COMP760, SUMMARY OF LECTURE 2.

HAMED HATAMI

- To every function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ we can associate a $2^n \times 2^n$ matrix M_f. Define $\mathrm{rank}_{\mathbb{F}}(f) = \mathrm{rank}_{\mathbb{F}}(M_f)$ as the rank of this matrix over the field $\mathbb{F}$. We use $\mathrm{rank}(f)$ to denote the rank over reals $\mathbb{R}$.
- $D(f) \geq \log_2 \mathrm{rank}_{\mathbb{F}}(f)$ for every field $\mathbb{F}$. See [KN97, Lemma 1.28].
- The log-rank *conjecture* ([LS88]): $D(f) \leq (\log_2 \mathrm{rank}(f))^{O(1)}$.
  - Until recently $D(f) \leq \log(4/3)\mathrm{rank}(f)$ was the best known upper-bound.
  - Recently [Lov14] proved $D(f) \leq O(\sqrt{\mathrm{rank}(f)} \log_2 \mathrm{rank}(f))$.
  - An equivalent formulation of the conjecture is that for every 0-1 matrix B, we have $\log_2 \mathrm{rank}^+(B) \leq (\log_2 \mathrm{rank}(B))^{O(1)}$, where $\mathrm{rank}^+(B)$ is the minimum k such that $B = \sum_{i=1}^k v_i w_i^T$ where $v_i, w_i \in \mathbb{R}^n$ are vectors with *non-negative* entries. (See [LS07], Sections 2.2 and 3.2)
- Definition: $C^0(f)$ and $C^1(f)$ are respectively the minimum number of monochromatic rectangles in a *cover* of 0's and 1's of f. The cover number is $C(f) = C^0(f) + C^1(f)$, and is obviously upper-bounded by the partition number $C^D(f)$.
- Theorem: $D(f) = O\left((\log_2 C(f))^2\right)$. See [KN97, Theorem 2.11] for a proof.
- Randomized models
  - Private coin: Alice and Bob have access to random strings r_A and r_B respectively. These strings are private and *independent*.
  - Public Coin: Alice and Bob both see a common public random string r.
- For $\epsilon > 0$, we define $R_\epsilon^{prv}(f)$ to be the smallest c such that there exists a randomized protocol $P(x, r_A, y, r_B)$ satisfying the following:
  - For every (x, r_A, y, r_B) the communication is at most c.
  - For every (x, y),

$$\Pr_{r_A, r_B}[P(x, r_A, y, r_B) \neq f(x, y)] \leq \epsilon.$$

- The public coin randomized communication complexity $R_\epsilon^{pub}(f)$ is defined similarly but now with public coin protocols $P(x, y, r)$.

- Some trivial facts:
  - $R^{prv}_{1/2}(f) = R^{pub}_{1/2}(f) = 0$: Just output uniformly at random.
  - $R^{prv}_{\epsilon}(f) \geq R^{pub}_{\epsilon}(f)$: We can have $r = (r_A, r_B)$. Namely, we can think of the public coin case as a scenario where Alice and Bob can see eachother's private random string.
  - $R_{\epsilon}(f) \geq R_{1/3}(f)O(\log(1/\epsilon))$: Let $\mathcal{P}$ be a protocol of cost $R_{1/3}(f)$ achieving error of $1/3$. Repeat $\mathcal{P}$, $O(\log(1/\epsilon))$ times and take the majority of the outputs, in order to achieve an error bound of ϵ.

References

[KN97] Eyal Kushilevitz and Noam Nisan, *Communication complexity*, Cambridge University Press, Cambridge, 1997. MR 1426129 (98c:68074)

[Lov14] Shachar Lovett, *Communication is bounded by root of rank*, Proceedings of the 46th Annual ACM Symposium on Theory of Computing (New York, NY, USA), STOC '14, ACM, 2014, pp. 842–846.

[LS88] L. Lovasz and M. Saks, *Lattices, mobius functions and communications complexity*, Proceedings of the 29th Annual Symposium on Foundations of Computer Science (Washington, DC, USA), SFCS '88, IEEE Computer Society, 1988, pp. 81–90.

[LS07] Troy Lee and Adi Shraibman, *Lower bounds in communication complexity*, Foundations and Trends in Theoretical Computer Science **3** (2007), no. 4, 263–399.

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