A Parametric version of Hilbert-Hurwitz method using Hypercircles

L.F. Tabera
Universidad de Cantabria/ Institut Mittag-Leffler

MEGA 2011, Stockholm

The implicit problem

- Let $\mathbb{K}$ be a characteristic zero element. $\mathbb{F}$ is algebraic closure.
- Let $F(x_0, x_1, x_2) \in \mathbb{K}[x_0, x_1, x_2]$ be an homogeneous polynomial of degree d representing a rational curve $\mathcal{C}$.
- What are the solutions of $F(x_0, x_1, x_2) = 0$ in $\mathbb{P}^2(\mathbb{K})$.

Hilbert-Hurwitz

Theorem[Hilbert-Hurwitz 1890] If $\mathcal{C}$ is of degree $d > 2$ and $\psi_1, \psi_2, \psi_3 \in \mathbb{K}[x_0, x_1, x_2]$ are generic *adjoints* of $\mathcal{C}$ of degree $d-2$, then the transformation

$$\begin{array}{ccc} \mathbb{P}^2(\mathbb{K}) & \to & \mathbb{P}^2(\mathbb{K}) \\ x = [x_0 : x_1 : x_2] & \mapsto & [\psi_1(x) : \psi_2(x) : \psi_3(x)] \end{array}$$

Transforms $\mathcal{C}$ $\mathbb{K}$-birationally onto a curve of degree $d-2$.

Corollary

- Every rational curve defined over $\mathbb{K}$ is $\mathbb{K}$-birational to a line or a conic.
- Every odd degree rational curve defined over $\mathbb{K}$ has smooth points with coordinates in $\mathbb{K}$.
- Every rational curve defined over $\mathbb{K}$ has points over an algebraic extension of $\mathbb{K}$ of degree at most 2.

$\mathbb{K}$-rational points in rational curves

Problem Given $\mathcal{C}$ a curve defined over $\mathbb{K}$ in $\mathbb{F}^m$. Find points over small (deg. 1 or 2) extensions of $\mathbb{K}$.

- Compute a plane curve $\mathcal{C}_1$ $\mathbb{K}$-birational to $\mathcal{C}$.
- Use Hilbert-Hurwitz to compute a line or a conic $\mathbb{K}$-birational to $\mathcal{C}$.
- Compute points over extensions of degree 1 or 2. In some cases, decide if there are $\mathbb{K}$-rational points. eg. $\mathbb{K} = \mathbb{Q}$, use Legendre method.

▶ This is useful to compute (if possible) parametrizations of $\mathcal{C}$ with coefficients in $\mathbb{K}$ (van Hoeij, Sendra-Winkler).

The parametric case

- $\mathcal{C}$ is defined over $\mathbb{K}$ if it is the zero locus of a set of polynomials with coefficients in $\mathbb{K}$.
- $\mathcal{C}$ is defined over $\mathbb{K}$ if it is invariant under $\mathbb{K}$-automorphisms of $\mathbb{F}$.
- $\mathcal{C}$ is parametrizable over $\mathbb{K}$ if there exists a proper parametrization of $\mathcal{C}$ with coefficients in $\mathbb{K}$.
- $\mathcal{C}$ is $\mathbb{K}$-parametrizable $\rightarrow$ $\mathcal{C}$ is $\mathbb{K}$-definable.
- $\mathcal{C}$ is $\mathbb{K}$-definable and has a smooth point with coefficients in $\mathbb{K}$ $\rightarrow$ $\mathcal{C}$ is $\mathbb{K}$-parametrizable.

The parametric case

$\mathbb{K} = \mathbb{Q}(w_1, \ldots, w_r)(\gamma)$. w_i algebraically independent. γ algebraic over $\mathbb{Q}(w_1, \ldots, w_r)$.

- Let α be an algebraic element of degree n over $\mathbb{K}$.
- Let $\psi = (\psi_1, \ldots, \psi_m) \in (\mathbb{K}(\alpha)(t))^m$ be a proper parametrization of a rational curve $\mathcal{C}$.

- Is $\mathcal{C}$ defined over $\mathbb{K}$?
- Is $\mathcal{C}$ parametrizable over $\mathbb{K}$?
- How to compute a parametrization?

Implicitization is expensive. We want to do it better.

