IAS/Park City Mathematics Series
Volume 3, 1993

Circuit and Communication Complexity

Ran Raz

LECTURE 8
Lower bound for $FORK$ (continued)

In the previous lecture, we have made two simple observations about $CC(\alpha, l)$.

Lemma 8.0.1. For any α, l, if $CC(\alpha, l) > 0$ then

$$CC(\alpha, l) \geq CC(\tfrac{\alpha}{2}, l) + 1.$$

Lemma 8.0.2. For any l and any $\alpha > 1/w$,

$$CC(\alpha, l) > 0.$$

Each application of Lemma 8.0.1 reduces the density α by a factor of 2. By Lemma 8.0.2, if we start from density $\alpha = 1$ we can apply Lemma 8.0.1 $\log_2(w)$ times, and obtain a lower bound of $\log_2(w)$ for $CC(1, l)$. After $\log_2(w)$ applications of Lemma 8.0.1, the density is too small and we cannot apply Lemma 8.0.1 any longer. To prove a stronger lower bound, we will need a mechanism to increase the density α.

8.1. Increasing the Density

The following lemma (which is the main lemma in the proof of the lower bound) shows how to increase the density from α to $\sqrt{\alpha}/2$, by reducing the length of the paths from l to $l/2$. In other words, the lemma shows that if there exists a protocol that works on a set of density α of paths of length l then there exists a protocol (with the same communication complexity) that works on a set of density $\sqrt{\alpha}/2$ of

[1]Faculty of Mathematics and Computer Science, The Weizmann Institute of Science, Rehovot 76100, Israel.
E-mail address: `ranraz@wisdom.weizmann.ac.il`.

July 21, 2000

Based on lecture notes taken by Dana Fisman, Nir Piterman and Yoad Lustig.

paths of length $l/2$. Note that if $\alpha < 1/4$ then $\sqrt{\alpha}/2$ is larger than α. If α is very small then $\sqrt{\alpha}/2$ is significantly larger than α. We can hence increase the density, while paying by reducing the length of the paths.

Lemma 8.1.1. (Main Lemma): For any (even) $l > 0$ and any $\alpha \geq 16/w$,

$$CC(\alpha, l) \geq CC(\tfrac{\sqrt{\alpha}}{2}, \tfrac{l}{2}).$$

Let us first show how to use Lemma 8.1.1 to prove the stronger lower bound for $FORK$. Intuitively, we apply Lemma 8.0.1 $O(\log(w))$ times, until the density gets close to $16/w$. We then apply Lemma 8.1.1 one time and obtain density larger than $2/\sqrt{w}$, while the length of the paths is reduced by a factor of 2. We can repeat the process $O(\log(l))$ times, until the length of the paths is 1. Altogether, we have applied Lemma 8.0.1 $O(\log(l) \cdot \log(w))$ times, and hence we get a lower bound of $\Omega(\log(l) \cdot \log(w))$ for $CC(1, l)$. More formally, by $O(\log(w))$ applications of Lemma 8.0.1 and one application of Lemma 8.1.1, we obtain that for any (even) l,

$$CC(\tfrac{2}{\sqrt{w}}, l) \geq CC(\tfrac{16}{w}, l) + \Omega(\log(w)) \geq CC(\tfrac{2}{\sqrt{w}}, \tfrac{l}{2}) + \Omega(\log(w)).$$

Applying the last inequality $O(\log(l))$ times, we obtain

$$CC(\tfrac{2}{\sqrt{w}}, l) \geq CC(\tfrac{2}{\sqrt{w}}, 1) + \Omega(\log(l)) \cdot \Omega(\log(w)) \geq \Omega(\log(l) \cdot \log(w)).$$

Hence,

$$CC(FORK) = CC(1, l) \geq CC(\tfrac{2}{\sqrt{w}}, l) = \Omega(\log(l) \cdot \log(w)).$$

Recall that this lower bound is tight.

8.2. Combinatorial Claim

For the proof of Lemma 8.1.1, we will need the following simple claim.

