6.S897 Algebra and Computation April 27, 2015

Lecture 21

Lecturer: Madhu Sudan *Scribe: Pritish Kamath*

1 Introduction

In this lecture, we will see that the Ideal Membership problem is EXPSPACE-complete, which was shown by Mayr and Meyer [1]. Next, we will see weak and strong statements of the Hilbert's Nullstellensatz.

2 Ideal Membership

The ideal membership question is defined as follows,

Problem 1 (Ideal-Membership)**.** *Given polynomials* $f, f_1, \cdots, f_m \in \mathbb{K}[\mathbf{x}]$*, decide whether* $f \in \langle f_1, \cdots, f_m \rangle$*, or in other words, does there exist polynomials* $g_1, \cdots, g_m \in \mathbb{K}[\mathbf{x}]$ *such that,* $f = \sum_i f_i g_i$

It turns out (due to [1]) that Ideal-Membership is EXPSPACE-complete! This is contrast with Radical-Ideal-Membership that we saw in last lecture to be in PSPACE.

2.1 EXPSPACE-hardness of Ideal-Membership

We show that Ideal-Membership is EXPSPACE-hard by obtaining a reduction from Commutative Word Equivalence Problem (CWEP), which is known to be EXPSPACE-complete. It is formulated as follows:

Problem 2. *We have an alphabet* Σ *(assume* $|\Sigma| = n$*) along with an implicit equivalence rule,*

$$\forall\ \sigma, \tau \in \Sigma \quad : \quad \sigma\tau \equiv \tau\sigma$$

and a set of m *equivalence rules of the type,*

$$\alpha_i \equiv \beta_i \qquad \text{where } i \in [m] \text{ and } \alpha_i, \beta_i \in \Sigma^* \tag{1}$$

Given two strings $\alpha, \beta \in \Sigma^*$*, we need to decide if* $\alpha \equiv \beta$*.*

Informally, the problem is to start with the string $\alpha \in \Sigma^*$, and we can do a series of operations which include either swapping two consecutive symbols or substituting a substring α_i by β_i or vice-versa for some i. Due to commutativity, the order of the symbols in α don't matter, and thus α is completely determined by $\mathbf{d} = (d_1, \cdots, d_n)$, where the i-th symbol in Σ appears d_i times in α, that is, we can think of α as $\sigma_1^{d_1}\sigma_2^{d_2}\cdots\sigma_n^{d_n}$. The relationship between the CWEP and the ideal membership problem becomes clear once we interpret the substitution rules in Equation 1 as relations that generate an ideal.

Hard instance of Ideal-Membership

We get a reduction from CWEP as follows. Consider a CWEP instance, where α_i's (resp. β_i's) correspond to the vectors $\mathbf{d}_i$ (resp. $\mathbf{e}_i$'s), and α (resp. β) corresponds to the vector $\mathbf{d}$ (resp. $\mathbf{e}$).
Let the polynomials $f_1, \cdots, f_m$ be given by $f_i = \mathbf{x}^{\mathbf{d}_i} - \mathbf{x}^{\mathbf{e}_i}$ and let $f = \mathbf{x}^{\mathbf{d}} - \mathbf{x}^{\mathbf{e}}$. It is easy to see that $f \in \langle f_1, \cdots, f_m \rangle$ if and only if $\alpha \equiv \beta$ under the equivalence rules of $\alpha_i \equiv \beta_i$. And thus, we conclude that Ideal-Membership is EXPSPACE-hard.