Example

$$\psi(t) = \left(\frac{t^2 + 2It - 2}{t^2 + 2It}, \frac{2t + 2I}{t^2 + 2It} \right)$$

This is a complex parametrization of the unit circle $x^2 + y^2 - 1$. The change of variables $t \mapsto t - I$ transforms ψ into a rational parametrization:

$$\psi(t - I) = \left(\frac{t^2 - 1}{t^2 + 1}, \frac{2t}{t^2 + 1} \right)$$

Example

$$\psi(t) = \left(\frac{It^2 - I}{t^2 + 1}, \frac{2It}{t^2 + 1} \right)$$

In this case, ψ parametrizes the curve $x^2 + y^2 + 1$, that is defined over $\mathbb{Q}$ but has no parametrization over $\mathbb{Q}$.

$$\psi(t) = (t, It)$$

In this case, ψ parametrizes $xI - y$, so the curve is not defined over $\mathbb{K}$ not it has a proper parametrization over $\mathbb{K}$. Note that $(0, 0)$ is a smooth point of $\mathcal{C}$.

Solution: Hypercircles

In 1999, C. Andradas, T. Recio and J.R. Sendra proposed to use a Weil descent method applied to the parametrization.

$\psi(t) = (\psi_1(t), \ldots, \psi_m(t)) \in \mathbb{K}(\alpha)(t)^m$. Substitute $t \to \sum_{i=0}^{n-1} t_i \alpha^i$, where t_i are new variables (and n is the degree of α over $\mathbb{K}$). Write

$$\psi_i \left(\sum_{i=0}^{n-1} t_i \alpha^i \right) = \sum_{j=0}^{n-1} \frac{F_{ij}(t_0, \ldots, t_{n-1})}{D(t_0, \ldots, t_{n-1})} \alpha^i$$

where F_{ij}, $D \in \mathbb{K}[t_0, \ldots, t_{n-1}]$.

We try to kill the "complex" parts.

$$\mathcal{Z} = \{F_{ij} = 0 | 1 \leq i \leq m, 1 \leq j \leq n-1\} - \{D = 0\}$$

The *witness* variety or the *parametric variety of Weil*.

Solution: Hypercircles

Theorem[Andradas, Recio, Sendra, 1999]

- $\mathcal{C}$ is $\mathbb{K}$-definable if and only if $dim(\mathcal{Z}) = 1$.
- $dim(\mathcal{Z}) \leq 1$ and has at most one component of dimension 1.
- $\mathcal{C}$ is parametrizable over $\mathcal{K}$ if and only if $\mathcal{U}$ is.
- If $\phi(t) = (\phi_0(t), \ldots, \phi_{n-1}(t))$ is a parametrization of $\mathcal{U}$ with coefficients in $\mathbb{K}$, then $\sum_{i=0}^{n-1} \phi_i(t)\alpha^i = u(t)$ is an automorphism of $\mathbb{P}^1(\mathbb{F})$ such that $\psi(u(t))$ has coefficients over $\mathbb{K}$.

Algorithm based on Hypercircles

This provides the following algorithm:
Input $\psi(t)$

1. **Compute** $\mathcal{Z}$ from ψ.
2. **If** $dim(\mathcal{Z}) = 0$, **return** $\mathcal{C}$ is not defined over $\mathbb{K}$ **end**.
3. Compute $\mathcal{U}$ the one-dimensional component of $\mathcal{Z}$.
4. **If** $\mathcal{U}$ is not parametrizable over $\mathbb{K}$ then **return** $\mathcal{C}$ is defined but not parametrizable over $\mathbb{K}$.
5. **Compute** a parametrization $\phi = (\phi_0, \ldots, \phi_{n-1})$ of $\mathcal{U}$ over $\mathbb{K}$.
6. **Return** $u = \sum_{i=0}^{n-1} \phi_i(t)\alpha^i$, $\psi(u(t))$.
7. Profit!

