PRINCETON UNIVERSITY COS 522: COMPUTATIONAL COMPLEXITY

Lecture 20: Circuit Lower Bounds Using Multiparty Communication Complexity

Lecturer: *Sanjeev Arora* Scribe:*Iannis Tourlakis*

We begin by defining some new circuit complexity classes which lie on the "frontier" of classes for which we can prove separations. Results known for such classes will be given. Next we will define multi-party communication and give its connection to circuit complexity.

1 Circuits With "Counters"

DEFINITION 1 *A language L is in* $\mathbf{ACC}^0$ *if there exists a circuit family $\{C_n\}$ with constant depth and polynomial size (and unbounded fan-in) consisting of $\wedge$, $\vee$, $\neg$ and* $\bmod m_1, \ldots, \bmod m_k$ *gates accepting L.*

Note that the number k of different moduli in the above definition is constant. It will be convenient to have a notation that indicates precisely the moduli allowed in an $\mathbf{ACC}^0$ family. To that end, let $\mathbf{ACC}^0(q)$ indicate the class of languages accepted by $\mathbf{ACC}^0$ circuits where all the mod gates have modulo q.

We do have some lower bounds for $\mathbf{ACC}^0(q)$ circuits when q is a prime:

THEOREM 1 (RAZBOROV,SMOLENSKY)
For distinct primes p and q, the function $\bmod p$ *is not in* $\mathbf{ACC}^0(q)$.

However, when q is not a prime (a prime power, to be exact) we reach the limits of our knowledge. Indeed it is consistent with current knowledge that the majority of n bits —to give one example— can be computed by linear size circuits of constant depth consisting entirely of $\bmod 6$ gates. The "high-level" reason for why the proof of Theorem 1 does not work in the $\bmod 6$ case is that the proof relies on polynomial representations of $\mathbf{ACC}^0$ circuits: in this representation, polynomials $\bmod 6$ seem to have surprising power.

Frontier 1: Is Clique in $\mathbf{ACC}^0(6)$?

It is worth noting that Theorem 1 concerns *non-uniform* circuits. Moreover, in the (weaker) uniform case some fairly strong lower bounds are known: Allender and Gore have shown that a decision version of the Permanent (and hence the Permanent itself) requires exponential size "Dlogtime-uniform" $\mathbf{ACC}^0$ circuits. (A circuit family $\{C_n\}$ is *Dlogtime uniform* if there exists a deterministic Turing machine M that given a triple (n, g, h) determines in linear time —i.e., $O(\log n)$ time when $g, h \leq \text{poly}(n)$— what types of gates g and h are and whether g is h's parent in C_n.)

Let us return again to the nonuniform $\mathbf{ACC}^0$. Let a *symmetric* gate be a gate whose output depends only on the number of inputs that are 1. For example, majority and mod gates are symmetric. Yao has shown that $\mathbf{ACC}^0$ circuits can be simplified to give an equivalenet depth 2 circuits with a symmetric gate at the output (figure 1). Beigel and Tarui subsequently improved Yao's result:

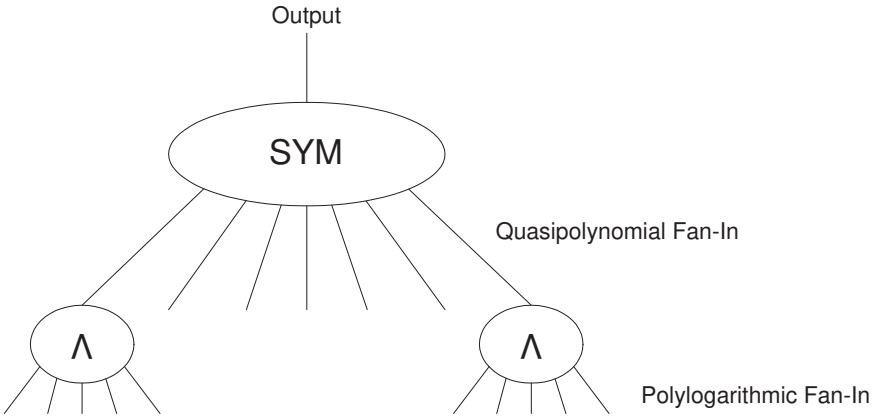

Figure 1: The depth 2 circuit with a symmetric output gate from Theorem 2.

