Private vs. Common Random bits in Communication Complexity

Ilan Newman *

November 8, 1995

Abstract

We investigate the relative power of the common random string model vs. the private random string model in communication complexity. We show that the two model are essentially equal.

Keywords: communication complexity, randomness, theory of computation.

Communication complexity is a model of computation where two parties, each with an input, want to mutually compute a Boolean function that is defined on pairs of inputs. Formally, let $f : X \times Y \mapsto \{0,1\}$ be a Boolean function. The communication problem for f is the following two-player game. Player A gets $x \in X$ and player B gets $y \in Y$. Their goal is to compute $f(x,y)$. They have unlimited computational power and a full description of f, but they don't know each other's input. They determine the output value by exchanging messages. Let n, the length of the input, be $\log(|X||Y|)$.

A protocol for computing f is a pair of algorithms (one for each player) according to which the players send binary messages. A protocol proceeds in rounds. In every round the protocol specifies which player's turn it is to send a message. Each player in his turn sends a bit message that may depend on

*Comp. Sci. dep. Hebrew University, Jerusalem.

her input and the previous messages she has received. A correct protocol for f should terminate for every input pair $(x, y) \in X \times Y$, when both players know $f(x, y)$ and that the protocol has terminated.

The communication complexity of a protocol P is the number of bits exchanged for the worst case input pair. The communication complexity of a Boolean function $f : X \times Y \mapsto \{0, 1\}$, is that of the best possible protocol for f.

The model was introduced by Yao, [13], and has been studied thoroughly, as has its probabilistic counterpart defined hereafter. For a survey and exact definitions see [2], [6]. The communication complexity model has gained increased attention recently due to the generalization of Karchmer and Wigderson, [8], which demonstrates its relation to formula complexity. See also [9].

We focus our attention on probabilistic protocols. In this setting, the algorithms of the players may be probabilistic; i.e, they may depend on tosses of random coins and may err. The complexity of a probabilistic protocol P on input (x, y) , denoted by $C_P(x, y)$, is the expected number of bits exchanged. The complexity of a protocol P is $C(P) = max_{(x,y)} C_P(x, y)$. We refer here to [2], [6] and [10] for definitions and discussion on the probabilistic communication complexity model.

Two models of access to the random bits are considered in the literature. The PRIVATE, in which each player tosses his private coin, and the COMMON, in which both players share a common random bit string. The PRIVATE model is clearly weaker than the COMMON (since the players may need to communicate their random bits). However, it is more realistic.

Our main objective is to compare the relative power of the two models.

Note that not only the cost but also the output of a probabilistic protocol P on input (x, y), denoted by $P(x, y)$, becomes a random variable. For $0 \le \epsilon < 1/2$ let

$$\mathcal{P}_\epsilon^{com}(f) = \{P \in COMMON \mid \forall (x, y) \in X \times Y \; Prob(P(x, y) \neq f(x, y)) \le \epsilon\}$$

$$\mathcal{P}_\epsilon^{pri}(f) = \{P \in PRIVATE \mid \forall (x, y) \in X \times Y \; Prob(P(x, y) \neq f(x, y)) \le \epsilon\}$$

In words, $\mathcal{P}_\epsilon^{com}(f)$ and $\mathcal{P}_\epsilon^{pri}(f)$ are the sets of all probabilistic protocols, of the two types, that have error probability of at most ϵ. Define

$$C_\epsilon^{com}(f) = min\{C(P) : \; P \in \mathcal{P}_\epsilon^{com}(f)\}, \qquad C_\epsilon^{pri}(f) = min\{C(P) : \; P \in \mathcal{P}_\epsilon^{pri}(f)\}$$

That is, $C_\epsilon^{com}(f)$, $(C_\epsilon^{pri}(f))$ is the best complexity that a COMMON, (PRIVATE) protocol can achieve if its error probability is bounded by ϵ.

