Presentations

See pdf file "Course Presentation Topics" to view suggested list of topics with links to papers/talks.

* You must sign up for your presentations by Feb 20
  Pick 3 topics:
  (i) Main presenter
  (ii) Helper
  (iii) Reviewer

Presentations cont'd

- Talk to me if you want to discuss possible topics before Feb 20

Your Presentation should include

- Presentation in class ~50 mins
- Lecture notes / slides
- Questions for discussion, open problems

- I will meet with main presenter & helper ahead of time to review your presentation

Last class

Randomized CC :

Different protocols for EQ_n, GT_n

Newman's Theorem

Public $\approx$ Private Coin

Briefly discussed : nondet CC, co-nondet CC

Set Disjointness $DISJ_n$

Today

(1) Deterministic CC(f) $\leq$ Nondet CC(f) $\cdot$ co-Nondet CC (f)

and similar result for decision tree complexity

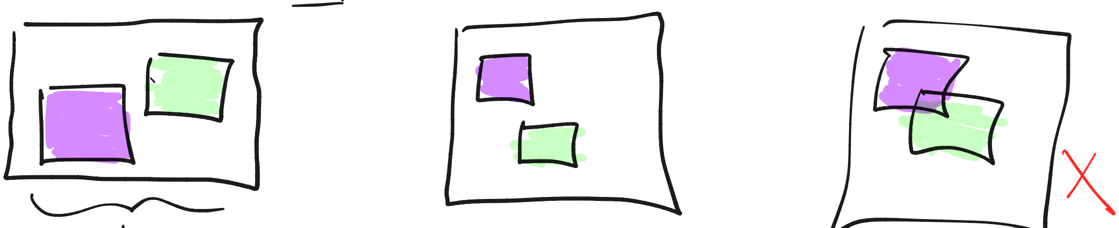
(2) Randomized CC vs Distributional CC

and Yao Minimax Thm

Theorem $P^{cc}(f) \le NP^{cc}(f) \cdot coNP^{cc}(f)$. [Yannakakis]

Recall the following fact (also used in Yannakakis' alg. for converting partition of M_f into monoch. subrectangles to a det. cc protocol for f)

Fact: any 2 disjoint rectangles cannot intersect in rows and in columns



intersect in rows

intersect in columns

Not disjoint

Theorem $P^{cc}(f) \leq NP^{cc}(f) \cdot coNP^{cc}(f)$.

Pf Let $\mathcal{R}$ = all 1-mono rectangles of NP^{cc} protocol for f

Let $\mathcal{Q}$ = all 0-mono rectangles of $coNP^{cc}$ protocol for f

Note $R, R' \in \mathcal{R}$ can intersect, and similarly $Q, Q' \in \mathcal{Q}$ can intersect

But by fact, any $R \in \mathcal{R}$ $Q \in \mathcal{Q}$ are disjoint

As in Yannakakis Alg 1 (see lecture 2),

If $(x,y) \in f^{-1}(1)$, $(x,y) \in R_{x,y}$ $R_{x,y} \in \mathcal{R}$ then either:

(1) $\leq$ half of rectangles in $\mathcal{Q}$ intersect $R_{x,y}$ in rows

(2) $\leq$ half of rectangles in $\mathcal{Q}$ " $R_{x,y}$ in cols

Yannakakis' Algorithm 2 :

$\boxed{\text{Protocol } \Pi}$ on input (x,y) :

0. $\mathcal{R}$ = all 1-mono rectangles of NP^{cc} protocol for f
   $\mathcal{Q}$ = " " " " " $coNP^{cc}$ " " "

Repeat until no 0-rectangles in $\mathcal{Q}$:

1A. Alice looks for a 1-mono R such that $x \in rows(R)$ and s.t. R row-intersects with $\leq \frac{1}{2}$ 0-rect's

    If she finds such an R, she sends name of R to Bob. + they can prune # possible 0-rect's by $\frac{1}{2}$

1B. OW (Alice cant find such an R), Bob looks for a 1-mono R st $y \in R$ and R col-intersects with $\leq \frac{1}{2}$ 0-rect's

    If Bob finds R, he sends name of R to Alice + they can prune # possible 0-rect's by $\frac{1}{2}$

2. If 1A, 1B fail $\longrightarrow$ $\Pi(x,y)$ outputs 0

Protocol Π:

