6.885 Algebra and Computation	November 16, 2005
Lecture 19	
Lecturer: Madhu Sudan	*Scribe: Swastik Kopparty*

1 Today

- Finish Groebner Basis (Recognition)
- Complexity of Ideal Membership

2 Groebner Bases

Recall that for an ideal J, we call $g_1, \ldots, g_t$ a Groebner Basis for J if

- $\forall i, g_i \in J$
- $I(LT(g_1), LT(g_2), \ldots, LT(g_t)) = I(LT(J))$

We further define two notions.

We say r is a *weak remainder* of f w.r.t. $g_1, \ldots, g_t$ if $f = r + \sum g_i q_i$ and $\forall$ monomials m of r and $\forall i$, $LT(g_i)$ does not divide m.

We say $(q_1, \ldots, q_m)$ is a *strong quotient* for f w.r.t. $g_1, \ldots, g_t$ if $\forall i, \deg(g_i q_i) \leq deg f$.

Recall that when we run our algorithm $DIVIDE$, we get a weak remainder.

For two polynomials f, g, we define the *Syzygy* to be the linear combination of them which cancels leading terms; i.e.

$$S(f,g) = LC(g)\frac{M}{LM(f)}f - LC(f)\frac{M}{LM(g)}g$$

where $M = LCM(LM(f), LM(g))$.

We can now give the test for a GB:

- Given $g_1, \ldots g_t$ as input
- Check that $\forall i, j$, $DIVIDE(S(g_i, g_j), g_1, \ldots, g_t)$ returns (0,strong quotient).
- Then $\{g_i\}$ form a GB iff it passes the check.

We now prove the validity of this test:

Proof Take $f \in J = I(g_1, \ldots, g_t)$. We need to show that $LT(f) \in I(LT(g_1), \ldots, LT(g_t))$.

First write $f = \sum m_j g_{i_j}$ where $i_j \in \{1, \ldots, t\}$. Amongst all such representations, pick the *reduced form*; i.e. the sequence with the smallest length satisfying $\deg(m_1 g_{i_1}) \geq \deg(m_2 g_{i_2}) \geq \ldots$ and also, if $\deg(m_j g_{i_j}) = \deg(m_{j+1} g_{i_{j+1}}$, then $i_j < i_{j+1}$.

Claim: $LT(f) = LT(m_1 g_{i_1})$.

Wlog, we can take $f = m_1 g_1 + m_2 g_2 + \ldots$. Suppose $\deg(m_1 g_1) = \deg(m_2 g_2)$. In this case we want to say that $m_2 g_2 = m_1 g_1 +$ lower degree terms. We use the Syzygy property:

$$m_1 g_1 = w\frac{M}{LM(g_1)}g_1$$

$$m_2 g_2 = w\frac{M}{LM(g_2)}g_2$$

$$S(g_1, g_2) = 0 + \sum g_i q_i$$

where degree$(g_i q_i)$ ¡ degree$(\frac{M}{LM(g_1)}g_1)$.

So, $m_2 g_2 = m_1 g_1 + \sum g_i q_i$. Thus reducedness is violated, and hence $deg(m_1 g_1) > deg(m_2 g_2)$, thus $LT(f) = LT(m_1 g_1)$, as desired. ■

3 Complexity of Ideal Membership Problem

- Given $f_0, \dots f_m \in K[X_1, \dots, X_n]$ of degree d
- Decide if $\exists q_1, \dots q_m$ s.t. $f_0 = \sum f_i q_i$.

We wish to bound the complexity (in operations over K) in terms of n, d, m.

Theorem 1 [Mayr, Meyer '81] *$IM \in EXPSPACE = SPACE(2^{poly(n,d,m)})$ and further, IM is $EXPSPACE$ hard!*

3.1 Hardness

The reduction is from the Commutative word equivalence problem (CWEP).

- Input:
- Σ a finite alphabet, $|\Sigma| = n$.
- Rules $\alpha_1 = \beta_1, \alpha_2 = \beta_2, \dots, \alpha_m = \beta_m$, $\alpha_i, \beta_i \in \Sigma^*$
- $\alpha, \beta \in \Sigma^*$
- Goal:
- Determine if $\alpha = \beta$.
- Using given rules and using commutativity of symbols in Σ.

It is known that $CWEP$ is $EXPSPACE$ hard.

The reduction is obvious. Every word is a monomial. Rules are binomials $f_i(x) = mono(\alpha_i) - mono(\beta_i)$. Membership in CWEP is asking if $f_0(x) = mono(\alpha_0) - mono(\beta_0) \in I$? Thus IM is EXPSPACE hard.

3.2 Upper bound

This result rests on 2 facts:

- Inverting a $m \times n$ linear system can be done in $SPACE(polylog(m+n))$.
- A 1926 result of Hermann that says that there exist q_i with $deg(q_i) \le D = (md)^{2^n}$

Note that finding q_i (if they exist) can be posed as inverting a linear system.

