LECTURE 16

4/9/2012

Note Title 4/9/2012

TODAY

1. Complexity of Ideal Membership
   - EXPSPACE hardness
   - Degree upper bounds.
2. Hilbert Nullstellensatz

I.A - EXPSPACE HARDNESS

① Known Hard Problem

CWEP: Commutative word equivalence Problem

Input:
- Σ, $|\Sigma| = n$
- Rules: $\alpha_i = \beta_i$ $\quad i = 1 \dots m$

  $\alpha_i, \beta_i \in \Sigma^*$
- (Implicit): $\sigma \tau = \tau \sigma$

  $\forall \sigma, \tau \in \Sigma$
- $\alpha, \beta \in \Sigma^*$

Task Determine if $\alpha = \beta$.

using commutativity & equivalence rules.

Reduction

- Let $\Sigma = \{\sigma_1 \cdots \sigma_n\}$

- $\#_i(w) = \#$ of occurrences of σ_i in w

- "$\alpha_j = \beta_j$" $\Longrightarrow$ $f_j(x_1 \ldots x_n)$

$$= \prod_{i=1}^{n} x_i^{\#_i(\alpha_j)} - \prod_{i=1}^{n} x_i^{\#_i(\beta_j)}$$

- $f(x_1 \ldots x_n) = \prod_{i=1}^{n} x_i^{\#_i(\alpha)} - \prod_{i=1}^{n} x_i^{\#_i(\beta)}$

Claim: $f \in \text{Ideal}(f_1 \ldots f_m)$

$\Longleftrightarrow$ "$\alpha = \beta$" $\Longleftarrow$ $\{\alpha_j = \beta_j\}_{j=1}^{m}$

Proof: Omitted.

$\boxtimes$

I.B : Degree Bounds

Recall: $f \in I(f_1 \dots f_m)$

$\Leftrightarrow \exists\, q_1 \dots q_m \in K[x_1 \dots x_n]$ s.t.

$$f = \sum f_i q_i$$

- To make bound "constructive" need upper bound on degree of $q_1 \dots q_m$.

[Assume $\deg(f, f_1, \dots f_m) \leq d$]

- Combined with polylog space algorithms for solving linear equations over field, we get complexity SPACE(POLYLOG(Degree Bound))

Two views of Ideal Membership

I. Linear equation over a ring

$\exists\ q_1 \dots q_m \in R = K[x_1 \dots x_n]$ s.t.

$$f = \sum f_i q_i$$

$\uparrow$

one big linear equation

II. Many linear equations over a field K

$\exists \{ q_{j,\alpha} \}$ $\begin{array}{l} j = 1 \dots m \\ \alpha \in (\mathbb{Z}^{\geq 0})^n \end{array}$ $\sum \alpha_i \leq D_n$ s.t.

$\forall \beta \in (\mathbb{Z}^{\geq 0})^n$, $\sum \beta_i \leq D_n + d$

$$f_\beta = \sum_i \sum_{\alpha \leq \beta} q_{i,\alpha} f_{i,\beta-\alpha}$$

(f_β, $f_{i,\beta}$, $q_{i,\alpha}$ denote coefficients of f, f_i, q_i)

Want to know: When does existence of solution to I $\Rightarrow$ existence of solution to II with parameter D_n.

Strategy:

- Build common generalized problem $\Pi(j)$.
- $\Pi(n) = \mathrm{I}$
- $\Pi(0) = \mathrm{II}$
- variable elimination:

$\Pi(j+1)$ has solution with m_{j+1} equations & degree D_{j+1}

$\Rightarrow \Pi(j)$ has solution with $m_j = \mathrm{poly}(m_{j+1}, D_{j+1})$ & $D_j = \mathrm{poly}(m_{j+1}, D_{j+1})$

$\Pi(j)$: j-variable linear system.

<u>Given</u>: f_β, $f_{i,\beta} \in K[x_1 \ldots x_j]$

$\exists\ q_{i,\alpha} \in K[x_1 \ldots x_j]$, $\sum d_i \leq D_j$

$$f_\beta = \sum_i \sum_{\alpha \leq \beta} f_{i,\alpha}\, q_{i,\beta-\alpha}\ ?$$

<u>Lemma</u>: $\Pi(j+1)$ instance with m equations of degree D has solution $\Rightarrow$ corresponding $\Pi(j+1)$ instance has solution with degree $\mathrm{poly}(m, D)$ & equations $\mathrm{poly}(m, D)$

Key supporting Lemma : (L1)

- Given linear system $Ax = b$,
  - $A \in R[z]^{m \times m}$, $b \in R[z]^m$

    $\max_{i,j} \{ \deg(A_{ij}), \deg(b_j) \} \leq D$
  - A has full rank minor with monic determinant.
- Then $Ax = b$ has solution $\Rightarrow$ it has a solution with $\deg(x_i) \leq \mathrm{poly}(m D)$.

Proof of L1

w.l.o.g.

$$A = \left[\begin{array}{c:c} \tilde{A} & B \\ \hdashline C & D \end{array}\right]$$

where $\tilde{A}$ is full rank & $\det(\tilde{A}) =$ monic.

Solution looks like

$$x = \left[\begin{array}{c} x_1 \\ \hdashline x_2 \end{array}\right] \qquad b = \begin{bmatrix} b_1 \\ b_2 \end{bmatrix}$$

Note, by rank, that (if solution exists)

$$\begin{bmatrix} \tilde{A} & B \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} b_1 \end{bmatrix}$$

$$\Rightarrow \begin{bmatrix} C & D \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} b_2 \end{bmatrix}$$

So, can ignore $\begin{bmatrix} C & D \end{bmatrix}$, $\begin{bmatrix} b_2 \end{bmatrix}$.

Want to show that w.l.o.g. $\deg\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$

$\leq$ small.

$$X_1 = \tilde{A}^{-1}(b_1 - Bx_2)$$

so $\deg(x_1) \leq \deg\Big(\operatorname{Adj}(A) + \deg b_1$

$+ \deg(B) + \deg(x_2)\Big)$

$$\left[\text{using } \tilde{A}^{-1} = \frac{\operatorname{Adj}(A)}{\det(A)}\right]$$

So suffices to show, can reduce $\deg(X_2)$.

Now use the fact

(X_1, x_2) solution $\Rightarrow$ so is

$$\left(x_1 + \operatorname{Adj}(\tilde{A}) B y_2,\ x_2 - \det(\tilde{A}) y_2\right)$$

So can reduce $\deg(x_2) \leq \deg(\det(\tilde{A}))$

$\leq mD$.

From above, follows that

$\deg(x_1) \leq O(mD)$ also. $\boxtimes$

How to use Lemma L1?

How to ensure $\det(\tilde{A})$ is monic?

Idea: Generic/Random invertible linear transform.

L2: Given $Ax = b$ with $A, b \in \mathbb{K}[x_1 \dots x_j]$

let T be an invertible affine transform

from $\mathbb{K}^j \to \mathbb{K}^j$,

then

1. x is solution to (A, b)

$\Longleftrightarrow$

$x(T)$ is solution to $(A(T), b(T))$;

& $\deg(x(T)) = \deg(x)$.

2. whp over choice of T

$\det(\tilde{A}(T))$ is monic in x_j

$\boxtimes$

Combining L1 & L2, we get proof of

[Hermann's] bound on $\deg q_1, \dots q_m$.