An application of elimination theory is the implicitization problem:

parametric description of variety $\rightsquigarrow$ defining polynomials

Example 8.14

Consider a curve (the twisted cubic)

$$V = \{(t, t^2, t^3) : t \in \mathbb{R}\} \subset \mathbb{R}^3$$

In this case an implicit description is easy to find:

$$V = V(y - x^2, z - x^3)$$

For a more complicated example, consider the surface W of all tangent lines to V:

At (t, t^2, t^3), the derivative in t is $(1, 2t, 3t^2)$

so the tangent line (parametrically) is given by

$$s \longmapsto (t+s, t^2+2ts, t^3+3t^2s)$$

Define

$$W = \{(t+s, t^2+2ts, t^3+3t^2s) : t, s \in \mathbb{R}\} \subset \mathbb{R}^3$$

and consider $p_1, p_2, p_3 \in \mathbb{R}[t, s, x, y, z]$:

$$p_1 = t + s - x$$

$$p_2 = t^2 + 2ts - y$$

$$p_3 = t^3 + 3t^2 s - z$$

Computing a Grobner basis for $I = \langle p_1, p_2, p_3 \rangle$ in the lex order, we find

$$g_1 = t + s - x$$
$$g_2 = s^2 - x^2 + y$$
$$g_3 = (x^2 - y)s + r_3$$
$$g_4 = (xy - z)s + r_4$$
$$g_5 = (xz - y^2)s + r_5$$
$$g_6 = (y^3 - z^2)s + r_6$$
$$g_7 = x^3 z - \frac{3}{4}x^2y^2 - \frac{3}{2}xyz + y^3 + \frac{1}{4}z^2$$

where $r_3, \ldots, r_6 \in \mathbb{R}[x, y, z]$

Hence

$$I_2 = I \cap \mathbb{R}[x, y, z]$$
$$= \langle x^3 z - \frac{3}{4}x^2y^2 - \frac{3}{2}xyz + y^3 + \frac{1}{4}z^2 \rangle$$

So at least $W = \pi_2(V(p_1, p_2, p_3)) \subset V(I_2)$.

Using the Extension Theorem we can test for "$\supset$":

Extension Theorem for $\mathbb{C}[s, x, y, z]$:

$g_2 = s^2 + \ldots \Rightarrow c_2 = 1 \neq 0 \Rightarrow$ partial solutions extend

for $\mathbb{C}[t, s, x, y, z]$:

$g_1 = t + \ldots \Rightarrow c_1 = 1 \neq 0 \Rightarrow$ partial solutions extend

Hence at least over $\mathbb{C}$ we would have

$$W = V(g_7) \subset \mathbb{C}^3.$$

What about over $\mathbb{R}$?

By the Extension Theorem for $(a_3, a_4, a_5) \in \mathbb{R}^3 \subset \mathbb{C}^3$ $\exists a_1, a_2 \in \mathbb{C}$ such that $(a_1, a_2, a_3, a_4, a_5) \in V(I)$, so

$$p_1 = t+s-x = 0 \quad \Rightarrow \quad a_1 + a_2 = a_3 \in \mathbb{R}$$
$$p_2 = t^2+2ts-y=0 \quad \Rightarrow \quad a_1^2 + 2a_1a_2 = a_4 \in \mathbb{R}$$
$$p_3 = t^3+3t^2s-z=0 \quad \Rightarrow \quad a_1^3 + 3a_1^2a_2 = a_5 \in \mathbb{R}.$$

Solving the polynomial system

$$\operatorname{Im}(a_1+a_2) = \operatorname{Im}(a_1^2+2a_1a_2) = \operatorname{Im}(a_1^3+3a_1^2a_2) = 0$$

we find

$$\operatorname{Im}(a_1) = \operatorname{Im}(a_2) = 0 \quad \Rightarrow \quad a_1, a_2 \in \mathbb{R}$$

(in fact a Gröbner basis in lex with variable order $\operatorname{Re}(a_1) > \operatorname{Re}(a_2) > \operatorname{Im}(a_1) > \operatorname{Im}(a_2)$ is

$$\operatorname{Re}(a_2)\cdot\operatorname{Im}(a_2), \quad \operatorname{Im}(a_1)+\operatorname{Im}(a_2), \quad \operatorname{Im}(a_2)^3 \text{)}$$

Hence $W = V(g_7)$ also over $\mathbb{R}$.

