# Lecture 9. Circuit Complexity

From this lecture we start to prove lower bounds in the circuit model. As we said, the task is too hard for general circuits. So people studied special types of circuits. One important class contains circuits with small depth.

Recall that a circuit is a DAG with each node associated with a gate that computes a basic function, such as AND, OR and NOT. The fanin of a gate can be arbitrary. (Namely, the AND and OR gates are not just binary.) We will draw a circuit in the top-down manner, s.t. the output gate is the top layer and gates in the bottom layer connect to the input variables.

## Depth 2: DNF and CNF

This section considers depth-2 circuits. If the top gate is AND, then the circuit is essentially a CNF or DNF. Recall:

CNF (conjunctive normal form): , where each is either a variable or the negation of a variable. Each is called a *literal*, and each is a called a *clause*.

DNF (Disjunctive normal form): , where each is a *literal*, and each is a called a *monomial*.

Any function can be written as a CNF and DNF. (Convince yourself.) We’d like to find an explicit function s.t. if we write it as a CNF or DNF, then the number of clauses/monomials is very large. Such a function is not hard to find, actually the Parity function serves as such an example. (Recall: .)

**Theorem 1.1**. Any depth-2 circuit that computes Parity needs at least gates.

Can you figure out a proof? (It’s not complicated; only one or two lines. And it’ll be used later.)

## Depth 3

Now we consider depth-3 circuits. If the top gate of a circuit is AND, then we call it a -circuit.

Let’s first prove that if the circuit has a small top fanin, then it has to have a large size.

**Theorem 2.1**. ([Tsa01]) If a -circuit computing the Parity function has fanout 1 and top fanin , then it has at least AND gates at the bottom layer.

*Proof*. The idea is to switch the AND and OR of the two top layers using de Morgan rule, and then the problem is reduced to the depth 2 case. Suppose that the i-th OR gate on the middle layer has fanin . Let be the -th AND of the -th OR gate of the top AND gate. Use de Morgan rule, we can change the depth-3 circuit to a depth-2 one, which has the top gate OR with fanin . Note that each AND can accept at most one input, so . Since each gate has fanout 1, the number of AND dates at the bottom layer is

From the bound, you can see that when *t* is large, then we need new method. Next we introduce the *k*-limit method.

Suppose that and . An input is a *lower k-limit* *for B* if for any , there is an input s.t. and . Recall that means each .

We will use the concept to prove an exponential lower bound for (the negation of) Majority. Formally, define

The result was proved in [HJP95].

**Theorem 2.2**. Any -circuit computing the function needs fanout.

*Proof*. The parameters in the following proof:

Solving it gives the following approximation:

We need to define two sets:

Now we’ll take three steps:

1. Set variables to be 1, s.t. after this, each bottom AND gate has at most *k* negated variables. Then we are left with a function with  
      
   (We will use Lemma 2.3 to prove this.)
2. Infer that there is an OR gate in the middle level s.t.   
    has , and does not have a lower *k*-limit in *A*.  
   (We will use Lemma 2.4 to prove this.)
3. Conclude that , and thus .  
   (We will use Lemma 2.5 to prove this.)

Next we prove the three lemmas needed, and show how to use them in the above proof of Theorem 2.2.

**Lemma 2.3**. If has , then there is a with to intersect all .

*Proof*. Since each has size more than *k*, at least one belong to at least fraction of sets in *F*. Put it in T. Remove those sets containing . This leaves fraction of *F*. Continue this. We claim that steps kill all . Indeed,

canceling the upper bound of in the assumption of the lemma.

To use this lemma, we take *F* to be the collection of bottom AND gates with more than *k* negated variables. By the lemma, there is a intersecting all of them. Set all variables in T to be 1, then these AND gates are eliminated. Thus each of the remaining AND gates contains at most *k* negated variables.

**Lemma 2.4**. Suppose that we have a -circuit computing , with top fanin at most and each bottom AND gate having at most *k* negated variables. Then there is an OR gate in the middle level s.t. the set

has

and does not have any lower *k*-limit in *A*.

*Proof*. Recall the set

.

Note that . Since the top gate is AND, there is at least one OR gate in the middle level evaluating to 0 for inputs in *B*. Thus there is an OR gate s.t.

Suppose the set has a lower k-limit , namely and for any , there is an input s.t. . Consider each AND gate *h* feeding in :

We claim that . Indeed, since , there is an or an . If the former, then and thus . If the latter, then since , we also have , which again implies that .

Since this holds for each *h*, we know that as well, violating the assumption that .

**Lemma 2.5**. For any set with , there is a lower *k*-limit for .

Proof. Induction on .

: is a lower *k*-limit for . First, it is lower to any other vector, namely for any *x*. Second, for any with , since when , we have some element s.t. the only 1 in *x* is not in . This element serves the lower k-limit definition.

Assuming , consider : If is not a lower *k*-limit for , then there is a set with s.t. every has at least one 1 in . Take the most “popular” at which at least fraction of have 1 at *i*-th position. Call the set of these elements . Flip these 1 to 0 and call the resulting set , then they each have ones. Note that . Use induction hypothesis to get a with less than ones s.t. *y* is lower *k*-limit for . Note that since *y* is lower than an element in . Flip to 1, and this element since . We claim that this is a lower *k*-limit for . The “lower” part is easy. For the “*k*-limit” part: for any with , there is a with and . Note that flipping the i-th bit from 0 to 1 makes to , and also make to . This implies that where is the string obtained from *x* by flipping the *i*-th bit. Note that . Thus is a lower k-limit for .

After the second step of the proof of Theorem 2.2, we get a set with , and does not have a lower *k*-limit in *A*. Thus by the above lemma, we know that .

## References

[Tsa01] Shi-Chun Tsai, **A depth 3 circuit lower bound for the parity function,** *Journal of Information Science and Engineering* 17(5), 857–860, 2001.

[HJP95] J. Hastad, S. Jukna, and P. Pudlak, **Top-down lower bounds for depth-three circuits**, *Computational Complexity* 5, 99–112, 1995.