COMP760, SUMMARY OF LECTURE 6.

HAMED HATAMI

- *Limitation of the discrepancy method*: The bound $R^{pub}_{\frac{1}{2}-\epsilon}(f) \geq \log \frac{2\epsilon}{\mathrm{Disc}(f)}$ provides a strong lower bound even when ϵ is very small, say $\epsilon \approx \frac{1}{n}$. This shows that the method cannot be applied to lower-bound $R^{pub}_{1/3}(f)$ if $R^{pub}_{\frac{1}{2}-O(\frac{1}{n})}(f)$ is small. Let's see an example.

  Recall
$$\mathrm{Disj} : S \times T \mapsto \begin{cases} 1 & S \cap T = \emptyset \\ 0 & \text{otherwise} \end{cases}$$
  Consider the following public coin protocol
  – Alice and Bob pick $i \in \{1, \dots, n\}$ uniformly at random.
  – If $x_i = y_i = 1$ they output $\mathrm{Disj}(x, y) = 0$.
  – Otherwise, with probability $\frac{1}{2} - \frac{1}{2n}$ they output $\mathrm{Disj}(x, y) = 0$, and with probability $\frac{1}{2} + \frac{1}{2n}$ they output $\mathrm{Disj}(x, y) = 1$.
  Note that the communication is $O(1)$ and
$$S \cap T \neq \emptyset \Rightarrow \Pr[\text{success}] \geq \frac{1}{n} + \frac{1}{2} - \frac{1}{2n} = \frac{1}{2} + \frac{1}{2n}.$$
  and
$$S \cap T = \emptyset \Rightarrow \Pr[\text{success}] \geq \frac{1}{2} + \frac{1}{2n}.$$
  Hence
$$R^{pub}_{\frac{1}{2}-\frac{1}{2n}}(\mathrm{Disj}) = O(1),$$
  which shows [1]
$$\mathrm{Disc}(\mathrm{Disj}) = \Omega(1/n).$$
  Thus using discrepancy method we can only get $R_{1/3}(\mathrm{Disj}) = \Omega(\log n)$. But we will see later that $R_{1/3}(\mathrm{Disj}) = \Theta(n)$.

- *Limitation of the discrepancy method*: While we are on the subject of limitations let us also look at the fooling set method.

  Proposition 1. *If $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$ has a 1-fooling set S, then $\mathrm{rank}_{\mathbb{F}}(M_f) \geq \sqrt{|S|}$ for every field $\mathbb{F}$.*

  Proof. Let A be the submatrix of M_f induced by the rows and columns corresponding to S. Since S is a 1-fooling set $A \odot A = I$ where $\odot$ represents the Hadaramard product (i.e. entrywise). Since $B \odot C$ is a submatrix of $B \otimes C$, we have
$$|S| = \mathrm{rank}_{\mathbb{F}}(A \odot A^T) \leq \mathrm{rank}_{\mathbb{F}}(A \otimes A^T) = \mathrm{rank}_{\mathbb{F}}(A)^2 \leq \mathrm{rank}_{\mathbb{F}}(M_f)^2.$$
  □

[1] Note that we used a protocol to prove a lower-bound on the discrepancy which is cool!

Let's consider the inner product function again. We have

$$M_{IP_n} = [\langle x, y\rangle]_{x,y\in\mathbb{F}_2^n} = \left[\sum_{i=1}^{n} x_i y_i\right]_{x,y\in\mathbb{F}_2^n} = \sum_{i=1}^{n} [x_i y_i]_{x,y\in\mathbb{F}_2^n}.$$

Note that obviously for every $1 \leq i \leq n$, we have

$$\mathrm{rank}_{\mathbb{F}_2}\left([x_i y_i]_{x,y\in\mathbb{F}_2^n}\right) = 1,$$

and hence $\mathrm{rank}_{\mathbb{F}_2}(\mathrm{IP}_n) \leq n$, which shows that the size of the largest 1-fooling set for IP_n is n^2. We can apply a similar argument to 0-fooling sets too, and thus the fooling set method would only show $D(\mathrm{IP}_n) \geq \Omega(\log n)$. However in the previous lecture we saw that $D(\mathrm{IP}_n) \geq n - 2$.

- Let A be a sign matrix (i.e. entries are ± 1). For $0 \leq \alpha < 1$ define the *α-approximate rank* as

$$\mathrm{rank}_\alpha(A) = \min_{\|A-B\|_\infty \leq \alpha} \mathrm{rank}(B).$$

The sign-rank of A is defined as

$$\mathrm{rank}_\pm(A) = \min_{B:\mathrm{sgn}(B_{ij})=A_{ij}} \mathrm{rank}(B).$$

- **Observation:** Note that in the definition of the sign-rank we can scale B so that $\|B\|_\infty < 1$. Hence

$$\mathrm{rank}(A) = \mathrm{rank}_0(A) \geq \mathrm{rank}_\alpha(A) \geq \lim_{\alpha\nearrow 1} \mathrm{rank}_\alpha(A) = \mathrm{rank}_\pm(A).$$

- Approximate rank is provides a lower-bound for the randomized communication complexity.

