LECTURE 17

4/11/2012

Note Title 4/10/2012

Today:

- Hilbert's Nullstellensatz
- Quantifier Elimination

φ

Hilbert's Nullstellensatz

- key ingredient in algebraic-geometry
- Viewing system of polynomials

$$f_1(x_1 \ldots x_n), \ \ldots \ f_m(x_1 \ldots x_n)$$

w/ constraints $(f_i = 0)$

Algebraic view: $I(f_1 \ldots f_m)$

Geometric view: $V(f_1 \ldots f_m) = \{(a_1 \ldots a_n) \mid f_j(\bar{a}) = 0 \ \forall j\}$

Ideal ↔ Variety Maps

- $\mathrm{Var}(I) = \{ \bar{a} \in \mathbb{K}^n \mid f(\bar{a}) = 0 \ \forall f \in I \}$
- $\mathrm{Ideal}(V) = \{ f \in \mathbb{K}[x_1..x_n] \mid f(\bar{a}) = 0 \ \forall \bar{a} \in V \}$

- If we keep taking Ideal(Var(Ideal(...))) do we converge?

- Clearly $\mathrm{Ideal}(\mathrm{Var}(I)) \supseteq I$

  Actually $\mathrm{Ideal}(\mathrm{Var}(I)) \supseteq \mathrm{Rad}(I)$

  $\mathrm{Rad}(I) = \{ f \mid \exists d \text{ s.t. } f^d \in I \}$

Claim: Rad(I) is an Ideal

Proof: Suffices to prove $f, g \in \mathrm{Rad}(I)$

$\Rightarrow f+g \in \mathrm{Rad}(I)$

Suppose $f^d, g^e \in I$

then $(f+g)^{d+e} \in I$ $\boxtimes$

Hilbert's (Strong) Nullstellensatz

Theorem: if $\mathbb{K}$ algebraically closed, then for all ideals I,

$$\text{Ideal}(\text{Variety}(I)) = \text{Rad}(I).$$

In particular, $\text{Ideal}(\text{Var}(\text{Rad}(I))) = \text{Rad}(I)$.

and so process converges.

Hilbert's Weak Nullstellensatz

Theorem: $\forall$ Ideals $I \subseteq \mathbb{K}[x_1 .. x_n]$, $\mathbb{K}$ algebraically closed,

$$\text{Var}(I) = \emptyset \iff 1 \in I$$

Strong HN $\Rightarrow$ Weak HN

- Wish to show

$$Var(I) = \phi \quad \& \quad Ideal(Var(I)) = Rad(I)$$

$$\Rightarrow 1 \in I$$

- Easy since $Ideal(Var(I)) = Ideal(\phi) \ni 1$

$$\Rightarrow 1 \in Rad(I) \Rightarrow 1^d \in I$$

$$\Rightarrow 1 \in I \quad \boxtimes$$

Weak HN $\Rightarrow$ Strong HN

Wish to show

$$\forall J \quad Var(J) = \phi \Rightarrow 1 \in J$$

$$\Rightarrow f \in Ideal(Var(I)) \Rightarrow \exists d \quad f^d \in I.$$

How should we create the ideal with empty variety?

- $I \subseteq \mathbb{K}[x_1 .. x_n]$
- $J \subseteq \mathbb{K}[x_1 .. x_n, y]$
- $J = \text{Ideal}(I, 1 - y \cdot f)$
- <u>Claim</u>: $\text{Var}(J) = \phi$

  $(a_1 ... a_n, b) \in \text{Var}(J)$

  $\Rightarrow f(a_1 .. a_n) = 0 \Rightarrow 1 - b \cdot 0 = 1 \neq 0$

  $\Rightarrow (1 - y \cdot f)(a_1 .. a_n, b) \neq 0$

- $1 \in J \Rightarrow \exists\, p \in \mathbb{K}[x_1 ... x_n, y],\ q \in I$

  s.t. $1 = p_0 (1 - y \cdot f) + q(x_1 .. x_n, y)$

  $$q = \sum_{i=0}^{d} y^i \cdot q_i(\bar{x}) \qquad q_i \in I$$

  [Rabinovich's] "trick" : $y = \dfrac{1}{f(x_1 .. x_n)}$

  $$\Rightarrow 1 = p_0 \left(1 - \frac{1}{f} \cdot f\right) + \sum_{i=0}^{d} \frac{1}{f^i} q_i(\bar{x})$$

$$\Rightarrow \quad f^d = \underbrace{\sum_{i=0}^{d} f^{d-i} \cdot q_i(x)}_{\in I\,!}$$

So ... Strong & weak H-N are equivalent. Will now prove weak H.N.

Key ingredient:

Extension Lemma:

Given $I \subseteq \mathbb{K}[x_1 \ldots x_n]$,

let $J = I \cap \mathbb{K}[x_1 \ldots x_{n-1}]$.

