6.966 Algebra and Computation	October 19, 1998
Lecture 14	
Lecturer: Madhu Sudan	*Scribe: Salil Vadhan*

Explicit Bounds for Ideal Membership

In this lecture, we will prove a result due to Mayr and Meyer, stating that the ideal membership problem can be solved in exponential space. Recall that this is simply the following decision problem:

IDEAL MEMBERSHIP (over any fixed field K)

Input Polynomials $g, f_1, \ldots, f_t \in K[x_1, \ldots, x_n]$.

Question Is $g \in (f_1, \ldots, f_t)$? That is, are there polynomials $q_1, \ldots, q_t \in K[x_1, \ldots, x_n]$ such that

$$g = \sum_{j=1}^{t} q_j f_j ? \tag{1}$$

The main step in showing that this problem can be solved in exponential space will be to show that the q_i's can be taken to be of "reasonable" (doubly-exponential) degree; such degree bounds date back to the work of G. Hermann in 1926. We have already seen one algorithm for solving the ideal membership problem, namely the Groebner basis algorithm. The exponential-space algorithm we'll be seeing will not be based on Groebner bases, though the literature suggests that there are ways of using the same ideas to implement the Groebner basis algorithm in exponential space.

The algorithm we give will be based on viewing Equation (1) as a *linear* system over K. This can be done as follows. Say that d is an upper bound on the (total) degree of the f_j's and g and that $D = D(n, d, t)$ is an upper bound on the (total) degree of the q_j's. Then for every $j \in [t]$ and $\overline{\alpha} \in \{0, \ldots, D\}^n$, we let $q_{j,\overline{\alpha}}$ be an unknown (taking values in K) corresponding to the coefficient of $x^{\overline{\alpha}}$ in q_j and $f_{j,\overline{\alpha}}$ the coefficient of $x^{\overline{\alpha}}$ in f_j. Then Equation (1) can be rewritten as the following linear system:

$$\sum_{j=1}^{t} \sum_{\overline{\beta} \leq \overline{\alpha}} q_{j,\overline{\beta}} \cdot f_{j,\overline{\alpha}-\overline{\beta}} = g_{\overline{\alpha}} \qquad \forall\, \overline{\alpha} \in \{0, \ldots, D\}^n, \tag{2}$$

where $\overline{\beta} \leq \overline{\alpha}$ means that $\beta_k \leq \alpha_k$ for every $k \in [n]$.

Since linear systems can be solved in polylogarithmic space, the above system (with $t \cdot D^n$ unknowns and D^n equations) can be solved in space $\mathrm{poly}(n \log D, \log t)$. Thus, to show that the system can be solved in exponential (in n, t, and d) space, it suffices to prove a doubly exponential bound on D. We will obtain this bound by passing back and forth between the formulation given in Equation (1) (one linear equation over $K[x_1, \ldots, x_n]$) and the formulation given in System of Equations (2) (many linear equations over K). To facilitate this, we consider the following common generalization of both of these formulations:

LINEAR SYSTEM OF POLYNOMIALS (over any fixed field K)

Input Polynomials $\{f_{ij}\}$ and $\{g_i\}$ in $K[x_1, \ldots, x_n]$ for $i = 1, \ldots, s$ and $j = 1, \ldots, t$.

Question Do there exist $q_1, \ldots, q_t \in K[x_1, \ldots, x_n]$ such that

$$g_i = \sum_{j=1}^{t} q_j f_{ij} \qquad \forall\, i \in [s] \tag{3}$$

Actually, this problem is not much more general than the ideal membership problem if we allow ourselves to introduce new variables, as System of Equations (3)can be rewritten as the single equation

$$\sum_{i=1}^{s} g_i \cdot y_i = \sum_{i=1}^{s} \left(\sum_{j=1}^{t} q_j \cdot f_{ij} \right) \cdot y_i,$$

over $K[x_1, \ldots, x_n, y_1, \ldots, y_s]$.

However, it is convenient to state and prove our result for the many-equations version.

