A Theorist's Toolkit **(CMU 18-859T, Fall 2013)**

Lecture 19: Communication complexity

11/11/2013

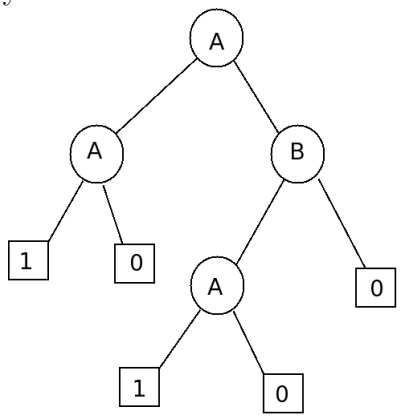
Lecturer: Ryan O'Donnell *Scribe: Livia Ilie*

1 Introduction

The topic for this lecture is "communication complexity". To explain what this means, say there are players Alice and Bob and there is a wall between them. Alice receives an n-bit string $x \in X$ and Bob receives an n-bit string $y \in Y$. Alice and Bob are both trying to compute $f : X \times Y \to \{0, 1\}$ for their inputs by sending 1-bit messages. By the end, both Alice and Bob should know $f(x, y)$. We would like to minimize the communication bits given that the two players have infinite computation power. This has been studied for two players, but it gets a lot harder for a large number of players.

2 Definitions

In this section we will define the communication protocol more carefully. A communication protocol π is a tree that has outcomes as leaves and at each node that is not a leaf it has a player and a function associated with it.



Definition 2.1. $cost_\pi(x, y)$ is the length of the path on input (x, y), or, in other words, it is the number of bits required to communicate for the input pair (x, y).

3 Examples

- EQ_n. This is the question of checking if the two n-bit strings are equal. It can be computed deterministically by communicating $n + 1$ bits and using randomness by

communicating $O(\log n)$ bits. For the deterministic algorithm, Alice sends to Bob all of her bits, Bob computes the result and sends it back to Alice. Actually, this procedure would work for any function.

- $Parity(x) + Parity(y)$. This can be done in two bits. Alice sends a bit representing the parity of her string and Bob sends back a bit representing the result.

- Alice gets a string representing a set $S \subseteq [n]$ and Bob gets a string representing the set $T \subseteq [n]$. They would like to compute the median of $S \cup T$. This can be achieved in $O(\log^2 n)$.

- Disjointness. Assume Alice and Bob have strings defined as above. They would like to compute $f(x, y)$ such that $f(x, y) = 1$ iff $S \cap T = \emptyset$. This can be achieved deterministically by using $n + 1$ bits.

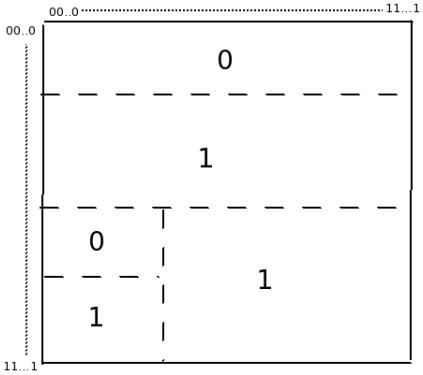
  Theorem 3.1. *[KS92] The disjointness problem requires n bits of communication even if we allow random bits.*

- Inner product. That is, Alice and Bob need to compute $\sum_{i=1}^{n} x_i y_i \mod 2$. This can be achieved with $n + 1$ bits deterministically and $\Omega(n)$ randomly.

4 Communication matrix

We define M_f to be the communication matrix of f. The matrix M_f has size $2^n \times 2^n$. Every row corresponds to a possible value of x and every column corresponds to a possible value of y. The entry at position (x, y) is the value of $f(x, y)$.

Each time Alice or Bob sends a bit of information, the matrix is divided into two rectangles. At the end of the protocol, we obtain a partition. In order for the protocol to work the division should give us monochromatic rectangles. These rectangles need not be contiguous.



In order to illustrate this we will describe the protocol for EQ_2 using a communication matrix. Figure 1 represents the initial M_{EQ_2}. Afterwards, Alice sends her bits to Bob and the matrix looks like Figure 2. However, since Bob knows his bits, the matrix actually looks like Figure 3 to him. So, he can send Alice back the correct value for $EQ_2(x, y)$

Figure 1

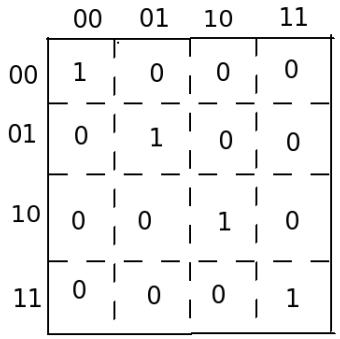


Figure 2

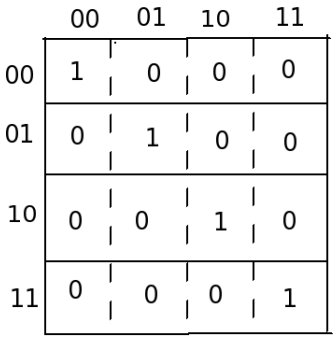
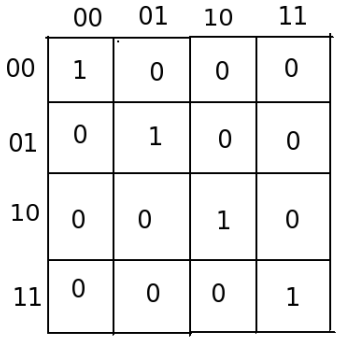