<u>Theorem 8.15</u> (Polynomial Implicitization)

Let K be an infinite field.

Let $P: K^m \to K^n$ be a polynomial mapping

i.e. $P = (p_1, \dots, p_n)$ with each $p_i \in K[t_1, \dots, t_m]$

Let $I = \langle x_1 - p_1, \dots, x_n - p_n \rangle \subset K[t_1, \dots, t_m, x_1, \dots, x_n]$

Let $I_m = I \cap K[x_1, \dots, x_n]$ be the m-th elimination ideal.

Then $V(I_m) \subset K^n$ is the smallest variety containing $P(K^m)$.

<u>Proof</u>

Consider the commutative diagram

$$\begin{tikzcd} & K^{m+n} \arrow[dr, "\pi_m"] & \\ K^m \arrow[ur, "\iota"] \arrow[rr, "P"] & & K^n \end{tikzcd}$$

where $\iota(t_1, \dots, t_m) = (t_1, \dots, t_m, p_1(t_1, \dots, t_m), \dots, p_n(t_1, \dots, t_m))$

Let $V = V(I) = \iota(K^m)$

$= \{(t_1, \dots, t_m, p_1(t_1, \dots, t_m), \dots, p_n(t_1, \dots, t_m)) : t_1, \dots, t_m \in K\}$

"$=$ graph of $P: K^m \to K^n$"

Lemma 8.10 $\Rightarrow$ $P(K^m) = \pi_m(V) \subset V(I_m)$

To show $V(I_m)$ is the smallest,

let $h \in K[x_1, \dots, x_n]$ be such that $h(a) = 0$ $\forall a \in P(K^m)$.

We need to show that $h \in I_m$.

Consider $h \in K[x_1, \dots, x_n]$ as $h \in K[x_1, \dots, x_n, t_1, \dots, t_m]$ with lex order (note reversal $x > t$!)

Polynomial division of h by $(x_1 - p_1, \dots, x_n - p_n)$ gives

$$h = q_1(x_1 - p_1) + \dots + q_n(x_n - p_n) + r, \quad q_j \in K[x_1, \dots, x_n, t_1, \dots, t_m]$$

where no term of r divisible by $x_1, \dots, x_n$

$\Rightarrow r \in K[t_1, \dots, t_m]$.

Let $a \in P(K^m)$ so $a = (p_1(b), \dots, p_n(b))$, $b \in K^m$.

Then

$$0 = h(a) = h(a,b) = q_1(a,b)(a_1 - p_1(b)) + \dots$$
$$+ q_n(a,b)(a_n - p_n(b)) + r(b)$$
$$= 0 + \dots + 0 + r(b)$$

$\Rightarrow r(b) = 0 \quad \forall b \in K^m$.

Since K is infinite, we obtain $r = 0$ and thus $h \in I \cap K[x_1, \dots, x_n] = I_m$. $\square$

Theorem 8.15 $\Rightarrow$ Implicitization algorithm:

Given a polynomial mapping $P: K^m \to K^n$.

1) Define the ideal
$$I = \langle x_i - p_i, i = 1, \dots, n \rangle \subset K[t_1, \dots, t_m, x_1, \dots, x_n]$$
2) Compute a lex Gröbner basis G.
3) The variety $V(G \cap K[x_1, \dots, x_n])$ is the smallest variety containing $P(K^m)$.