Theorem 1 (Mayr–Meyer, Hermann) *If* Linear System of Polynomials *has a solution, then it has a solution in which every q_i has total degree at most $D = (t \cdot d)^{2^n}$.*

Applying this to the special case of Ideal Membership and reducing to solving a linear system as described earlier, we get

Corollary 2 Ideal Membership *(for $K = \mathbb{Q}$ or $K =$ any fixed finite field) in* EXPSPACE*.*

Before proceeding to the proof, we observe that, in proving Theorem 1, we may assume that the field K is infinite without loss of generality. This is because the existence of a solution using polynomials of a given degree can be expressed as a linear system with coefficients in K (as in Equation (2)). We know that if such a linear system with coefficients in K has a solution in any field L containing K, then it also has a solution in K itself. So we can take L to be any infinite field containing L and prove the theorem for L. Thus, in the following two sections we will assume that K is infinite.

A special case: univariate polynomials

In this section, we treat the special case of Theorem 1 when the polynomials are all univariate, i.e. $n = 1$. We're given a $s \times t$ matrix $M = (f_{ij})$ with entries in $K[x]$ and a $g \in K[x]^s$ such that there exists a solution $q \in K[x]^t$ to $Mq = g$ and we want to prove that there exists a solution in which all entries of q have small degree.

First, let us see that, without loss of generality, we may assume that M is of full row rank (i.e., $\text{rank}(M) = s$), over $K(x)$. If this is not the case, there is some linear relationship among the rows $M_i = h_1 M_{i_1} + \cdots + h_k M_{i_k}$, where the h_ℓ's are in $K(x)$ and $i \notin \{i_1, \ldots, i_k\}$. We must also have $g_i = h_1 g_{i_1} + \cdots + h_k g_{i_k}$ or else the system $Mq = g$ would have no solution even over $K(x)$. From these two linear relationships it follows that removing row i from the system does not change the set of solutions, and hence we can keep removing rows until M has full row rank.

So, now let us assume that M has full row rank and hence $s \leq t$. If $s = t$, then M is a nonsingular square matrix and the unique solution is $q = M^{-1} g$, where M^{-1} is the inverse of M (computed in $K(x)$). In general, however, s can be less than t and the system will have many solutions. To deal with this possibility, we will obtain a description of *all* solutions in $K(x)$. Since M has rank s, some subset of its columns of size s are linearly independent. By permuting the columns, we may assume that these are the first s columns, so we can describe M as a nonsingular $s \times s$ matrix A together with $r = t - s$ column vectors $v_1, \ldots, v_r$:

$$M = \left[\begin{array}{c|cccc} & | & | & & | \\ A & v_1 & v_2 & \cdots & v_r \\ & | & | & & | \end{array} \right] \tag{4}$$

Now, if we write $q = (z, a_1, \ldots, a_r)$, where $z \in K(x)^s$ and $a_1, \ldots, a_r \in K(x)$, then $Mq = Az + \sum_j a_j v_j$. So, q is a solution to $Mq = g$ iff $z = A^{-1}(g - \sum_j a_j v_j)$. We are interested in solutions where all the entries of q are polynomials (rather than rational functions); that is, where $a_1, \ldots, a_r$ and z are all in $K[x]$. However, understanding polynomial solutions are complicated by the fact that the entries of A^{-1} are rational functions. Here Cramer's Rule comes to the rescue — we can write $A^{-1} = [\mathrm{adj}(A)]/\det(A)$, where $\mathrm{adj}(A)$ is the $s \times s$ matrix whose ij'th entry is $(-1)^{i+j}$ times the determinant of A with row i and column j removed. The key point is that the entries of $\mathrm{adj}(A)$ are polynomials (of degree at most $(s-1)d$) and $\det(A)$ is a polynomial (of degree at most sd). Now, let $q = (z, a_1, \ldots, a_r)$ be any *polynomial* solution to $Mq = g$ (which exists by hypothesis). Then, for any $b_1, \ldots, b_r \in K[x]$, $q' = (z', a'_1, \ldots, a'_r)$ is also a polynomial solution for $a'_j \triangleq a_j - b_j \det(A)$ and

$$z' \triangleq A^{-1}\left(g - \sum_j a'_j v_j\right) = z + \sum_j b_j[\mathrm{adj}(A) v_j].$$