Since $\mathcal{P}_\epsilon^{pri}(f) \subseteq \mathcal{P}_\epsilon^{com}(f)$ we have $C_\epsilon^{com}(f) \leq C_\epsilon^{pri}(f)$. Our main observation is that the relative power of the two models is nearly the same. This is due to the fact that the model is non-uniform. A similar phenomenon was first observed by Adleman [1] for the model of Boolean circuits.

Theorem 1.1 *Let* $0 \leq \epsilon < 1/2$ *and* $0 < \delta \leq 1$ *then*

$$C_{(1+\delta)\epsilon}^{pri}(f) = O(C_\epsilon^{com}(f) + \log \frac{n}{\epsilon\delta})$$

Proof It is enough to show that there is a protocol $P^* \in \mathcal{P}_{(1+\delta)\epsilon}^{com}(f)$ that uses $O(\log \frac{n}{\epsilon\delta})$ random bits. P^* can be directly made to work with private random bits. Player A tosses the necessary random bits, communicates them to B at a cost of $O(\log \frac{n}{\epsilon\delta})$ and then they follow P^*.

The existence of P^* is asserted by proposition 1.1. □

Proposition 1.1 *Let* $P \in \mathcal{P}_\epsilon^{com}(f)$, $0 \leq \epsilon < 1/2$ *then for any* $0 < \delta \leq 1$ *there is a protocol* $P^* \in \mathcal{P}_{(1+\delta)\epsilon}^{com}(f)$ *such that* $C(P^*) = O(C(P))$ *and* P^* *uses only* $O(\log \frac{n}{\epsilon\delta})$ *random bits.*

Proof Let $c = C(P)$. P may be thought of as a probability distribution on a finite collection of deterministic protocols $P = \{P_r\}_{r=1}^{r=t}$, each P_i defined by some fixed random string. Furthermore, since there is no cost for random bits in this model, we may assume that the probability distribution over $\{P_r\}$ is uniform (by allowing identical copies of protocols in this collection). (We avoid here questions of irrational values of probability , which are handled in standard ways in many other discussions on the general theory of probabilistic algorithms).

Claim 1.1 *There is a collection of* $l = \max(\frac{n}{(\epsilon\delta)^2}, \frac{(n+1)^2}{c})$ *protocols* $\{P_{i_1}, .., P_{i_l}\} = \mathcal{P}_1$ *with the properties:*

$$\forall (x,y) \in X \times Y \quad \frac{1}{l} |\{P \in \mathcal{P}_1 : \ P(x,y) \neq f(x,y)\}| \leq (1+\delta)\epsilon \tag{1}$$

$$\forall (x,y) \in X \times Y \quad \frac{1}{l} \Sigma_{P \in \mathcal{P}_1} C_P(x,y) = O(c) \tag{2}$$

Proof Pick a collection L of $l = \max(\frac{n}{(\epsilon\delta)^2}, \frac{(n+1)^2}{c})$ protocols out of the original collection $P = \{P_r\}_{r=1}^{r=t}$, by picking l times a random protocol out of P, independently and with equal probability. We will show that L has properties (1) and (2) with non zero probability. For a fixed $(x, y) \in X \times Y$ let $A(x, y) = \{P_i \in L | \ P_i(x, y) \neq f(x, y)\}$ Note that by the assumption on P, $Prob(P_r \in A(x, y)) \leq \epsilon$ for every input (x, y). By a Chernofflike inequality ([11], [4])

$$Prob(|A(x, y)| \geq (1 + \delta)\epsilon l) \ \leq \ exp(-2\delta^2\epsilon^2 l) \leq exp(-2n)$$

Thus, (for $n \geq 2$)

$$Prob(\exists(x, y), \ |A(x, y)| \geq (1 + \delta)\epsilon l) \leq 2^n exp(-2n) < 0.25 \tag{3}$$

Observe that this corresponds to the probability that L does not have property (1). We need a similar statement for property (2), for which we use Hoeffding inequality