Theorem 2 (Yao, Beigel and Tarui)
If $f \in \mathbf{ACC}^0$, then f can be computed by a depth 2 circuit C with a symmetric gate with quasipolynomial (i.e., $2^{\log^k n}$) fan-in at the output level and $\vee$ gates with polylogarithmic fan-in at the input level.

We will revisit this theorem below in section 4.

2 Linear Circuits With Logarithmic Depth

In this section concentrate on circuits with *bounded* fan-in in contrast to the previous section. To that end, consider the question of finding an explicit function $f : \{0,1\}^n \to \{0,1\}$ that cannot be computed by bounded fan-in circuits of linear size and logarithmic depth. (Note that by counting one can easily show that *some* function on n bits requires superpolynomial size circuits and hence bounded fan-in circuits with more than logarithmic depth).

Frontier 2: Find an explicit function that cannot be computed by circuits of linear size and logarithmic depth.

Valiant thought about this problem in the '70s. His initial candidates for lowerbounds boiled down to showing that a certain graph called a *superconcentrator* needed to have superlinear size. He failed to prove thisand instead ended up proving that such superconcentrators do exist!

Another sideproduct of Valiant's investigations was the following important lemma concerning depth-reduction for such circuits.

Lemma 3 (Valiant)
In any circuit with m edges and depth d, there are $km/\log d$ edges whose removal leaves a circuit with depth at most $d/2^{k-1}$.

This lemma can be applied as follows. Suppose we have a circuit C of depth $c \log n$ with n inputs $\{x_1, \ldots, x_n\}$ and n outputs $\{y_1, \ldots, y_n\}$, and suppose $2^k \sim c/\epsilon$ where $\epsilon > 0$ is

arbitrarily small. Removing $O(n/\log\log n)$ edges from C then results in a circuit with depth at most $\epsilon \log n$. But then, since C has *bounded* fan-in, we must have that each output y_i is connected to at most $2^{\epsilon \log n} = n^\epsilon$ inputs. So each output y_i in C is completely determined by n^ϵ inputs and the values of the omitted edges. So we have a "dense" encoding for the function $f_i(x_1, \ldots, x_n) = y_i$. We do not expect this to be the case for any reasonably difficult function.

3 Multiparty Communication Protocols

Multiparty communication games can be used to model some circuit classes. The model of multiparty communication that we use is the "number on the forehead" model (found for example in math puzzles that involve people in a room, each person having a bit on their head). More concretely, when trying to compute $f(x_1, \ldots, x_k)$, $x_i \in \{0,1\}^n$ for some function f, the communicating parties have as input the x_i's where the ith party can see all the x_j such that $j \neq i$. The parties have a protocol for communicating where all communication is posted on a "public blackboard". At the end of the protocol all parties must know $f(x_1, \ldots, x_k)$.

In the 2-party model we introduced the notion of a monochromatic rectangles in order to prove lower bounds. For proving lower bounds in the multiparty model we have the notion of cylinder intersections. A *cylinder in dimension i* is a subset S of the inputs such that if $(x_1, \ldots, x_k) \in S$ then for all x_i' we have that $(x_1, \ldots, x_{i-1}, x_i', x_{i+1}, \ldots, x_k) \in S$ also. A *cylinder intersection* is simply an intersection of cylinders. So, similarly to the 2-party case, if f has a multiparty protocol that communicates c bits, then its matrix has a tiling using at most 2^c monochromatic cylinder intersections.

EXAMPLE 1 Consider computing in the 3-party model the function $f(x_1, x_2, x_3) = \bigoplus_{i=1}^n \mathrm{maj}(x_{1i}, x_{2i}, x_{3i})$ where the x_i are n bits number. The communication complexity of this function is 3: each player counts the number of i's such that she can determine the majority of x_{1i}, x_{2i}, x_{3i} by examining the bits available to her. She writes the parity of this number on the blackboard, and the final answer is the parity of the players' bits. This protocol is correct because the majority for each row is known by either 1 or 3 players.