2.2 EXPSPACE algorithm for Ideal-Membership

To show that Ideal-Membership is in EXPSPACE, we will prove the following theorem (originally due to Hermann [2]) as follows,

Theorem 1 (Degree bound in Ideal-Membership [2])**.** *Consider an instance of* Ideal-Membership *as defined in Problem 1. Suppose that* $\deg(f_i) \leq d$ *for all* i *and* $\deg(f) \leq d$*. Then for any* $f \in \langle f_1, \cdots, f_m \rangle$*, it is possible to write* $f = \sum_i g_i f_i$ *where* $\deg(g_i) \leq (md)^{2^{O(n)}}$*.*

Assuming the above theorem, it is easy to see that Ideal-Membership is in EXPSPACE. Namely, since we know that $\deg(g_i) \leq \deg(f) + (md)^{2^{O(n)}} \stackrel{\text{def}}{=} D$, we can set up $f = \sum_i g_i f_i$ as a linear system in $m \cdot \binom{n+D}{n}$ variables. In particular, if $f = \sum_\beta f^{[\beta]} \mathbf{x}^\beta$, and $f_i = \sum_\beta f_i^{[\beta]} \mathbf{x}^\beta$. We want to know if there exist $g_i = \sum_\alpha g_i^{[\alpha]} \mathbf{x}^\alpha$ such that the following is true,

$$\forall\ \beta \text{ s.t. } |\beta| \leq D + d \quad : \quad f_\beta = \sum_{i=1}^{m} \sum_{\alpha \preceq \beta} g_i^{[\alpha]} f_i^{[\beta - \alpha]}$$

This linear system can be solved in EXPSPACE. Note that we cannot do this by explicitly computing the entries because the linear system is doubly-exponentially large in n. However, we can still solve the system in EXPSPACE, by only implicitly dealing with the values involved in the linear system.

If we were allowed to formulate linear equations over a ring, instead of a field, then we can expressed the ideal membership as a single linear equation over the ring $R = \mathbb{K}[\mathbf{x}]$, namely,

$$f = \sum g_i f_i \text{ where } g_i \in R$$

However, in a ring, this problem is hard since we cannot do inversions like we could in a field. We wish to bridge the gap between the two views, namely the *huge* linear system over $\mathbb{K}$ and the single linear equation over $R = \mathbb{K}[\mathbf{x}]$. We will do this by a hybrid-type inductive argument over the number of variables n.

Define $\Pi(j)$ to be the problem obtained by looking at f, f_i's and g_i's as polynomials in $R_j[x_{j+1}, \cdots, x_n]$, where $R_j = (\mathbb{K}[x_1, \cdots, x_j])$. Note that $\Pi(n)$ is the single linear equation over $R_n = \mathbb{K}[\mathbf{x}]$, whereas $\Pi(0)$ is the original linear system over $\mathbb{K}$.

Our inductive claim is: If $\Pi(j+1)$ has M equations with each variable of degree D then, $\Pi(j)$ has $\text{poly}(M, D)$ equations with constants of degree $\text{poly}(M, D)$. To this end, we prove the following lemma,

Lemma 2. *Suppose* $A\mathbf{x} = \mathbf{b}$ *is a* $M \times M$ *linear system, where the entries in* A *and* $\mathbf{b}$ *are univariate polynomials in* $R[z]$*, and each entry in* A *has degree* $\leq D$*, and* A *has full rank minor with monic determinant*[1]*. Then if* $A\mathbf{x} = \mathbf{b}$ *has a solution, then it has a solution* $\mathbf{x}$ *where for all* i*,* $\deg(x_i) \leq \text{poly}(MD)$*.*

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. Suppose the solution looks like

$$\mathbf{x} = \begin{bmatrix} \mathbf{x}_1 \\ \mathbf{x}_2 \end{bmatrix} \quad \text{and} \quad \mathbf{b} = \begin{bmatrix} \mathbf{b}_1 \\ \mathbf{b}_2 \end{bmatrix}$$

[1] here, we mean that A has a minor $\tilde{A}$ such that $\text{rank}(A) = \text{rank}(\tilde{A})$ and $\text{Det}(\tilde{A})$ is a monic polynomial in z