By choosing the b_j's appropriately, we may assume that all the a'_j's are reduced modulo $\det(A)$ and hence have degree smaller than $\ell \triangleq \deg(\det(A)) \leq sd$. Then, defining the degree of a matrix or vector to be the maximum degree of its entries, we have

$$\begin{aligned}
\deg(z') &\leq \deg\left(A^{-1}\right) + \deg\left(g - \sum_j a'_j v_j\right) \\
&\leq \deg(\mathrm{adj}(A)) - \deg(\det(A)) + \max\left(\deg(g), \deg\left(\sum_j a'_j v_j\right)\right) \\
&\leq (s-1)d - \ell + \max(d, \ell - 1 + d) \\
&\leq sd
\end{aligned}$$

Thus, all the entries of q' have degree at most $sd \leq td$. This completes the proof of the univariate case of Theorem 1.

Extending to multivariate polynomials

To prove Theorem 1 for multivariate polynomials (i.e. arbitrary n), we will work one variable at a time, viewing the multivariate polynomials in $x_1, \ldots, x_n$ as univariate polynomials in x_1 with coefficients in $K[x_2, \ldots, x_n]$. Then, almost everything we did in the last section will work, except the step when we reduced the a_i's modulo $\det(A)$. We can only reduce a polynomial modulo $\det(A)$ (with respect to variable x_1) only if $\det(A)$ is *monic* in x_1 (i.e., its maximum power of x_1 has a coefficient in K rather than $K[x_2, \ldots, x_n]$). Fortunately, it is easy to guarantee that this holds by using a random linear transformation to change variables.

Lemma 3 *Let $r_2, \ldots, r_n$ be chosen uniformly and independently from some subset $U \subset K$ of size u. For every polynomial $P \in K[x_1, \ldots, x_n]$, define $\tilde{P} \in K[y_1, \ldots, y_n]$ by $\tilde{P}(y_1, \ldots, y_n) = P(y_1, r_2y_1+y_2, \ldots, r_ny_1+y_n)$. Then,*

1. *For every choice of $r_2, \ldots, r_n$, $P \mapsto \tilde{P}$ is a ring isomorphism which preserves degree. That is,*
   (a) *The map $P \mapsto \tilde{P}$ is a bijection.*
   (b) *For any polynomials P and Q, $\widetilde{P+Q} = \tilde{P} + \tilde{Q}$ and $\widetilde{PQ} = \tilde{P}\tilde{Q}$.*
   (c) $\deg(\tilde{P}) = \deg(\tilde{Q})$.
2. *For any P of degree m, $\tilde{P}(\overline{y})$ is monic in y_1 with probability $\geq 1 - \frac{m}{u}$.*

Proof To see that $P \mapsto \tilde{P}$ is a bijection, note that it can be inverted by the rule $P(x_1, \ldots, x_n) = \tilde{P}(x_1, x_2 - r_2x_1, \ldots, x_n - r_nx_1)$. The remaining parts of Item 1 are straightforward. For Item 2, it suffices to show that the coefficient of y_1^m in $\tilde{P}(\overline{y})$ vanishes with probability at most m/u, as $\tilde{P}$ is of degree m. A straightforward calculation shows that the coefficient of y_1^m in $\tilde{P}(\overline{y})$ is exactly $P_m(1, r_2, \ldots, r_n)$, where P_m is the homogeneous degree m part of P. This is a nonzero polynomial of degree at most m in $r_2, \ldots, r_n$, so, by the Schwartz–Zippel Lemma, it vanishes with probability at most m/u. ■

Remark. In class, we did the change of variables using a random linear transformation chosen from the set of all $n \times n$ matrices over K. Above, we selected from a smaller set of linear transformations to avoid having to deal with the possibility that the transformation is not invertible.

