

COMP760, SUMMARY OF LECTURE 8.

HAMED HATAMI

1. REDUCTIONS

- **Reductions:** Given families $f_n, g_n : \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}$, we say $\{f_n\} \leq_{cc} \{g_n\}$ if for every n , there exists $h_1, h_2 : \{0, 1\}^n \rightarrow \{0, 1\}^m$ for $\log(m) \leq \log^{O(1)}(n)$ such that $f_n(x, y) = g_m(h_1(x), h_2(y))$. Note that for all the communication complexity classes C that we defined in the previous lecture, if $\{g_n\} \in C$ and $\{f_n\} \leq_{cc} \{g_n\}$, then $\{f_n\} \in C$.
- **Completeness:** A problem $\{g_n\}$ is C -complete for a communication complexity class C if and only if
 - (i) $\{g_n\} \in C$.
 - (ii) $\{f_n\} \leq_{cc} \{g_n\}$ for every $\{f_n\} \in C$.
- One can think of C -complete problems as the hardness problems in the class C . The next proposition shows that DISJ is the hardness problem in the class CoNP.

Proposition 1. *The disjointness problem DISJ is CoNP-complete.*

Proof. First note that DISJ \in CoNP as if $S \cap T \neq \emptyset$ then the oracle can send an $i \in S \cap T$ and Alice and Bob can both verify this. To show the completeness, consider $\{f_n\} \in$ CoNP. Then by definition of CoNP we have $m := C^0(f_n) \leq 2^{\log^c n}$. Consider the following reduction: $h_1(x)$ is the list of the rectangles in the cover that contain x , and $h_2(y)$ is the rectangles in the cover that contain y . Obviously

$$f(x, y) \Leftrightarrow h_1(x) \cap h_2(y) \neq \emptyset.$$

□

2. MATRIX NORMS

- Let $A \in \mathbb{R}^{m \times n}$. The singular values $\sigma_1 \geq \dots \geq \sigma_{\min(m, n)} \geq 0$ of A are the square roots of the eigenvalues of AA^T . The singular decomposition theorem says

$$A = U\Sigma V^T,$$

for unitary matrices $U_{m \times m}$ and $V_{n \times n}$, where $\Sigma_{m \times n}$ is a diagonal matrix with $\sigma_1, \dots, \sigma_{\min(m, n)}$ on the diagonal.

- **Matrix inner product:** For $A, B \in \mathbb{R}^{m \times n}$, we have $\langle A, B \rangle := \text{tr}(AB^T) = \sum_{i,j} A_{ij}B_{ij}$.
- **Spectral Norm:** $\|A\| = \max_{\|x\|=1} \|Ax\| = \sigma_1 = \|\vec{\sigma}\|_\infty$.
- **Trace Norm:** $\|A\|_\Sigma = \sum \sigma_i = \|\vec{\sigma}\|_1$.

- **Frobenius Norm:** $\|A\|_F = \sqrt{\sum \sigma_i^2} = \|\vec{\sigma}\|_2 = \sqrt{\sum_{i,j} A_{ij}^2} = \sqrt{\langle A, A \rangle}$.
- Some of the classical inequalities about the L_p spaces easily extend to the matrix norms:

Exercise 2. Show that

$$(1) \sqrt{\text{rank}(A)} \geq \|A\|_\Sigma / \|A\|_F.$$

$$(2) \langle A, B \rangle \leq \|A\|_F \|B\|_F.$$

$$(3) \langle A, B \rangle \leq \|A\| \|B\|_\Sigma.$$

■

3. FORSTER'S THEOREM

The goal of this section is to prove Forster's theorem that the inner product function IP_n has large sign-rank. We start from the following technical lemma whose proof is not very easy.

Lemma 3 (Forster [For02]). *Let $U \subseteq \mathbb{R}^r$ be a finite set of vectors in general positions¹, and suppose $|U| \geq r$. There exists a non-singular $A \in \mathbb{R}^{r \times r}$ such that*

$$\sum_{u \in U} \frac{1}{\|Au\|^2} (Au)(Au)^T = \frac{|U|}{r} I_r.$$

Proof. See Forster's paper [For02] or David Stuerer's exposition on this theorem <http://www.cs.princeton.edu/courses/archive/spr08/cos598D/forster.pdf>. □

Proposition 4. *Let $M \in \mathbb{R}^{X \times Y}$. There exists a matrix R that sign-represents M , $\text{rank}(R = \text{rank}_\pm(M))$, $\|R\|_\infty \leq 1$, and*

$$(1) \quad \|R\|_F = \sqrt{\frac{|X||Y|}{\text{rank}_\pm(M)}}.$$

Proof. Obviously there exists a matrix Q that sign-represents M and $\text{rank}(Q) = \text{rank}_\pm(M) =: r$. We can decompose Q and obtain vectors $\{u_x\}_{x \in X}, \{v_y\}_{y \in Y} \subseteq \mathbb{R}^r$ such that

$$Q = [\langle u_x, v_y \rangle]_{x \in X, y \in Y}.$$

We can assume that $\{u_x\}_{x \in X}$ are in the general position (Otherwise we could perturb them a little bit, and obtain another matrix \tilde{Q} with the same rank sign-represents M). Since $\text{rank}_\pm(M) \leq \text{rank}(M)$, we know $|X| \geq r$, and thus we can apply Lemma 3 to obtain a non-singular $A \in \mathbb{R}^{r \times r}$ with

$$\sum_{x \in X} \frac{1}{\|Au_x\|^2} (Au_x)(Au_x)^T = \frac{|X|}{r} I_r.$$

Define

$$R = \left[\frac{\langle Au_x, (A^{-1})^T v_y \rangle}{\|Au_x\| \|(A^{-1})^T v_y\|} \right]_{x \in X, y \in Y} = \left[\frac{\langle u_x, v_y \rangle}{\|Au_x\| \|(A^{-1})^T v_y\|} \right]_{x \in X, y \in Y}.$$

