6.S897 Algebra and Computation April 15, 2015

Lecture 19

Lecturer: Madhu Sudan *Scribe: Luke Schaeffer*

1 Circuits Wrap-up

Let us review the lower bounds we have for algebraic circuits. First, there are results analogous to Shannon's counting argument for boolean circuits. Counting polynomials directly will not work over an infinite field, but slightly more sophisticated techniques can be made to work.

Theorem 1 *There exist degree d polynomials over $\mathbb{C}$ in n variables that require circuits of size $\Omega\binom{n+d}{n}$.*

This is a purely existential result, and does not provide an explicit polynomial. The best bounds we have for specific polynomials are of the form $O(n \log n)$, for instance, for the polynomial

$$\psi(x_1, \ldots, x_n, y_1, \ldots, y_n) = \sum_{i=1}^{n} x_i^n y_i,$$

as we saw earlier.

One can also reduce to low-depth lower bounds. Nisan and Wigderson give a method based on the dimension of a space of partial derivatives of the function. Let $\partial_S f$ denote the partial derivative of a polynomial with respect to a set of variables S. Define $\dim(f)$ to be the dimension of

$$D(f) = \{\partial_S f : S \subseteq \{x_1, \ldots, x_n\}\},$$

the set of partial derivatives with respect to every set of variables (including the empty set!). The dimension is subadditive/submultiplicative in the following sense.

Proposition 2 *For all polynomials $f_1, \ldots, f_r$ and $\alpha \neq 0$,*

$$\dim(\alpha f) = \dim(f),$$
$$\dim\left(\sum_i f_i\right) \leq \sum_i \dim(f_i),$$
$$\dim\left(\prod_i f_i\right) \leq \prod_i \dim(f_i).$$

Proof In the case of αf, observe that $D(\alpha f) = \alpha D(f)$, so the space spanned by $D(\alpha f)$ is identical to the space spanned by $D(f)$ (and so are the dimensions).

The derivative of a sum, $\partial_S \sum_i f_i$, is the sum of the derivatives, $\sum_i \partial_S(f_i)$, and therefore contained in the space spanned by $D(f_1) \cup D(f_2) \cup \cdots \cup D(f_r)$. This space has dimension at most $\sum_i \dim(f_i)$.

Finally, the partial derivative of a product is

$$\partial_S\left(\prod_i f_i\right) = \sum_{S_1 \sqcup \cdots \sqcup S_r = S} \prod_i \partial_{S_i}(f_i),$$

a sum (over all ways to partition the variables in S over the functions) of terms in $D(f_1)D(f_2)\cdots D(f_n)$. Clearly $D(f_1)\cdots D(f_n)$ has dimension at most $\prod_i \dim(f_i)$, completing the proof. ■

In particular, suppose we have a depth 3 circuit (with layers $\Sigma\Pi\Sigma$) computing a polynomial f with multiplication gates of fan-in at most d. Any function g on the bottom layer must be linear, and therefore g has constant derivative (with respect to any non-empty set of variables) or derivative g (with respect to the empty set of variables), so $\dim(g) = 2$. Then the multiplication gates produce functions h with $\dim(h) \leq 2^d$, since the fan-in is d, and each bottom layer gate computes a function of dimension 2. Finally, we conclude that

$$\dim(f) \leq \text{size}(f) \cdot 2^d,$$

since the final layer is the sum of fewer than size(f) second layer gates.

Nisan and Wigderson use this approach to give bounds for the iterated matrix multiplication problem.

Problem 3 (Iterated Matrix Multiplication) *Given m matrices $M_1, \ldots, M_d$ of $n \times n$ as input, compute the upper left entry of their product, $M_1 M_2 \cdots M_d$.*

They show that this problem has a large space of partial derivatives and, under various restricted kinds of circuits, it must have large depth-3 circuits, or deep ($\Omega(\log n \log d)$) circuits.

An alternative approach, proposed by Mulmuley and Sohoni, is geometric complexity theory. The idea is to consider the automorphism group of linear functions preserving a polynomial. That is,

$$\text{Aut}(P) = \{A \in \mathbb{C}^{n \times n} : P(A(x_1, \ldots, x_n)) = P(x_1, \ldots, x_n)\}.$$

For the determinant function, recall that

$$\det(BM) = \det(B)\det(M).$$

For every $B \in \mathbb{C}^{n \times n}$ with determinant 1, there is a corresponding $A \in \mathbb{C}^{n^2 \times n^2}$ in Aut, acting on the n^2 input variables (representing the entries of M) to the determinant, which implements the equivalent of matrix multiplication by B. Hence, $\text{SL}_n(\mathbb{C})$ is a subgroup of Aut(det). On the other hand, the permanent has relatively few symmetries (one can permute the rows and columns of the matrix, but not much else), so

$$\text{Aut(perm)} \cong S_n \times S_n.$$

The hope is that powerful theorems from algebraic geometry and representation theory can be applied to prove lower bounds, but it is currently a struggle to recover known results.

2 Ideal Membership and Strong Nullstellensatz

We have seen that finding roots of polynomials is tractable. What about finding simultaneous roots of several polynomial equations? For instance, what is the complexity of the following problem?

Problem 4 *Given polynomials $f_1, \ldots, f_m, g_1, \ldots, g_n$, does there exist x such that*

$$f_1(x), \ldots, f_m(x) = 0, \text{ and}$$
$$g_1(x), \ldots, g_n(x) \neq 0?$$

Observe that this reduces to checking two parts.