Note, since the rows of $\begin{bmatrix} C & D \end{bmatrix}$ are contained in the linear span of the rows of $\begin{bmatrix} \tilde{A} & B \end{bmatrix}$, we have that if a solution to $A\mathbf{x} = \mathbf{b}$ exists, then in fact

$$\begin{bmatrix} \tilde{A} & B \end{bmatrix} \begin{bmatrix} \mathbf{x}_1 \\ \mathbf{x}_2 \end{bmatrix} = \begin{bmatrix} \mathbf{b}_1 \end{bmatrix} \implies \begin{bmatrix} C & D \end{bmatrix} \begin{bmatrix} \mathbf{x}_1 \\ \mathbf{x}_2 \end{bmatrix} = \begin{bmatrix} \mathbf{b}_2 \end{bmatrix}$$

Therefore we can ignore the second constraint of $\begin{bmatrix} C & D \end{bmatrix} \mathbf{x} = \begin{bmatrix} \mathbf{b}_2 \end{bmatrix}$, and only focus on the first constraint. Thus, we want to show that if a solution to $\begin{bmatrix} \tilde{A} & B \end{bmatrix} \mathbf{x} = \begin{bmatrix} \mathbf{b}_1 \end{bmatrix}$ exists, then in fact there exists a solution $\mathbf{x}$ such that $\deg(\mathbf{x}) \leq \text{poly}(M, D)$.
We start with any solution to $\begin{bmatrix} \tilde{A} & B \end{bmatrix} \mathbf{x} = \begin{bmatrix} \mathbf{b}_1 \end{bmatrix}$. Since $\tilde{A}$ has non-trivial determinant, we can write,

$$\mathbf{x}_1 = \frac{\text{Adj}(\tilde{A})}{\text{Det}(\tilde{A})}(\mathbf{b}_1 - B\mathbf{x}_2)$$

so $\deg(\mathbf{x}_i) \leq [\deg(\text{Adj}(A)) + \deg(\mathbf{b}_1) + \deg(B) + \deg(\mathbf{x}_2)]$. So it suffices to show that we can obtain a solution where $\deg(\mathbf{x}_2)$ is bounded by $\text{poly}(M, D)$.

Now we use the observation that if $\begin{bmatrix} \mathbf{x}_1 & \mathbf{x}_2 \end{bmatrix}^T$ is a solution to the linear system then $\begin{bmatrix} (\mathbf{x}_1 + \text{Adj}(\tilde{A})B\mathbf{y}) & (\mathbf{x}_2 - \text{Det}(\tilde{A})\mathbf{y}) \end{bmatrix}^T$ is also a solution. Therefore by the division algorithm, we can make $\deg(\mathbf{x}_2) \leq \deg(\text{Det}(\tilde{A})) \leq MD$. Thus, we can obtain a solution $\mathbf{x}$ where $\deg(\mathbf{x}) \leq \text{poly}(MD)$. □

To show that our original problem satisfies the condition of having a full rank minor with monic determinant, we use the technique of applying a generic/random invertible linear transform. It allows us to use Lemma 2 and to ensure $\text{Det}(\tilde{A})$ is monic.

Lemma 3. *Given $A\mathbf{x} = \mathbf{b}$ with $A, \mathbf{b} \in \mathbb{K}[x_1, \cdots, x_j]$, let $T : \mathbb{K}^j \to \mathbb{K}^j$ be an invertible affine transform. Then*

1. *$\mathbf{x}$ is a solution to $A\mathbf{x} = \mathbf{b}$ if and only if $\mathbf{x}(T)$ is a solution to $A(T)\mathbf{x}(T) = \mathbf{b}(T)$ and $\deg(\mathbf{x}(T)) = deg(\mathbf{x})$.*
2. *With high probability over choices of T, $\text{Det}(\tilde{A}(T))$ is monic in x_j.*

