University of California, Los Angeles
CS 289A Communication Complexity

Instructor: Alexander Sherstov
Scribe: Matt Brown
Date: January 25, 2012

LECTURE
5

Nondeterminism

In this lecture, we introduce nondeterministic communication complexity. This model is analogous to nondeterministic computational complexity and can similarly be defined in terms of a proof system. We explore the relative power of nondeterminism and deterministic communication. We analyze the nondeterministic complexity of several common functions, including equality, greater-than, disjointness, and k-disjointness. We also obtain tight lower bounds on nondeterministic and deterministic communication complexity of random functions. We conclude by introducing the log-rank conjecture and presenting some known results in that direction.

5.1 Nondeterminism as a proof system

The *nondeterministic communication complexity* of a function $f : X \times Y \to \{0,1\}$ can be defined in terms of the minimum cost of a *proof system* for f. Consider inputs x and y such that $f(x,y) = 1$. In a proof system (Figure 5.1), an all-powerful prover knows both inputs and sends to Alice and Bob a *certificate* that $f(x,y) = 1$, which they must verify. We define the *cost* of a proof system $C_{pf} = C_1 + C_2$, where C_1 is the size (in bits) of the certificate, and C_2 is the maximum cost of a verification protocol used by Alice and Bob upon receipt of the certificate. A proof system must satisfy the following two criteria (satisfying either criterion without the other is trivial):

Completeness: If $f(x,y) = 1$, then there exists a certificate that the prover can send that forces Alice and Bob to declare that $f(x,y) = 1$.

Soundness: If $f(x,y) = 0$, then Alice and Bob will declare that $f(x,y) = 0$ for every certificate.

Example 5.1. Consider the disjointness function, $\mathrm{DISJ}_n : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$. The negation of this function, $\neg\mathrm{DISJ}_n$, has a highly efficient proof system. A certificate that the input sets x and y are not disjoint is an index i such that $x_i = y_i = 1$. On receipt of an index i, Alice sends Bob x_i, and Bob sends Alice y_i. They output $x_i \wedge y_i$. Note that the described proof system is both sound and complete.

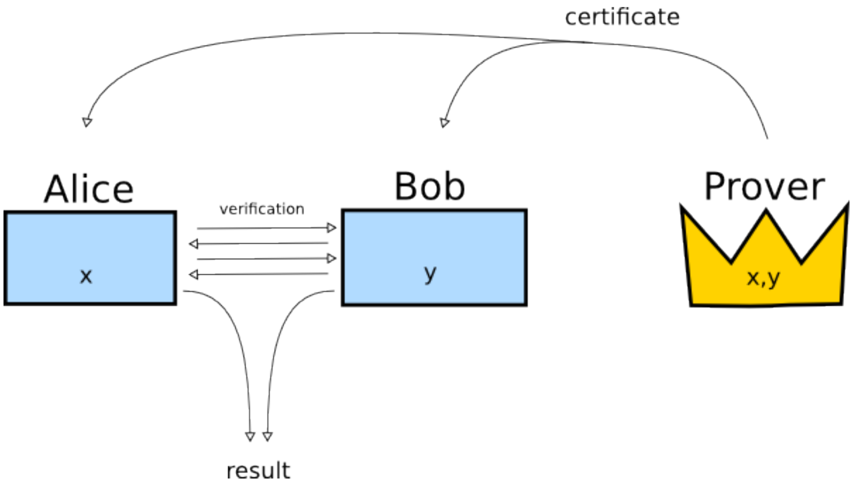


FIGURE 5.1: A proof system.

5.2 Nondeterminism as a cover

Here we explore the relationship between a function's cover size and its nondeterministic communication complexity. Specifically, we show that an efficient proof system gives rise to a small cover of $f^{-1}(1)$ and vice versa.

LEMMA 5.2. *Every* $f\colon X \times Y \to \{0,1\}$ *has a valid proof system with cost* $\log_2 |C^1(f)| + 2$.