Algorithm based on Hypercircles

This provides the following algorithm:
Input $\psi(t)$

1. **Compute** $\mathcal{Z}$ from ψ.
2. **If** $dim(\mathcal{Z}) = 0$, **return** $\mathcal{C}$ is not defined over $\mathbb{K}$ **end**.
3. Compute $\mathcal{U}$ the one-dimensional component of $\mathcal{Z}$.
4. **If** $\mathcal{U}$ is not parametrizable over $\mathbb{K}$ then **return** $\mathcal{C}$ is defined but not parametrizable over $\mathbb{K}$.
5. **Compute** a parametrization $\phi = (\phi_0, \ldots, \phi_{n-1})$ of $\mathcal{U}$ over $\mathbb{K}$.
6. **Return** $u = \sum_{i=0}^{n-1} \phi_i(t)\alpha^i$, $\psi(u(t))$.
7. Profit!

Parametrizations of $\mathcal{U}$ over $\mathbb{K}$

▶ *(Recio, Sendra, Villarino 2004)*, provided an algorithm to compute the change of variables $u(t)$ from *the standard parametrization* of $\mathcal{U}$ and a point in $\mathcal{U} \cap \mathbb{K}^n$.

Parametrizations of $\mathcal{U}$ over $\mathbb{K}$

▶ *(Recio, Sendra, Villarino 2004)*, provided an algorithm to compute the change of variables $u(t)$ from *the standard parametrization* of $\mathcal{U}$ and a point in $\mathcal{U} \cap \mathbb{K}^n$. Provided that $deg(\mathcal{U}) = n$.

Parametrizations of $\mathcal{U}$ over $\mathbb{K}$

- *(Recio, Sendra, Villarino 2004)*, provided an algorithm to compute the change of variables $u(t)$ from *the standard parametrization* of $\mathcal{U}$ and a point in $\mathcal{U} \cap \mathbb{K}^n$. Provided that $deg(\mathcal{U}) = n$.

- *(Recio, Sendra, T. Villarino 2010)* an algorithm to detect if an arbitrary rational curve $\mathcal{U}$ is a hypercircle and compute the associated unit $u(t)$.

Parametrizations of $\mathcal{U}$ over $\mathbb{K}$

▶ *(Recio, Sendra, Villarino 2004)*, provided an algorithm to compute the change of variables $u(t)$ from *the standard parametrization* of $\mathcal{U}$ and a point in $\mathcal{U} \cap \mathbb{K}^n$. Provided that $deg(\mathcal{U}) = n$.

▶ *(Recio, Sendra, T. Villarino 2010)* an algorithm to detect if an arbitrary rational curve $\mathcal{U}$ is a hypercircle and compute the associated unit $u(t)$. Provided that we have a point in $\mathcal{U} \cap \mathbb{K}^n$.

Algorithm based on Hypercircles, revisited

Input $\psi(t)$

1. **Compute** $\mathcal{Z}$ from ψ.
2. **If** $dim(\mathcal{Z}) = 0$, **return** $\mathcal{C}$ is not defined over $\mathbb{K}$ **end**.
3. Compute $\mathcal{U}$ the one-dimensional component of $\mathcal{Z}$.
4. **If** $\mathcal{U}$ is not parametrizable over $\mathbb{K}$ then **return** $\mathcal{C}$ is defined but not parametrizable over $\mathbb{K}$.

5.1 **Compute** a point $p \in \mathcal{U} \cap \mathbb{K}^n$.

5.2 **Compute** a parametrization $\phi = (\phi_0, \ldots, \phi_{n-1})$ over $\mathbb{K}$ from p.

6 **Return** $u = \sum_{i=0}^{n-1} \phi_i(t)\alpha^i$, $\psi(u(t))$.

7 Profit!

Computing rational points in $\mathcal{U}$

- Hilbert-Hurwitz ensures that there are always points in $\mathcal{U}$ over an extension of $\mathbb{K}$ of degree at most 2.

- Use the geometry of hypercircles to compute such points.

Hypercircles

Definition Let $\mathbb{K} \subseteq \mathbb{K}(\alpha)$ as before and $u(t) = \frac{at+b}{ct+d} \in \mathbb{K}(\alpha)(t)$, $ad - bc = 0$ a linear fraction. Write

$$u(t) = \phi_0(t) + \alpha\phi_1(t) + \ldots + \alpha^{n-1}\phi_{n-1}, \phi_i(t) \in \mathbb{K}(t)$$

The α-*hypercircle* associated to $\mathcal{U}$ is the rational curve parametrized by $(\phi_0, \ldots, \phi_{n-1})$.

