Lecture 19: Arithmetic Circuits

Anup Rao

June 3, 2020

Given the difficulty of proving lower bounds on boolean circuits, we have been studying boolean circuits with some restrictions. So far, we have talked about formulas (which restrict the circuit to be a tree), ACo (where the number of alternations is bounded) and monotone circuits (where there are no negations). Today, we discuss another model, the model of arithmetic circuits.

An arithmetic circuit is just like a normal circuit, except that each gate computes either the sum or product of its inputs, and outputs the corresponding integer. We allow arbitrary constants to be plugged in as inputs as well. So far, the model is the same as boolean circuits, since when computing $f : \{0,1\}^n \to \{0,1\}$, every arithmetic circuit can be converted into a boolean circuit and vica versa, without changing the size by too much.

One can view the circuits as operating over any field, but here we work over the real numbers.

The key difference is that we shall think of the circuit as computing a formal multivariate polynomial $f(X)$. We require that the polynomial corresponding to the output gate is the correct one, which is much stronger than asking for the output to be correct on boolean inputs.

The product of two bits is the same as the AND of two bits. The sum may be an integer, but it is enough to carry out the computation modulo 2, so this can also be simulated by a boolean circuit.

Monotone Lower bound for Permanent

We start by proving a lower bound for computing the permanent of a matrix. Recall that the permanent is the polynomial

$$\mathsf{PERM}(X) = \sum_{\sigma} \prod_{i=1}^{n} X_{i,\sigma(i)},$$

where the sum is taken over all permuatations $\sigma : \{1,2,\ldots,n\} \to \{1,2,\ldots,n\}$.

We prove the following theorem:

Theorem 1. *If an arithmetic circuit computes the permanent over the reals, and it does not use any negative constants, then its size must be at least* $\binom{n}{n/3} \geq 2^{\Omega(n)}$.

The proof has two steps. In the first step, we show the following claim:

Lemma 2. *If* $\mathsf{PERM}(X)$ *can be computed by a circuit of size* s *with no negative constants, then we can express*

$$\mathsf{PERM}(X) = \sum_{j=1}^{s} u_j(X) \cdot v_j(X),$$

where here the degree of each $u_j(X)$ *is in between* $n/3$ *and* $2n/3$*, and all coefficients are non-negative.*

Let us start by showing how to use the lemma to complete the proof. Consider a particular pair $u_j(X), v_j(X)$. Since all the coefficients in these polynomials are non-negative, the set of monomial in the product $u_j(X)v_j(X)$ must be a subset of the monomials in the permanent. Say that monomial touches a row if it contains a variable from the row. For each monomial in $u_j(X)$, the set of rows touched by this monomial must be the complement of the set of rows touched by $v_j(X)$, and the same holds for the columns. The only way this can happen is if there are k rows A and k columns B such that u_j only touches the rows and columns corresponding to A, B, and v_j touches the rows and columns corresponding to the complementary rows and columns. Moreover, by the lemma, we must have that $n/3 \leq k \leq 2n/3$.

This means that the total number of monomials contributed by $u_j(X)v_j(X)$ is at most

$$k! \cdot (n-k)! = n! / \binom{n}{k} \leq n! / \binom{n}{n/3}.$$

Since the permanent has $n!$ monomials, we conclude that $s \geq \binom{n}{n/3}$.

It only remains to prove the lemma.

Proof The proof has a similar idea to something you did in your homework. Let $g_0, g_1, \ldots$ be a sequence of gates in the circuit, where g_0 is the output gate, and g_i is the input to g_{i-1} of maximal degree. The degrees of the polynomials in this sequence can only decrease by a factor of two in each step, and the degree of the input variables is 1, so at some point, there must be a gate g_i whose degree is $\geq 2n/3$, and yet g_{i+1} has degree in between $n/3$ and $2n/3$.

Now if we substitute a new variable Y for g_i in the circuit, the output gate must be a new polynomial $f(X, Y)$ whose degree in Y can be at most 1, since Y corresponds to a gate of degree $\geq 2n/3$. So, we can write $\mathsf{PERM}(X) = a(X) + b(X).g_i(X) = a(X) + b(X)b'(X)g_{i+1}(X)$. Let $u_1(X) = g_{i+1}(X)$, $v_1(X) = b(X)b'(X)$. If we substitute $Y = 0$ in $f(X, Y)$, we get $f(X, 0) = a(X)$, and $a(X)$ can be computed by an arithmetic circuit of size $s - 1$. So, proceeding inductively, we obtain that $\mathsf{PERM}(X) = \sum_{j=1}^{s} u_j(X)v_j(X)$ as required.

■