6.S897 Algebra and Computation April 2, 2012

Lecture 14

Lecturer: Madhu Sudan *Scribe: Yohay Kaplan*

1 Today

- Systems of polynomial equations.
- Ideals and varieties
- Groebner bases

2 Solving a system of polynomial equations

Given $f(x) \in \mathbb{F}[x]$, $\deg f \leq n$ we can find a zero of this polynomial in time $poly(n) \cdot \log |\mathbb{F}|$. This problem is no harder for a system of polynomial equations, as we can just reduce it to finding a zero of the GCD of the polynomials. So we consider the following problem: given m polynomials in n variables over a field K,

$$f_1, ..., f_m \in K[x_1, ..., x_n],$$

does there exist a vector $\bar{a} \overset{\text{def}}{=} (a_1, ..., a_n) \in K^n$ such that

$$f_1(\bar{a}) = ... = f_m(\bar{a}) = 0?$$

This problem can be solved in exponential time over finite fields, but is NP-hard even when $\deg f$ is just 2. Consider the following reduction from $3SAT$:

- For each variable x_i define the polynomial $x_i(1 - x_i)$.
- For each clause $(x_1 \vee x_2 \vee \overline{x_3})$ define the polynomial $(1 - x_1)(1 - x_2)x_3$.

The exact hardness of the problem can depend on the setting (m, n, particular families of polynomials) and the field we are working over. A commonly looked at setting is over the reals.

3 Existential theory of the reals

$f_1, ..., f_m \in \mathbb{R}[x_1, ..., x_n]$, does there exist a vector $\bar{a} \in \mathbb{R}^n$ such that

$$f_1(\bar{a}) = ... = f_m(\bar{a}) = 0?$$

We create boolean variables $z_1, ..., z_m$ where z_i = true if $f_i(\bar{a}) = 0$. We can ask whether $\exists \bar{a}$ such that $\varphi(z_1, ..., z_m)$ = true, this is called the *Existential Theory of the Reals*. ETR in fact studies the more general question where z_i is true when $f_i(\bar{a}) \geq 0$, so it can also be seen as a generalization of linear programing. [Tarski51] showed that ETR is decidable. [Canny88],[Renegar88] and [reif] showed that ETR is in PSPACE

We note that we can make the problem even broader by adding more layers of quantification: given $f_1, ..., f_m$ is it the case that $\exists a_1 \forall a_2 \exists a_3 ... Q a_n$ s.t.

$$f_1(\bar{a}) = ... = f_m(\bar{a}) = 0?$$

These questions form the *Quantified Theory of the Reals*, which is also decidable. The decidability of these problems means that there exist proofs of non-feasibility of polynomial systems. In fact, we will see that there exists algebraic proofs of non-feasibility.

4 Hilbert's Nullstellensatz

We'll look at a benign setting where the field is algebraically closed, and where we are interested in polynomial equalities (and not inequalities). An algebraically closed field is a field where every polynomial splits into linear factors. There are such fields with any prime characteristic (and obviously with characteristic 0).

So we're examining the problem of given m polynomials in n variables over an algebraically closed field K, $f_1, ..., f_m \in K[x_1, ..., x_n]$ does there exist a vector $\bar{a} \in K^n$ such that $f_1(\bar{a}) = ... = f_m(\bar{a}) = 0$?

A proof of feasibility would be a point where all the polynomials are zero. What would a proof of non-feasibility be? To answer that we introduce Hilbert's nullstellensatz (null locus theorem):

Theorem 1 (Nullstellensatz (weak version)) *Given polynomials $f_1, ..., f_n \in K[\bar{x}]$, the following two statements are equivalent:*

$$\exists \bar{a} \quad \textit{such that} \quad f_1(\bar{a}) = ... = f_m(\bar{a}) = 0$$

and

$$\neg \left(\exists q_1, ..., q_m \in K[\bar{x}] \quad \textit{such that} \quad \sum f_i q_i = 1 \right).$$

We might prove this later in the course. For now we note that one direction is clear: if there exists a polynomial combination of the polynomials f that is identically 1, then the polynomials can never be simultaneously 0.

So it seems we should be looking at $(f_1, ..., f_m)$ and asking if a particular polynomial (in this case 1) is in the ideal generated by them.

5 Ideal membership question

Definition 2 (Ideal) *$J \subseteq K[\bar{x}]$ is an* ideal *if:*

- $\forall p, q \in J : p + q \in J$
- $\forall p \in J$ *&* $q \in K[\bar{x}] : p \cdot q \in J$

Definition 3 (Generated ideal) *We define $(g_1, ..., g_t) = \{\sum q_i \cdot g_i | q_i \in K[\bar{x}]\}$, clearly this is an ideal.*

Can we bound t? Not in general. For instance the ideal $\{x^i y^{d-i}\}_{i=0}^d$ must have at least $d+1$ generators. To be able to bound t we must limits the degree in J in some way. However, we can say that there is a finite generating set for every polynomial ideal:

Theorem 4 (Hilbert's basis theorem (relies on Dixon's lemma)) *Every polynomial ideal J is finitely generated.*

Hilbert's basis theorem holds over any noetherian ring, in particular, it hold over every field.

Hilbert's nullstellensatz gave us a criteria for the non-feasibility of a polynomial set of equations: is 1 in the ideal generated by these polynomials? We generalize this question to the *Ideal Membership Question*:

Given $f_1, ..., f_m \in K[\bar{x}]$ and $f_0 \in K[\bar{x}]$ is $f_0 \in (f_1, ..., f_m)$?