(0) $\mathcal{R}$ = all 1-mono rectangles of NP^{cc} protocol for f
Q = " " " " " $coNP^{cc}$ " " "

Repeat until no 0-rect's in Q:

(1A) Alice looks for a 1-mono R such that $x \in rows(R)$ and st. R row-intersects with $\leq \frac{1}{2}$ 0-rect's

If she finds such an R, she sends name of R to Bob. + they can prune # possible 0-rect's by $\frac{1}{2}$

(1B) OW (Alice can't find such an R), Bob looks for a 1-mono R st $y \in R$ and R col-intersects with $\leq \frac{1}{2}$ 0-rect's
If Bob finds R, he sends name of R to Alice + they can prune # possible 0-rect's by $\frac{1}{2}$

(2) If (1A), (1B) fail $\longrightarrow$ $\Pi(x,y)$ outputs 0

cost of Π: # iterations = $\log(|Q|) \leq coNP^{cc}(f)$

each iteration has cost $\sim \log(|\mathcal{R}|) \leq NP^{cc}(f)$

$\therefore$ total cc cost $= O(coNP^{cc}(f) \cdot NP^{cc}(f))$

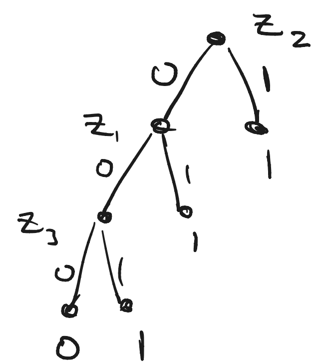
Similar Result for Decision Tree Complexity

Let $h : \underbrace{\{0,1\}^n}_{z_1, \ldots, z_n} \to \{0,1\}$ [Note h is an n-variable Boolean function]

A <u>decision tree</u> for h is a binary tree. Internal Nodes labelled by variables z_i, edges labelled $0/1$ and leaves labelled $0/1$

A dec. tree T computes h if $\forall$ assignment $\alpha \in \{0,1\}^n$, $T(\alpha) = h(\alpha)$

<u>Ex</u> $h : \{0,1\}^3 \to \{0,1\}$



$\leftarrow$ h is the OR function

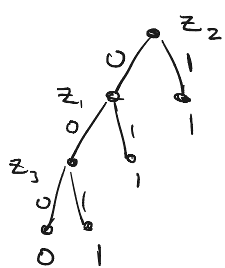
Similar Result for Decision Tree Complexity

A **decision tree** for h is a binary tree. Internal nodes labelled by variables z_i, edges labelled 0/1 and leaves labelled 0/1

A dec. tree T computes h if $\forall$ assignment $\alpha \in \{0,1\}^n$, $T(\alpha) = h(\alpha)$

Dec. tree complexity of h = min depth over all dec. trees computing f $\Big\}$ Notation $P^{dt}(h)$

A decision tree for h partitions all inputs $\alpha \in \{0,1\}^n$ into disjoint monochromatic subcubes



subcubes: ρ_1: 0 0 0 $\leftarrow$ 0 - mono

ρ_2: 0 0 1 $\leftarrow$ 1 - mono

ρ_3: 1 0 $*$ $\leftarrow$ ''

ρ_4: $*$ 1 $*$ $\leftarrow$ ''

$|\rho|$ = # set vars   size of subcube$(\rho) = 2^{n-|\rho|}$

Similar Result for Decision Tree Complexity

Notation

Nondeterministic decision tree complexity of h = $\min_{K}$ [there is a KDNF for h] $\Big\}$ $NP^{dt}(h)$

K-DNF for h: cover of the 1's of h by all-1 subcubes: $\rho_1 \vee \rho_2 \vee \dots \vee \rho_m$ where $|\rho_i| \leq K$

co-Nondeterministic dec. tree complexity of h = $\min_{K'}$ [there is a K'-DNF for $\bar{h}$] $\Big\}$ $coNP^{dt}(h)$

K'-DNF for h: cover of 0's of h by all-0 subcubes $\rho_1' \vee \rho_2' \vee \dots \vee \rho_m'$ $|\rho_j'| \leq K'$

Similar Result for Decision Tree Complexity

Notation

Nondeterministic decision tree complexity of h =
$\min_{k}$ [there is a kDNF for h] $\Big\}$ $NP^{dt}(h)$

co-Nondeterministic dec. tree complexity of h =
$\min_{k'}$ [there is a k'-DNF for $\bar{h}$] $\Big\}$ $coNP^{dt}(h)$