EXAMPLE 2 Consider computing the generalized inner product $f(x_1, \ldots, x_k) = \bigoplus_{i=1}^n \bigwedge(x_{1i}, x_{2i}, x_{3i})$. There is a multiparty protocol with communication complexity $n/2^k$. Babai, Nisan and Szegedy (1989) have shown a lower bound of $n/4^k$ bits of communication for this problem.

4 Tying Everything Together

In this section we show how to reduce the problem of computing lower bounds for $\mathbf{ACC}^0$ circuits and for linear size logarithmic depth circuits to communication complexity questions using the machinery developed in the previous sections.

4.1 $\mathbf{ACC}^0$ Circuits

Suppose $f(x_1, \ldots, x_k)$ has a depth-2 circuit with a symmetric gate with fan-in N at the output and $\wedge$ gates with fan-in $k-1$ at the input level (figure 2). The claim is that f's

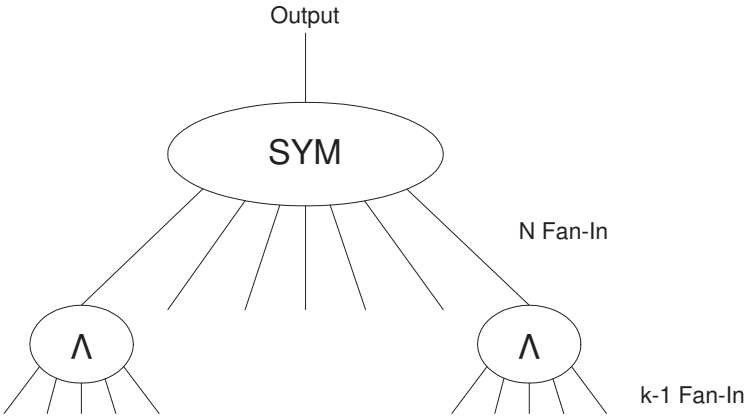

Figure 2: If f is computed by the above circuit, then f has a k-party protocol of complexity $k \log N$.

k-party communication complexity is at most $k \log N$. To see the claim, first partition the $\wedge$ gates amongst the players. Each bit is not known to exactly one player, so the input bits of each $\wedge$ gate are known to at least one player; assign the gate to such a player with the lowest index. Players then broadcast how many of their gates output 1. Since this number has at most $\log N$ bits, the claim follows.

Our hope is to employ this connection with communication complexity in conjunction with Theorem 2 to obtain lower bounds on $\mathbf{ACC}^0$ circuits. For example, note that the function in Example 2 above cannot have $k < \log n/4$. However, this is not enough to obtain a lower bound on $\mathbf{ACC}^0$ circuits since we need to show that k is not polylogarithmic to employ Theorem 2. Thus a strengthening of the Babai Nisan Szegedy lowerbound to $\Omega(n/\text{poly}(k))$ for say the CLIQUE function would close Frontier 1.

4.2 Linear Size Logarithmic Depth Circuits

Suppose that $f : \{0,1\}^n \times \{0,1\}^{\log n} \to \{0,1\}^n$ has bounded fan-in circuits of linear size and logarithmic depth. If $f(x,j,i)$ denotes the ith bit of $f(x,j)$, then Valiant's Lemma implies that $f(x,j,i)$ has a simultaneous 3-party protocol—that is, a protocol where all parties speak only once and write simultaneously on the blackboard (i.e., non-adaptively)—where,

- (x,j) player sends $n/\log\log n$ bits;
- (x,i) player sends n^ϵ bits; and
- (i,j) player sends $O(\log n)$ bits.

So, if we can show that a function does not have such a protocol, then we would have a lower bound for the function on linear size logarithmic depth circuits with bounded fan-in.

Conjecture: The function $f(x,j,i) = x_{j \oplus i}$, where $j \oplus i$ is the bitwise xor, is conjectured to be hard, i.e., f should not have a compact representation.