This Course

1. Basic Information Theory
   - Notions: Entropy, Information, Divergence
   - Tools: Chain Rules, Inequalities

2. Applications
   - Compression of Information
   - Design of codes + algorithms
   - Analyze Communication Complexity
   - Analyze limiting behavior of games
   - Limits of Data Structures
   - Tight analysis in differential privacy

Today: Information Theory in Combinatorics
Basics (informally):

- $X$ - random variable
- $P_x$ - distribution of $X$

- Suppose Alice + Bob know $P_x$; Alice also knows $X$
- How many bits (in expectation) does Alice have to send to Bob to convey $X$?

"Entropy of $X" \rightarrow H(X) \text{ roughly measures this.}

- Conditional Entropy: $(X,Y) \sim P_{xy}$
- Alice + Bob know $X \& P_{xy}$
- How many bits (in expectation over $X,Y$) does Alice send + Bob to convey $Y$?

"Conditional Entropy of $Y \mid X" \text{ denoted } H(Y \mid X)"

- Key relationships
  1. $H(X) \leq \log |2^X|
  2. $H(X,Y) = H(X) + H(Y \mid X)$
  3. $H(Y \mid X) \leq H(Y)$
Today's Application

Shearer's Lemma (Baby Version?):

Let: \( \mathbb{S} \subseteq [N]^d \)

for: \( S \subseteq [d] \) let \( F_S \subseteq [N]^{|S|} \)

\[ S = \{i_1, \ldots, i_s\} \]

\[ = \{ (x_{i_1}, x_{i_2}, \ldots, x_{i_s}) \mid (x_1, \ldots, x_d) \in F_S \} \]

"Projection of \( F \) to \( S \)."

Theorem: \([d=3]\) version

\[ \# |F|^2 \leq |F_{\{1,2,3\}}| \cdot |F_{\{2,3\}}| \cdot |F_{\{1,3\}}| \]

(\(d, k\) - version ("exercise")

\[ |F| \leq \prod_{S \subseteq [d], \ |S| = k} |F_S| \]
Motivation

1. d=3, r=1 version

Lemma asserts \(|F| \leq |F_1| \cdot |F_2| \cdot |F_3|\)

But this is obvious since

\[ F \subseteq F_1 \times F_2 \times F_3 \]

\[ |F| \leq |F_1| \cdot |F_2| \cdot |F_3| \]

r=2 quite non-trivial!

2. Lemma is tight: Suppose \( F = F_1 \times F_2 \times \ldots \times F_d \)

Then

\[ F_S = \prod_{j \in S} F_j \]

\[ \prod_{S \subseteq [d]} \prod_{j \in S} F_j = \prod_{j=1}^{n} F_j^{(d-1)} = F^{(d-1)} \]
Our Proof [due to "Rudra"]

Idea: find distribution (random variable) \((X, Y, Z)\) supported on \(F\)

\[
\text{a.t.: } H(X, Y, Z) = \log |F|
\]

- Have

\[
H(X, Y) \leq \log |F_{12}|
H(Y, Z) \leq \log |F_{23}|
H(X, Z) \leq \log |F_{13}|
\]

- Sufficient to prove:

\[
2 \log |F| = 2 H(X, Y, Z) \leq H(X, Y) + H(X, Z) + H(Y, Z)
\leq \log F_{12} + \log F_{23} + \log F_{13}
\]

\[
H(X, Y) = H(X) + H(Y|X)
\]

\[
H(X, Z) = H(X) + H(Z|X)
\]

\[
H(Y, Z) = H(Y) + H(Z|Y)
\]

\[
2H(X) \geq 2H(Y|X) \geq 2H(Z|XY)
\]
Moral:
- Somewhere out there, there was a deep theorem.
- Which one?

Rest of the course:
- Fill in basics (relatively short)
- Get to applications

Your tasks:
1. Scribe work - sign up! (15%)
2. Problem sets - 40%
3. Project - 30%
4. Participation - 15%

Remember to sign up on Piazza.
Follow class website
http://madhu.cs.harvard.edu/courses/Spring2019