Theorem $P^{cc}(h) \le NP^{dt}(h) \cdot coNP^{dt}(h)$

Let h be computed by a kDNF : $F_1 = t_1 \vee t_2 \vee \dots \vee t_m$, $|t_i| \le k$

and Let $\bar{h}$ " " " " k'DNF : $F_0 = s_1 \vee s_2 \vee \dots \vee s_{m'}$ $|s_i| \le k'$

Then $\forall t_i \in F_1$ $\forall s_j \in F_0$: t_i and s_j intersect in some variable

Similar Result for Decision Tree Complexity

Theorem $P^{cc}(h) \le NP^{dt}(h) \cdot coNP^{dt}(h)$

Let h be computed by a kDNF : $F_1 = t_1 \vee t_2 \vee \dots \vee t_m$, $|t_i| \le k$

and Let $\bar{h}$ " " " " k'DNF : $F_0 = s_1 \vee s_2 \vee \dots \vee s_{m'}$ $|s_i| \le k'$

FACT $\forall t_i \in F_1$ $\forall s_j \in F_0$: t_i and s_j intersect in some variable

F_1 = kDNF for h $\quad$ F_0 = k'-DNF for $\bar{h}$

Decision tree construction (F_1, F_0, k, k') $\quad$ F_1 : kDNF for h $\quad$ F_0 : k'DNF for $\bar{h}$

If $F_1 = 1$ halt & output 1.
If $F_0 = 1$ halt & output 0

Else: • Pick a term $t \in F_1$ and query all vars in t

• for each assignment α to t (corresponds to a partial path in tree)

Recurse on $\left(F_1 := F_1|_\alpha \,,\, F_0 := F_0|_\alpha\right)$

Depth of dec tree for h: Let $D(k, k')$ = max depth of Dec tree where F_1 = kDNF, F_0 = k'DNF for $\bar{h}$

Base Case $\quad D(0, k') = 0 \,,\, D(k, 0) = 0$

Induction $\quad D(k, k') \leq k \cdot D(k, k'-1)$ $\Big\}$ since every $s \in F_0$ must intersect with some variable in t

$\leq k \cdot k'$

<u>Note</u> the decision tree version of Yannakakis $\left(P^{dt}(h) \leq NP^{dt}(f) \cdot coNP^{dt}(f)\right)$ is a special case of comm. compl. version where we only consider "simple" query protocols where Alice/Bob are restricted to sending <u>bits</u> of their input (not <u>general</u> functions of their input & transcript so far)

ie. Let $h: \{0,1\}^n \to \{0,1\}$.

h^{cc}: Alice gets $x \in \{0,1\}^{n/2}$ 1st half of input to h
Bob gets $y \in \{0,1\}^{n/2}$ 2nd half " " " h.

then a dec. tree for h is just a "simple" query cc protocol for h^{cc}.

<u>Question</u> Is there also a "decision-tree" / "query" analog of Yannakakis Alg 1 ?

Let $\{\rho_1, \ldots, \rho_m\}$ be a partition of $\{0,1\}^n$ into monochrom subcubes

Can we show $\exists$ a decision tree for h of cost (depth) $\leq O(\log(m))$?

We <u>can</u> prove a <u>size</u> analog :

<u>Theorem</u>

If h has a partition into M monochrom. subcubes then $\exists$ a decision tree for h of <u>size</u> (= # of leaves) $2^{\text{polylog}(m)}$

$\boxed{\text{* We skipped slides 16 - 21 since it is a bit of a digression}}$

Theorem [subcube partition # vs dec tree size]

If h has a partition into M monochrom. subcubes then $\exists$ a decision tree for h of size (= # of leaves) $O(M \cdot n)$

Idea: Let $P = \{\rho_1, \dots, \rho_m\}$ be a partition of all $\alpha \in \{0,1\}^n$ into mono. subcubes.

Claim There must exist a $\rho_i \in P$ s.t. $|\rho_i| \leq \log m$ where $|\rho_i|$ = # of vars set by ρ_i.