Example 8.16

Consider the rational mapping

$R : (u,v) \longmapsto (x,y,z)$

$$x = \frac{u^2}{v}, \quad y = \frac{v^2}{u}, \quad z = u$$

(defined when $u \neq 0$ and $v \neq 0$)

Trying to mimic polynomial implicitization, we could expand denominators and consider

$$I = \langle vx - u^2, uy - v^2, z - u \rangle \subset K[u,v,x,y,z]$$

Then $I_2 = I \cap K[x,y,z] = \langle x^2yz - z^4 \rangle$

so $V(I_2) = V((x^2y - z^3)z)$

$= V(x^2y - z^3) \cup V(z)$

However $R(u,v) \in V(x^2y - z^3)$ $\forall u,v$

so $V(I_2)$ is not the smallest variety containing the image of the parametrization.

The issue: R defined on $K^2 \setminus W$, $W = V(uv)$

so on the image $z = u \neq 0 \Rightarrow$ we can divide by z, but polynomial computations don't directly see this.

Solution: introduce a new variable "z^{-1}" and the polynomial relation $z \cdot z^{-1} = 1$

In greater generality:

Consider a rational mapping

$$R : (t_1, \dots, t_m) \mapsto (x_1, \dots, x_n)$$

$$x_i = \frac{p_i(t_1, \dots, t_m)}{q_i(t_1, \dots, t_m)}, \quad p_i, q_i \in K[t_1, \dots, t_m]$$

defined on $K^m \setminus W$, $W = V(q_1) \cup \dots \cup V(q_n) = V(q_1 \cdot \dots \cdot q_n)$

Denote $q := q_1 \cdot \dots \cdot q_n \in K[t_1, \dots, t_n]$

Analogously to polynomial mappings

we have the commutative diagram

$$\begin{tikzcd} & K^{m+n} \arrow[dr, "\pi_m"] & \\ K^m \setminus W \arrow[ur, "\iota"] \arrow[rr, "R"] & & K^n \end{tikzcd}$$

$\iota(t) = (t, R(t))$

Introduce an extra variable y "$= \frac{1}{q}$"

and consider $K[y, t_1, \dots, t_m, x_1, \dots, x_n]$ and the diagram

$$\begin{tikzcd} & K^{1+m+n} \arrow[dr, "\pi_{1+m}"] & \\ K^m \setminus W \arrow[ur, "j"] \arrow[rr, "R"] & & K^n \end{tikzcd}$$

$$j(t) = \left(\frac{1}{q(t)}, t, R(t)\right) = \left(\frac{1}{q(t)}, t_1, \dots, t_m, \frac{p_1(t)}{q_1(t)}, \dots, \frac{p_n(t)}{q_n(t)}\right)$$

<u>Theorem 8.17</u> (Rational implicitization)

Let K be an infinite field.

Let $R: K^m \setminus W \to K^n$ be a rational mapping $R_i = \frac{p_i}{q_i}$.

where $W = V(q)$, $q = q_1 \cdot \ldots \cdot q_n$. Let

$$J := \langle q_1 x_1 - p_1, \ldots, q_n x_n - p_n, qy - 1 \rangle$$
$$\subset K[y, t_1, \ldots, t_m, x_1, \ldots, x_n]$$

Let $J_{1+m} = J \cap K[x_1, \ldots, x_n]$ be the $(1+m)$-th elimination ideal.

Then $V(J_{1+m}) \subset K^n$ is the smallest variety containing $R(K^m \setminus W)$.