Lemma 1.1 *Hoeffding(1963), [4], [5] Let $Y_1, ..., Y_l$ be independent random variables with values in the interval $[0, z]$. Let $\mu = E(\frac{1}{l}\Sigma_{j=1}^{j=l} Y_i)$ Then*

$$Prob(\frac{1}{l}\Sigma_{j=1}^{j=l} Y_i \geq d\mu) \leq (d^{-d\mu}(\frac{z - \mu}{z - d\mu})^{z-d\mu})^{l/z}$$

For $d \in [1, z/\mu]$ this simplifies to

$$Prob(\frac{1}{l}\Sigma_{j=1}^{j=l} Y_i \geq d\mu) \leq (\frac{e^{(d-1)}}{d^d})^{l\mu/z}$$

Let our L be $L = \{P'_1, .., P'_l\}$. For a fixed $(x, y) \in X \times Y$ let $Y_i(x, y) = C_{P'_i}(x, y)$. Observe that $Y_1(x, y), ..., Y_l(x, y)$ meet the assumption of the lemma with $z = n + 1$ (since n is an upper bound on the complexity of any protocol for f). Note that $E(C_{P'_i}(x, y)) = C_P(x, y)$ we have,

$$\mu = E(\frac{1}{l}\Sigma_{j=1}^{j=l} C_{P'_j}(x, y)) = \frac{1}{l}\Sigma_{j=1}^{j=l} E(C_{P'_j}(x, y)) = C_P(x, y) \ \leq c$$

We may assume $c < n/3$ (otherwise, we are immediately done). We get (for $d = 3$)

$$\forall(x, y) \in X \times Y \quad Prob(\frac{1}{l}\Sigma_{j=1}^{j=l} C_{P'_j}(x, y) \geq 3c) \leq (\frac{e^2}{27})^{\frac{lc}{n+1}} \leq (\frac{e^2}{27})^{n+1} \leq 3^{-n-1}$$

Thus

$$Prob(\exists(x,y),\ \ \frac{1}{l}\Sigma_{j=1}^{j=l}C_{P'_j}(x,y)\geq 3c)\ \leq\ 2^n 3^{-n-1}\ \leq 0.25 \tag{4}$$

Therefore, there is some choice of L for which both properties (1) and (2) hold. This completes the proof of the claim. $\Box$

We let P^* be the probabilistic protocol that picks at random, with uniform distribution, a protocol from the set L. It is guaranteed by claim 1.1 that P^* has error bound of $(1+\delta)\epsilon$ and it uses only $\log l = O(\log n + \log(1/(\epsilon\delta)))$ random bits. This completes the proof of proposition 1.1 $\Box$.

Corollary 1.1 *Let $n^{-c} < \epsilon < 1/2 - n^{-c}$ for some constant c. Then*

$$C_\epsilon^{pri}(f) = O(C_\epsilon^{com}(f) + \log n)$$

Proof: Pick δ so that $\epsilon(1+\delta) < 1/2 - n^{-c}$ and $\delta > n^{-2c}$ (clearly such δ exists). By theorem 1.1, for any $P \in \mathcal{P}_\epsilon^{com}$ there is a protocol $P_1 \in \mathcal{P}_{\epsilon(1+\delta)}^{pri}$ with $C(P_1) = O(C(P) + \log n)$. The error of P_1 can be reduced (back) to ϵ, keeping the same order of magnitude of complexity, by standard amplification methods. (We repeat P_1 a constant number of times with independent coin flips and take the majority of the outputs). $\Box$.

An important class of protocols are $\mathcal{P}_0^{com}(f)$, and $\mathcal{P}_0^{pri}(f)$. Those are protocols that always answer correctly (Las Vegas). We have

Theorem 1.2

$$C_0^{pri}(f) = O(C_0^{com}(f) + \log n)$$

Proof: As in the proof of theorem 1.1, except that property (1) holds with probability 1 for every L. So it suffices to pick $l = (n+1)^2/c$ in order to guarantee property (2). $\Box$.