Pf Since P is a partition of all assignments, if $\forall i$ $|\rho_i| \geq \log m + 1$ then:

$$2^n = \sum_{i=1}^{m} 2^{n-|\rho_i|} \leq m \cdot 2^{n-(\log m+1)} = 2^{n-1}! \quad \text{contradiction} \checkmark$$

Theorem [subcube partition # vs dec tree size]

If h has a partition into M monochrom. subcubes then $\exists$ a decision tree for h of size (= # of leaves) $O(M \cdot n)$

Idea: Let $P = \{\rho_1, \dots, \rho_m\}$ be a partition of all $\alpha \in \{0,1\}^n$ into mono. subcubes.

Alg on input $P = \{ \underbrace{\rho_1^0, \dots, \rho_m^0}_{0\text{-subcubes}}, \underbrace{\rho_1^1 \dots \rho_m^1}_{1\text{-subcubes}} \}$

Repeat until all subcubes in P are all-1 subcubes or all 0-subcubes

Find largest subcube -- so find ρ_i $|\rho| \le \log m$

Query all vars set by ρ_i. Suppose ρ_i is a 0-subcube

Since every 1-subcube is falsified by ρ_i, each 1-subcube has a variable in common with ρ_i

Query vars in ρ_i from most popular to least popular

Analysis

when we query a 0-subcube p_i $|p_i| \le \log m$, this gives a size $2^{\log m}$ subtree. Each of the leaves has at most $m - \frac{m}{\log m}$ p_j's not forced to 0

So we went from initial problem with $\le m$ 0-subcubes
$\le m$ 1-subcubes

to m instances where now we have $\le m$ 0-subcubes
$\le m - \frac{m}{\log m}$ 1-subcubes.

Similarly if we query a 1-subcube q_j size $\le \log m$.

$\therefore$ after $O(\log m \cdot \log\log m)$ iterations either. $\qquad m\left(1-\frac{1}{\log m}\right)^x$

0-subcubes is 0 or # 1 subcubes is 0

$\therefore$ dec tree size $= 2^{O(\log^2 m \cdot \log\log m)}$

<u>Question</u> Is there also a "decision-tree" / "query" analog of Yannakakis Alg 1?

Let $\{\rho_1, \dots, \rho_m\}$ be a partition of $\{0,1\}^n$ into monochrom subcubes

Can we show $\exists$ a decision tree for h of cost (depth) $\leq O(\log m)$?

No! there is <u>no</u> depth analog for decision tree complexity

reason (high level): we cannot in general <u>balance</u> decision trees like we can for cc protocols!

so a small size S dec tree does not imply a dec tree of depth $\log S$

<u>example:</u> $h = \mathrm{OR} \wedge \mathrm{AND}$

GPW proved that it is impossible to get a true depth version of Yannakakis Alg 1 in dec tree setting:

Thm $\exists\, h: \{0,1\}^N \to \{0,1\}$ that has a partition into $2^{O(\sqrt{N})}$ mono. subcubes but every det. dec tree requires depth $\Omega(N)$

RANDOMIZED CC

Recall: for $0 < \varepsilon < \frac{1}{2}$

a 2-sided cc protocol for f is a protocol Π such that:

$$\forall (x,y) \quad \Pr\left[\Pi(x,y) = f(x,y)\right] \geq 1-\varepsilon$$

$$BPP_{\varepsilon}^{cc}(f) = \min_{\substack{\text{protocols } \Pi \\ \text{with error } \varepsilon}} \; \max_{\substack{(x,y) \\ |x| = |y| = n}} \left[\#\text{bits sent by } \Pi \text{ on } (x,y)\right]$$

(public coin)

DISTRIBUTIONAL COMPLEXITY

Let μ be a probability distribution over $X \times Y$,
$X, Y = \{0,1\}^n$.

A deterministic protocol Π computes $f: X \times Y \to \{0,1\}$
with error $\le \varepsilon$ wrt μ if: $\Pr_{(x,y)\sim\mu}[\Pi(x,y) = f(x,y)] \ge 1-\varepsilon$

The (μ, ε)-distributional cc of f, $D_\varepsilon^\mu(f)$,
is the minimum cost over all deterministic protocols
that compute f over μ with error $\le \varepsilon$

DISTRIBUTIONAL COMPLEXITY

Let μ be a probability distribution over $X \times Y$, $X, Y = \{0,1\}^n$.