Theorem 2 ([Kra96])**.** *For $f : \{0,1\}^n \times \{0,1\}^n \to \{-1,1\}$ and $0 < \epsilon < 1/2$, we have*

$$R_\epsilon^{prv}(f) \geq \log \mathrm{rank}_{2\epsilon}(f).$$

Proof. For this proof it will be easier to work with Boolean functions. Thus let $g = \frac{1+f}{2} : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$. Consider a randomized protocol $P(x, r_A, y, r_B)$ with communication cost $c = R_\epsilon^{prv}(f)$ and error

$$\forall x, y \qquad \mathrm{Pr}_{r_A,r_B}[P(x, r_A, y, r_B) \neq g(x, y)] \leq \epsilon.$$

Let $B(x, y) = \mathrm{Pr}_{r_A,r_B}[P(x, r_A, y, r_B) = 1]$. We have $M_g = \frac{J+M_f}{2}$, and

$$\|M_g - B\|_\infty \leq \epsilon \Rightarrow \|M_f - (2B - J)\|_\infty \leq 2\epsilon.$$

It remains to bound $\mathrm{rank}(B)$ (as $\mathrm{rank}(J) = 1$). We will show that $\mathrm{rank}(B) \leq 2^c$. Consider a leaf ℓ in the communication tree, and let $v_1, \ldots, v_k, \ell$ be the path from the root to this leaf, and let $s_1, \ldots, s_k$ be the bits communicated through this path. Without loss of generality assume that Alice and Bob alternate on this path and that Bob speaks on ℓ. On an input (x, y), the probability that the protocol arrives at the leaf ℓ and outputs 1 is

$$\mathrm{Pr}[a_{v_1}(x, r_A) = s_1]\mathrm{Pr}[b_{v_2}(y, r_B) = s_2] \ldots \mathrm{Pr}[b_\ell(y, r_B) = 1] = U_\ell(x)V_\ell(y),$$

for some functions U_ℓ and V_ℓ. Hence

$$B(x, y) = \mathrm{Pr}_{r_A,r_B}[P(x, r_A, y, r_B) = 1] = \sum_\ell U_\ell(x)V_\ell(y).$$

Note that $\mathrm{rank}([U_\ell(x)V_\ell(y)]_{x,y\in\{0,1\}^n}) = 1$. This shows $\mathrm{rank}(B) \le \#\text{leaves} \le 2^c$. □

- The following lemma shows that for the purposes of lower-bounds in communication complexity, for a constant $0 < \alpha < 1$, rank_α and $\mathrm{rank}_{1/3}$ are equivalent.

Lemma 3. *For every* $0 < \alpha < 1$, *we have* $\log \mathrm{rank}_\alpha(A) = \theta_\alpha(\log \mathrm{rank}_{1/3}(A))$.

Proof. We assume $\alpha < 1/3$, the other case is similar. Suppose B is a matrix with $\|A - B\|_\infty < \frac{1}{3}$. By a basic fact from approximation theory [Riv81, Corollary 1.4.1] we know that there exists a polynomial $p : \mathbb{R} \to \mathbb{R}$ such that $d := \deg(p) = O(1/\alpha)$ and it satisfies

$$p([2/3, 4/3]) \subseteq [1-\alpha, 1+\alpha],$$

and

$$p([-4/3, -2/3]) \subseteq [-1-\alpha, -1+\alpha].$$

We will apply $p()$ to B entry-wise: Let $C = [p(B_{ij})]_{ij}$ so that $\|A - C\|_\infty \le \alpha$. It remains to show that the rank does not increase by much.

$$\mathrm{rank}(C) \le \sum_{k=0}^{d} \mathrm{rank}(B^{\odot k}) \le \sum_{k=0}^{d} \mathrm{rank}(B^{\otimes k}) = \sum_{k=0}^{d} \mathrm{rank}(B)^k \le d \cdot \mathrm{rank}(B)^d.$$

Hence

$$\log \mathrm{rank}(C) \le \log(1/\alpha) + \frac{1}{\alpha} \log \mathrm{rank}(B),$$

which proves the desired result. □

In light of this lemma, when we talk about the approximate rank of a matrix A, we often mean $\mathrm{rank}_{1/3}(A)$.

References

[Kra96] Matthias Krause, *Geometric arguments yield better bounds for threshold circuits and distributed computing*, Theoret. Comput. Sci. **156** (1996), no. 1-2, 99–117. MR 1382842 (97a:68082)

[Riv81] Theodore J. Rivlin, *An introduction to the approximation of functions*, Dover Publications, Inc., New York, 1981, Corrected reprint of the 1969 original, Dover Books on Advanced Mathematics. MR 634509 (83b:41001)

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