If $(a_1 \ldots a_{n-1}) \in \text{Variety}(J)$

$\exists\, a_n \in \mathbb{K}$ s.t. $(a_1 \ldots a_n) \in \text{Variety}(I)$

Proof of Weak H-N assuming Extension Lemma

Will show $1 \notin I \Rightarrow \exists (a_1 \dots a_n) \in Var(I)$

- Let $J = I \cap \mathbb{K}[x_1 \dots x_{n-1}]$
- $1 \notin I \Rightarrow 1 \notin J$
- By induction $\exists (a_1 \dots a_{n-1}) \in Var(J)$
- By Extension Lemma $\exists (a_1 \dots a_n) \in Var(I)$

$\boxtimes$

Proof of Extension Lemma

Special Case: $I = I(f_1, f_2)$

Let $R(x_1 \dots x_{n-1}) = \text{Resultant}_{x_n}(f_1, f_2)$

Recall $R \in I$

$\Rightarrow R \in J$

Since $(a_1 \dots a_{n-1}) \in \text{Variety}(J)$

we have $R(a_1 \dots a_{n-1}) = 0$

Now let $h_i(x_n) = f_i(a_1 \dots a_{n-1}, x_n)$

Recalling "determinantal defn." of resultant

we have

$$\text{Res}_{x_n}(h_1, h_2) = \text{Res}_{x_n}(f_1 f_2)\Big|_{a_1 \dots a_{n-1}} = R(a_1 \dots a_{n-1}) = 0$$

$\Rightarrow \exists\ g(x_n)$ s.t. $g(x_n) \mid h_1(x_n)$

$g(x_n) \mid h_2(x_n)$

Since $\mathbb{K}$ is algebraically closed

$\exists\ a_n$ s.t. $g(a_n) = 0$

$\Rightarrow f_1(a_1 \ldots a_n) = f_2(a_1 \ldots a_n) = 0$

$\boxtimes$ (Special Case)

General Case: By reduction to special case.

let $I = I(f_1 \ldots f_m) \subseteq \mathbb{K}[x_1 \ldots x_n]$

$J = I \cap \mathbb{K}[x_1 \ldots x_{n-1}]$; $(a_1 \ldots a_{n-1}) \in Var(J)$

Consider

$$\tilde{I} = I(f_1, F) \subseteq K[x_1 \ldots x_n, y_2 \ldots y_m]$$

where

$$F(x_1 \ldots x_n, y_2 \ldots y_m) = \sum_{i=2}^{m} f_i(\bar{x}) \cdot y_i$$

Let $R(x_1 \ldots x_{n-1}\ y_2 \ldots y_m) = \mathrm{Res}_{x_n}(f_1, F)$

Claim: $R(a_1 \ldots a_{n-1}, y_2 \ldots y_m) \equiv 0$

Proof: $\forall\ b_2 \ldots b_m \in \mathbb{K}$

$$R(x_1 \ldots x_{n-1}, b_2 \ldots b_m) \in \mathrm{Ideal}(f_1, F(x_1 \ldots x_n, b_2 \ldots b_m))$$

$$\in \mathrm{Ideal}(f_1 \ldots f_m) = I$$

$$\Rightarrow R(x_1 \ldots x_{n-1}, b_2 \ldots b_m) \in J$$

$$\Rightarrow R(a_1 \ldots a_{n-1}, b_2 \ldots b_m) = 0$$

$$\Rightarrow R(a_1 \ldots a_{n-1}, y_2 \ldots y_m) \equiv 0$$

$\boxtimes$ (Claim)

Now, viewing $f_1, F \in \mathbb{L}[x_1 \ldots x_n]$

where $\mathbb{L} = \overline{\mathbb{K}(y_2 \ldots y_m)}$ (algebraic closure of $\mathbb{K}(y_2 \ldots y_m)$)

we have

$f_1(a_1 \dots a_{n-1}, x_n)$ & $F(a_1 \dots a_{n-1}, x_n)$

share a common root $a_n \in \mathbb{L}$

But all roots of f_1 are in $\mathbb{K}$

So $a_n \in \mathbb{K}$

$(x_n - a_n) \mid f_1(a_1 \dots a_{n-1}, x_n)$

Δ $(x_n - a_n) \mid \sum y_i f_i (a_1 \dots a_{n-1}, x_n)$

$\Rightarrow$ $(x_n - a_n) \mid f_i(a_1 \dots a_{n-1}, x_n) \quad \forall i$

$(a_1 \dots a_n) \in Var(I)$

$\boxtimes$

Comments on degree bounds

if $f_1 \ldots f_m$ have deg $\leq d$,

& $\exists\, q_1 \ldots q_m$ s.t. $1 = \sum f_i q_i$

then what is degree bound on q_i ?

[Hermann] : $\deg(q_i) \leq (mdn)^{2^{O(n)}}$

[Brownawell '87] : $\deg(q_i) \leq (md)^n$

using complex analysis

[Kollar '88] " using cohomology

[Dubé 92] " elementary commutative algebra

Quantifier Elimination

Example: [2nd Level]

$\forall\, x_1 \dots x_n\ \exists\, y_1 \dots y_n$ s.t.

$$\phi_1(x_1 \dots x_n\ y_1 \dots y_n) = 0$$
$$\phi_2(\qquad\qquad) = 0$$
$$\vdots$$
$$\phi_m(\quad \text{"} \qquad \text{"} \quad) = 0 \quad ?$$

Main Result of area

Such problems can also be solved ...
("efficiently")

Insight

Fix $x_1 \dots x_n$ to $\alpha_1 \dots \alpha_n$

- Now, we have standard HN.
- Can ask, if $q_1 \dots q_m$ exist
- can find them if they exist by solving big linear system.
- Entries of matrix are polynomials in $x_1 \dots x_n$.
- Solution exists if some determinants are non-zero & others are zero.
- Solution exists if some system of poly constraints always has a zero!
- But these are equations only in $x_1 \dots x_n$!
- We have eliminated one quantifier.

$\boxtimes$