Claim 8.2.1. Consider an $N \times N$ matrix of zeros and ones. Denote by α the fraction of ones in the matrix and by α_i the fraction of ones in the i^{th} row of the matrix. We say that a row i is dense if $\alpha_i \geq \alpha/2$. Then, at least one of the following holds.

(1) There exists a row i, such that, $\alpha_i \geq \sqrt{\alpha/2}$.
(2) The number of dense rows is at least $\sqrt{\alpha/2} \cdot N$.

Proof. The proof follows by counting the number of ones in the matrix. Assume for a contradiction that none of the above two possibilities holds. Since the second possibility does not hold, there are less than $\sqrt{\alpha/2} \cdot N$ dense rows. Since the first possibility does not hold, each of these rows contains less than $\sqrt{\alpha/2} \cdot N$ ones. Hence, the total number of ones in all the dense rows is less than $(\alpha/2) \cdot N^2$. Every non-dense row contains less than $(\alpha/2) \cdot N$ ones, and there are at most N non-dense rows. Hence, the total number of ones in all the non-dense rows is less than $(\alpha/2) \cdot N^2$. Thus, the total fraction of ones in the matrix is less than α. ■

Intuitively, Claim 8.2.1 states that either, one of the rows is very dense, or, there are a lot of dense rows.

8.3. Proof of The Main Lemma

Proof. (Of Lemma 8.1.1)
Given an (α, l)-protocol, we will show the existence of a $(\sqrt{\alpha}/2, l/2)$-protocol (with the same communication complexity). Let P be an (α, l)-protocol that works on a set $S \subset [w]^l$, such that, $\alpha(S) = \alpha$. We think of a path in S as a concatenation of two paths of half the length. We denote a path $s = (s_1, ..., s_l) \in S$ by $s = a \circ b$, where $a = (s_1, ..., s_{l/2})$ and $b = (s_{l/2+1}, ..., s_l)$. For every $a \in [w]^{l/2}$, we denote by $Suffix(a)$ the set of all suffixes b, such that, the concatenated path $a \circ b$ is in S. That is,

$$Suffix(a) = \{b \in [w]^{\frac{l}{2}} \mid a \circ b \in S\}.$$

For every $a \in [w]^{l/2}$, we denote

$$\alpha_a = \frac{|Suffix(a)|}{w^{l/2}},$$

that is, the density of $Suffix(a)$ in $[w]^{l/2}$. We say that a is dense if $\alpha_a \geq \alpha/2$. Denote by $\hat{S}$ the set of all dense prefixes $a \in [w]^{l/2}$. That is,

$$\hat{S} = \{a \in [w]^{\frac{l}{2}} \mid \alpha_a \geq \alpha/2\}.$$

Consider a matrix $[w]^{l/2} \times [w]^{l/2}$ of zeros and ones, with rows and columns corresponding to prefixes and suffixes in $[w]^{l/2}$. Define an entry (a, b) of the matrix to be 1 iff the path $a \circ b$ is in S. The fraction of ones in the matrix is α (i.e., the density of S). Applying Claim 8.2.1 to the matrix, we conclude that at least one of the following two possibilities holds.

(1) There exists a prefix $a \in [w]^{l/2}$, such that, $\alpha_a \geq \sqrt{\alpha/2}$.
(2) The set of dense prefixes $\hat{S} \subset [w]^{l/2}$ is of density larger than $\sqrt{\alpha/2}$.

In the first case, we will show the existence of a protocol (with the same communication complexity as P) that works on the set $Suffix(a) \subset [w]^{l/2}$. In the second case, we will show the existence of a protocol (with the same communication complexity as P) that works on a large subset of $\hat{S}$. In both cases, we will end up with a $(\sqrt{\alpha}/2, l/2)$-protocol, with the same communication complexity as P.

First Case:

Let a be a prefix with $\alpha_a \geq \sqrt{\alpha/2}$. We will show a protocol P_a (with the same communication complexity as P) that works on the set $Suffix(a) \subset [w]^{l/2}$. Note that $Suffix(a)$ is a set of density larger than $\sqrt{\alpha/2}$, of paths of length $l/2$, and hence the lemma follows.

