f_1, f_2, f_3)$.

Remark.

- $\operatorname{rank} \mathtt{M}(\phi)_\nu(s,t) < \nu + 1$ for any point $(s:t) \in \mathbb{P}^1$
- The entries of $M(s,t)$ are homogeneous polynomials of two variables of the same degree d.

The singular factor of the parameterization ϕ

$D_i(s,t) :=$ gcd of all the i-minors of $\mathtt{M}(\phi)_\nu(s,t)$

Definition

A collection of homogeneous polynomials $d_1(s,t), \ldots, d_{\nu+1}(s,t)$ in $\mathbb{K}[s,t]$ such that for all integer $i = 1, \ldots, \nu+1$

$$D_i(s,t) = d_{\nu+1}^i d_\nu^{i-1} \ldots d_{\nu+1-i+2}^2 d_{\nu+1-i+1}$$

is called a collection of singular factors of the parameterization ϕ.

Remark. The computation of the singular factors can be done through Smith form computation.

Singularity factors of matrix

Theorem

- $d_{\nu+1}(s,t) = d_{\nu}(s,t) = \cdots = d_{\mu_3+1}(s,t) = 1$ *and* $d_1(s,t) = 0$.
- *For any singular point* $P \in \mathcal{C}$, $h_P(s,t) \mid d_{m_P(\mathcal{C})}(s,t)$ *and* $\gcd(h_P(s,t), d_k(s,t)) = 1$ *for all* $k > m_P(\mathcal{C})$.

Corollary

- *Let* $P = \phi(s_0 : t_0)$ *be a point on* $\mathcal{C}$, *then* $d_{m_P(\mathcal{C})}(s_0 : t_0) = 0$ *and* $d_k(s_0 : t_0) \neq 0$ *for all* $k > m_P(\mathcal{C})$.
- *For any integer* k *such that* $2 \leq k \leq \mu_3$, *the product*

$$\prod_{P \in \mathcal{C} \,:\, m_P(\mathcal{C}) = k} h_p(s,t)$$

that runs over all the singular points on $\mathcal{C}$ *of multiplicity* k, *divides the singular factor* $d_k(s,t)$.

Example

Let $\mathcal{C}$ be the rational space curve given by parameterized

$$\mathbf{f}(s,t) = (s^5, s^3t^2, s^2t^3, t^5)$$

then matrix representation of $\mathcal{C}$ is

$$\mathtt{M}(\phi) = \begin{pmatrix} y & 0 & 0 & x & 0 & z & 0 \\ -z & y & 0 & 0 & x & 0 & z \\ x & -z & y & -y & 0 & -w & 0 \\ 0 & 0 & -z & 0 & -y & 0 & -w \end{pmatrix},$$

Substitute $x = s^5, y = s^3t^2, z = s^2t^3, w = t^5$, we have matrix representation of $\mathcal{C}$ is

$$\mathtt{M}(\phi)(s,t) = \begin{pmatrix} s^3t^2 & 0 & 0 & s^5 & 0 & s^2t^3 & 0 \\ -s^2t^3 & s^3t^2 & 0 & 0 & s^5 & 0 & s^2t^3 \\ 0 & -s^2t^3 & s^3t^2 & -s^3t^2 & 0 & -t^5 & 0 \\ 0 & 0 & -s^2t^3 & 0 & -s^3t^2 & 0 & -t^5 \end{pmatrix},$$

The form Smith of $\mathtt{M}(\phi)(s,1), \mathtt{M}(\phi)(1,t)$ are respectively

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & s^2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & t^2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

Factor singular of $\mathcal{C}$: $d_4(s,t) = 1, d_3(s,t) = 1, d_2(s,t) = s^2t^2$.
Thus, we have only two singular points of multiplycities 2, $A = (0:0:0:1), B = (1:0:0:0)$ corresponds to $(s_0 : t_0) = (0:1), (1:0)$.

