Implicitization

Consider a polynomial map

$$f : k^m_z \longrightarrow k^n_x$$
$$p = (p_1, \dots, p_m) \longmapsto (f_1(p), \dots, f_n(p))$$

where $f_1, \dots, f_n \in k[z_1, \dots, z_m]$

$$im(f) = f(k^m) \subseteq k^n$$

↑ this need not be a variety

We seek to compute $\overline{im(f)} \subseteq k^n$

$$f : k^2 \longrightarrow k^3$$
$$(z_1, z_2) \longmapsto (z_1, z_1 z_2, z_1 z_2^2)$$

$V = \overline{im(f)} = V(x_1 x_3 - x_2^2)$

but $(0,0,1) \in V$ but $z_1 = 0 \Rightarrow z_1 z_2^2 = 0 \neq 1$

$\therefore (0,0,1) \notin im(f)$

But if $k = \mathbb{C}$, take $z_1 = \varepsilon^2$, $z_2 = \frac{1}{\varepsilon}$

then $(z_1, z_1 z_2, z_1 z_2^2) = (\varepsilon^2, \varepsilon, 1)$

$$\lim_{\varepsilon \to 0} (\varepsilon^2, \varepsilon, 1) = (0,0,1)$$

To compute $\overline{im(f)}$ we will work with graph

Suppose $f : k^m_z \longrightarrow k^n_x$

$z \longmapsto (f_1(z), \ldots, f_n(z))$

The graph is

$$\mathrm{im}(\mathrm{graph}(f)) \subseteq k^m_z \times k^n_x$$

$$\mathrm{graph}(f) : k^m \longrightarrow k^m \times k^n$$

$$z \longmapsto (z, f(z))$$

Idea $I = (x_1 - f_1(z), \ldots, x_n - f_n(z))$

$$\mathrm{im}(\mathrm{graph}(f)) = \overline{\mathrm{im}(\mathrm{graph}(f))} = V(I) \subseteq k^m \times k^n$$

to see that $\mathrm{im}(\mathrm{graph}(f)) = V(I)$ note

$\gamma = \mathrm{im}(\mathrm{graph}(f)) \subseteq V(I)$

Since if $(z, x) \in \gamma$

then $(z, x) = (z, f(z))$

sub in

$x_i - f_i(z) = f_i(z) - f_i(z) = 0 \quad \therefore (z, x) \in V(I)$

Conversely if $(z, x) \in V(I)$

$\Rightarrow \quad x_i - f_i(z) = 0 \quad \forall i$

$\Rightarrow \quad x_i = f_i(z)$

$\Rightarrow \quad (z, x) = (z, f(z)) \in \gamma$

Cor | Given a map $f : k_z^m \to k_x^n$, $z \mapsto (f_1(z), \ldots, f_n(z))$

Let $I = (x_1 - f_1(z), \ldots, x_n - f_n(z)) \subseteq k[z_1, \ldots, z_m, x_1, \ldots, x_n]$ and $J = I \cap k[x_1, \ldots, x_n]$

$$\overline{\operatorname{im}(f)} = V(J) = \overline{\pi(\operatorname{im}(\operatorname{graph}(f)))}$$

Similarily if $X = V(I_X) \subseteq k^m$ then

$$\overline{\operatorname{im}(f)}\big|_X = \overline{f(X)} = V(W) \text{ where } W = (I + I_X) \cap k[x_1, \ldots, x_n].$$

This follows directly from elimination theorem and fact that $\operatorname{im}(\operatorname{graph}(f))$ is closed.

Computing intersections of ideals

Thm | Given ideals I, J in $k[x_1, \ldots, x_n]$

$$I \cap J = \underbrace{(t \cdot I + (1-t)J)}_{\in k[x_1, \ldots, x_n, t]} \cap k[x_1, \ldots, x_n]$$

Proof | Let $f \in I \cap J \Rightarrow f \in I, f \in J$

$\therefore$ the expression $tf(x) + (1-t)f(x)$ occurs in $(t \cdot I + (1-t) \cdot J)$

and $tf + (1-t)f = tf + f - tf = f \in k[x_1, \ldots, x_n]$

$\therefore f \in (tI + (1-t)J) \cap k[x_1, \ldots, x_n].$

Let $f \in (tI + (1-t)J) \cap k[x_1, \dots, x_n]$

$\Rightarrow \exists \quad h(x) \in I$ and $g(x) \in J$

s.t. $f(x) = t\,h(x) + (1-t)g(x)$

$= t(h(x) - g(x)) + g(x)$

$f(x) - g(x) = t(h(x) - g(x))$

$\Rightarrow f(x) = g(x) = h(x) \Rightarrow f(x) \in I, f \in J$

$f \in I \cap J$. ■

<u>Thm (Tarski-Seidenberg)</u> Consider a poly map

$f : \mathbb{R}_z^m \longrightarrow \mathbb{R}_x^n$

$p \longmapsto (f_1(p), \dots, f_n(p))$ and let $I \subseteq k[z_1, \dots, z_m]$ an ideal