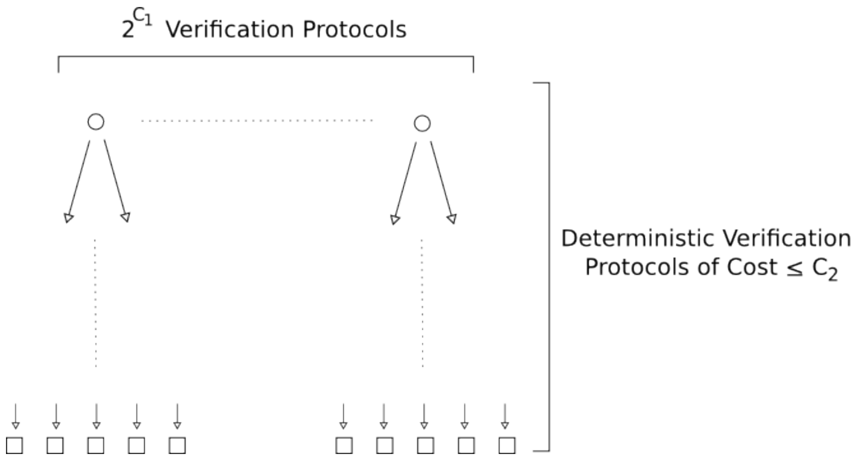
Proof. Let Z be a cover for $f^{-1}(1)$ by f-monochromatic rectangles. Then the following is a valid proof system:

1. The prover sends the index of a rectangle $R \in Z$. ($\log_2 |Z|$ bits)
2. Alice verifies $x \in R$, sends the result to Bob. (1 bit)
3. Bob verifies $y \in R$, sends the result to Alice. (1 bit) □

As we will now show, this lemma has an essentially exact converse.

LEMMA 5.3. *Any proof system for a function* $f : X \times Y \to \{0,1\}$ *must cost* $\geq \log_2 |C^1(f)|$ *bits.*

Proof. A proof systems gives an alternate representation of the function f, as shown in Figure 5.2. The proof system is composed of 2^{C_1} deterministic verification protocols, each of which has maximum deterministic communication complexity C_2. The certificate serves as the index of the verification protocol Alice and Bob will use. Therefore, the total cost of the proof system is $C_1 + C_2$. In other words, the proof system covers $f^{-1}(1)$ with $2^{C_1+C_2}$ f-monochromatic rectangles. By definition, the minimum number of f-monochromatic rectangles needed to cover $f^{-1}(1)$ is $C^1(f)$. Therefore, the cost of the proof system $C_1 + C_2 \geq \log_2 C^1(f)$. □



2^{C_1} Verification Protocols
Deterministic Verification Protocols of Cost ≤ C_2

Figure 5.2: Verification protocols arising from a proof system.

This equivalence between proof systems and covers motivates the following alternate definition of nondeterministic communication complexity.

Definition 5.4. For a function $f : X \times Y \to \{0,1\}$, the *nondeterministic* communication complexity of f is defined as $N(f) = \log_2 C^1(f)$. The *co-nondeterministic* communication complexity of f is defined as $N(\neg f) = \log_2 C^0(f)$.

Note that while $D(f)$ is always an integer, $N(f)$ and $N(\neg f)$ can be fractional numbers.

5.3 Nondeterminism vs. deterministic communication

We now prove some relationships between deterministic and nondeterministic communication complexity.

Theorem 5.5. *For all $f : X \times Y \to \{0,1\}$,*

$$N(f) \le D(f) \le 2^{N(f)} + 1.$$

Proof. Recall from last lecture that $D(f) \ge \log_2 C(f)$. Therefore,

$$N(f) = \log_2 C^1(f) \le \log_2 C(f) \le D(f),$$

proving the first inequality in the theorem. The second inequality follows from the fact that $D(f) \le C^1(f) + 1$, proved during last lecture (Proposition 4.9). □

Example 5.6 (Equality). As we proved earlier, $D(EQ_n) = n + 1$. By the fooling set argument, we have $C^1(EQ_n) \ge 2^n$. Therefore, $N(EQ_n) \ge n$. This shows that the gap between $N(EQ_n)$ and $D(EQ_n)$ is very near the minimum, as established by Theorem 5.5. On the other hand, the gap between $N(\neg EQ_n)$ and $D(\neg EQ_n) = D(EQ_n)$ is very near the maximum possible. To see why, consider a proof system for $\neg EQ_n$. The prover need only identify a single index $i \in \{1, 2, 3, \ldots, n\}$ such that $x_i \ne y_i$. Alice and Bob need only exchange the values of x_i and y_i to verify. Therefore, $N(\neg EQ_n) \le \log_2(n) + 2$.

