6.885 Algebra and Computation November 23, 2005

Lecture 21

Lecturer: Madhu Sudan *Scribe: Michael Manapat*

1 Quantified Statements

Let $\phi : K^n \to \{\mathrm{T}, \mathrm{F}\}$ be a Boolean function defined as follows:

$$\phi(\mathbf{x}_1) = \exists \mathbf{x}_1 \forall \mathbf{x}_2 \exists \mathbf{x}_3 \cdots \mathrm{Q}_w \mathbf{x}_w,$$

Q a quantifier, such that

$$f_i(\mathbf{x}_0, \ldots, \mathbf{x}_w) = 0$$

and

$$g_j(\mathbf{x}_0, \ldots, \mathbf{x}_w) \neq 0$$

for $i, j = 1, \ldots, m$, where the f_i and g_j are polynomials of degree at most d. The goal of this lecture is to show how we can generate polynomaisl $P_1, \ldots, P_m$ such that $\phi(\mathbf{x}_0) = \mathrm{T}$ if and only if $P_i(\mathbf{x}_0) = 0$ for all i. We will assume throughout that the ground field k is algebraically closed (and thus infinite) so, in particular, we will be able to use Hilbert's Nullstellensatz. Note, however, that the result is fairly trivial if k is a finite field since all functions on a finite field are polynomial functions.

We begin with the simple case in which $w = 1$, $g_j = 1$ for all j, and $\mathbf{x}_0 = 0$. Then $\phi(\mathbf{x}_0) = \mathrm{T}$ iff there exists an $\mathbf{x}_1$ such that $f_i(\mathbf{x}_1) = 0$ for $i = 1, \ldots, m$ (where $\mathbf{x}_0$ has been abosrbed into the polynomials f_i). By the Nullstellensatz, this happens if and only if there do not exist polynomials $q_1, \ldots, q_m \in k[\mathbf{x}_1]$ such that $\sum q_i f_i = 1$. There are several results concerning the bounds of these q_i:

- Mayr and Meyer showed that if such q_i's exist, then $q_i\prime$'s with the same property exist and have degrees bounded by d^{n^2}, which puts the "Hilbert Nullstellensatz Problem" in EXPSPACE (since we can find the coefficients of the q_i by solving a linear system in logarithmic space in the size of the linear system).
- Brownawell (87) showed, using complex analysis, that if such q_i's exist, then $q_i\prime$'s with the same property exist and have degree at most $O(md)^n$, putting the problem in PSPACE.
- Kollár (88) and Dubé (92) proved Brownawell's bound using cohomology and elementary commutative algebra (respectively).

Now instead of fixing $\mathbf{x}_0$ to be 0, suppose it is an arbitrary vector $\bar{\alpha}$ in K^n. For that specific vector $\bar{\alpha}$, we can formulate the question as to whether polynomials q_i as above exist as a linear system: namely, we seek a vector $\mathbf{q}$, whose entries are the coefficients of the polynomials q_i, satisfying $M_\alpha \mathbf{q} = \mathrm{e}_1$, where e_1 is the standard basis vector with a 1 in the first entry and zeroes everywhere else. The length of $\mathbf{q}$ and the dimension of $M_{\bar{\alpha}}$ will depend on our bounds for the degrees of the q_i—from what we saw above, the linear system will have dimension $(md)^{n^2}$.

We obtained the matrix $M_{\bar{\alpha}}$ from the coefficients of the polynomials f_i (after α had been absorbed into those coefficients), but we can instead produce a similar matrix M with the formal variable $\mathbf{x}_1$ instead of the constant vector $\bar{\alpha}$. Observe now that the new system $M\mathbf{q} = \mathrm{e}_1$ will have a solution if there is a nonsingular (square) submatrix S extending from the first row. For each such submatrix S, we have a polynomial $P_S(\mathbf{x}_0) = \det(S)$, and thus we can say that there exist q_i's such that $\sum q_i f_i = 1$ if and only if $P_S(\mathbf{x}_0) \neq 0$ for some S. Negating this, we have the following:

For a given $\mathbf{x}_0$, there exists an $\mathbf{x}_1$ such that $f_i(\mathbf{x}_0, \mathbf{x}_1) = 0$ for all i iff for all square submatrices S of M as above, $P_S(\mathbf{x}_0) = \det(S) = 0$.

Now the number of polynomial constraints will be bounded by 2^{D^n}, where D is the degree of the polynomials q_i. By the bounds above, this means that the number of constraints is around $2^{d^{n^2}}$, which is quite large. We can reduce the number of constraints by finding a set of generators for the radical of the ideal generated by the P_S, and we can do this by finding vector space generators for that radical. Now the P_S have degree at most $d \cdot D^n$, so there are at most d^{n^2+1} linearly independent polynomials in the radical ideal, whence we can take the number of polynomial constraints to be less than d^{n^2+1}.

Now that we know how to address the special case above, we can generalize to get a solution for the problem we originally stated. First, if we want to know if there is an $\mathbf{x}_1$ such that $f_j(\mathbf{x}_0, \mathbf{x}_1) = 0$ and $g_j(\mathbf{x}_0, \mathbf{x}_1) \neq 0$ for all j, where the g_j's are no longer trivial, we need only determine if there exist $\mathbf{x}_1$ and y such that $f_j(\mathbf{x}_0, \mathbf{x}_1) = 0$ for all j and

$$1 - y \prod g_j(\mathbf{x}_0, \mathbf{x}_1) = 0.$$

Second, given the quantified statement

$$\exists \mathbf{x}_1 \forall \mathbf{x}_2 \exists \mathbf{x}_3 \cdots \mathrm{Q}_w \mathbf{x}_w,$$

we can produce an equivalent statement with only existential quantifiers by writing the statement above as

$$\exists \mathbf{x}_1 \neg (\exists \mathbf{x}_2 \neg (\cdots)).$$

We can then work our way from the inside out inductively, using the solution for the $w = 1$ case at each step. If v, c, and d denote the original number of variables, the original number of constraints, and the original degree of the polynomials, and the primed v, c, and d the new values after one iteration, we have

- $v\prime \leq v + 1$
- $d\prime \leq d^v$
- $c\prime \leq (cd)^v$.

The only complication arises in how we can (algebraically) express the condition that the polynomials P_i are not all zero: the negation of $P_1(x) = 0, \ldots, P_M(x) = 0$ holds if and only if there exists a y such that

$$\sum p_j(x) y^j \neq 0,$$

which itself holds if and only if there exists a z such that

$$1 - z \left(\sum p_j(x) y^j \right) = 0.$$

After these manipulations, the final collection of polynomials we obtain $P_1, \ldots, P_M$, satisfying the original goals set-forth at the beginning of the lecture, are such that both M and the degrees of the P_i are bounded by d^{n^w} (with big-O's suppressed).

2 Computation over the reals

We briefly state some results on real root-finding:

- There is a nice algorithm for finding the number of roots of a polynomial in an interval $[a, b]$ that uses only field arithmetic (the "Sturm sequence").

- Distinct roots are well-separated (try to show this as an exercise).

The existential theory of the reals consists of questions of the following sort: do there exist $x_1, \ldots, x_n$ such that $P_i(x_1, \ldots, x_n) \geq 0$? Tarski (1950) showed that the existential theory is decidable, and Collins (70), Conway (87), Kozen and Reit (87), and Renegar (92) showed that the existential theory is in PSPACE and that the theory for a constant number of variables is in P.