Then $f(V(I))$ is a semi-algebraic set

a set given by poly equalities and inequalities (in $k[x_1, \dots, x_n]$)

<u>Thm (Chevalley)</u> If k is algebraically closed

$f : k^m \to k^n$

$z \mapsto (f_1(z), \dots, f_n(z))$, and $V \subseteq k^m$ a subvariety

then $f(k^m)$ is a constructable set

Poly. eqs and inequations in $k[x_1, \dots, x_n]$.

<u>Thm</u> | Let $X \subseteq \mathbb{P}_z^m$ be a projective variety over an algebraically closed field. If $f : X \to \mathbb{P}^n$

$z \longmapsto (f_1(z), \dots, f_n(z))$

and $V(f_1, \ldots, f_n) \cap X = \phi$ (suppose $\deg(f_i) = \deg(f_j)$ $\forall\, i,j$)

then $f(x) = \overline{f(x)}$

Nullstellensatz

Fix an alg. closed field k. Note if $1 \in I$ then 1 is the reduced G.B. of I.

Thm (weak Nullstellensatz) If $I \subseteq k[x_1, \ldots, x_n]$ is an ideal then $V(I) \neq \phi$ iff $1 \notin I$. (eq. $V(I) = \phi$ iff $1 \in I$).

Proof If $1 \in I$ clearly $V(I) = \phi$. Show that if $1 \notin I$ $\Rightarrow V(I) \neq \phi$.

Suppose $1 \notin I$. Proceed by induction on n. Since $k[x_1]$ is a PID and $1 \notin I \Rightarrow I = \langle g(x) \rangle$, $g(x) \neq c \in k$

$\therefore$ by Fund. Thm. of Alg. $g(x)$ has a root.

$\therefore V(I) \neq \phi$.

Now $n \geq 2$. For any $a \in k$ write $I_{x_n = a} \subseteq k[x_1, \ldots, x_{n-1}]$ for the ideal obtained by setting $x_n = a$ in I

Claim: $\exists\, a \in k$ s.t. $1 \notin I_{x_n = a}$.

If this holds $\Rightarrow$ By induction $\exists\, (a_1, \ldots, a_{n-1}) \in V(I_{x_n = a})$

$\Rightarrow (a_1, \ldots, a_{n-1}, a) \in V(I)$.

Proof of claim:

Consider the elimination ideal $I \cap k[x_n]$

Case 1 $I \cap k[x_n] \neq \{0\}$

Since $1 \notin I$ and $I \cap k[x_n] \neq \{0\}$ then

$$I \cap k[x_n] = \langle f(x_n) \rangle$$

where $\quad f(x_n) = \prod_{i=1}^{r} (x_n - b_i)^{m_i}$

If $1 \notin I_{x_n = b_i}$ for some i then we have the claim.

Suppose $1 \in I_{x_n = b_i} \ \forall i$

$\therefore \exists \quad B_1, \dots, B_r \in I \quad$ s.t. $\quad B_i(x_1, \dots, x_{n-1}, b_i) = 1 \quad \forall i$

$$\Rightarrow \quad B_i \equiv 1 \mod \langle x_n - b_i \rangle$$

$$\Rightarrow \quad B_i - 1 \in \langle x_n - b_i \rangle$$

$$\Rightarrow \quad \prod (B_i - 1)^{m_i} \in \langle f \rangle$$

$f \in I$ (since $f \in I \cap k[x_n]$) and $B_i \in I$

$\therefore$

$$0 \equiv \underbrace{\prod (B_i - 1)^{m_i}}_{\in \langle f \rangle \subseteq I} \mod I$$

$$\equiv \prod (-1)^{m_i} \mod I \quad \text{since } B_i \in I$$

$$\equiv \pm 1 \mod I \quad \Rightarrow \quad 1 \in I$$

But this contradicts $1 \notin I$.

$\Rightarrow \quad 1 \notin I_{x_n = b_i}$ for some i.