Proof of Theorem 1: We start by writing a linear system in $\Pi(n)$, with a single equation $f = \sum_{i=1}^{m} g_i f_i$. We successively apply the inductive step to convert the linear system in $\Pi(j+1)$ to a linear system in $\Pi(j)$. Lemma 2, in addition to Lemma 3 guarantees that if the degrees of polynomials in number of equations in $\Pi(j+1)$ in M_{j+1}, then the degrees of the solution in $\Pi(j)$ can be made to be less than $\text{poly}(M_{j+1}, d)$ (since the enties in the linear system have degree at most $d = \max_i \deg(f_i)$). Also, going from $\Pi(j+1)$ to $\Pi(j)$ increases the number of linear equations to $M_j = \text{poly}(M_{j+1}, d)$ (with degree at least 2 in M_{j+1}). Thus finally when we get to $\Pi(0)$, the degrees of the solution can be brought down to $(md)^{2^{O(n)}}$. □

3 Hilbert's Nullstellensatz

Hilbert's Nullstellensatz deals with the problem of finding common roots to a given set of polynomials.

Problem 3. *Given polynomials $f_1, \cdots, f_m \in \mathbb{K}[\mathbf{x}]$ (where $\mathbb{K}$ is algebraically closed), decide whether there exists $(\alpha_1, \cdots, \alpha_n) = \alpha \in \mathbb{K}^n$ such that $f_j(\alpha) = 0$ for all $j \in [m]$.*

A more generalized version of this problem is as follows,

Problem 4. *Given polynomials $f_1, \cdots, f_m, f'_1, \cdots, f'_{m'} \in \mathbb{K}[\mathbf{x}]$ (where $\mathbb{K}$ is algebraically closed), decide whether there exists $(\alpha_1, \cdots, \alpha_n) = \alpha \in \mathbb{K}^n$ such that $f_j(\alpha) = 0$ for all $j \in [m]$ and $f'_j(\alpha) \neq 0$ for all $j \in [m']$.*

We note that Problem 4 in fact reduces to Problem 3. Firstly, observe that $f'_j(\alpha) \neq 0$ for all $j \in [m']$ if and only if $F(\alpha) \stackrel{\text{def}}{=} \prod_{j\in[m']} f'_j(\alpha) \neq 0$. Next we can reduce this to Problem 3 by adding an extra variable y and noting that the polynomials $f_1, \cdots, f_m, (1 - yF(\mathbf{x})) \in \mathbb{K}[\mathbf{x}, y]$ have a common root if and only if there exists $\alpha \in \mathbb{K}^n$ such that $f_j(\alpha) = 0$ for all $j \in [m]$ and $F(\alpha) \neq 0$.

The statement of Hilbert's Weak Nullstellensatz is as follows,

Theorem 4 (Weak Hilbert Nullstellensatz (WHN)). *For any ideal I in $\mathbb{K}[\mathbf{x}]$,*

$$V(I) = \emptyset \quad \Leftrightarrow \quad 1 \in I$$

(Note that $1 \in I \;\Leftrightarrow\; I = \mathbb{K}[x_1, \ldots, x_n]$.)
In other words, polynomials $f_1, \cdots, f_m$ do not have a common zero iff there exist $g_1 \cdots g_m$ such that $1 = \sum_i f_i g_i$.

The statement of the Strong Nullstellensatz is defined in terms of the Radical Ideal, which is defined as follows,

Definition 5 (Radical Ideal). *For any ideal $I \subseteq \mathbb{K}[\mathbf{x}]$, the radical ideal of I is* $\mathrm{Rad}(I) = \{f : \exists d \; f^d \in I\}$.

Theorem 6 (Strong Hilbert Nullstellensatz (SHN)). *For any ideal I in $\mathbb{K}[x_1, \ldots, x_n]$,*

$$I(V(I)) = \mathrm{Rad}(I)$$

In other words, the following are equivalent,

- *polynomials $f_1, \cdots, f_m, F \in \mathbb{K}[\mathbf{x}]$ are such that for every $\alpha \in \mathbb{K}^n$, if $f_i(\alpha) = 0$ for all $i \in [m]$, then $F(\alpha) = 0$*
- *there exists $d \geq 1$ such that $F^d \in \langle f_1, \cdots, f_m \rangle$*

