Recent advances in Complexity CIS 6930/CIS 4930 October 3, 2002

Lecture 12

Lecturer: Dr. Meera Sitharam Scribe: Erwin Jansen

Today Zia finished part 3 of his talk.

Depth Complexity

Definition 1 (Depth Complexity). *For a function f, the depth complexity $d(f)$ is the minimum depth of a circuit computing f. The depth of a circuit C is denoted by $d(C)$.*

Definition 2. *For a boolean function $f : \{0,1\}^n \to \{0,1\}$, let $X = f^{-1}(1)$ (i.e. the set of all x's such that $f(x) = 1$) and $Y = f^{-1}(0)$. Let $R_f \subseteq X \times Y \times \{1, ..., n\}$ consist of all triples (x, y, i) such that $x_i \neq y_i$.*

Notice that there is always an i such that (x, y, i) satisfies the relation R_f since $f(x) = 1$ and $f(y) = 0$, and so $x \neq y$.

Communication Problem

Definition 3 (Communication Problem). *The communication problem for R_f is the following: Alice is given $x \in X$, Bob is given $y \in Y$ and their task is to find some $i \in \{1, ..., n\}$ such that $(x, y, i) \in R_f$.*

The definition of a protocol as was given in the previous lecture remains unchanged. Based upon these definitions we can define the communication complexity as follows:

Communication Complexity

Definition 4 (Communication Complexity). *A protocol $\mathcal{P}$ computes R_f if for every input $(x, y) \in X \times Y = f^{-1}(1) \times f^{-1}(0)$, the protocol reaches a leaf labeled by some $i \in \{1, ..., n\}$ such that $(x, y, i) \in R_f$. The deterministic communication complexity of R_f denoted $D(R_f)$, is the minimum cost of $\mathcal{P}$ over all protocols $\mathcal{P}$ that compute R_f.*

Monochromatic Rectangle

Definition 5 (Monochromatic Rectangle). *The set $A \times B \subseteq X \times Y = f^{-1}(1) \times f^{-1}(0)$ is an R_f-monochromatic rectangle if there exists an $i \in \{1, ..., n\}$ such that for every $(x, y) \in A \times B$, we have $(x, y, i) \in R_f$.*

Proposition 6. *Any depth t protocol that computes the relation R_f induces a partition $X \times Y = f^{-1}(1) \times f^{-1}(0)$ into at most 2^t R_f-monochromatic rectangles.*

Proof. The same as the proof for functions given in the previous lecture, mutatis mutandis □

Lemma 7. *For every circuit C for f, there is a corresponding protocol $\mathcal{P}$ for R_f such that the depth of $\mathcal{P}$ is at most $d(C)$, i.e., at most $d(C)$ bits are exchanged during the run of $\mathcal{P}$*

Proof. Given a circuit C computing f, the idea of the protocol $\mathcal{P}$ for R_f is the following: Alice knows $x \in f^{-1}(1)$ whereas Bob knows $y \in f^{-1}(0)$. Alice and Bob traverse the nodes of C, starting from the output node, and they continue toward the input nodes in such a way as to maintain an invariant, namely that the function g computed by the current node satisfies $g(x) = 1$ and $g(y) = 0$. We will now show that Alice (who only knows x) and Bob (who only knows y) can indeed traverse C in a way that maintains the above invariant.

Since $x \in X = f^{-1}(1)$ and $y \in Y = f^{-1}(0)$, the invariant is true at the output node of C. Now suppose that the current node reached by Alice and Bob is an $\vee$ gate computing a function g, and the invariant is true at this $\vee$ gate, i.e., that $g(x) = 1$ and $g(y) = 0$. Let g_1 and g_2 be the functions corresponding to the nodes of C entering the current $\vee$ node. Then $g = g_1 \vee g_2$. Since $g(y) = 0$, we have $g_1(y) = g_2(y)$. And since $g(x) = 1$, either $g_1(x) = 1$ or $g_2(x) = 1$ (or both). Alice, who knows x and g_1 and g_2 (since she obviously knows C), sends a single bit to Bob indicating for which $i \in \{1, 2\}$ the function $g_i(x) = 1$. In the case where both are 1 she chooses g_1. They then both proceed to the corresponding node, where the invariant clearly holds.

Symmetrically, if the current node is an $\wedge$ gate computing a function g such that $g(x) = 1$ and $g(y) = 0$, and g_1 and g_2 are the functions corresponding to the nodes entering the current $\wedge$ node, then $g = g_1 \wedge g_2$, and so $g_1(x) = g_2(x) = 1$, while either $g_1(y) = 0$ or $g_2(y) = 0$ (or both). This time Bob sends a single bit indicating for which $i \in \{1, 2\}$ the function $g_i(y) = 0$, and the both proceed to the corresponding node.