Given inputs $x, y \in Suffix(a)$, the protocol P_a operates as follows. Player 1 concatenates a to x, and obtains the path $a \circ x \in S$. Player 2 concatenates a to y, and obtains the path $a \circ y \in S$. The two players apply the protocol P on input $(a \circ x, a \circ y)$. The output of P is a correct answer for the input $(a \circ x, a \circ y)$, since P works on S. Since the paths coincide in their first halves, the answer must be in the second half, and hence it is a correct answer for the inputs $x, y \in Suffix(a)$. The protocol P_a can hence output this answer. Note that if the first coordinate of x is different than the first coordinate of y then the answer may also be the last coordinate of a. This is considered to be the zero coordinate of x and y, that is, the vertex s.

Second Case:

In this case, we will show the existence of a protocol P' (with the same communication complexity as P) that works on a large subset $S' \subset \hat{S}$. Note that $\hat{S}$ is a set of density larger than $\sqrt{\alpha/2}$, of paths of length $l/2$. The set S' will contain almost all the elements of $\hat{S}$ and hence its density will be only slightly smaller than the density of $\hat{S}$. In particular, we will have that the density of S' is larger than $\sqrt{\alpha}/2$, and hence the lemma follows.

For every $a \in S'$, we will have two special suffixes, $b_1(a)$ and $b_2(a)$, such that, the following property will hold: For any two inputs $x, y \in S'$, the two suffixes $b_1(x)$ and $b_2(y)$ differ in all their coordinates (i.e., for every i, we have $b_1(x)_i \neq b_2(y)_i$).

Assume that we have a set S' and suffixes $b_1(a)$ and $b_2(a)$ (for every $a \in S'$), such that, the above property is satisfied. Given inputs $x, y \in S'$, the protocol P' operates as follows. Player 1 concatenates x to $b_1(x)$, and obtains the path $x \circ b_1(x) \in S$. Player 2 concatenates y to $b_2(y)$, and obtains the path $y \circ b_2(y) \in S$. The two players apply the protocol P on input $(x \circ b_1(x), y \circ b_2(y))$. The output of P is a correct answer for the input $(x \circ b_1(x), y \circ b_2(y))$, since P works on S. Since $b_1(x)$ and $b_2(y)$ differ in all their coordinates, the answer must be in the first half of the paths, and hence it is a correct answer for the inputs $x, y \in S'$. The protocol P' outputs this answer. If in addition we know that S' is of density larger than $\sqrt{\alpha}/2$ then we are done.

Let us now show how to construct the set S' and the suffixes $b_1(a)$ and $b_2(a)$ (for every $a \in S'$), such that, the above property is satisfied. Assume for simplicity that w is even. For each layer $L_{l/2+1}, ..., L_l$, we will color at random half of the vertices in the layer in orange and the other half in purple. The set S' and the suffixes $b_1(a)$ and $b_2(a)$ (for every $a \in S'$) will be such that, for every $a \in S'$, the suffix $b_1(a)$ is colored orange and the suffix $b_2(a)$ is colored purple. That is, for every $x, y \in S'$, every coordinate of $b_1(x)$ is a vertex colored orange, and every coordinate of $b_2(y)$ is a vertex colored purple (and hence, these two vertices are different). Thus, the above property trivially holds.

The following claim shows that for some coloring, such a set S' and suffixes $b_1(a)$ and $b_2(a)$ (for every $a \in S'$) can be constructed. (The proof actually shows that a random coloring will do).

Claim 8.3.1. There exists a coloring of all the vertices in layers $L_{l/2+1}, ..., L_l$, such that, for fraction 0.9 of the elements $a \in \hat{S}$, there exist two suffixes $b_1(a)$ and $b_2(a)$, such that,

(1) $a \circ b_1(a) \in S$ and $a \circ b_2(a) \in S$.
(2) Every vertex of $b_1(a)$ is colored orange.
(3) Every vertex of $b_2(a)$ is colored purple.