A deterministic protocol Π computes $f: X \times Y \to \{0,1\}$ with error $\leq \varepsilon$ wrt μ if: $\Pr_{(x,y)\sim\mu}[\Pi(x,y) = f(x,y)] \geq 1-\varepsilon$

The (μ, ε)-distributional cc of f, $D_\varepsilon^\mu(f)$, is the minimum cost over all deterministic protocols that compute f over μ with error $\leq \varepsilon$

Theorem $BPP_\varepsilon^{cc}(f) = \max_\mu D_\varepsilon^\mu(f)$

25

Theorem $BPP_\varepsilon^{cc}(f) = \max_\mu D_\varepsilon^\mu(f)$

Proof

① $BPP_\varepsilon(f) \geq \max_\mu D_\varepsilon^\mu(f)$:

Let Π be a BPP_ε^{cc} protocol for f of cost c

$\therefore \Pr_r[\Pi(x,y,r) = f(x,y)] \geq 1-\varepsilon$

Let μ be any distrib over $X \times Y$

$\therefore$ by averaging, there exists some r^* st

$$\Pr_{(x,y)\sim\mu}[\Pi(x,y,r^*) = f(x,y)] \geq 1-\varepsilon \quad ✓$$

Theorem $BPP^{cc}_{\varepsilon}(f) = \max_{\mu} D^{\mu}_{\varepsilon}(f)$

Proof

(2) $BPP_{\varepsilon}(f) \leq \max_{\mu} D^{\mu}_{\varepsilon}(f)$:

This direction will follow from a more general "minimax" theorem for 2-player zero sum games, which in turn follows from Linear programming Duality

We'll give a direct pf via LP duality

Idea: We will write a Linear Program (LP) whose optimal solution is a randomized cost-c protocol for f of minimal error ϵ^*. This will be a minimization problem (Find lowest error randomized protocol)

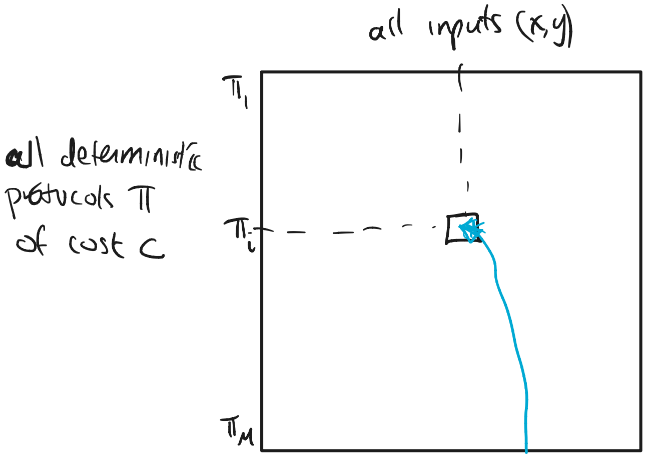
Then the dual LP will be a maximization problem whose optimal solution is a distribution over inputs μ that has maximal error F^* (for computing f) -- that is all cost-c deterministic protocols for f have error $\geq F^*$ with respect to μ.

By LP duality, $\epsilon^* = F^*$.

Therefore there exists a randomized cost-c protocol Π_μ for f with error $\leq \varepsilon$

iff there exists a distrib σ over inputs such that every deterministic cost-c protocol for f has error $\geq \varepsilon$

Utility Matrix $\mathcal{U}$ for $f: X \times Y \to \{0,1\}$



Let $\mu = \mu_1 \ldots \mu_M$ be a distribution over rows of $\mathcal{U}$ (so π_μ is a randomized c-bit protocol)

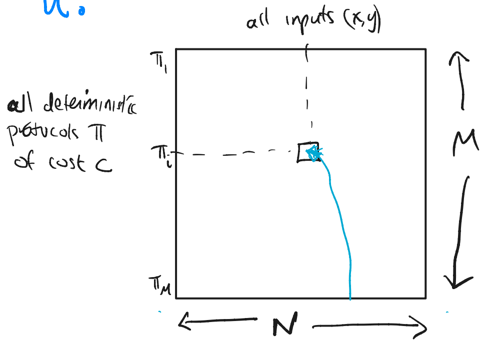
Let $\sigma = \sigma_1 \ldots \sigma_N$ be a distribution over columns of $\mathcal{U}$ (so σ is a distribution over $X \times Y$)

$$\mathcal{U}(i,j) = \begin{cases} 1 & \text{if } \pi_i(j) = f(j) \\ 0 & \text{ow} \end{cases}$$