Now suppose Alice and Bob have reached an input node of C. Assuming f is a function of the variables $z_1, ..., z_n$, this input node is labeled with z_i or $\neg z_i$ for some $i \in \{1, ..., n\}$. We claim that both players know that i is a correct output, i.e., that $(x, y, i) \in R_f$. To see this, let g be the function computed by this input node. If the node is labeled z_i than by the invariant, we have $g(x) = 1$ an d $g(y) = 0$. But $g(y) = y_i$. Hence $x_i \neq y_i$; and so $(x, y, i) \in R_f$. Similarly, if the input node is labeled $\neg z_i$, then by the invariant, $g(x) = 1$ and $g(y) = 0$ once again. But this time $g(x) = \neg x_i$ and $g(y) = \neg y_i$, and we hence $x_i = 0$ and $y_i = 1$. So in this case we have $x_i \neq y_i$ as well, and hence $(x, y, i) \in R_f$. □

Lemma 8. *For every protocol $\mathcal{P}$ for R_f, there is a corresponding circuit C for f such that $d(C)$ is the depth of $\mathcal{P}$, i.e. the communication complexity $\mathcal{P}$*

Proof. Given a protocol $\mathcal{P}$ for R_f, we will convert this binary tree $\mathcal{P}$ into a circuit C as follows: Each internal node in which Alice speaks (i.e., a node labeled by a function with domain X) is labeled by $\vee$ and each internal node in which Bob speaks is labeled by $\wedge$. As for the leaves of $\mathcal{P}$, by proposition 6, each leaf is an R_f-monochromatic rectangle $A \times B$ with which an output i is associated. Take any $x \in A$ and let $x_i = \psi$. Then since for all $y \in B$, the value i is a legal output on (x, y) for $\mathcal{P}$, we must have $y_i = \neg\psi$ for all $y \in B$. This in turn implies $x_i = \psi$ for every $x \in A$. Therefore either:

1. $\forall_{x \in A} \forall_{y \in B} \langle x_i = 1 \wedge y_i = 0 \rangle$
2. $\forall_{x \in A} \forall_{y \in B} \langle x_i = 0 \wedge y_i = 1 \rangle$

In the first case we label the leaf by z_i whereas in the second case we label the leaf by $\neg z_i$.

Clearly the depth of C equals the depth of $\mathcal{P}$. It remains to prove that C computes f. We claim that for every node of C, the function g corresponding to that node satisfies:

$$\forall_{z \in A} \forall_{z' \in B} \langle g(z) = 1 \wedge g(z') = 0 \rangle$$

where $A \times B$ are the inputs that reach the corresponding node of $\mathcal{P}$. This immediately implies that the function computed by the output node of C (i.e., the function computed by C) is 1 for all $z \in X = f^{-1}(1)$ and 0 for all $z \in Y = f^{-1}(0)$. Hence C computes f.

The claim is proved by induction, starting from the input nodes of C and moving toward the output node of C. The claim is true for the input nodes because of the way in which these input nodes were labeled. Now consider an internal node w of V computing a function g such that the claim is true for its two children computing the functions g_1 and g_2 respectively4. Let $A \times B$ be the inputs reaching this node w in $\mathcal{P}$. Assume without loss of generality, that Alice speaks in this node. (The case for Bob is similar). Tat means w is labeled by $\vee$ in C, i.e., $g = g_1 \vee g_2$. In $\mathcal{P}$, since Alice speaks at w, this entails a partitioning of A into A_1 and A_2, where the inputs in A_1 travel to the left subtree of $\mathcal{P}$ and those in A_2 travel to the right subtree. By the induction hypothesis, for all $y \in B$ we have $g_1(y) = g_2(y) = 0$, and for all $x \in A_1$ we have $g_1(x) = 1$, while for all $x \in A_2$, we have $g_2(x) = 1$. Hence for all $y \in B, g(y{=}g_1(y) \vee g_2(y) = 0$, and for all $x \in A = A_1 \cup A_2$, we have $g(x) = g_1(x) \vee g_2(x) = 1$. □

Theorem 9. *For ever $f : \{0,1\}^n \rightarrow \{0,1\}$, we have $d(f) = D(R_f)$.*

Proof. Applying lemma 7 to the circuit C^* with minimal depth that compute f, we see that there exists a protocol $\mathcal{P}$ for R_f such that the depth of $\mathcal{P} \leq d(C^*) = d(f)$. Hence $D(R_f) \leq d(f)$. Apply lemma 8 to the protocol $\mathcal{P}^*$ with minimal depth for R_f, we see that there exists a circuit C for f such that $d(C) =$ depth of $\mathcal{P}^* = D(R_f)$. Hence $d(f) \leq D(R_f)$. □