Proof. Consider the following way to choose a random coloring of layers $L_{l/2+1}, ..., L_l$.

- Choose randomly $w/2$ paths $r_1, ..., r_{w/2}$ in $[w]^{l/2}$ and think of these paths as paths on layers $L_{l/2+1}, ..., L_l$. That is, each path starts in layer $L_{l/2+1}$ and ends at layer L_l. Color in orange all the vertices in these paths.
- In layers where the paths covered less than $w/2$ vertices (i.e., less than half of the vertices are colored orange), choose randomly additional vertices and color them orange, until exactly $w/2$ vertices are colored orange.
- Color the rest of the vertices in purple.

By a symmetry argument, it follows that this procedure for coloring layers $L_{l/2+1}, ..., L_l$ produces the exact same distribution as choosing at random $w/2$ vertices in each layer and coloring them in orange (and coloring all other vertices in purple). We use the above procedure (to produce the distribution), because it makes some of the probabilistic calculations much simpler.

We will show that for any $a \in \hat{S}$, there is a high probability that two suffixes $b_1(a)$,$b_2(a)$ as above do exist. Thus, one can define S' to be the set of all prefixes $a \in \hat{S}$, such that, two suffixes $b_1(a)$,$b_2(a)$ as above do exist. Note that the set S' depends on the specific coloring chosen. The expected size of S' will be close to the size of $\hat{S}$ (where the expectation is taken over the random coloring). Therefore, for some coloring, the size of the set S' will be very close to the size of $\hat{S}$.

Let us now show that indeed for any $a \in \hat{S}$, there is a high probability that two suffixes $b_1(a)$,$b_2(a)$ as above do exist. By the definition of $\hat{S}$, for any $a \in \hat{S}$,

$$\alpha_a \geq \alpha/2.$$

Hence, for any $1 \leq i \leq w/2$, the probability that the random path r_i (chosen by the above procedure) is not in $Suffix(a)$ is at most $(1 - \alpha/2)$, that is,

$$Pr[r_i \notin Suffix(a)] \leq \left(1 - \frac{\alpha}{2}\right).$$

Since the paths $r_1, ..., r_{w/2}$ were chosen independently, and since $\alpha > 16/w$, the probability that none of the $w/2$ paths is in $Suffix(a)$ is bounded by

$$Pr[\forall i,\ r_i \notin Suffix(a)] \leq \left(1 - \frac{\alpha}{2}\right)^{\frac{w}{2}} < \left(1 - \frac{8}{w}\right)^{\frac{w}{2}} < e^{-4} < 0.05,$$

(where the probability is over the choice of the $w/2$ paths $r_1, ..., r_{w/2}$).

Hence, for every $a \in \hat{S}$, with probability of at least 0.95, there exists $b_1(a) \in Suffix(a)$, such that, $b_1(a)$ is colored orange (where the probability is over the coloring). In the same way, by a symmetry argument, for every $a \in \hat{S}$, with probability of at least 0.95, there exists $b_2(a) \in Suffix(a)$, such that, $b_2(a)$ is colored purple. By the union bound, we conclude that for every $a \in \hat{S}$, with probability of at least 0.9, both suffixes $b_1(a)$ and $b_2(a)$ as above do exist. Therefore, the expected size of S' is at least $0.9 \cdot |\hat{S}|$, where the expectation is over the coloring. In particular, there exists one specific coloring for which $|S'|$ is at least $0.9 \cdot |\hat{S}|$. ∎

To finish the proof of the lemma (in the second case), take a coloring that satisfies Claim 8.3.1 and define S' as in the proof of Claim 8.3.1. The density of S' is at least $0.9 \cdot (\alpha/2)$, which is larger than $\sqrt{\alpha}/2$. As we saw above, we have a protocol P' (with the same communication complexity as P) that works on S'. That is, P' is a $(\sqrt{\alpha}/2, l/2)$-protocol.
∎