Curve/Curve intersection problem

Suppose given rational space curve $\mathcal{C}_1$ with $M(\phi_1)(x, y, z, w)$ to be a matrix representation and a rational space curve $\mathcal{C}_2$ represented by a parameterization

$$\Psi : \mathbb{P}^1_{\mathbb{K}} \to \mathbb{P}^3_{\mathbb{K}} : (s : t) \mapsto (x(s,t) : y(s,t) : z(s,t) : w(s,t))$$

where $x(s,t), y(s,t), z(s,t), w(s,t)$ are homogeneous polynomials of the same degree and without common factor in $\mathbb{K}[s,t]$.
Determine the set $\mathcal{C}_1 \cap \mathcal{C}_2 \subset \mathbb{P}^3_{\mathbb{K}}$

Matrix representation of $\mathcal{C}_1 \cap \mathcal{C}_2$

By replacing the variables x, y, z, w by the homogeneous polynomials $x(s,t), y(s,t), z(s,t), w(s,t)$ respectively, we get the matrix

$$M(\phi_1)(s,t) = M(\phi_1)(x(s,t), y(s,t), z(s,t), w(s,t)).$$

Lemma

For all point $(s_0 : t_0) \in \mathbb{P}^1_{\mathbb{K}}$, rank $M(\phi_1)(s_0, t_0)$ drops if and only if the point $(x(s_0,t_0) : y(s_0,t_0) : z(s_0,t_0) : w(s_0,t_0)) \in \mathcal{C}_1 \cap \mathcal{C}_2$.

It follows that the points in $\mathbf{C}_1 \cap \mathbf{C}_2$ associated to points $(s : t)$ such that $s \neq 0$, are in correspondence with the set of values $t \in \mathbb{K}$ such that $M(\phi_1)(1,t)$ drops of rank strictly less than its row and column dimensions.

Linearization of a polynomial matrix

Given an $m \times n$-matrix $M(t) = (a_{i,j}(t))$ with $a_{i,j}(t) \in \mathbb{K}[t]$.

$$M(t) = M_d t^d + M_{d-1} t^{d-1} + \ldots + M_0$$

where $M_i \in \mathbb{K}^{m \times n}$ and $d = \max_{i,j}\{\deg(a_{i,j}(t))\}$.

Definition

The generalized companion matrices A, B of the matrix $M(t)$ are the matrices with coefficients in $\mathbb{K}$ of size $((d-1)m+n) \times dm$ that are given by

$$A = \begin{pmatrix} 0 & I & \dots & \dots & 0 \\ 0 & 0 & I & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & \dots & I \\ M_0^t & M_1^t & \dots & \dots & M_{d-1}^t \end{pmatrix}$$

$$B = \begin{pmatrix} I & 0 & \dots & \dots & 0 \\ 0 & I & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & I & 0 \\ 0 & 0 & \dots & \dots & -M_d^t \end{pmatrix}$$

The Algorithm for extracting the regular part

Theorem

$$\operatorname{rank} M(t) < \ \mathit{drops} \ \Leftrightarrow \operatorname{rank}(A - tB) < \ \mathit{drops} \ .$$

In the paper (joint work with L. Busé and B. Mourrain (SNC09)), we have given an algorithm allows to remove the singular blocks of the pencil of matrices $A - tB$ and obtain a regular pencil of matrix $A' - tB'$

Theorem

$$\operatorname{rank}(A - tB) \ \mathit{drops} \ \Leftrightarrow \operatorname{rank}(A' - tB') \ \mathit{drops}.$$

Remark.

- The idea of using matrix representations for computing the intersection is quite old.
- The novelty of our contribution is to enable non squares matrices.
- Matrix representation of $\mathcal{C}_1 \cap \mathcal{C}_2$ is almost always non square matrix.

Matrix intersection algorithm

Input : Two rational space curves $\mathcal{C}_1$ and $\mathcal{C}_2$ parameterized by ϕ_1 and ϕ_2 respectively.

Output : The intersection points of $\mathcal{C}_1$ and $\mathcal{C}_2$.