Lemma 7. *SHN and WHN are equivalent.*

Proof. Both the SHN and the WHN have trivial directions (namely, $I(V(I)) \supseteq \mathrm{Rad}(I)$ and $V(I) = \emptyset \Leftarrow 1 \in I$ respectively). So we only need to prove the equivalence of the non-trivial directions of the SHN and the WHN (namely, $I(V(I)) \subseteq \mathrm{Rad}(I)$ and $V(I) = \emptyset \Rightarrow 1 \in I$ respectively).
[SHN $\implies$ WHN] So suppose that $V(I) = \emptyset$. Then, by the SHN, $\mathrm{Rad}(I) = I(\emptyset) = \mathbb{K}[\mathbf{x}]$. Hence, $1 \in \mathrm{Rad}(I)$ and thus $1 \in I$, as claimed in the WHN.
[WHN $\implies$ SHN] Let $F \in I(V(I))$; we need to show that $F \in \mathrm{Rad}(I)$. If F is identically 0, we are done; so assume that F is not identically 0. Consider the ideal J in $\mathbb{K}[x_1, \ldots, x_n, y]$, where y is an auxiliary variable, defined by $J = \langle I, 1 - yF \rangle$.

Notice that $V(J) = \emptyset$. Indeed, suppose by way of contradiction that there is $(a_1, \ldots, a_n, b) \in V(J)$; then $(a_1, \ldots, a_n) \in V(I)$ and thus $f(a_1, \ldots, a_n) = 0$, and thus $1 - bF(a_1, \ldots, a_n) = 1 - 0 = 1 \neq 0$; we conclude that $V(J)$ must indeed be empty.

By the WHN, since $V(J) = \emptyset$, we know that $1 \in J$, so that there must exist $p \in \mathbb{K}[x_1, \ldots, x_n, y]$ and $q_1, \ldots, q_d \in I$ such that $1 = p(1 - yF) + \sum_{i=0}^{d} y^i q_i$. This polynomial identity holds in $\mathbb{K}[\mathbf{x}, y]$, and thus also in $\mathbb{K}(\mathbf{x})[y]$; furthermore, since F is not identically 0, $1/F$ is a well defined element in $\mathbb{K}(x_1, \ldots, x_n)$. By setting $y = 1/F$, we deduce that $1 = \sum_{i=0}^{d} F^{-i} q_i$, and thus $F^d = \sum_{i=0}^{d} F^{d-i} q_i$, which means that $F^d \in I$, and thus $F \in \mathrm{Rad}(I)$, as we wanted to show. □

3.1 Remarks on the Nullstellensatz

Brownawell [3] showed that in the statement of Weak Nullstellensatz [Theorem 4] we can have $\deg(g_i) \leq \prod_i \deg(f_i)$. Note that one can try to invoke Theorem 1 (due to Hermann) here, since we are trying to solve an ideal membership problem here of writing $1 = \sum_i g_i f_i$. However, the bound we get is doubly-exponential in n, whereas Brownawell's result gives a much stronger bound.

This suggests that perhaps finding witnesses g_i's such that $1 = \sum_i g_i f_i$ should not be a very hard problem. In particular, it is clear that it is in PSPACE. More strongly though, Koiran showed that assuming the Generalized Riemann Hypothesis, Hilbert Nullstellensatz is in $\mathrm{RP}^{\mathrm{NP}}$ [4].

References

[1] Ernst Mayr and Albert Meyer The complexity of the word problems for commutative semigroups and polynomial ideals *Advanced in Mathematics*, Volume 46, Issue 3, December 1982, Pages 305329

[2] G. Herrmann Die Frage der endlich vielen Schritte in der Theorie der Polynomideale *Math. Ann.* 95, (1926), 736-788.

[3] W. Dale Brownawell Bounds for the Degrees in the Nullstellensatz *Annals of Mathematics* Second Series, Vol. 126, No. 3 (Nov., 1987), pp. 577-591

[4] Pascal Koiran Hilbert's Nullstellensatz is in the polynomial hierarchy. *Journal of Complexity*, 12(4):273-286, 1996.