<u>Proof</u>

<u>$R(K^m \setminus W) \subset V(J_{1+m})$:</u>

Let $V = V(J) \subset K^{1+m+n}$

If $b \in K^m \setminus W$, then $j(b) = \Big(\overset{y}{\overset{\shortparallel}{\tfrac{1}{q(b)}}}, \overset{t}{\overset{\shortparallel}{b}}, \overset{x}{\overset{\shortparallel}{R(b)}}\Big) \in V$, since

$$q_\ell x_\ell - p_\ell \rightsquigarrow q_\ell(b) \cdot \frac{p_\ell(b)}{q_\ell(b)} - p_\ell(b) = 0 \quad \text{and}$$

$$qy - 1 \rightsquigarrow q(b) \cdot \frac{1}{q(b)} - 1 = 0.$$

Conversely, if $(\overset{y}{\overset{\shortparallel}{c}}, \overset{t}{\overset{\shortparallel}{b}}, \overset{x}{\overset{\shortparallel}{a}}) \in V$ then

$$qy - 1 = 0 \Rightarrow q(b) \cdot c - 1 = 0 \Rightarrow c = \frac{1}{q(b)} \neq 0$$

$$q_\ell x_\ell - p_\ell = 0 \Rightarrow q_\ell(b) \cdot a_\ell - p_\ell(b) = 0 \Rightarrow a_\ell = \frac{p_\ell(b)}{q_\ell(b)}$$

so $(c, b, a) = j(b) \in j(K^m \setminus W)$.

Hence $V(J) = j(K^m \setminus W)$ and from Lemma 8.10 we get

$$R(K^m \setminus W) \subset \pi_{1+m} \circ j(K^m \setminus W) = \pi_{1+m} V(J) \subset V(J_{1+m})$$

$V(J_{1+n})$ is the smallest variety containing $R(k^n \setminus W)$:

Let $h \in k[x_1, \dots, x_n]$ be such that $h(R(k^n \setminus W)) = 0$
We need to show that $h \in J_{1+n}$.

Let $h = \sum_\alpha c_\alpha x^\alpha$, $c_\alpha \in k$ and consider the polynomial

$$h(q_1 \cdot x_1, \dots, q_n \cdot x_n) = \sum_\alpha c_\alpha q_1^{\alpha_1} \cdot \dots \cdot q_n^{\alpha_n} x^\alpha$$
$$\in k[x_1, \dots, x_n, t_1, \dots, t_m]$$

Let $N = \max\{\alpha_i : 1 \le i \le n, c_\alpha \ne 0\}$.
Then

$$q^N h = \sum_\alpha c_\alpha q_1^N \cdots q_n^N x^\alpha$$
$$= \sum_\alpha c_\alpha q_1^{N-\alpha_1} \cdots q_n^{N-\alpha_n} (q_1 x_1)^{\alpha_1} \cdot \dots \cdot (q_n x_n)^{\alpha_n}$$
$$= F(q_1 x_1, \dots, q_n x_n, t_1, \dots, t_m)$$

for some polynomial $F(x_1, \dots, x_n, t_1, \dots, t_m)$
Dividing F by $(x_1 - p_1, \dots, x_n - p_n)$ we get
$$F = f_1 \cdot (x_1 - p_1) + \dots + f_n \cdot (x_n - p_n) + r$$
with $r \in k[t_1, \dots, t_m]$.
Hence
$$q^N h = f(q_1 x_1, \dots, q_n x_n, t_1, \dots, t_m)(q x_1 - p_1) + \dots + r$$

Then for $b \in k^m \setminus W$, evaluating at $(x,t) = (R(b), b)$ we get

$$r(b) = q^N(b) \cdot h(b) = 0$$

Since $k^m \setminus W$ is infinite we obtain $r = 0$.

$\Rightarrow q^N h \in J$

Finally, "divide by q", i.e. observe that

$$h = y^N \cdot q^N h + h \cdot (1 - q^N y^N)$$

$$= y^N \cdot \underbrace{q^N h}_{\in J} + h \cdot \underbrace{(1-qy)}_{\in J}(1 + qy + q^2y^2 + \dots + q^{N-1}y^{N-1})$$

$\Rightarrow h \in J \cap k[x_1, \dots, x_n]$ $\square$

In this setting,

"$f = q^{-1} \cdot q f$" is written as

$f = y \cdot qf + f \cdot (1 - qy)$ or

$f = y \cdot qf$ modulo $\langle 1 - qy \rangle$