¹General position means that any set of at most r points in U are linearly independent

Obviously $\text{rank}(R) = r$, R sign-represents M and also by Cauchy-Schwarz $\|R\|_\infty \leq 1$. It remains to verify (1). For a fixed y , we have

$$\begin{aligned} \sum_{x \in X} R_{xy}^2 &= \sum_{x \in X} \frac{\langle Au_x, (A^{-1})^T v_y \rangle^2}{\|Au_x\|^2 \|(A^{-1})^T v_y\|^2} \\ &= \sum_{x \in X} \frac{(v_y^T A^{-1})(Au_x)(Au_x)^T ((A^{-1})^T v_y)}{\|Au_x\|^2 \|(A^{-1})^T v_y\|^2} \\ &= \frac{(v_y^T A^{-1})(\frac{|X|}{r} I_r)((A^{-1})^T v_y)}{\|(A^{-1})^T v_y\|^2} = |X|/r \frac{\langle (A^{-1})^T v_y, (A^{-1})^T v_y \rangle}{\|(A^{-1})^T v_y\|^2} \\ &= |X|/r. \end{aligned}$$

Hence

$$\|R\|_F^2 = \sum_{x,y} R_{x,y}^2 = \frac{|Y||X|}{r},$$

and this verifies (1). □

Theorem 5 (Forster [For02]). *For M be a sign-matrix. Then*

$$\text{rank}_\pm(M) \geq \frac{\sqrt{|X||Y|}}{\|M\|}.$$

Proof. Let R be as in Proposition 4 with $r := \text{rank}(R) = \text{rank}_\pm M$. Since M is a sign-matrix, and R sign-represents M and satisfies $\|R\|_\infty \leq 1$, we have

$$\|R\|_F^2 \leq \sum |R_{x,y}| \leq \langle M, R \rangle \leq \|M\| \|R\|_\Sigma \leq \|M\| \|R\|_F \sqrt{r},$$

where the last two inequalities are from Exercise 2. Replacing $\|R\|_F = \sqrt{\frac{|X||Y|}{r}}$ by (1), this simplifies to $r \geq \frac{\sqrt{|X||Y|}}{\|M\|}$. □

Recall that all the eigenvalues of M_{IP_n} are of the form $\pm 2^{n/2}$. Thus $\|M_{\text{IP}_n}\| = 2^{n/2}$. Replacing this in the above theorem proves Forster's theorem that

$$\text{rank}_\pm(\text{IP}_n) \geq \frac{\sqrt{2^n \times 2^n}}{2^{n/2}} = 2^{n/2},$$

which in particular shows that $U(\text{IP}_n) \geq \frac{n}{2}$. Hence inner product does not belong to the class UPP^{cc} .

Finally let us mention an extension of Theorem 5 that we will need later in the course.

Theorem 6 (Razborov-Sherstov [RS10]). *Let $M \in \mathbb{R}^{X \times Y}$ and $\gamma \geq 0$ we have*

$$\text{rank}_\pm(M) \geq \frac{\gamma s}{\|M\| \sqrt{s} + \gamma h},$$

where $s = |X||Y|$ and $h = |\{(x, y) : |M(x, y)| < \gamma\}|$.

Proof. Let R be as in Proposition 4 with $r := \text{rank}(R) = \text{rank}_\pm M$. On the one hand we have

$$\begin{aligned} \langle M, R \rangle &= \sum M_{xy} R_{xy} \geq \sum_{x,y: |M_{xy}| \geq \gamma} M_{xy} R_{xy} \geq \gamma \left(\sum_{x,y} R_{x,y} - h \right) \geq \gamma \left(\sum_{x,y} R_{x,y}^2 - h \right) \\ &= \gamma \|R\|_F^2 - \gamma h. \end{aligned}$$

On the other hand

$$\langle M, R \rangle \leq \|M\| \|R\|_{\Sigma} \leq \|M\| \|R\|_F \sqrt{r}.$$

Hence

$$\|M\| \|R\|_F \sqrt{r} \geq \gamma \|R\|_F^2 - \gamma h,$$

which using $\|R\|_F = \sqrt{\frac{|X||Y|}{r}}$ from (1) simplifies to the desired result. \square

REFERENCES

- [For02] Jürgen Forster, *A linear lower bound on the unbounded error probabilistic communication complexity*, J. Comput. System Sci. **65** (2002), no. 4, 612–625, Special issue on complexity, 2001 (Chicago, IL). MR 1964645 (2004b:68062)
- [RS10] Alexander A. Razborov and Alexander A. Sherstov, *The sign-rank of AC^0* , SIAM J. Comput. **39** (2010), no. 5, 1833–1855. MR 2592035 (2011b:03061)

SCHOOL OF COMPUTER SCIENCE, MCGILL UNIVERSITY, MONTRÉAL, CANADA
E-mail address: `hatami@cs.mcgill.ca`