So, $\mathcal{C}$ is parametrizable over $\mathbb{K}$ if and only if the corresponding curve $\mathcal{U}$ is an α-hypercircle.

Theorem If $\mathcal{U}$ is the one-dimensional component of $\mathcal{Z}$ and $\mathbb{K} = \mathbb{Q}(x_1, \ldots, x_n)(\gamma)$, there is always a β of degree ≤ 2 over $\mathbb{K}$ such that $[\mathbb{K}(\alpha) : \mathbb{K}] = [\mathbb{K}(\beta, \alpha) : \mathbb{K}]$ and $\mathcal{U}$ is a hypercircle for the extension $\mathbb{K}(\beta) \subseteq \mathbb{K}(\alpha)$.

Properties of Hypercircles

(Recio, Sendra, T., Villarino, 2008)

- $\mathcal{U}$ is always a rational normal curve.
- The degree of $\mathcal{U}$ is a divisor of n. It is equal to the degree of the pole of $u(t) = \frac{at+b}{ct+d}$ over $\mathbb{K}$.
- If the degree of $\mathcal{U}$ is n, we can read the points at infinity from the minimal polynomial of α.
- The hypercircle can be parametrized by the pencil of hyperplanes

$$\mathcal{L}(t) = \{x_0 + \alpha x_1 + \ldots + \alpha^{n-1} x_{n-1} = t\}.$$

  The parametrization obtained by this pencil is called the *standard parametrization* of the hypercircle.

Computing points of $\mathcal{U}$ over extensions of degree at most 2

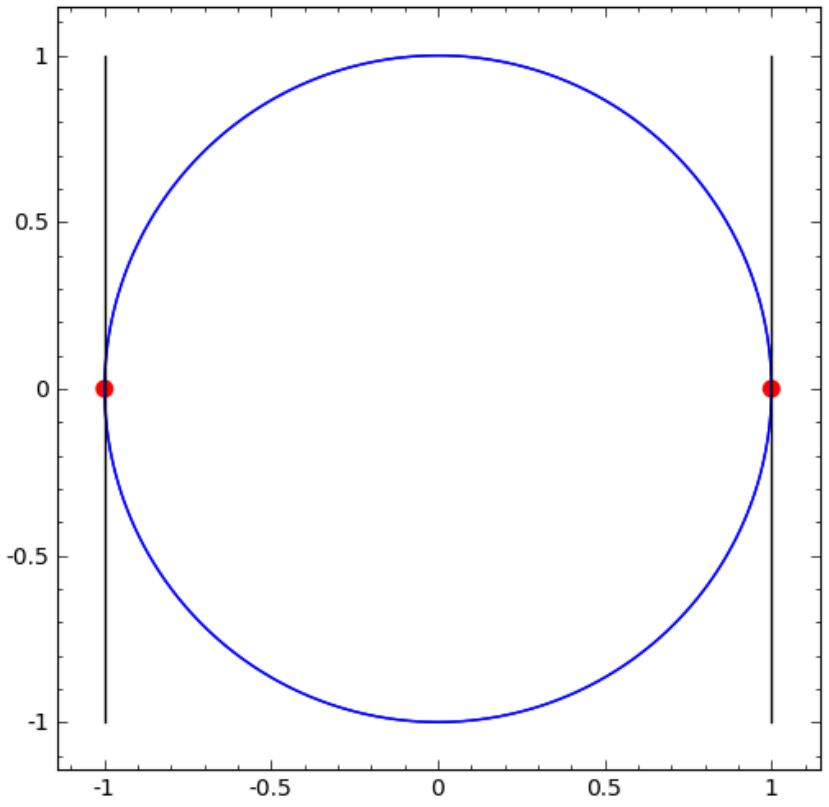
Theorem Let ϕ be the standard parametrization of $\mathcal{U}$. Let $r = deg(\mathcal{U})$ and $\phi_i(t)$ be a non-constant component of ϕ, then the differential

$$dx_i = \phi'(t) \cdot dt$$

defines a canonical divisor $Z - P$ such that Z, the divisor of zeros, is of degree $2r - 2$ and consists only on affine points. The divisor of poles P is of degree $2r$ and consists in twice the points at infinity of $\mathcal{U}$.