1. There is some common zero of $f_1, \ldots, f_m$. It is known that the polynomials have a common zero if and only if the ideal $I := (f_1, \ldots, f_m)$ generated by the polynomials is nontrivial. The easy direction is that if $1 \in (f_1, \ldots, f_m)$ then

$$1 = f_1 q_1 + \ldots + f_m q_m,$$

and at any common zero we would have $1 = 0$, a contradiction. The converse is a deep result of Hilbert called the weak Nullstellensatz.

2. The product of the g_is is not in the radical of the ideal I. Clearly if the product *is* in the ideal then there can be no solution, since any common zero of $f_1, \ldots, f_m$ is a common zero of the product, and hence a zero of some g_i. Conversely, if for every common zero of $f_1, \ldots, f_m$ there is some g_i which is zero, then the product of the g_is vanishes at every common zero, so

Both of these reduce to some form of the following problem.

Problem 5 (Radical Ideal Membership Problem) *Given polynomials $f_1, \ldots, f_m$ and g, do there exist polynomials $q_1, \ldots, q_m$ and an integer $d > 0$ such that*

$$g^d = \sum_i f_i q_i?$$

In other words, is g in the radical of $(f_1, \ldots, f_m)$?

We can also consider membership in the ideal itself.

Problem 6 (Ideal Membership Problem) *Given polynomials $f_1, \ldots, f_m$ and g, do there exist polynomials $q_1, \ldots, q_m$ such that*

$$g = \sum_i f_i q_i?$$

In other words, is g in $(f_1, \ldots, f_m)$?

The two problems are decidable because there exist effective upper bounds on the degree of the q_i. For instance, for Problem 5 we have the following upper bound.

Theorem 7 *Given polynomials $f_1, \ldots, f_m$ and some $g \in \mathrm{Rad}(f_1, \ldots, f_m)$, there exist polynomials $q_1, \ldots, q_m$ and an integer $d > 0$ such that*

$$g^d = \sum_{i=1}^{m} f_i q_i$$

with $d, \deg(q_1), \ldots, \deg(q_m) \leq D$, where $D = \prod_{j=1}^{m} \deg(f_j)$.

This gives an exponential ($D = 2^{O(n)}$) upper bound on the degree of $q_1, \ldots, q_m$. Now write each q_i as a sum of (at most exponentially many) monomial terms:

$$q_i = \sum_{\mathbf{t} \leq D} a_{i,\mathbf{t}} \mathbf{x}^{\mathbf{t}}.$$

Then the equation $g^d = \sum_{i=1}^{m} f_i q_i$ can be expressed as an exponentially large system of linear equations in the variables $\{a_{i,\mathbf{t}}\}_{i,\mathbf{t}}$. Since we can test whether a linear system has a solution in polylogarithmic space, we can check if the required $q_1, \ldots, q_m$ exist (for each $d \leq D$) using polynomial space. Hence, Problem 5 is in PSPACE. We do not believe it to be PSPACE-complete, since the special case $g = 1$ is known to be in Σ_2^p, assuming the generalized Riemann hypothesis.

On the other hand, Problem 6 is known to be EXPSPACE-complete, as shown by Mayr and Meyer. The same kind of algorithm can be used to show Problem 6 is in EXPSPACE, since we have the following effective upper bound due to Hermann.

Theorem 8 *Given polynomials $f_1, \ldots, f_r$ over variables X, and some $g \in (f_1, \ldots, f_r)$, then there exist polynomials $q_1, \ldots, q_m$ of degree at most*

$$D = \deg(g) + (rd)^{2^{|X|}},$$

such that $g = \sum_{i=1}^{r} f_i q_i$.

In this case, the problem reduces to a doubly-exponential linear system, which we solve in (singly) exponential space.

3 Quantified Theory of $\mathbb{K}$

Assume we are in an algebraically closed field $\mathbb{K}$ for this section. The problem of finding a common zero of polynomials $f_1, \ldots, f_n$ is equivalent to the following logical expression:

$$\exists x_1 \exists x_2 \cdots \exists x_n (f_1(x_1, \ldots, x_n) = 0) \wedge \cdots \wedge (f_r(x_1, \ldots, x_n) = 0)$$

It turns out that this is a special case of a more general problem:

Problem 9 *Suppose $f_1, \ldots, f_r$ are polynomials in variables $x_1, \ldots, x_n$. Given a boolean formula $\psi(z_1, \ldots, z_r)$. Is it the case that*

$$\exists x_1 \forall x_2 \cdots Q_n x_n \quad \psi(f_1(x_1, \ldots, x_n) = 0, \ldots, f_r(x_1, \ldots, x_n) = 0)?$$

This problem is decidable.

Furthermore, if some of the variables are left unquantified, e.g.,

$$\exists x_1 \forall x_2 \cdots Q_n x_n \quad \psi(f_1(x_1, \ldots, x_n, y_1, \ldots, y_k) = 0, \ldots, f_r(x_1, \ldots, x_n, y_1, \ldots, y_k) = 0)$$

then the result, $\Phi(y_1, \ldots, y_k)$, depends on $y_1, \ldots, y_k$. Surprisingly, Φ is itself of the form

$$\exists y_1 \cdots \exists y_k \phi(q_1(y_1, \ldots, y_k), \ldots, q_N(y_1, \ldots, y_k)),$$

for polynomials $q_1, \ldots, q_N$ in k variables, and where ϕ is a boolean formula.