Taking $f_0 = 1$ seems to be the hardest setting for this problem, thus implying that nullstellensatz and the IMQ equivalent. However, this turns out not to be the case. To show this, we first state the strong version of the nullstellensatz:

Theorem 5 (Nullstellensatz (strong version)) *Given polynomials $f_0, f_1, ..., f_n \in K[\bar{x}]$, such that f_0 is zero on all common zeros of $f_1, ..., f_m$ then $\exists d$ such that $f_0^d \in (f_1, ..., f_m)$*

Testing this criteria, which is all we need for feasibility, turns out to be significantly easier than IMQ. The difference between the two will stem from the degree bounds we are able to find for the polynomial coefficients placing f_0 (or f_0^d) in $(f_1, ..., f_m)$

Let $\deg f_1, ..., f_m \leq d$ [Hermann26] gave a bound on the degree of the coefficients q_i in the expression $f_0 = \sum q_i \cdot f_i$ that is doubly exponential. If we represent this as a linear system of equations, we can solve it in exponential space. This seems outrageously wasteful, but [Mayr-Meyer82] showed that IMQ is EXPSPACE complete. So we cannot hope to significantly improve this algorithm.

Solving for $f_0^d = \sum q_i \cdot f_i$ allows us to drop one exponent from the degree of the coefficient, thus putting the strong nullstellensatz problem (and the problem of determining the feasibility of a polynomial system of equations) in PSPACE.

$\exists \bar{a}$ such that $f_1(\bar{a}) = ... = f_m(\bar{a}) = 0$ seems like an NP problem, as we can just guess $\bar{a}$. The problem is that we cannot bound the size of $\bar{a}$, even when the coefficients of the polynomials are small (only $0, 1$).

In fact, this approach wasn't proven to give anything until [Koiran96] which showed that, assuming the GRH, the nullstellensatz is in AM$\subseteq \Sigma_2^p$.

In summery:

- IMQ: Groebner basis shows decidability. Linear algebra gives EXPSPACE algorithm. Problem is EXPSPACE-complete.
- Hilbert's nullstellensatz:
  - PSPACE unconditionally
  - AM under GRH
  - NP-hard

6 The basis for groebner basis

Definition 6 (Radical) *The* radical *of an ideal J is defined: $R(J) = \{f \in K[\bar{x}] | \exists d, f^d \in J\}$.*

The radical of an ideal is an ideal.

Definition 7 (Radical ideal) *A* radical ideal *is an ideal that is equal to its radical. So J is a radical ideal iff $J = R(J)$.*

Definition 8 (Variety) *The* variety *of $f_1, ..., f_m$ is defined as $V(\{f_1, ..., f_m\}) = \{\bar{a} \in K^n | f_1(\bar{a}) = ... = f_m(\bar{a}) = 0\}$.*

In the groebner basis method we seek to transform an input set of polynomials $f_1, ..., f_m$ into a set of polynomials $g_1, ..., g_t$ which generate the same ideal but are easier to work with. To motivate, consider the following naive algorithm for IMQ:

If $f_0 = \sum q_i \cdot f_i$ then we can take $f_0(\bmod f_1)$, we would have like if that would have equaled $\sum_{i=2}^m q_i \cdot f_i$. But in general there is no nice notion of a remainder when dividing by multivariate polynomials. For example, when $f_0 = x^2y + y^2x = xy$, $f_1 = xy - 1$ and $f_2 = y^2 - 1$ then $f(\bmod f_1 f_2) = x + y + 1 = 2x + 1$. In the groebner basis method we arrange a basis such that the remainder is unique.

Let $x^a \overset{\text{def}}{=} x_1^{a_1} ... x_n^{a_n}$

Definition 9 (admissible ordering of monomials) *A total ordering on all monomials is an ordering for which holds:*

- $x^a < x^b \Rightarrow \forall d$: $x^a x^d < x^b x^d$.
- $\forall d$: $1 < x^d$.

While any admissible total ordering of the monomials would be fine for our purposes, a couple of popular ones are:

1. Lexicographical ordering: In which we compare x^α and x^β thus: if the first $k-1$ indices agree, $\alpha_i = \beta_i, i \leq k-1$ and the kth differ, we decide based on that index $\alpha_k \leq \beta_k \Rightarrow \alpha \leq \beta$, and the reverse.
2. Graded lexicographical order: in which the order is by the degree of the monomials and ties are broken using lexicographical ordering.

Definition 10 (Leading term of a polynomial) *Fix some admissible ordering of the monomials, the* leading term *of a polynomial $f = \sum c_d x^d$ is defined as $c_d x^d$ for the greatest d for which $c_d \neq 0$. We mark it as $LT(f)$. We also define the* leading monomial*: $LM(f) = x^d$ and the* leading coefficient*: $LC(f) = c_d$*

For an ideal J let $LT(J)$ be all the leading terms of polynomials in J and $(LT(J))$ the ideal generated by the set $LT(J)$.

Definition 11 (Groebner basis) *We call $\{g_1, ..., g_t\}$ a* groebner basis *of J if $(LT(g_1), ..., LT(g_t)) = (LT(J))$ and $g_1, ..., g_t \in J$.*

Implied is that a groebner basis for an ideal is also a basis for that ideal.