Case 2 | $I \cap k[x_n] = \{0\}$. Let $\{g_1, \dots, g_t\}$ be a Grobner basis for I w.r.t lex $x_1 > \dots > x_n$

write $g_i = c_i(x_n)\, x_1^{\alpha_1^{(i)}} \cdots x_{n-1}^{\alpha_{n-1}^{(i)}}$ + lower terms

Since k is an infinite field $\exists\, a \in k$ s.t. $c_i(a) \neq 0$ $\forall i$

Since $x_1 > \cdots > x_n$ and $c_i(a) \neq 0$ $\forall i$

$\Rightarrow$ $\overline{g_i} = g_i(x_1, \ldots, x_{n-1}, a)$ is a G.B. for $I_{x_n = a}$

and $in_<(I_{x_n=a}) = \langle x_1^{\alpha_1^{(i)}} \cdots x_{n-1}^{\alpha_{n-1}^{(i)}} \mid i = 1, \ldots, r \rangle$

Since $I \cap k[x_n] = \{0\}$ none of $g_i \in k[x_n]$

$\therefore$ no monomial in $in_<(I_{x_n=a})$ is $= 1$

$\therefore$ $1 \notin I_{x_n=a}$ since 1 is the reduced G.B. for $(1) \subseteq k[x_1, \ldots, x_n]$

Thm | (Hilbert's Nullstellensatz)

For any ideal $I \subseteq k[x_1, \ldots, x_n]$ with k alg. closed we have

$$I(V(I)) = \sqrt{I}$$

Proof | Since $f^m(a) = 0 \Rightarrow f(a) = 0$ $\forall a \in k^n$

$$\Rightarrow \quad \sqrt{I} \subseteq I(V(I))$$

Now show $I(V(I)) \subseteq \sqrt{I}$. Let $I = \langle f_1, \ldots, f_r \rangle$

and suppose $h \in I(V(I))$

Consider $J = \langle f_1, \dots, f_r, yh - 1 \rangle \subseteq k[x_1, \dots, x_n, y]$

$V(J) = \emptyset$ since if $a \in V(f_1, \dots, f_r) \Rightarrow h(a) = 0$

$\Rightarrow (yh-1)(a) = -1 \neq 0$

$\therefore$ By the weak Nullstellensatz, since $V(J) = \emptyset$

$\Rightarrow \exists \; g_1, \dots, g_r, v \in k[x_1, \dots, x_n, y]$ s.t.

$$\sum g_i f_i + v(x,y)\underbrace{(y\,h(x) - 1)}_{=0} = 1$$

Subbing $y = \frac{1}{h(x)}$ which gives $\frac{h(x)}{h(x)} - 1 = 1 - 1 = 0$

gives

$$\sum g_i\left(x, \frac{1}{h(x)}\right) \cdot f_i(x) = 1$$

clearing denominators gives

$$\sum p_i(x) \cdot f_i(x) = (h(x))^m$$

largest power of $h(x)$ in

$$\Rightarrow (h(x))^m \in I \Rightarrow h(x) \in \sqrt{I}$$

$$\therefore h \in I(V(I)) \Rightarrow h \in \sqrt{I}. \quad \blacksquare$$

<u>Cor</u> The map $V \mapsto I(V)$ defines a bijection between varieties in k^n and radical ideals in $k[x_1, \dots, x_n]$ (for k alg. closed)

i.e. Varieties in $k^n \longleftrightarrow$ radical ideals in $k[x_1, \dots, x_n]$

$$V \longmapsto I(V)$$
$$V(I) \longleftarrow\!\shortmid\; I$$

Cor | The map $V \mapsto I(V)$ gives a bijection between irreducible varieties in k^n and prime ideals in $k[x_1,\dots,x_n]$.

Real Nullstellensatz

Note the complex version does not work in $\mathbb{R}$

E.g. $I = \langle x^2+y^2+1 \rangle \subsetneq \mathbb{R}[x,y]$ but $V_{\mathbb{R}}(I) = \emptyset$

↑ Contradicts weak Nullstellensatz

$I = \langle x^2+y^2 \rangle \subsetneq \mathbb{R}[x,y]$, $V_{\mathbb{R}}(I) = \{(0,0)\}$

So $I(V_{\mathbb{R}}(I)) = \langle x,y \rangle \supsetneq \langle x^2+y^2 \rangle = I = \sqrt{I}$

Thm (Real weak Nullstellensatz) Let I be an ideal in $\mathbb{R}[x_1,\dots,x_n]$ s.t. $V_{\mathbb{R}}(I) = \emptyset$. Then -1 is a sum of squares of polys mod I. That is

$$1 + p_1^2 + \dots + p_r^2 \in I \quad \text{for some } p_1,\dots,p_r \in \mathbb{R}[x_1,\dots,x_n].$$

Thm (Artin's Theorem) If $f(x) \in \mathbb{R}[x_1,\dots,x_n]$ is non-negative on $\mathbb{R}^n$, i.e. $f(a) \geq 0 \ \forall a \in \mathbb{R}^n$, then there exists polynomial $p_1,\dots,p_r, q_1,\dots,q_r \in \mathbb{R}[x_1,\dots,x_n]$ s.t.

