COMP760, SUMMARY OF LECTURE 7.

HAMED HATAMI

- **Unbounded-error model** is due to Paturi and Simon [PS86]. The *unbounded-error communication complexity* of a function f, denoted by $U(f)$ is the least cost of a *private coin* randomized protocol that computes f with the error probability strictly less than $\frac{1}{2}$. That is $\Pr[P(x,y,r) \neq f(x,y)] < \frac{1}{2}$ for all (x,y). Note

$$U(f) = \lim_{\epsilon \nearrow \frac{1}{2}} R_\epsilon^{prv}(f).$$

It is important that protocol is in the private coin model. Indeed for every function f, we have $U^{pub}(f) = O(1)$ (See assignment 2).

In the previous lecture we saw that $R_\epsilon^{prv}(f) \geq \log \operatorname{rank}_{2\epsilon}(f)$. Taking the limit shows

$$U(f) = \lim_{\epsilon \nearrow \frac{1}{2}} R_\epsilon^{prv}(f) \geq \lim_{\epsilon \nearrow \frac{1}{2}} \log \operatorname{rank}_{2\epsilon}(f) = \log \operatorname{rank}_{\pm}(f).$$

Theorem 1 (Paturi-Simon [PS86]). *For every $f : \{0,1\}^n \times \{0,1\}^n \to \{-1,1\}$, we have $\log \operatorname{rank}_{\pm}(f) \leq U(f) \leq \log(\operatorname{rank}_{\pm}(f) + 1)$.*

Proof. As we discussed above the lower-bound follows from Krause's result $R_\epsilon^{prv}(f) \geq \log \operatorname{rank}_{2\epsilon}(f)$. It remains to prove $U(f) \leq \log(\operatorname{rank}_{\pm}(f)+1)$. Suppose that A sign-represents f and $\operatorname{rank}(A) = d$. Hence there exists $2^n \times d$ and $d \times 2^n$ matrices B and C such that $A = BC$. First we note that if all the entries of B are positive, each row of B sums up to 1, and $|C_{ij}| \leq \frac{1}{2}$, then we can design an unbounded protocol for f that uses $\log_2 d$ bits of communication. Then we will show that at the cost of increasing d by at most 1 we can easily satisfy these conditions.

- Alice chooses $j \in \{1, \ldots, d\}$ randomly s.t. $\Pr[j = i] = B_{xi}$, and sends j to Bob.
- Bob outputs
  1 with probability $\frac{1}{2} + C_{jy}$
  -1 with probability $\frac{1}{2} - C_{jy}$.

Since $A = BC$, we have

$$\Pr[P(x,y) = 1] = \sum_{j=1}^{d} B_{xj} \left(\frac{1}{2} + C_{jy}\right) = \frac{1}{2} + A(x,y).$$

and

$$\Pr[P(x,y) = -1] = \sum_{j=1}^{d} B_{xj} \left(\frac{1}{2} - C_{jy}\right) = \frac{1}{2} - A(x,y).$$

Since A sign-represents f, this is an unbounded protocol with cost $\log(d)$.

It remains to show that at the cost of increasing d by 1, we can satisfy the conditions that we used above. Indeed let C' be obtained by adding a new row to C to make sure that every column adds up to 0. That is the y-th entry in this new row is $C'(d+1,y) = -\sum_{j=1}^{d} C(j,y)$.

Let $\lambda > 0$ be sufficiently large so that the entries of

$$B' = B \oplus \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix} + \lambda J_{2^n \times (d+1)}$$

are all positive. Here $J_{2^n \times (d+1)}$ denotes the all 1 matrix of dimensions $2^n \times (d+1)$. Note that $B'C' = BC$, and that the entries of B' are all positive. Now we can divide every row of B' by a positive number to make sure that it adds up to 1, and we can divide C' by a large positive number so that all its entries are at most $1/2$ in absolute value. Obviously this re-scaling does not change the sign of the entries of the product, and thus we obtain the desired matrices. □

- **Non-determinism $N^1(f)$ and $N^0(f)$:** Consider a function f. An oracle who sees both x and y wants to convince Alice and Bob that $f(x,y) = 1$. The smallest amount of communication required between the oracle and Alice and Bob, so that Alice and Bob get convinced that $f(x,y) = 1$ on all such inputs is denoted by $N^1(f)$. Obviously if $f(x,y) = 0$, no matter what Oracle says, they must not come to the conclusion that $f(x,y) = 1$. The communication parameter $N^0(f)$ is defined similarly but with swapping the roles of 0 and 1.

  As a simple example consider the equality function EQ_n. Here if $\mathrm{EQ}_n(x,y) = 0$, meaning that $x \neq y$, the oracle can tell to Alice and Bob a coordinate i with $x_i \neq y_i$, and then they can verify this by communicating x_i and y_i. Hence $N^0(\mathrm{EQ}_n) = O(\log_2 n)$.