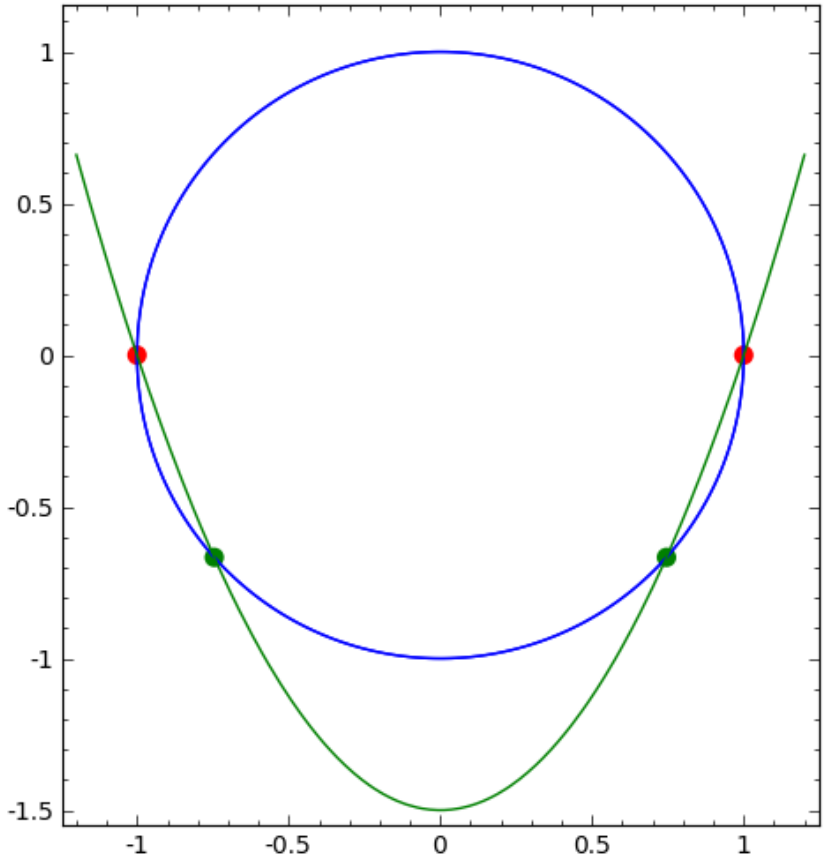
- If we intersect $\mathcal{U}$ with a quadric $\mathcal{W}$ defined over $\mathbb{K}$ passing through P, the intersection will be $\mathcal{W} \cap \mathcal{U} = P + P_1 + P_2$, with P_1, P_2 defined over an extension of degree at most two over $\mathbb{K}$.

Example, conics $r = 2$



$u = \frac{t+I}{t-I}$, dx defines $[1:0:1] + [-1:0:1] - 2[1:I:0] - 2[1:-I:0]$

Example, conics $r = 2$



$u = \frac{t+I}{t-I}$, dx defines $[1:0:1] + [-1:0:1] - 2[1:I:0] - 2[1:-I:0]$
Any conic passing through $[1:0:1]$, $[-1:0:1]$ should cut the circle in two other conjugate points.

Quadrics containing $\mathcal{U}$

▶ The hypercircle is a rational normal curve of degree r, so it is an intersection of quadrics and a linear space of dimension r.

Theorem
Let $\mathcal{U}$ be a hypercircle of degree r in $\mathbb{F}^n$ and Z the divisor of zeros of dx_i.

- The space of quadrics $\mathcal{W}_Z = \{\mathcal{W} | \mathcal{W} \cap \mathcal{U} \succeq Z\}$ is of dimension $\binom{n+2}{2} - 2r + 1$.
- The space of quadrics containing containing $\mathcal{U}$ is of dimension $\binom{n+2}{2} - 2r - 2$.

So, the set of bad quadrics is of codimension 3. If we compute a basis of $\mathcal{W}_Z$ one of the elements of the basis will not contain $\mathcal{U}$.