($j = j^{th}$ input (x,y) and $i = i^{th}$ cost c deterministic protocol)

An LP for the best (lowest error E) randomized cost c protocol for f

$\mathcal{U}$:



$\mathcal{U}(i,j) = 1$ if $\Pi_i(j) = f(j)$
$\qquad\qquad 0$ ow

($j = j^{th}$ input (x,y)
and $i = i^{th}$ cost c
deterministic protocol)

Randomized cost-c protocol Π_μ described by variables μ_1, μ_M where
μ_i = probability assigned to Π_i

$\boxed{LP}$: vars: $c_1 \dots c_N, \mu_1, \dots, \mu_M, E$

minimize E

satisfying (1) $\forall j \quad c_j = \sum_{i=1}^{M} \mu_i \cdot \mathcal{U}(i,j) / M$ } Error of Π_μ on the j^{th} input

(2) $\forall i \quad 0 \le \mu_i \le 1$
$\qquad \sum \mu_i = 1$ } $\mu_1 \dots \mu_M$ is a distribution over rows of $\mathcal{U}$

(3) $\quad E \ge c_j \ \forall j$

$\boxed{LP}$: vars: $c_1 \ldots c_N, \mu_1, \ldots, \mu_M, E$

minimize E

satisfying (1) $\forall j \quad c_j = \sum_{i=1}^{M} \mu_i \cdot U(i,j)/M$ } Error of Π_μ on input j

(2) $\forall i \quad 0 \le \mu_i \le 1$
$\sum \mu_i = 1$ } $\mu_1 .. \mu_M$ is a distrib over rows of U

(3) $E \ge c_i \quad \forall j$

↑ soln finds "best" randomized cost-c protocol Π_μ for f with minimal error E^* over all cost-c randomized protocols

$\boxed{\text{Dual LP}}$: vars $r_1 \ldots r_M, \sigma_1 \ldots \sigma_N, F$

maximize F

satisfying: (1) $\forall i \quad r_i = \sum_{j=1}^{N} \sigma_j \, U(i,j)/N$ } Error of Π_i on distrib $\sigma_1 .. \sigma_N$

(2) $\forall j \quad 0 \le \sigma_j \le 1$
$\sum \sigma_i = 1$ } σ is a distrib over columns of U

(3) $F \le r_i$

↖ soln finds a "hardest" distribution σ over inputs so that every cost-c deterministic protocol Π_i is guaranteed to have error at least F^* over σ.

Linear programming duality says $E^* = F^*$

The minimal value of E $(= E^*)$ is equal to the maximal value of F $(= F^*)$ in dual LP

In game theory terminology:

$$U: \quad \begin{array}{c|ccc|} & (x,y)_1 & \cdots & (x,y)_N \\ \hline \pi_1 & & & \\ \vdots & & & \\ \pi_M & & & \\ \hline \end{array}$$

Think of a game between 2 players

Player I (protocol designer):

"pure" strategies: all c-bit deterministic protocols

mixed strategies: distrib over all c-bit deterministic protocols

Player II (Lower Bound Player):

Pure strategies: all inputs (x,y)

mixed strategies: all distributions over $X \times Y$

$$M: \begin{array}{c|ccc} & (x,y)_1 & \cdots & (x,y)_N \\ \hline \Pi_1 & & & \\ \vdots & & & \\ \Pi_M & & & \end{array}$$

In game theory terminology:

Think of a game between 2 players

Player I (protocol designer):

"pure" strategies: all c-bit deterministic protocols

mixed strategies: distrib over all c-bit deterministic protocols

Player II (Lower Bound Player):

Pure strategies: all inputs (x,y)

mixed strategies: all distributions over $X \times Y$

Player I wants to find optimal mixed strategy (= randomized protocol Π_{μ^*}) where optimal means it has minimal error E^* over all randomized c-bit protocols)

Player II wants to find a hardest distrib over inputs σ^* where hardest means every c-bit deterministic strategy has error $\geq F^*$ and F^* is maximal over all distributions σ

In game theory terminology:

Think of a game between 2 players

$$U: \quad \begin{array}{c|ccc} & (x,y)_1 & \cdots & (x,y)_N \\ \hline \pi_1 & & & \\ \vdots & & & \\ \pi_M & & & \end{array}$$

The MiniMax Thm (proved via LP duality like we just did)

says the minimal ε^* equals the maximum F^*.