- We have $N_1(f) = \log C^1(f) \pm O(1)$, and $N_0(f) = \log C^0(f) \pm O(1)$.

- We proved in Lecture 2 that $D(f) \leq \log C^0(f) \log C^1(f)$. With the new notation this means $D(f) \leq N^0(f)N^1(f)$.

1. Communication complexity classes:

As in the rest of complexity theory by a communication problem we mean a sequence of functions $f_n : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ for $n \in \mathbb{N}$. For example equality EQ_n, disjointness DISJ_n, and inner product IP_n are all communication problems.

- **Class P^{cc}:** is the set of problems with efficient deterministic communication complexity. That is $D(f_n) \leq \log^c(n)$ for some constant $c > 0$.

- **Class NP^{cc}:** is the set of problems with efficient non-deterministic communication complexity. That is $N^1(f_n) \leq \log^c(n)$.

- **Class CoNP^{cc}:** is the negation of the problems in NP^{cc}. That is $N^0(f_n) \leq \log^c(n)$.

- **Class Σ_k^{cc}:** For a fixed integer $k \geq 1$, a family $\{f_n\}$ is in Σ_k^{cc} if and only if for some constant $c > 0$,

$$f_n = \bigvee_{i_1=1}^{2^{\log^c n}} \bigwedge_{i_2=1}^{2^{\log^c n}} \bigvee_{i_3=1}^{2^{\log^c n}} \cdots \bigwedge_{i_k=1}^{2^{\log^c n}} g_{i_1,\ldots,i_k},$$

here $\bigvee$ and $\bigwedge$ alternate, and thus when k is odd, the inner most one must be $\bigvee$ (instead of $\bigwedge$). If k is odd then $g_{i_1,\ldots,i_k}$ are rectangles, and if k is even then they are complements of rectangles.

- **Class** Π_k^{cc}**:** A family $\{f_n\}$ is in Π_k^{cc} if and only if $\{\neg f_n\}$ is in Σ_k^{cc}.
- **Class** PH^{cc}**:** The polynomial hierarchy is defined as $\mathrm{PH}_{cc} = \cup_{k=1}^{\infty}\Sigma_k^{cc} = \cup_{k=1}^{\infty}\Pi_k^{cc}$.
- **Class** PSPACE^{cc}**:** A family $\{f_n\}$ is in $\mathrm{PSPACE}^c c$ if and only if for some constant $c > 0$ and odd $k < \log^c n$,

$$f_n = \bigvee_{i_1=1}^{2^{\log^c n}} \bigwedge_{i_2=1}^{2^{\log^c n}} \bigvee_{i_3=1}^{2^{\log^c n}} \cdots \bigvee_{i_k=1}^{2^{\log^c n}} g_{i_1,\ldots,i_k},$$

where $g_{i_1,\ldots,i_k}$ (alternatively we could take k even and then the functions g would become complements of rectangles...)

- **Class** BPP^{cc}**:** Problems with $R_{1/3}(f_n) \le \log^c(n)$.
- **Class** PP^{cc}**:** Problems with $R_{\frac{1}{2}-2^{\log^c(n)}}(f_n) \le \log^c(n)$.
- **Class** UPP^{cc}**:** Problems with $U(f_n) \le \log^c(n)$.

2. Some relations between these classes

- $\mathrm{NP}^{cc} = \Sigma_1^{cc}$ and $\mathrm{CoNP}^{cc} = \Pi_1^{cc}$.
- $\Sigma_k^{cc}, \Pi_k^{cc} \subseteq \Sigma_{k+1}^{cc} \cap \Pi_{k+1}^{cc}$.
- Since $D(f) \le N^0(f)N^1(f)$, we have $\mathrm{P}^{cc} = \mathrm{NP}^{cc} \cap \mathrm{CoNP}^{cc}$.
- $\mathrm{BPP}^{cc} \subseteq \mathrm{PP}^{cc} \subseteq \mathrm{UPP}^{cc}$.
- $\mathrm{PH}^{cc} \subseteq \mathrm{PSPACE}^{cc}$.
- In light of the Paturi-Simon theorem, UPP^{cc} can be characterized as the class of problems with $\mathrm{rank}_{\pm}(f_n) \le \log^c(n)$.
- It's not hard to see that PP^{cc} can be characterized as the class of problems with non-negligible discrepancy $\mathrm{disc}(f_n) \le 2^{-\log^c(n)}$. (See Assignment 2)
- It's not hard to see $\mathrm{NP}, \mathrm{CoNP}^{cc} \subseteq \mathrm{PP}^{cc}$. (See Assignment 2)

References

[PS86] Ramamohan Paturi and Janos Simon, *Probabilistic communication complexity*, J. Comput. System Sci. **33** (1986), no. 1, 106–123, Twenty-fifth annual symposium on foundations of computer science (Singer Island, Fla., 1984). MR 864082 (88e:68041)

School of Computer Science, McGill University, Montréal, Canada
E-mail address: hatami@cs.mcgill.ca