Computing a parametrization over $\mathbb{K}(\beta) = \mathbb{K}(P_1)$

- If $[\mathbb{K}(\beta, \alpha) : \mathbb{K}(\beta)] = [\mathbb{K}(\alpha) : \mathbb{K}]$, we can use P_1 and the known algorithm to compute a linear fraction $u(t)$ such that $\psi(u)$ has coefficients in $\mathbb{K}(\beta)$.
- Case $\mathbb{K} \subsetneq \mathbb{K}(\beta) \subsetneq \mathbb{K}(\alpha)$. we defined the hypercircle $\mathcal{U}$ associated to ψ for the extension $\mathbb{K} \subsetneq \mathbb{K}(\alpha)$. We can also define the hypercircle $\mathcal{U}_\beta$ associated to ψ for the extension $\mathbb{K}(\beta) \subsetneq \mathbb{K}(\alpha)$. But computing $\mathcal{U}_\beta$ is easy:

Theorem Let M be the $n/2 \times n$ matrix whose i-th column contains the coordinates of α^{i-1} in the base $\{1, \alpha, \ldots, \alpha^{n/2}\}$ of $\mathbb{K}(\alpha)$ as a vector space over $\mathbb{K}(\beta)$. Let ϕ be the standard parametrization of the hypercircle $\mathcal{U}$ then $M \cdot \phi$ is the standard parametrization of $\mathcal{U}_\beta$.

- So, if $\beta \in \mathbb{K}(\alpha)$, we can compute $\mathcal{U}_\beta$ and $M \cdot P_1$ a point in $\mathcal{U}_\beta$ with coefficients in $\mathbb{K}(\beta)$ and apply the known algorithm to compute u such that $\psi(u(t)) \in \mathbb{K}(\beta)(t)^m$.

The birational conic

- Given ψ, we are able to compute a unit u such that $\psi(u(t))$ has coefficients in $\mathbb{K}(\beta)$. If $\beta \in \mathbb{K}$ we are done. If $\beta \notin \mathcal{C}$ we can compute the hypercircle $\mathcal{V}$ associated to $\psi(u)$ with respect to the extension $\mathbb{K} \subseteq \mathbb{K}(\beta)$.
- $\mathcal{V}$ will always be a birational line or conic in the plane.
- If $deg(\mathcal{C})$ is odd or $[\mathbb{K}(\alpha) : \mathbb{K}]$ is odd (or we have an odd divisor defined over $\mathbb{K}$ over $\mathcal{C}$), we can define a divisor D of $\mathcal{V}$ of odd degree s defined over $\mathbb{K}$.
- If we intersect $\mathcal{V}$ with a $\mathbb{K}$-curve $\mathcal{W}$ of degree $(s+1)/2$ passing through D, then $\mathcal{W} \cap \mathcal{V} = D + P$, where $P \in \mathcal{V} \cap \mathbb{K}^2$, so we can parametrize $\mathcal{V}$ (and $\mathcal{C}$ over $\mathbb{K}$).

Algorithm based on Hypercircles, revisited

Input $\psi(t)$

1. **Compute** $\mathcal{Z}$ from ψ.
2. **If** $dim(\mathcal{Z}) = 0$, **return** $\mathcal{C}$ is not defined over $\mathbb{K}$ **end.**
3. Compute $\mathcal{U}$ the one-dimensional component of $\mathcal{Z}$.
4. **If** $\mathcal{U}$ is not parametrizable over $\mathbb{K}$ then **return** $\mathcal{C}$ is defined but not parametrizable over $\mathbb{K}$.

5.1 **Compute** a point $p \in \mathcal{U} \cap \mathbb{K}(\beta)^n$. Where $[\mathbb{K}(\beta) : \mathbb{K}] \leq 1$.

5.2 **Compute** a parametrization $\phi = (\phi_0, \ldots, \phi_{n-1})$ of $\mathcal{U}$ over $\mathbb{K}(\beta)$ from p.

5.3 **Compute** a parametrization of $\mathcal{C}$ over $\mathbb{K}(\beta)$ and the birational conic.

6 **If** $\mathcal{C}$ is of odd degree or α is of odd degree or if we can compute a rational point, **compute** a parametrization of $\mathcal{C}$ over $\mathbb{K}$

7 Profit!

Computing the standard parametrization of $\mathcal{U}$

- If we use the definition to compute $\mathcal{U}$, the computation is not polynomially bounded in $n = [\mathbb{K}(\alpha) : \mathbb{K}]$.