$$f = \left(\frac{p_1}{q_1}\right)^2 + \left(\frac{p_2}{q_2}\right)^2 + \cdots + \left(\frac{p_r}{q_r}\right)^2 .$$

Proof 1 Consider the poly $g = f(x)y^2 + 1 \in \mathbb{R}[x_1, \ldots, x_n, y]$

Since f is non-negative $V_{\mathbb{R}}(g) = \phi \subseteq \mathbb{R}^{n+1}$

By "Real weak Nullstellensatz" $\exists$ $p_1, \ldots, p_r \in \mathbb{R}[x, y]$

s.t. $1 + p_1^2 + \cdots + p_r^2 \in \langle g \rangle$

i.e. for some h

$$1 + p_1(x,y)^2 + \cdots + p_r(x,y)^2 + h(x,y)\, g(x,y) = 0$$

Now sub in $y = \frac{\pm 1}{\sqrt{-f(x)}}$ into, note $g\left(x, \frac{1}{\sqrt{-f}}\right) = \frac{-f}{f} + 1 = 0$

$$p_i\left(x, \frac{1}{\sqrt{-f}}\right) = \sum_{i=0}^{\deg_y p_i} c_i(x) \left(\frac{1}{\sqrt{-f}}\right)^i = c_0(x) + \frac{c_1(x)}{\sqrt{-f}} + \frac{c_2(x)}{-f} + \frac{c_3(x)}{(\sqrt{-f})^{3/2}} + \cdots$$

$$= a_i(x) + \frac{1}{\sqrt{-f}} b_i(x)$$

rational functions in $x_1, \ldots, x_n$

$$p_i\left(x, \frac{-1}{\sqrt{-f}}\right) = a_i(x) - \frac{b_i(x)}{\sqrt{-f}}$$

Hence we have if we sub $y = \frac{\pm 1}{\sqrt{-f}}$

in $1 + p_1^2 + \cdots + p_r^2 + hg = 0$

$$1 + \sum a_i(x)^2 - \frac{1}{f} \sum b_i(x)^2 \pm \frac{2}{\sqrt{-f}} \sum_{i=1}^{r} a_i b_i = 0$$

Now add exp. with $y = \frac{1}{\sqrt{-f}}$ to that with $y = \frac{-1}{\sqrt{-f}}$

$$\frac{1}{2}\left(\begin{array}{l} 1+\sum a_i(x)^2 - \frac{1}{f}\sum b_i(x)^2 + \cancel{\frac{2}{\sqrt{f}}\sum_{i=1}^{n}} a_i b_i = 0 \\ + \\ 1+\sum a_i(x)^2 - \frac{1}{f}\sum b_i(x)^2 - \cancel{\frac{2}{\sqrt{f}}\sum_{i=1}^{n}} a_i b_i = 0 \end{array}\right)$$

we get

$$1+\sum a_i(x)^2 - \frac{1}{f}\sum b_i(x)^2 = 0$$

or

$$f(x) = \frac{\sum b_i^2}{1+\sum a_i^2} = \frac{\left(\sum b_i^2\right)\left(1+\sum a_i^2\right)}{\left(1+\sum a_i^2\right)^2}$$

$$= \frac{\sum b_i^2}{\left(1+\sum a_i^2\right)^2} + \frac{\sum b_i^2 \cdot \sum a_i^2}{\left(1+\sum a_i^2\right)^2}$$

$\therefore$ f is a sum of rational squares

Ex) (Motzkin Poly) work in $\mathbb{R}[x,y]$

$$M(x,y) := x^4y^2 + x^2y^4 + 1 - 3x^2y^2$$

$$= \frac{x^4y^2(x^2+y^2-2)^2 + x^2y^4(x^2+y^2-2) + (x^2+y^2-2)^2 + (x^2-y^2)^2}{(x^2+y^2)^2}$$

$M(x,y)$ is a sum of 4 rational squares and is non-negative

However $M(x,y)$ is <u>Not</u> a sum of poly squares

Suppose $M(x,y) = \sum f_i^2$, $f_i \in \mathbb{R}[x,y]$

$(x + \text{stuff})^2 + ($

f_i cannot have monomials x, y, x^2, y^2 since x^2, y^2, x^4, y^4 are not in $M(x,y)$

Further x^d, y^d cannot be a monomial in f_i

$\therefore$ $f_i = \alpha_i + \beta_i xy + \hat{f}_i$ where $\hat{f}_i$ has degree ≥ 3

But M has no monomials of degree > 6

$\therefore$ $\hat{f}_i$ has monomials of degree 3 only

But x^2y^2 can arise only from f_i^2 by squaring $\beta_i xy$

$\Rightarrow$ coefficient of $x^2y^2 = \sum \beta_i^2 \neq -3$