EXAMPLE 5.7 (Greater-than). Recall that $D(GT_n) = n + 1$. By the fooling set argument, we have $N(GT_n) \geq n$ and likewise $N(\neg GT_n) \geq n - 1$. For this function, the deterministic, nondeterministic, and co-nondeterministic communication complexities essentially coincide.

While the gap between the deterministic and nondeterministic communication complexities can be exponential, we have the following important theorem:

THEOREM 5.8. *For every function $f : X \times Y \to \{0, 1\}$,*

$$D(f) = O(N(f)N(\neg f)).$$

Proof. Recall from last lecture that $D(f) \leq O((\log_2 C^0(f))(\log_2 C^1(f)))$. The theorem now follows from the definitions of nondeterministic and co-nondeterministic communication complexity. ∎

5.4 Complexity of random functions

In this section, we prove that a random communication problem has high communication complexity in the deterministic and nondeterministic models. We give two different proofs of this result, the first of which implicitly uses the rectangle size bound and the second uses basic counting.

THEOREM 5.9. *Let $f : \{0, 1\}^n \times \{0, 1\}^n \to \{0, 1\}$ be a uniformly random communication problem. Then w.v.h.p.,*

$$C(f) > 2^{n-2},$$
$$D(f) \geq n - 1.$$

Proof. Since $D(f) \geq \lceil \log_2 C(f) \rceil$, it suffices to prove the lower bound on $C(f)$. Let $\alpha \in [0, 1]$ be a parameter to be fixed later, and let R be a rectangle with size $|R| \geq \alpha 4^n$. We first establish the probability such a rectangle is f-monochromatic:

$$\begin{aligned}\mathbb{P}[R \text{ is } f\text{-monochromatic}] &= \mathbb{P}[R \text{ is 0-monochromatic for } f] + \mathbb{P}[R \text{ is 1-monochromatic for } f] \\ &= 2\left(\frac{1}{2}\right)^{|R|} \leq \frac{1}{2^{\alpha 4^n - 1}}.\end{aligned}$$

Since the total number of rectangles, regardless of size, is $|\mathscr{P}(\{0, 1\}^n) \times \mathscr{P}(\{0, 1\}^n)| = 2^{2 \cdot 2^n}$, the union bound implies that

$$\mathbb{P}_f[\exists R \text{ s.t. } |R| \geq \alpha 4^n, R \text{ is } f\text{-monochromatic }] \leq 2^{2 \cdot 2^n - \alpha 4^n + 1}. \tag{5.1}$$

At the same time, every f has an f-monochromatic rectangle of size $4^n / C(f)$, so that

$$\mathbb{P}_f[\exists R \text{ s.t. } |R| \geq \alpha 4^n,\ R \text{ is } f\text{-monochromatic }] \geq \mathbb{P}_f\left[C(f) \leq \frac{1}{\alpha}\right]. \tag{5.2}$$

Comparing (5.1) and (5.2), we see that

$$\mathbb{P}_f\left[C(f) \leq \frac{1}{\alpha}\right] \leq 2^{2 \cdot 2^n - \alpha 4^n + 1}.$$

Letting $\alpha = 1/2^{n-2}$, we conclude that $C(f) > 2^{n-2}$ w.v.h.p. ∎

Using a different argument, based on elementary counting, we can prove the following stronger result.

Theorem 5.10. *Let $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ be a uniformly random communication problem. Then w.v.h.p.,*

$$\begin{aligned} C^1(f) &\geq 2^{n-1} + 1, \\ N(f) &> n - 1, \\ D(f) &\geq n. \end{aligned}$$

Proof. Again, it suffices to prove the lower bound on $C^1(f)$. Let N be a parameter to be fixed later. By definition, a cover is a family of rectangles. Since there are $2^{2\cdot 2^n}$ distinct rectangles on $\{0,1\}^n \times \{0,1\}^n$, the total number of covers with N rectangles is $\binom{2^{2\cdot 2^n}}{N}$. Since the total number of distinct functions $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ is 2^{4^n}, we conclude that

$$\mathbb{P}_f[C^1(f) \leq N] \leq 2^{-4^n} \binom{2^{2\cdot 2^n}}{N} \leq \frac{2^{2\cdot 2^n \cdot N - 4^n}}{N!}.$$