- We have an algorithm that computes the standard parametrization of $\mathcal{U}$ in $\mathcal{O}(md^5n^8)$ operations in $\mathbb{K}$, m is the ambient dimension $d = deg(\mathcal{C})$, $n = [\mathbb{K}(\alpha) : \mathbb{K}]$.

- This algorithm makes use of conjugate parametrizations of $\mathcal{C}$.

- Write $\alpha = \alpha_0, \alpha_1, \ldots, \alpha_{n-1}$ the conjugates of α over $\mathbb{F}$. Let σ_i and $\mathbb{K}$-automorphism of $\mathbb{F}$ such that $\sigma_i(\alpha) = \alpha_i$.

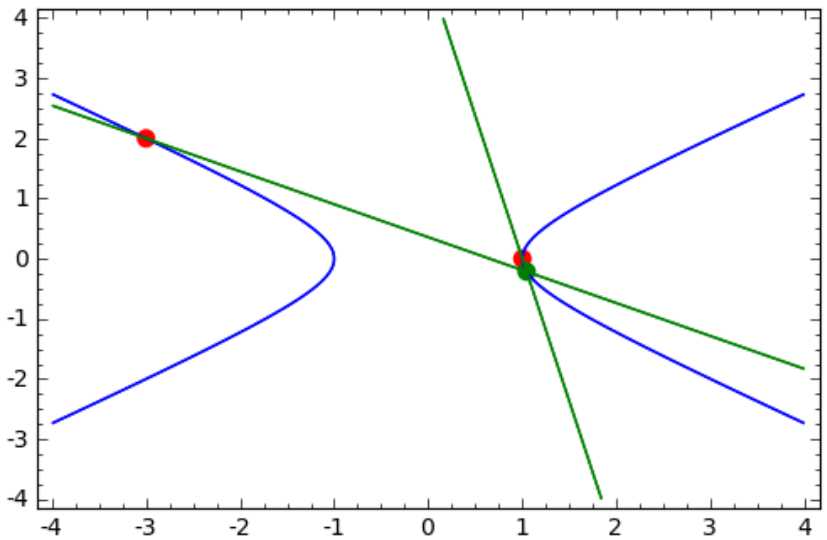
- if $f \in \mathbb{K}(\alpha)(t)$, we write $f^{\sigma_i} \in \mathbb{K}(\alpha_i)(t)$ the conjugate rational function obtained by applying σ_i to the coefficients of σ.

Conjugate parametrizations

- Assume that $\mathcal{C}$ is defined over $\mathbb{K}$. The pencil of hyperplanes $\mathcal{L}_i(t) = \{x_0 + \alpha_i x_1 \dots \alpha_i^{n-1} x_{n-1} = t\}$ parametrizes $\mathcal{U}$ over $\mathbb{K}(\alpha_i)(t)$.

Theorem[Harris 92] The rational normal curve define a birational morphism $u_i(t)$ between $\mathcal{L}_0(t)$ and $\mathcal{L}_i(t)$ given by

$$\mathcal{L}_0(t) \cap \mathcal{U} = \mathcal{L}_i(u(t)) \cap \mathcal{U}$$



recovering the parametrization from the morphisms u_i

- If we know the isomorphisms u_i we can recover the standard parametrization of $\mathcal{U}$. The standard parametrization is the unique solution to the system of equations.

$$\begin{pmatrix} 1 & \alpha & \dots & \alpha^{d-1} \\ 1 & \alpha_2 & \dots & \alpha_2^{d-1} \\ & & \dots & \\ 1 & \alpha_n & \dots & \alpha_n^{d-1} \end{pmatrix} \begin{pmatrix} \phi_0 \\ \phi_1 \\ \dots \\ \phi_{n-1} \end{pmatrix} = \begin{pmatrix} u_0(t) = t \\ u_1(t) \\ \dots \\ u_{n-1}(t) \end{pmatrix}$$

Computing the isomorphisms u_i

Theorem If ψ is the starting parametrization and ψ^{σ_i} is a conjugate parametrization then $u_i = (\psi^{\sigma_i})^{-1} \circ \psi$.

- We can compute u_i by interpolation, resolving s_k in the equality $\psi(t_k) = \psi^{\sigma_i}(s_k)$ for three given t_k allows us to recover u.