We will prove Hermann's result. We want to get an understanding of solutions to the following kind of question, a linear equation over a ring:

- Determine if $\exists q_1, q_2, \dots, q_m \in K[X_1, \dots, X_n]$ s.t. $\sum f_i q_i = f_0$

Note that this question can be posed as a linear system over a field, a kind of question that we do understand:

- Determine $\exists q_{i,\alpha} \in K$ s.t. $\forall \beta \sum_{i,\alpha+\alpha'=\beta} q_{i,\alpha} f_{i,\alpha'} = f_{0,\beta}$, where β ranges over all multi-indices over n variables of degree $\le \deg(f_0)$

In order to bound the degree, we introduce a common generalization, the j-variable linear system, that will help us make the transition between the problems

- Given polynomials $f_{i,\alpha} \in K[X_1, \dots, X_j]$, $i \in \{0, 1, \dots, m\}, \alpha \in A$

- Determine if $\exists q_i \in K[X_1, \ldots, X_j]$ s.t. $\forall \alpha \in A, \sum_i q_i f_{i,\alpha} = f_{0,\alpha}$

The strategy will be to eliminate 1 variable at a time. The crux of the Hermann result is that a j variable linear system with M equations and n unknowns reduces to a $j-1$ variable linear system in $poly(M, n, d)$ equations and $poly(M, n, d)$ unknowns.

Lemma 2 *Let $f_i \in K[X_1, \ldots, X_j]$. Suppose $\exists q_i \in K[X_1, \ldots, X_j]$ with X_j degree $< D$ satisfying $f_0 = \sum_{i=1}^m f_i q_i$. Then the following system of equations over has a solution $q'_{i,\alpha} \in K[X_1, \ldots, X_{j-1}]$*

$$\forall \gamma < D, \sum_{i,\beta,\alpha,\beta+\alpha=\gamma} f_{i,\beta} q'_{i,\alpha} = f_{0,\gamma}$$

where $f_{i,\beta} \in K[X_1, \ldots, X_{j-1}$ is the coefficient of X_j^β in f_i. Furthermore, any solution to this system of equations yields a solution to the original equation with X_j degree $< D$.

Proof Simply take $q'_{i,\alpha}$ to be the coefficient of X_j^α in q_i. ■

Definition 3 *Let R be a ring. We call an $r \times s$ matrix A with entries in $R[z]$* good *if*

- *$r < s$*
- *There exists an $r \times r$ minor $\tilde{A}$ with $\det \tilde{A}$ monic and nonzero.*

Lemma 4 *Let R be a ring. Let A be a good matrix in $R[z]$ with each entry having degree $\leq D$. Let b be a vector with entries in $R[z]$ with each entry having degree $\leq D$. Suppose $Ax = b$ has a solution in $R[z]$. Then $Ax = b$ has a solution with each entry having degree $\leq O(MD)$.*

Proof Consider the minor $\tilde{A}$ guaranteed to exist by the goodness of A. We can rearrange the columns and have $A = [\tilde{A}|B]$. For a vector w with $w^T = (w_1|w_2)$, we have that $Aw = \tilde{A}w_1 + Bw_2$. Thus, if we pick w_2 arbitrarily, then if $Aw = b$, it must be that $w_1 = \tilde{A}^{-1}(b - Bw_2)$.

Note that $\tilde{A}^{-1} = \frac{Adj(\tilde{A})}{\det(\tilde{A})}$. Thus if (x_1, x_2) is a solution, then for any vector c, so is $w = (x_1 + Adj(\tilde{A})Bc, x_2 - \det(\tilde{A})c)$. Now, by the goodness hypothesis, $\det(\tilde{A})$ is monic, and since its degree $\leq O(MD)$, then by choosing c appropriately, make $\deg(w_2) = O(MD)$. Then, $\deg(w_1) < \deg\left(\frac{Adj(\tilde{A})}{\det(\tilde{A})}(b - Bw_2)\right)$ which $= O(MD)$, as desired. ■

With this lemma in hand, it is essentially clear what to do. Suppose we are given a system of M equations $Ax = b$ with coefficients in $R = K[X_1, \ldots, X_j]$ and degree bounded by D. Suppose that we also know that there is a solution to this system. Then by lemma 4, there is a solution with X_j degree $< O(MD)$. Thus by lemma 2 we can reduce to $O(M^2 D)$ equations in over $K[X_1, \ldots, X_{j-1}]$ with degree at most D. Continuing this way, we get a linear system over K which has a solution, from which we can reconstruct a solution to the original problem with degree at most $(MD)^{O(2^n)}$ (note that the degree was squaring at each stage).

Actually, to apply lemma 4 we required some goodness from our linear system at each stage. This can be achieve by doing the following at every stage: we throw away all row dependencies to make the matrix of full row rank. Then applying a random linear transformation to the $X_1, \ldots X_n$, we get that with high probability for any single polynomial and any fixed variable, the modified polynomial will be monic in that variable. This holds in particular for the determinant of a nonsingular $r \times r$ minor of our A, thus making it good.

To see the high probability result, let us be a bit more precise. Given a polynomial $f(x)$ homogenous of degree n, not identically 0. Pick a random orthogonal matrix P (uniform from $S^{n-1}, S^{n-2}, \ldots, S_0$) and consider the polynomial $g(x) = f(Px)$. Then the resulting polynomial is homogenous of degree n and is not monic if and only if $g(1, 0, \ldots, 0) = 0$. However $P \cdot (1, 0, \ldots 0)$ is a point uniformly chosen from the surface of the sphere and by Schwarz Zippel, $f(P \cdot (1, 0, \ldots, 0))$ is nonzero almost everywhere. Thus w.h.p. g is monic.