6.S897 Algebra and Computation April 9, 2012

The Complexity of the Ideal Membership Problem

Instructor: Madhu Sudan *Scribe: Jing Jian*

1 Overview

Today we will discuss the complexity of the ideal membership problem. We will show a lowerbound of EXPSPACE hardness via a reduction to the "commutative word problem." We will then prove a doubly-exponential via degree upperbounds by the Hilbert Nullstellensatz.

2 Formulation

As a reminder, the formulation of ideal membership problem we are using today is as follows: given $f_0, f_1, \ldots, f_m \in \mathbb{K}[x_1, \ldots, x_n]$, are there $q_1, \ldots, q_m \in \mathbb{K}[x_1, \ldots, x_n]$ such that $f_0 = \sum_{i=1}^m q_i f_i$?

3 CWEP: The Commutative Word Equivalence Problem

We show that Ideal Membership is EXPSPACE-Hard by reduction from the known EXPSACE-Complete commutative word equivalence problem. It is formulated as follows:

Definition 3.1. We have an alphabet $\Sigma, |\Sigma| = n$ along with the implicit equivalence rule

$$\sigma\tau = \tau\sigma, \forall \tau, \sigma \in \Sigma$$

and a set of equivalence rules

$$\alpha_i = \beta_i, i = 1, ...m....(*)$$

Given two strings α, β, we need to decide if $\alpha \equiv \beta$ in the setting.

Due to the implicit rule, we can freely permute the letters in a string so that in any string α_i appears before β_i and etc. Therefore what determines string α is the nubmer of occurences of the jth symbol for $j \in 1 \ldots n$. The relationship between the CWEP and the ideal membership problem becomes clear since the (*) equations can be seen as relations that generate an ideal.

3.1 Reduction

The reduction is as follows:

- Let $\Sigma = \sigma_1, \ldots, \sigma_n$

- Let

$$\alpha_i = \sigma_1^{i_1}\sigma_2^{i_2}...\sigma_n^{i_n}\beta_i = \sigma_1^{j_1}\sigma_2^{j_2}...\sigma_n^{j_n}$$

- $\alpha_i = \beta_i \implies (\sigma_1^{i_1} + \sigma_2^{i_2} + ... + \sigma_n^{i_n}) - (\sigma_1^{j_1} + \sigma_2^{j_2} + ... + \sigma_n^{j_n}) = 0$
- $f(x_1, \ldots, x_n) = (\sigma_1^{i_1} + ... + \sigma_n^{i_n}) - (\sigma_1^{j_1} + ... + \sigma_n^{j_n})$

Claim 3.2. *The polynomial f is in $Ideal(f_1, \ldots f_n)$ if and only if $\{\alpha_i = \beta_i\}_{j=1}^m$ implies $\alpha = \beta$.*

Proof. Omitted. □

4 Upper Bounds

To get EXPSPACE bounds on the problem, we need the following two things:

1. Linear systerm over K with m equations and n variables can be solved in space $(log(m+n)^{O(1)})$
2. Degree of q_i in solution only need to be doubly exponentially large in n: $deg(q_i) \leq D = (mnd)^{2^{O(n)}}$

Combining the above we can get complexity SPACE(polylog(degree bound)). We will not prove statement 1 since it can be obtained via standard methods. We will focus on statement 2.

4.1 Two Views On Ideal Membership

We can formulate the problem of ideal membership testing in two ways:

1. As *one* linear equation over ring. Namely, given

$$f, f_1...f_m \in R = \mathbb{K}[x_i...x_n]$$

   We want to know if there exist q_i such that

$$f = \sum f_i q_i, q_i \in R$$

   In a ring, this problem is hard, since we cannot do inversions like we could in a field.

2. However, we can also view it as *many* linear equations over a field $\mathbb{K}$.

   We are given vectors of coefficients $f_{\vec{\beta}}, f_{1,\vec{\beta}}, ..f_m \in \mathbb{K}[x_1 \ldots x_n]$, and we want to know if there exist $\{q_{j,\vec{\alpha}}\}_{\vec{\alpha}\in(\mathbb{Z}^{\geq 0})^n}^{j=1...m}$, $\sum \alpha_i \leq D_n$ such that $\forall \vec{\beta} \in (\mathbb{Z}^{\geq 0})^n, \sum \beta_i \leq D_n + d$ we have

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

We want to know when does the existance of a solution to 1 implies the the existance of solutions to 2 with parameter D_n.