Figure 3



00

00

Theorem 4.1. *Any c-bit communication protocol π that is deterministic and computes f correctly, partitions f into at most 2^c rectangles that are f-monochromatic.*

Theorem 4.2. $D(EQ_n) = n + 1$

Proof. We notice that in the communication matrix of EQ_n we have n ones placed on the diagonal and zeros everywhere else. Because of this structure, each 1 should be in its own rectangle. So, since the zeros require at least one rectangle, the total number of rectangles is at least $2^n + 1$. So, by the theorem above the communication requires at least $\lceil \log(2^n + 1) \rceil = n + 1$ bits

□

Theorem 4.3. *[MS82]* $D(f) \geq \log(2rank(M_f) - 1)$

Corollary 4.4. *The lower bound for the communication complexity of EQ_n follows from this theorem.*

Proof. $rank(M_{EQ_n}) = rank(I_{2^n \times 2^n}) = 2^n$. By the theorem above, $D(EQ_n) \geq \lceil \log(2 \cdot 2^n - 1) \rceil = n + 1$ □

Corollary 4.5. *Communicating whether two sets are disjoint takes at least n bits.*

Proof.

$$M_{DISJ_n} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^{\otimes n}$$

This matrix also has rank 2^n □

It was conjectured([LS88]) that $D(f) \leq polylog(rank(M_f)$. The best known upper bound is $D(f) \leq \tilde{O}(rank(M_f)$.

Theorem 4.6. *There exists F such that* $D(f) \geq \log(rank(M_f))^{\log_3 6}$

5 Randomized communication complexity

So far we have analyzed examples assuming that all algorithms are deterministic. Now, assume that the players also base their communication on some random bits. The model always considers the worst case over all inputs. A good algorithm should give the right answer over all inputs with high probability. There are two types of model we can use: private coin or public coin. In the first case, Alice knows only her set of random bits and Bob knows only his set of random bits. In the second case, there are some random bits in the sky that both Alice and Bob can look at. These two models are actually very nearly equivalent.

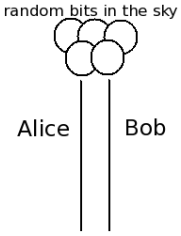
Definition 5.1. $R_\epsilon^{pri}(f)$ is the number of bits communicated on worst case input for a private coins protocol which computes f with probability $1 - \epsilon$ for all inputs (x, y)

Example 5.2. $R_{1/3}^{pri}(EQ_n) = O(\log n)$

First, Alice and Bob agree on a prime p. Each of their strings can be viewed as the coefficients of a polynomial in $\mathbb{Z}_p$. *Alice picks a random number r with* $1 \leq r \leq p$ *and computes her polynomial for value r. Then, she sends the number r and her result to Bob. Bob computes his polynomial at r. If the results agree they say that the two strings are equal.*

Another way to do this is to have Alice and Bob agree on an asymptotically good code $[O(n), n, .1n]_2$. *Then, it would be enough for Alice to send* $(i, Enc(x)_i)$ *for a random i.*

Now, we look at the same problem for public coins.



Theorem 5.3. $R_{1/3}^{pub}(EQ_n) \leq 3$

Proof. We interpret the random bits in the sky as two strings in $\mathbb{F}_n$, r_1 and r_2. Alice sends $x \cdot r_1, x \cdot r_2$ to Bob. Then, Bob checks if the results would be the same for string y and tells Alice the answer. For t bits this gives a probability of error of 2^{-t} □

Theorem 5.4. *[New91] We can convert a public coin protocol to a private coin protocol only incurring an additional error of δ and using $O(\log n + \log \delta)$ bits.*

Proof. Assume a function can be computed by a protocol using m random bits. In order to create an appropriate private coin protocol Alice and Bob first jointly write down $t = O(n/\delta^2)$ random strings $r_1, r_2, \ldots r_t \in \{0,1\}^m$. Afterwards they go to separate rooms and Alice picks j randomly from t and tells it to Bob. Then, they can use the public coin protocol with r_j as the random bits. □

In general, the "standard" randomized protocol is the public-coin protocol. So, we will define $R_\epsilon(f) = R_\epsilon^{pub}(f)$.

Let μ be a distribution on inputs (x, y).

Definition 5.5. The distributional complexity D_ϵ^μ is the cost of the best determnistic protocol that gives the correct value of f for at least $1 - \epsilon$ of the inputs, weighed by μ.

Corollary 5.6.

$$R_\epsilon(f) \geq D_\epsilon^\mu$$

This corollary is usually used to prove lower bounds. For example, to compute the inner product, $R_{1/3}(IP_2) \geq \Omega(n)$ one can choose μ to be the uniform distribution and apply Fourier Analysis (this is hard.)

References

[KS92] B. Kalyanasundaram and G. Schintger. The probabilistic communication complexity of set intersection. *SIAM Journal on Discrete Mathematics*, 5(4):545–557, 1992.

[LS88] L Lovasz and M. Saks. Lattices, mobius functions and communication complexiy. *Proc 29th IEEE FOCS*, pages 81–90, 1988.

[MS82] K. Mehlhorn and E. Schmidt. Las vegas is better than determinism in vlsi and distributed computing. *STOC '82 Proceedings of the fourteenth annual ACM symposium on Theory of computing*, pages 330–337, 1982.

[New91] I. Newman. Private vs. common random bits in communication complexity. *Information processing letters*, 39(2):67–71, 1991.