1. Build the matrix representation $M(\phi_1)_\nu$ of $\mathcal{C}_1$ for a suitable ν.

2. Build the generalized companion matrices A and B of $M(\phi_1)(1,t)$.

3. Compute the companion regular matrices A' and B'.

4. Compute the eigenvalues of (A', B').

5. For each eigenvalue t_0, the point $\phi_2(1 : t_0)$ is one of the intersection points.

Example

Let $\mathcal{C}_1$ be the rational space curve given by the parameterization

$$\begin{aligned}
f_0(s,t) &= 3s^4t^2 - 9s^3t^3 - 3s^2t^4 + 12st^5 + 6t^6, \\
f_1(s,t) &= -3s^6 + 18s^5t - 27s^4t^2 - 12s^3t^3 + 33s^2t^4 + 6st^5 - 6t^6, \\
f_2(s,t) &= s^6 - 6s^5t + 13s^4t^2 - 16s^3t^3 + 9s^2t^4 + 14st^5 - 6t^6, \\
f_3(s,t) &= -2s^4t^2 + 8s^3t^3 - 14s^2t^4 + 20st^5 - 6t^6.
\end{aligned}$$

and $\mathcal{C}_2$,the twisted cubic, is parameterized by

$$x(t) = 1, y(t) = t, z(t) = t^2, w(t) = t^3.$$

$$M(\phi_1) = \begin{pmatrix} x+y & 0 & 3y-3z & 0 & 2z-2w & 0 \\ -3x & x+y & -y-3z & 3y-3z & -2w & 2z-2w \\ x & -3x & y+3z & -y-3z & w & -2w \\ 0 & x & 0 & y+3z & 0 & w \end{pmatrix}.$$

Substitute : $x(t) = 1, y(t) = t, z(t) = t^2, w(t) = t^3$

$$M(\phi_1)(t) = \begin{pmatrix} 1+t & 0 & 3t-3t^2 & 0 & 2t^2-2t^3 & 0 \\ -3 & 1+t & -t-3t^2 & 3t-3t^2 & -2t^3 & 2t^2-2t^3 \\ 1 & -3 & t+3t^2 & -t-3t^2 & t^3 & -2t^3 \\ 0 & 1 & 0 & t+3t^2 & 0 & t^3 \end{pmatrix}.$$

We have $M(\phi_1)(t) = M_3 t^3 + M_2 t^2 + M_1 t + M_0$ and the generalized companion matrices of $M(t)$ are

$$A = \begin{pmatrix} 0 & I & 0 \\ 0 & 0 & I \\ M_0^t & M_1^t & M_2^t \end{pmatrix}, B = \begin{pmatrix} I & 0 & 0 \\ 0 & I & 0 \\ 0 & 0 & -M_3^t \end{pmatrix}.$$

$$A' = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, B' = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Then, we compute the following eigenvalues : $t = 0$ and thus $\mathcal{C}_1$ intersect $\mathcal{C}_2$ at the only point $(1:0:0:0)$.

Conclusion

- Introduce new matrix- based representation of rational space curves.
- The detection of singularities points via matrix-based representation of rational space curves.
- Transfer the solving of the curve/curve intersection problem into the eigenvalues computing problems.

Computer algebraic system

- Maple 12.
- Mathemagix (Packtage MMX).
- Macaulay 2.

References

1. Busé, L., D'Andrea, C., 2009. Singular factors of rational plane curves, preprint arXiv :0912.2723.
2. Busé, L., Jouanolou, J.-P., 2003. On the closed image of a rational map and the implicitization problem. J. Algebra 265 (1), 312–357.
3. Chen, F., Wang, W., Liu, Y., 2008. Computing singular points of plane rational curves. J. Symbolic Comput. 43 (2), 92–117.
4. Jia, X., Wang, H., Goldman, R., 2010. Set-theoretic generators of rational space curves. Journal of Symbolic Computation 45 (4), 414 – 433.
5. Luu Ba, T., Busé, L., Mourrain, B., 2009. Curve/surface intersection problem by means of matrix representations. In : SNC '09 : Proceedings of the 2009 conference on Symbolic numeric computation. ACM, New York, USA, pp. 71–78.
6. Song, N., Goldman, R., 2009. μ-bases for polynomial systems in one variable. Comput. Aided Geom. Design 26 (2), 217–230.

7. Wang, H., Jia, X., Goldman, R., 2009. Axial moving planes and singularities of rational space curves. Comput. Aided Geom. Design 26 (3), 300–316.

Thank you for your attention