- Computing s_k is a univariate gcd over $\mathbb{K}(\alpha, \alpha_i)$.

- There are at most $d^2 - d - n + 1$ parameters where the above gcd may fail.

Check $\mathbb{K}$-definability

- In practice, the computation of u_i detects if the curve is not $\mathbb{K}$-definable with high probability. If we want a certificate...

Theorem $\mathcal{C}$ is $\mathbb{K}$-definable if and only if $\psi(t) = \psi^{\sigma_i}(u_i(t))$, $0 \leq i \leq n-1$, for the u_i computed by interpolation.

Solving the Vandermonde System

$$\begin{pmatrix} 1 & \alpha & \dots & \alpha^{d-1} \\ 1 & \alpha_2 & \dots & \alpha_2^{d-1} \\ & & \dots & \\ 1 & \alpha_n & \dots & \alpha_n^{d-1} \end{pmatrix} \begin{pmatrix} \phi_0 \\ \phi_1 \\ \dots \\ \phi_{n-1} \end{pmatrix} = \begin{pmatrix} u_0(t) = t \\ u_1(t) \\ \dots \\ u_{n-1}(t) \end{pmatrix}$$

- The problem of this system is that we have to work in the normal closure of $\mathbb{K}(\alpha)$ that has degree $n!$ in the generic case.

- Note that we are trying to solve an interpolation problem. We are looking for an $F(x) \in \mathbb{K}(\alpha)(t)[x]$ such that $F(\alpha_i) = u_i(t)$.

- If α_i and α_j are conjugate over $\mathbb{K}(\alpha)$ and τ is a $\mathbb{K}(\alpha)$-automorphism of $\mathbb{F}$ such that $\tau(\alpha_i) = \alpha_j$ then $\tau(u_i)(t) = u_j(t)$.

Lagrange interpolation

$$F(x) = \sum_{i=0}^{n-1} \frac{(x-\alpha_0)\dots(x-\alpha_{i-1})(x-\alpha_{i+1})\dots(x-\alpha_{n+1})}{(\alpha_i-\alpha_0)\dots(\alpha_i-\alpha_{i-1})(\alpha_i-\alpha_{i+1})\dots(\alpha_i-\alpha_{n-1})} u_i(t)$$

- If $M(x)$ is the minimal polynomial of α over $\mathbb{K}$ and $m(\alpha, x) = M(x)/(x-\alpha)$ then the numerator of a summand of F is $m(\alpha_i, x) \cdot num(u_i)$ and the denominator is $m(\alpha_i, \alpha_i) \cdot den(u_i)$.

- Let $S = \{\alpha_{i_1}, \dots, \alpha_{i_k}\}$ be a system of representatives of the sets of conjugate roots of $M(x)$ over $\mathbb{K}(\alpha)$ we get

$$F = \sum_{j=i}^{k} trace\left(\frac{m(\alpha_{i_k}, x)}{m(\alpha_{i_k}, \alpha_{i_k})} u_{i_k}(t)\right)$$

where the trace is computed for the extension $\mathbb{K}(\alpha, t) \subseteq \mathbb{K}(\alpha, \alpha_{i_k}, t)$. This trace can be computed knowing the minimal polynomial of the pole of u_{i_k} and Newton sums.

Solving the Vandermonde system

$$F = \sum_{j=i}^{k} trace\left(\frac{m(\alpha_{i_k}, x)}{m(\alpha_{i_k}, \alpha_{i_k})} u_{i_k}(t)\right)$$

- F can be computed making computations in at most $n-1$ fields of the form $\mathbb{K}(\alpha, \alpha_i)$ of degree at most $n^2 - n$, avoiding $n!$ splitting field.

- Once we know $F = \phi_0 + x\phi_1 + \ldots + x^{n-1}\phi_{n-1}$ the standard parametrization is $(\phi_0, \ldots, \phi_{n-1})$.

- *(Sendra, Villarino, 2002)* proposed an alternative algorithm to compute $\mathcal{U}$. In theory the algorithm explained here is better than theirs if $n << d$ and theirs is better if $n >> d$. Experimentation suggest that the method presented here is better in many cases.

Getting your hands dirty. A full example

- There is a lot of room for improvement in the case $\mathbb{K} = \mathbb{Q}$.