4.2 Strategy

The strategy we wil use is to build a common generalized problem $\Pi(j)$ such that $\Pi(n)$ is equivalent to formulation 1 and $\Pi(0)$ is equivalent to formulation 2.

Π_j is a j-variable linear system formulated as follows:

Definition 4.1. Given $f_{\vec{\beta}}, f_{i,\vec{\beta}} \in \mathbb{K}[x_1 \dots x_n]$, does there exist $\{q_{i,\vec{\alpha}}\}, \sum_{\alpha_i \leq D_j}$ such that

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

With this general formulation, if we can find a way to eliminate variables, we can interpolate between the two views of ideal membership. If we can prove the following statement, we can prove the degree bound:

Lemma 4.2. $\Pi(j+1)$ *has a solution with degree* $\leq D_{j+1}$ *implies* $\Pi(j)$ *has a solution with degree* $\leq poly(d, D_j + 1, m)$.

5 Proof of The Variable-elimination Statement

We write the collection of linear equations as $A\vec{x} = \vec{b}$. Since we are interested in eliminating variable j, we see $\vec{x}, \vec{b}$ as elements of $\mathbb{K}[x_1, ...x_j][x_j] = R[z]$ where $\mathbb{K}[x_1, ...x_j] = R$. We need the following key supporting lemma:

Lemma 5.1. *Given* $A\vec{x} = \vec{b}$ *is a* $M \times M$ *linear system over* $R[z]$ *of degree* $\leq D$*, and* A *has full rank miner with monic determinant, then* $A\vec{x} = \vec{b}$ *has solution implies that it has a solution with* $deg(x_i) \leq poly(mD)$.

Proof. Without the loss of generality we write

$$A = \begin{bmatrix} \tilde{A} & B \\ C & D \end{bmatrix}$$

Where $\tilde{A}$ is full rank and $\det(\tilde{A})$ is monic. The solution looks like

$$x = \begin{bmatrix} x_i \\ x_2 \end{bmatrix},\ b = \begin{bmatrix} b_i \\ b_2 \end{bmatrix}$$

Note, by rank, that (if solution exists)

$$\begin{bmatrix} \tilde{A} & B \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} b_1 \end{bmatrix} \implies \begin{bmatrix} C & D \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} b_2 \end{bmatrix}$$

Therefore we can ignore $\begin{bmatrix} C & D \end{bmatrix}, \begin{bmatrix} b_2 \end{bmatrix}$. We want to show that WLOG $\deg(\begin{bmatrix} x_1 \\ x_2 \end{bmatrix})$ is small. In the case of x_1, we have

$$x_1 = \tilde{A}^{-1}(b_1 - Bx_2)$$

so $deg(x_i) \leq deg(Adj(A) + deg(b_i) + deg(B) + deg(x_2))$, due to the fact $\tilde{A}^{-1} = Adj(A)/det(A)$. So it suffices to show that we can reduce the degree of x_2.

Now we use the fact that $[x_i, x_2]$ has a solution implies $(x_1 + Adj(\tilde{A})By_2, x_2 - det(\tilde{A}y_2)$ also has a solution. Therefore we can reduce $deg(x_2) \leq deg(det(\tilde{A})) \leq mD$.

From above, it follows that $deg(x_i) \leq O(mD)$ also. □

To show that our original problem satisfies the above technical condition, we use a technique called Generic/Random invertible linear transform. It allows us to use Lemma 5.1 and to ensure $det(\tilde{A})$ is monic.

Lemma 5.2. *Given* $A\vec{x} = \vec{b}$ *with* $A, \vec{b}, \in \mathbb{K}[x_1, ...x_j]$*, let* $T : \mathbb{K}^j \to K^j$ *be an invertible affine transform. Then*

1. *x is a solution to $(A, \vec{b})$ iff and only if $\vec{x}(T)$ is a solution to $(A(T), \vec{b}(T))$; and $deg(\vec{x}(T)) = deg(\vec{x})$.*

2. *With high probability over choices of T, $det(\tilde{A}(T))$ is monic in x_j.*

Combining Lemma 5.1 and Lemma 5.2, we get proof of Hermann's bound on degrees of $q_1, \ldots, q_m$.