Now we proceed with the proof of Theorem 1. We're given an $s \times t$ matrix $M = (f_{ij})$ with entries in $K[\overline{x}] \triangleq K[x_1, \ldots, x_n]$ and $g \in K[\overline{x}]^s$ such that there exists a polynomial solution $q \in K[\overline{x}]^s$ to $Mq = g$. As in the univariate case, we may assume that M is of full row rank over $K(\overline{x}) \triangleq K(x_1, \ldots, x_n)$ and can be written as a nonsingular $s \times s$ matrix A together with $r = t - s$ column vectors $v_1, \ldots, v_r$ (as in Equation (4)). Now suppose we choose $r_2, \ldots, r_n \in K$ randomly from subset $U \subset K$ of size $u = sd + 1$ and transform every polynomial as in Lemma 3 (and hence also transform every vector and matrix with polynomial entries). By Lemma 3, $\widetilde{\det(A)}$ is monic in y_1 with nonzero probability (as $\deg(\det(A)) \leq sd$). Hence, we may fix $r_2, \ldots, r_n$ such that $\widetilde{\det(A)}$ is monic in y_1.

Now we have the matrix $\tilde{M} = (\tilde{f}_{ij}) = (\tilde{A}|\tilde{v}_1 \cdots \tilde{v}_r)$ and vectors $\tilde{g}$ and $\tilde{q} \triangleq (\tilde{z}, \tilde{a}_1, \ldots, \tilde{a}_r)$. Since the transformation is a ring isomorphism, polynomial solutions q' to $Mq' = g$ of a given degree are in 1–1 correspondence with polynomial solutions $\tilde{q}'$ to $\tilde{M}\tilde{q}' = \tilde{g}$. In particular, we have $\tilde{M}\tilde{q} = \tilde{g}$ and our problem is reduced to finding another polynomial solution $\tilde{q}'$ to $\tilde{M}\tilde{q}' = \tilde{g}$ such that $\tilde{q}'$ is of low degree. As in the univariate case, for any $\tilde{b}_1, \ldots, \tilde{b}_r \in K[\overline{y}]$, $\tilde{q}' = (\tilde{z}', \tilde{a}_1', \ldots, \tilde{a}_r')$ is also a polynomial solution for $\tilde{a}_j' = \tilde{a}_j - \tilde{b}_j \det(\tilde{A})$ and $\tilde{z}' = \tilde{A}^{-1}(g - \sum_j \tilde{a}_j' \tilde{v}_j)$. Since the transformation is an isomorphism, $\det(\tilde{A}) = \widetilde{\det(A)}$, which is monic in y_1. Thus, by choosing $\tilde{b}_1, \ldots, \tilde{b}_r$ appropriately, we may assume that all the $\tilde{a}_j'$'s are of degree smaller than $\ell \triangleq \deg_{y_1}(\det(\tilde{A})) \leq sd$ in y_1. As in the univariate case, it then follows that $\tilde{z}'$ is of degree at most sd in y_1.

We have argued that the system $\tilde{M}\tilde{q}' = \tilde{g}$ has a solution $\tilde{q}'$ in which all the entries are of degree at most sd in y_1. Hence, we can restrict to such solutions and expand everything in terms of y_1 as follows: $\tilde{q}' = \tilde{q}_0' + \tilde{q}_1' y_1 + \tilde{q}_2' y_1^2 + \cdots + \tilde{q}_{sd}' y_1^{sd}$, $\tilde{M} = \tilde{M}_0 + \tilde{M}_1 y_1 + \cdots + \tilde{M}_d y_1^d$, and $\tilde{g} = \tilde{g}_0 + \tilde{g}_1 y_1 + \cdots + \tilde{g}_d y_1^d$. Equating terms of the same degree in y_1 in $\tilde{M}\tilde{q}' = \tilde{g}$, we obtain a system of $(sd + d)s$ equations over $K[y_2, \ldots, y_n]$ with $(sd)t \leq t^2 d$ unknowns in which all coefficients still have degree at most d. Moreover, any solution to the new system of total degree k yields a solution to the original system of total degree at most $k + sd \leq k + td$.