Letting $N = 2^{n-1}$ shows that $C^1(f) > 2^{n-1}$ w.v.h.p. □

5.5 The log-rank conjecture

In lecture 3, we proved the rank lower bound on the deterministic communication complexity, due to Mehlhorn and Schmidt [3]:

$$D(f) \geq \log_2(\operatorname{rk}_{\mathbb{R}} M_f).$$

It is an open problem whether the rank lower bound is reasonably tight. Specifically, Lovász and Saks [2] proposed the following *log-rank conjecture*: for some absolute constant constant $c > 1$ and all f,

$$D(f) \leq (\log_2(\operatorname{rk}_{\mathbb{R}} M_f))^c + c.$$

The status of this conjecture remains wide open. In this lecture, we present a construction of f, due to Nisan and Wigderson [4], with a polynomial gap between $D(f)$ and $\log_2(\operatorname{rk}_{\mathbb{R}} M_f)$. In particular, we show that if the constant c exists, it obeys $c > 1.58$.

Theorem 5.11. *There exists a function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ such that*

$$\begin{aligned} D(f) &= \Omega(n), \\ \log_2(\operatorname{rk}_{\mathbb{R}} M_f) &\leq O(n^{0.631\ldots}). \end{aligned}$$

Proof. Let $h \colon \{0,1\}^3 \to \{0,1\}$ be the Boolean function given by

$$\begin{aligned} h(a,b,c) &= a + b + c - ab - bc - ac \\ &= \begin{cases} 0 & \text{if } a+b+c = 0, \\ 1 & \text{if } a+b+c = 1, \\ 1 & \text{if } a+b+c = 2, \\ 0 & \text{if } a+b+c = 3. \end{cases} \end{aligned}$$

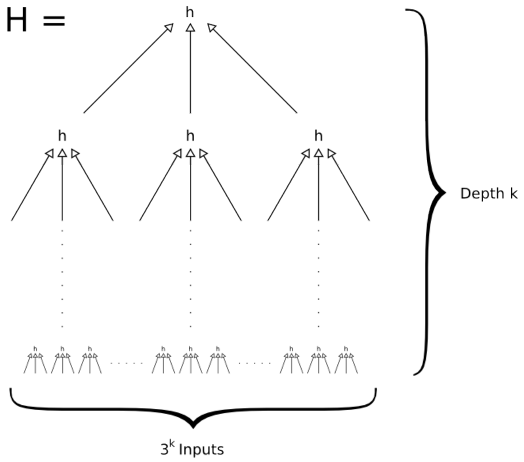


FIGURE 5.3: The function H, defined as k recursive applications of h.

Let H be a function on $n = 3^k$ bits, as shown in Figure 5.3. The following properties are immediate by induction on k: $H(z) = 0$ when $z = (0, \ldots, 0)$, and $H(z) = 1$ for when $z_1 + \cdots + z_n = 1$.

Let $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ be defined as:

$$f(x, y) = H(x_1y_1, x_2y_2, \ldots, x_ny_n).$$

By the properties of H, we have that $f(x, y) = 0$ when $x_1y_1 + \cdots + x_ny_n = 0$, and $f(x, y) = 1$ when $x_1y_1 + \cdots + x_ny_n = 1$. In lectures to come, we will see a proof, due to Razborov [5], that any such function f has $D(f) = \Omega(n)$.