Remarks:

1. An important generalization of this classical communication problem is the Karchmer-Wigderson game [8]. Namely, let $g : \{0,1\}^n \mapsto \{0,1\}$ be a Boolean function, let $X = g^{-1}(1)$ and $Y = g^{-1}(0)$. Define the relation $R_g \subseteq X \times Y \times \{1,..,n\}$ by $(x,y,i) \in R_g$ iff $x_i \neq y_i$, where x_i, (y_i) is

the $i-$th bit of x (y). The communication problem for R_g is as follows. One player get input $x \in X$ and the other gets $y \in Y$. Their task is to **agree** on an i such that $(x, y, i) \in R_g$. The importance of this game is its relation to the formula size of g [8]. Probabilistic protocols are defined in a manner similar to the classical case. Our result carries on to this framework too, by the same proof.

2. In the proofs of theorem 1.1 and theorem 1.2 we only used the inherent power of the nonuniformity of the model, and the fact that the complexity was naturally bounded by $n+1$. For any nonuniform model with a similar property, our proof asserts that one can use a small amount of randomness, (i.e, the decision tree model, non uniform routing etc.). Indeed the same idea was used in [1], [7].

3. It is well known that for every pair of constants $0 \leq \epsilon, \epsilon'$ if $P \in \mathcal{P}_{\epsilon}^{com}(f)$ with $C(P) = c$, there exists a $P' \in \mathcal{P}_{\epsilon'}^{com}(f)$ whose complexity is $O(c)$ for every (x, y) and all coin tosses. Using this, theorem 1.1 can be proved just by asserting property (1) (property (2) will hold with probability 1). However, this does not work for non-constant error.

4. Our result was recently used in the work of Canetti, and Goldreich, in a study on communication-randomness tradeoffs [3].

References

[1] L. Adleman, Two theorems om random polynomial time, Proceedings of the 19th Annual IEEE Symposium on Foundation of Computer Science, 75-83.

[2] L. Babai, P. Frankl, J. Simon, Complexity classes in communication complexity theory, Proc. 27th Annual IEEE Symp. on Foundation of computer science, 1986, 337-347

[3] R. Canetti, O. Goldreich, Bounds on Tradeoffs between randomness and communication complexity, 31th Annual IEEE Symp. on Foundation of computer science, 1990, 767-775.

[4] W. Hoeffding, Probability inequalities for sums of bounded random variables, American Statistical Association Journal (1963), 13-30

[5] M. Hofri, Probabilistic Analysis of algorithms, Springer Verlag, New York, 1987, pp 104

[6] L. Lovasz, Communication complexity: a survey, in Path flowers and VLSI, (Ed, B. Korte, L.Lovasz, A. Schrijver,), Springer Verlag, 1990.

[7] Krizanc, D. Peleg, E. Upfal, A Time-Randomness Tradeoff for oblivious routing, Proc. 20th Annual ACM Symp. on theory of computing, 1988, 93-102.

[8] M. Karchmer, A. Wigderson, Monotone circuits for connectivity require super- logarithmic depth, Proceedings of 20th Annual ACM Symposium on Theory of Computing, (1988) 539-550.

[9] R. Raz, A. Wigderson, Monotone circuits for matching require linear depth, Proc. 22th Annual ACM Symp. on theory of computing, 1990, 287-292.

[10] R. Raz, A. Wigderson, Probabilistic communication complexity of Boolean relations, Proc. 30th Annual IEEE Symp. on Foundation of Computer Science, 1989, 562-567.

[11] J. Spencer, Probabilistic methods in combinatorics, to appear in Handbook of combinatorics.

[12] A. C. Yao, Probabilistic computation, towards a unified measure of complexity, Proc. 18th Annual IEEE Symp. on Foundation of Computer Science, 1977, 222-227.

[13] A.C. Yao, Some complexity questions related to distributive computing, Proc. 11th Annual IEEE Symp. on Foundation of computer science, 1979, 151-158