Now we proceed inductively. A system with $t_0 = t$ unknowns in n variables yields a system $t_1 = t_0^2 d$ unknowns in $n - 1$ variables, which in turn yields $t_2 = t_1^2 d = t_0^4 d^3$ unknowns in $n - 2$ variables, and so on with $t_i = t_0^{2^i} d^{2^i - 1}$ unknowns in $n - i$ variables. Since passing from $n - i$ variables to $n - i - 1$ variables contributes degree at most $t_i d$ to the total degree of the solution, we end up with a solution of total degree $\sum_{i=0}^{n-1} t_i d < (td)^{2^n}$.

EXPSPACE-completeness

Because an exponential space is far from "efficient" by our usual standards, one might wonder whether there's a better algorithm for Ideal Membership. Unfortunately, we cannot hope to do better.

Theorem 4 (Mayr–Meyer) Ideal Membership *is* EXPSPACE-*complete.*

To show that Ideal Membership is EXPSPACE-hard, Mayr and Meyer reduce from the following EXPSPACE-hard problem.

Input $(\Sigma, R, \alpha, \beta)$, where $\Sigma = \{\sigma_1, \ldots, \sigma_n\}$ is a finite alphabet, $\alpha, \beta \in \Sigma^*$, and S is a set of rewrite rules of the form "$\gamma = \delta$" for $\gamma, \delta \in \Sigma^*$ such that S also contains all rules of the form $\sigma_i = \sigma_j$.

Output Can $\alpha = \beta$ be derived from the rewrite rules in S?

To reduce this problem to Ideal Membership, Mayr and Meyer define polynomials in $\mathbb{Q}[x_1, \ldots, x_n]$ where $n = |\Sigma|$. To every string $\gamma \in \Sigma^*$, they associate the monomial $x^\gamma \triangleq x_1^{d_1} \cdots x_n^{d_n}$, where d_i is the number of times the symbol σ_i occurs in γ. To a rewrite rule $\gamma = \delta$, they associate the polynomial $f_{\gamma,\delta} = x^\gamma - x^\delta$. Then, one can show that $f_{\alpha,\beta}$ is in the ideal generated by $\{f_{\gamma,\delta} \colon \text{“}\gamma = \delta\text{”} \in S\}$ iff $\alpha = \beta$ can be derived from S.

What about the Nullstellensatz?

Recall that our initial motivation for looking at the ideal membership problem was the problem of deciding whether a system of polynomial equations $\{f_i = 0\}$ has a solution (in, say, some algebraically closed field). By Hilbert's (Weak) Nullstellensatz (which we will prove in upcoming lectures), the latter problem is equivalent to deciding whether 1 is the ideal $(f_1, \ldots, f_i)$. Today we studied a more general problem, testing whether an arbitrary polynomial is in an ideal. Although one might naively guess that the two problems are equally hard, testing whether 1 is in an ideal is in fact provably easier. Specifically, this problem is in PSPACE (“polynomial space”), which is strictly contained in EXPSPACE by the space hierarchy theorem. In fact, Koiran has shown that it is even in the Polynomial-Time Hierarchy if the Extended Riemann Hypothesis is true, as we'll see several lectures from now.

The PSPACE result is proven by showing *singly* exponential degree bounds on the solutions $\{q_i\}$ to $1 = \sum_i q_i f_i$ (when they exist). Such bounds were exhibited by Brownawell in 1986, and decidability in polynomial space follows immediately by viewing it as a linear system, as described at the beginning of this lecture. A generalization of this was given by Kollar in 1988, who showed a singly exponential degree bounds on solutions $\{q_i\}$ to the question “$\exists k\ f^k = \sum_j q_j f_j$” (also known as testing membership in the “radical” of an ideal).

Despite the impractical size of the degree bounds we proved today, what we did to obtain these bounds is in fact useful. It allows us to eliminate a constant number of variables (in a linear system of polynomials) with only a polynomial blowup in degree. Eliminating variables (and quantifiers) “efficiently” in a more general setting will be the focus of the next couple of lectures.