It remains to show that $\log_2(\operatorname{rk}_{\mathbb{R}} M_f) \le O(n^{0.631\cdots})$. H is polynomial with $A(k)$ monomials, where $A(k)$ is given by the recurrence

$$\begin{aligned} &A(1) = 6, \\ &A(k) \le 3A(k-1) + 3A(k-1)^2, \qquad k = 2, 3, 4, \ldots. \end{aligned}$$

Thus $A(k) \le 6A(k-1)^2$, which by induction gives $A(k) \le 6^{2^k - 1}$. The characteristic matrix M_f is the sum of rank-1 matrices corresponding to the monomials of H, so that

$$\log_2(\operatorname{rk}_{\mathbb{R}} M_f) = O(2^k) = O((3^k)^{\log_3 2}) = O(n^{0.631\cdots}). \qquad \square$$

5.6 Nondeterministic and co-nondeterministic complexity of k-disjointness

For a set S and a natural number k, let $\binom{S}{k}$ denote the family of all cardinality-k subsets of S. The k-disjointness function $\mathrm{DISJ}_k^n \colon \binom{\{1,\ldots,n\}}{k} \times \binom{\{1,\ldots,n\}}{k} \to \{0,1\}$ is given by

$$\mathrm{DISJ}_k^n(x, y) = \begin{cases} 1, & x \cap y = \varnothing, \\ 0, & \text{otherwise.} \end{cases}$$

In this section, we analyze the nondeterministic and co-nondeterministic communication complexity of k-disjointness. In the next lecture, we will additionally determine the deterministic communication complexity of this function and thereby show that the upper bound in Theorem 5.8 is tight in general.

Theorem 5.12. *The k-disjointness function* DISJ_k^n *obeys*

$$\begin{aligned} N(\neg\mathrm{DISJ}_k^n) &\leq O(\log n), \\ N(\mathrm{DISJ}_k^n) &\leq O(k + \log\log n). \end{aligned}$$

Proof. The first upper bound is immediate; the proof system is described in Example 5.1. It remains to show that $C^1(\mathrm{DISJ}_k^n) \leq 2^{\Theta(k)} \log n$. We do so using the probabilistic method. For a subset $S \subseteq \{1, 2, \dots, n\}$, consider the following 1-monochromatic rectangle for DISJ_k^n:

$$R_S = \left\{ x \in \binom{\{1,2,\dots,n\}}{k} : x \subseteq S \right\} \times \left\{ y \in \binom{\{1,2,\dots,n\}}{k} : y \subseteq \overline{S} \right\}.$$

Let $S \subseteq \{1, 2, \dots, n\}$ be a uniformly random set. Then for any (x, y) with $\mathrm{DISJ}_k^n(x, y) = 1$,

$$\mathbb{P}_S\left[(x, y) \in R_S\right] = \frac{1}{4^k}.$$

Now let $R_{S_1}, \dots, R_{S_N}$ be random rectangles. Then,

$$\begin{aligned} &\mathbb{P}\left[R_{S_1}, \dots, R_{S_N} \text{ fail to cover } \mathrm{DISJ}_k^{n-1}(1)\right] \\ &\qquad \leq |\mathrm{DISJ}_k^{n-1}(1)|\, \mathbb{P}\left[R_{S_1}, \dots, R_{S_N} \text{ do not cover } (\{1, \dots, k\}, \{k+1, \dots, 2k\})\right] \\ &\qquad \leq \left(n^k\right)^2 \left(1 - \frac{1}{4^k}\right)^N \\ &\qquad \leq n^{2k}\, e^{-N/4^k}, \end{aligned}$$

which is less than 1 whenever $N > 4^k \ln n^{2k} = 2^{\Theta(k)} \log n$. Thus, $\mathrm{DISJ}_k^{n-1}(1)$ has a cover of the claimed size. □

References

[1] E. Kushilevitz and N. Nisan. *Communication complexity.* Cambridge University Press, 2nd edition, 2006.

[2] L. Lovasz and M. Saks. Lattices, mobius functions and communications complexity. In *Proceedings of the 29th Annual Symposium on Foundations of Computer Science*, pages 81–90, Washington, DC, USA, 1988. IEEE Computer Society.

[3] K. Mehlhorn and E. M. Schmidt. Las vegas is better than determinism in vlsi and distributed computing (extended abstract). In *Proceedings of the fourteenth annual ACM symposium on Theory of computing*, STOC '82, pages 330–337, New York, NY, USA, 1982. ACM.

[4] N. Nisan and A. Wigderson. On rank vs. communication complexity. In *Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on*, pages 831 –836, nov 1994.

[5] A. A. Razborov. On the distributional complexity of disjointness. *Theor. Comput. Sci.*, 106(2):385–390, 1992.